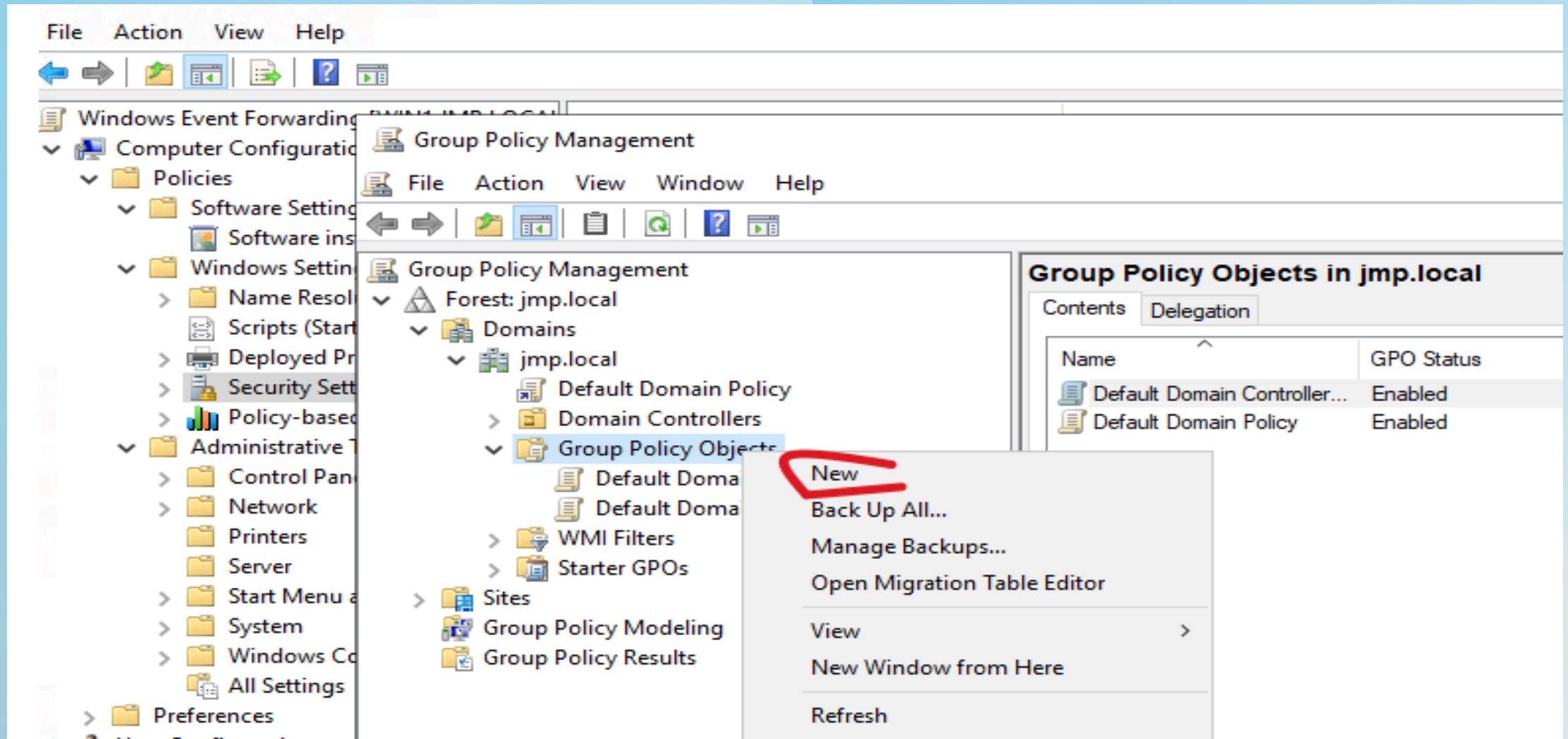
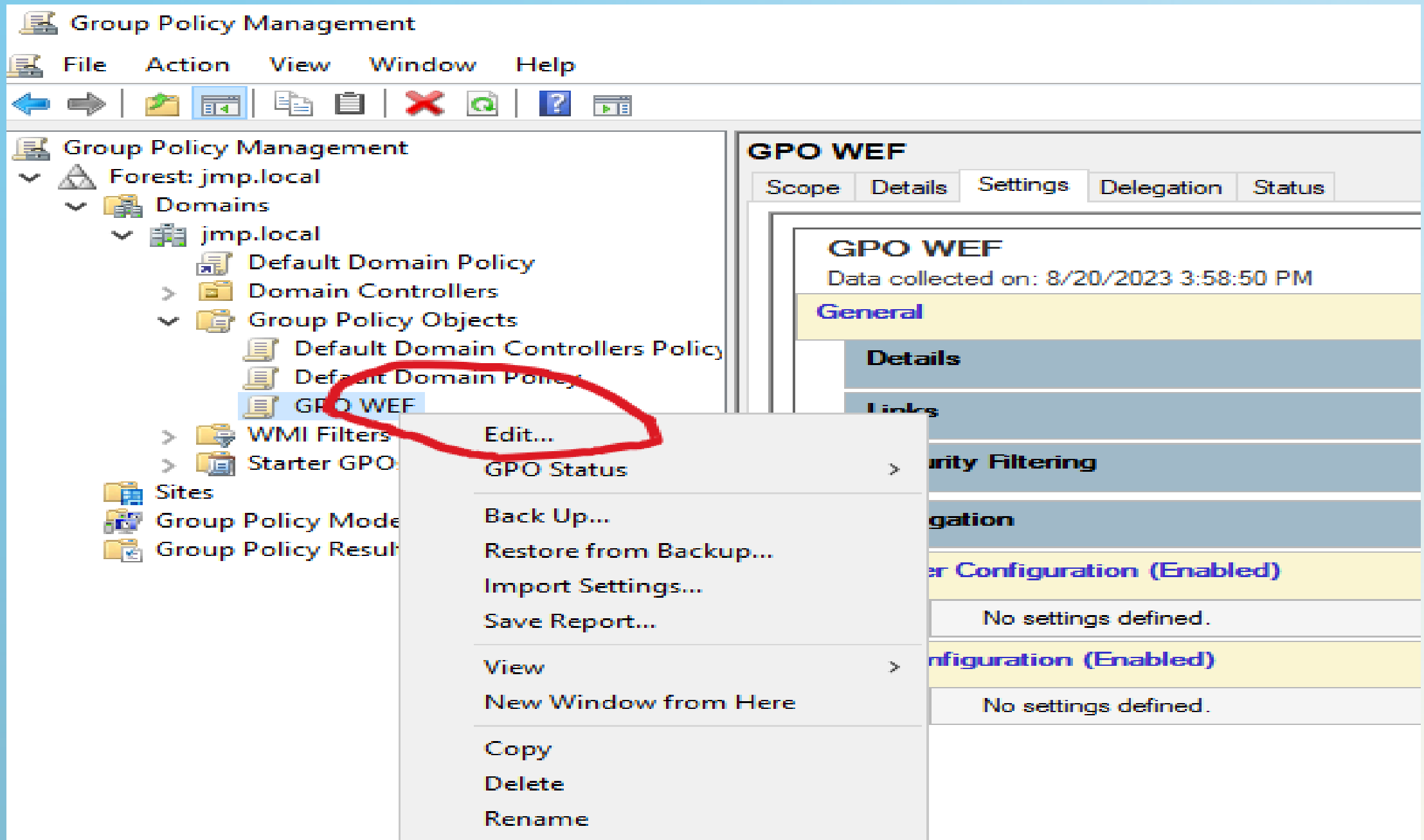
