Procédure de déploiement de l'agent GLPI avec PDQ Deploy sur un poste local hors domaine.

Phase 1 Prérequis :

Paramétrage du pare-feu de Windows de la machine locale :

Les règles à appliquer sont les suivantes :

- Ouverture du port ICMP : seulement sur la machine distance PDQ Serveur : 192.168.4.26
- Ouverture du port TCP : 445 pour le partage SMB seulement sur la machine distante PDQ Serveur : 192.168.4.26
- Ouverture du port TCP : 6336 seulement pour la machine distante PDQ Serveur : 192.168.4.26
- Ouverture du port TCP : 7337 seulement pour la machine distante PDQ Serveur : 192.168.4.26

Allow ICMPv4-In from PDQ Server	Tout	Oui	Autoris...	Non	Tout	Tout	192.168.4.26	ICMPv4	Tout
Allow SMB TCP 445-In from PDQ Server	Tout	Oui	Autoris...	Non	Tout	Tout	192.168.4.26	TCP	445
Allow TCP 6336-In from PDQ Server	Tout	Oui	Autoris...	Non	Tout	Tout	192.168.4.26	TCP	6336
Allow TCP 7337-In from PDQ Server	Tout	Oui	Autoris...	Non	Tout	Tout	192.168.4.26	TCP	7337
SMB	Domaine, Privé	Oui	Autoris...	Non	Tout	Tout	Tout	TCP	445

Le script à copier/coller sur les machines windows 10 est le suivant :

```
# Récupérer le nom de l'ordinateur
$hostname = $env:COMPUTERNAME

# Récupérer l'adresse IP principale (hors APIPA et loopback)
$ip = (Get-NetIPAddress -AddressFamily IPv4 | Where-Object { $.IPAddress -notlike '169.254*' -and
$.IPAddress -ne '127.0.0.1' -and $_.PrefixOrigin -ne 'WellKnown' } | Sort-Object InterfaceMetric |
Select-Object -First 1 -ExpandProperty IPAddress)

# Afficher les informations
Write-Host "Nom de la machine : $hostname" Write-Host "Adresse IP principale : $ip"

# Enregistrer dans le fichier C:\Tools\infos_machine.txt
"$hostname;$ip" | Out-File -Append -Encoding UTF8 "C:\Tools\infos_machine.txt"

# Création du compte en user et admin
$User = "PDQDeployAdmin" $Pass = "Simplepass123!" net user $User $Pass /add net localgroup
Administrateurs $User /add

# Vérif de la présence dans les comptes
net user PDQDeployAdmin net localgroup Administrateurs


# Activation accès local à distance
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

 # Adresse IP du serveur PDQ Deploy
$PDQServerIP = "192.168.4.26"

 # Adresse IP du serveur GLPI
$GLPIServerIP = "192.168.1.10"
---- Règles INBOUND pour PDQ Deploy ----

 # Ouvrir ICMP Echo Request (ping) pour toutes les IP
New-NetFirewallRule -DisplayName "Allow ICMPv4-In from All" -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow -Profile Domain,Private,Public -Description "Autorise le ping depuis toutes les sources" -ErrorAction SilentlyContinue

 # Ouvrir SMB (port TCP 445) pour toutes les IP
New-NetFirewallRule -DisplayName "Allow SMB TCP 445-In from All" -Direction Inbound -Protocol TCP -LocalPort 445 -Action Allow -Profile Domain,Private,Public -Description "Autorise SMB/partage fichiers depuis toutes les sources" -ErrorAction SilentlyContinue

 # Ouvrir les ports TCP 6336 et 7337 INBOUND depuis PDQ Server (optionnel MD-Inventory/Deploy Server)

New-NetFirewallRule -DisplayName "Allow TCP 6336-In from PDQ Server" -Direction Inbound -Protocol TCP -LocalPort 6336 -Action Allow -RemoteAddress $PDQServerIP -Profile Domain,Private,Public -Description "PDQ Deploy port 6336" -ErrorAction SilentlyContinue

New-NetFirewallRule -DisplayName "Allow TCP 7337-In from PDQ Server" -Direction Inbound -Protocol TCP -LocalPort 7337 -Action Allow -RemoteAddress $PDQServerIP -Profile Domain,Private,Public -Description "PDQ Inventory port 7337" -ErrorAction SilentlyContinue

 # Port GLPI Agent TCP 62354 INBOUND depuis PDQ Server

New-NetFirewallRule -DisplayName "Allow GLPI Agent TCP 62354-In from PDQ Server" -Direction Inbound -Protocol TCP -LocalPort 62354 -Action Allow -RemoteAddress $PDQServerIP -Profile Domain,Private,Public -Description "Port par défaut GLPI Agent" -ErrorAction SilentlyContinue

 # Ports HTTP/HTTPS GLPI INBOUND depuis PDQ Server (80 et 443)

New-NetFirewallRule -DisplayName "Allow GLPI TCP 80-In from PDQ Server" -Direction Inbound -Protocol TCP -LocalPort 80 -Action Allow -RemoteAddress $PDQServerIP -Profile Domain,Private,Public -Description "Port HTTP par défaut pour GLPI" -ErrorAction SilentlyContinue New-NetFirewallRule -DisplayName "Allow GLPI TCP 443-In from PDQ Server" -Direction Inbound -Protocol TCP -LocalPort 443 -Action Allow -RemoteAddress $PDQServerIP -Profile Domain,Private,Public -Description "Port HTTPS pour GLPI" -ErrorAction SilentlyContinue

 # ---- Règles OUTBOUND pour GLPI Agent ----

 # Port GLPI Agent TCP 62354 OUTBOUND vers serveur GLPI

New-NetFirewallRule -DisplayName "Allow GLPI Agent TCP 62354-Out to GLPI Server" -Direction Outbound -Protocol TCP -RemotePort 62354 -Action Allow -RemoteAddress $GLPIServerIP -Profile Domain,Private,Public -Description "Sortant agent GLPI vers serveur" -ErrorAction SilentlyContinue

 # Ports HTTP/HTTPS OUTBOUND vers serveur GLPI (optionnel accès web)

New-NetFirewallRule -DisplayName "Allow GLPI HTTP TCP 80-Out to GLPI Server" -Direction Outbound -Protocol TCP -RemotePort 80 -Action Allow -RemoteAddress $GLPIServerIP -Profile Domain,Private,Public -Description "Sortant HTTP GLPI agent" -ErrorAction SilentlyContinue

New-NetFirewallRule -DisplayName "Allow GLPI HTTPS TCP 443-Out to GLPI Server" -Direction Outbound -Protocol TCP -RemotePort 443 -Action Allow -RemoteAddress $GLPIServerIP -Profile Domain,Private,Public -Description "Sortant HTTPS GLPI agent" -ErrorAction SilentlyContinue

 # ---- Vérification des règles créées ----

Write-Output "== Règles firewall INBOUND PDQ Deploy créées : =="

Get-NetFirewallRule -DisplayName "PDQ Server" | Format-Table -AutoSize

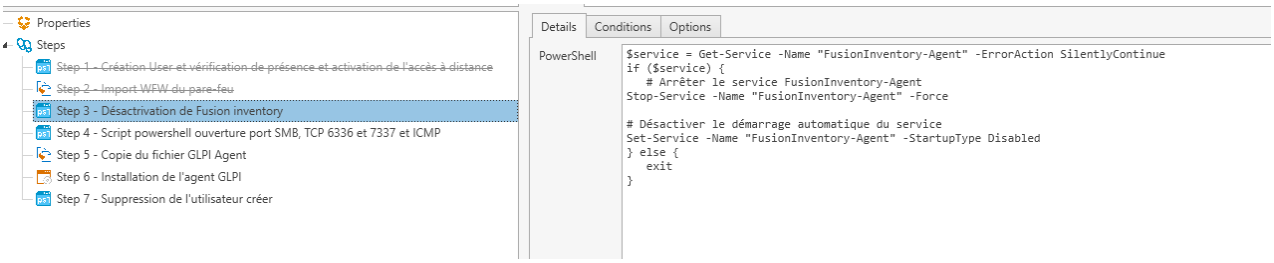
Write-Output "== Règles firewall OUTBOUND GLPI créées : =="

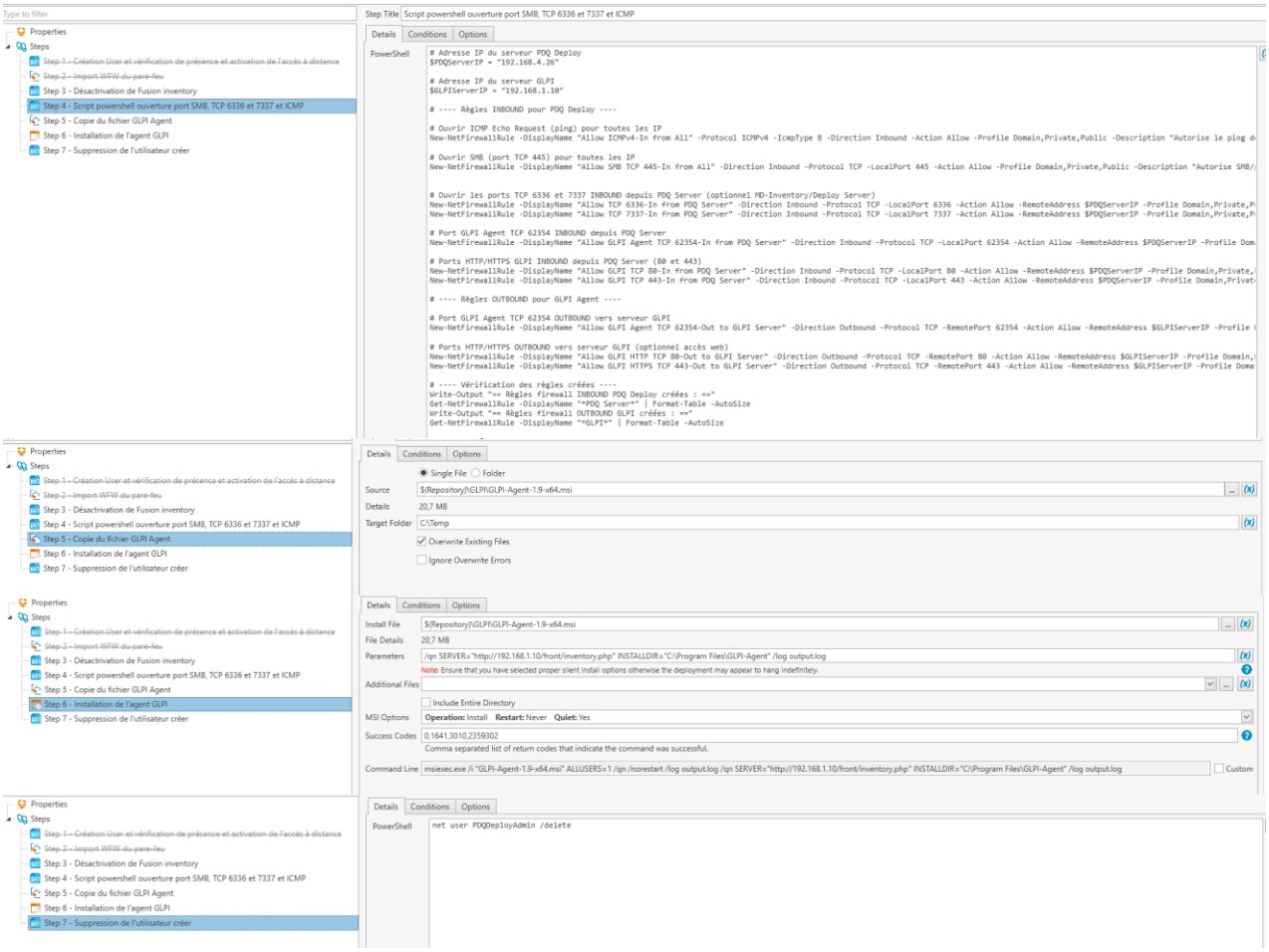
Get-NetFirewallRule -DisplayName "GLPI" | Format-Table -AutoSize

Phase 2 Paramétrage :

Le paramétrage de PDQ Deploy et de paramétrer le Package de déploiement de L'agent GLPI :

- Les étapes du package Install GLPI :
- Etape 1 : Désactivation de Fusion Inventory
- Etape 2 : Script PowerShell ouverture port SMB, TCP et protocole ICMP
- Etape 3 : Copie du fichier GLPI Agent
- Etape 4 : Intallation de l'agent GLPI
- Etape 5 : Script Suppression de l'utilisateur créer

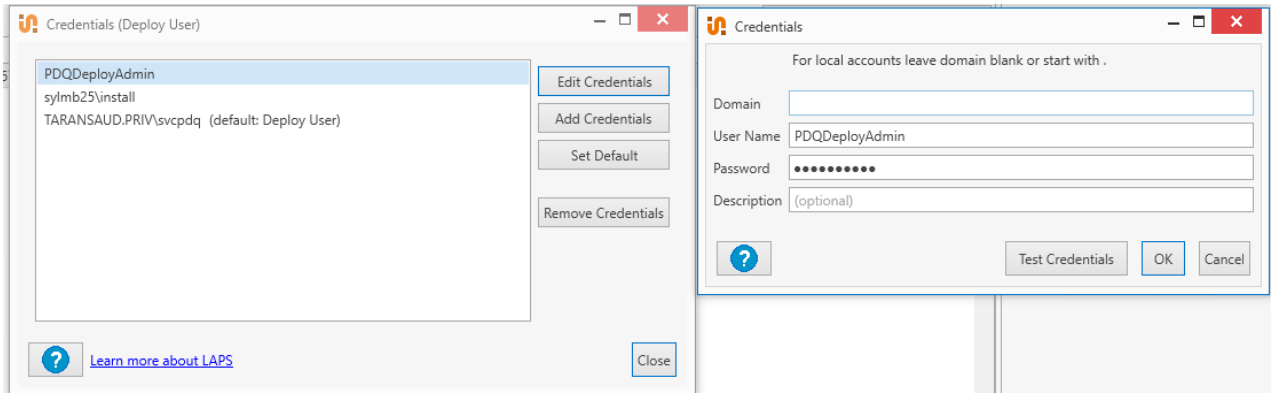




Le paramétrage du credential :

Le script qui doit être lancé manuellement en accédant à la machine distance via TightVNC (voir procédure ci-dessus)

Le script ajoute un utilisateur en local sur la machine avec des droits d'Administrateur.



Phase 3 : Déploiement :

Afin de lancer le déploiement sur des machines hors domaine il faut :

- Se connecter à distance via TightVNC à l'aide de son adresse IP et le MDP .

En fonction du Site : BEAUNE, SEGONZAC, CERILLY, LA CHARTRE, ST LAURENT, ST MAURICE

- Une fois connecté sur la machine distante, il fait ensuite ouvrir Powershell ISE en Administrateur et copier/coller le script Windows 10 au-dessus.

Une fois le script exécuté il faut ensuite aller dans le dossier *C:\Tools* et dans ce dossier ouvrir le document texte : *infos_machine.txt*

Copier les informations présente et les copier dans un fichier de référencement des machines du parc.