installation d'une GPO "WEF" en images

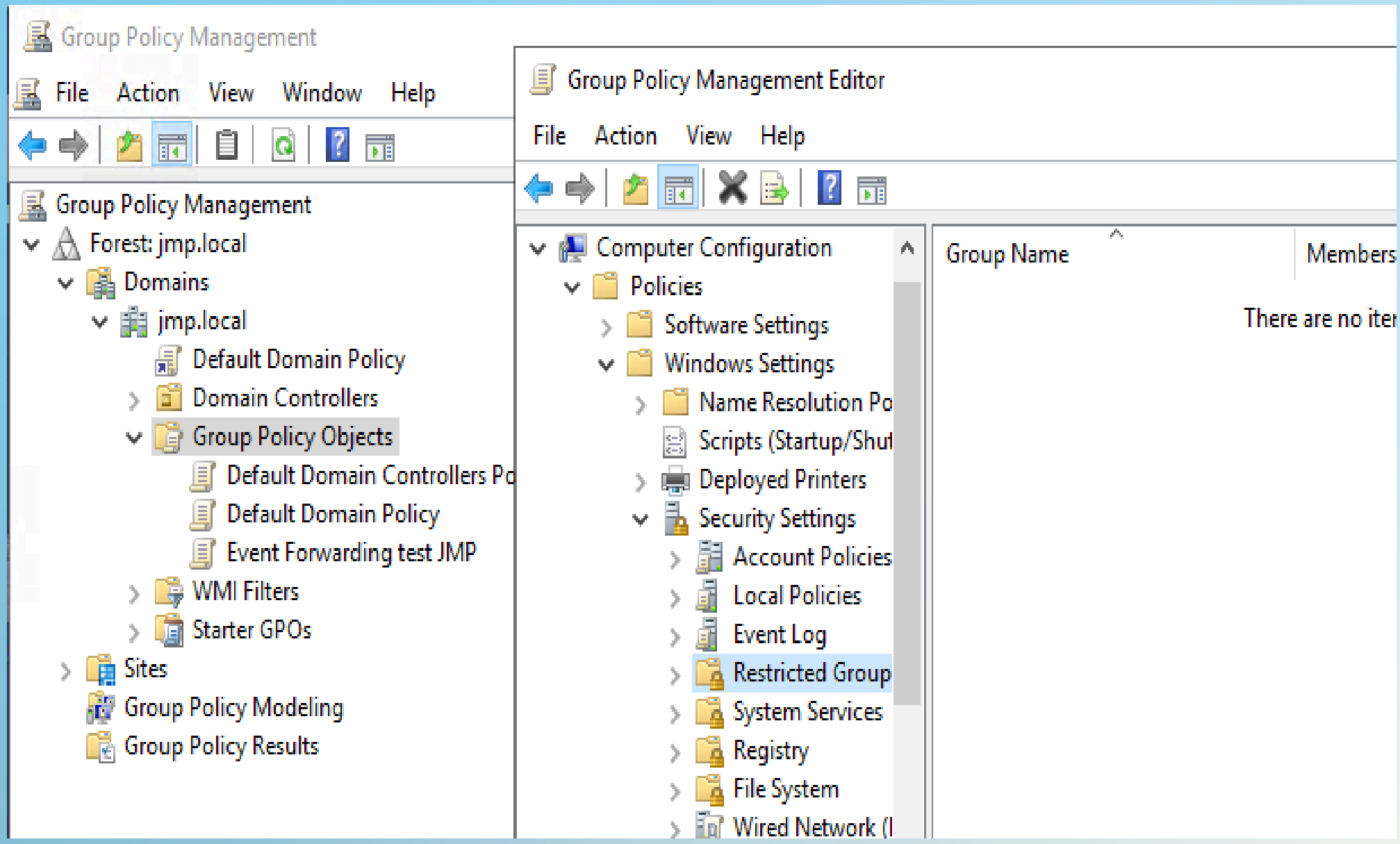
Lancez "Group Policy Management Tools" sur le serveur "win-1" (DC)

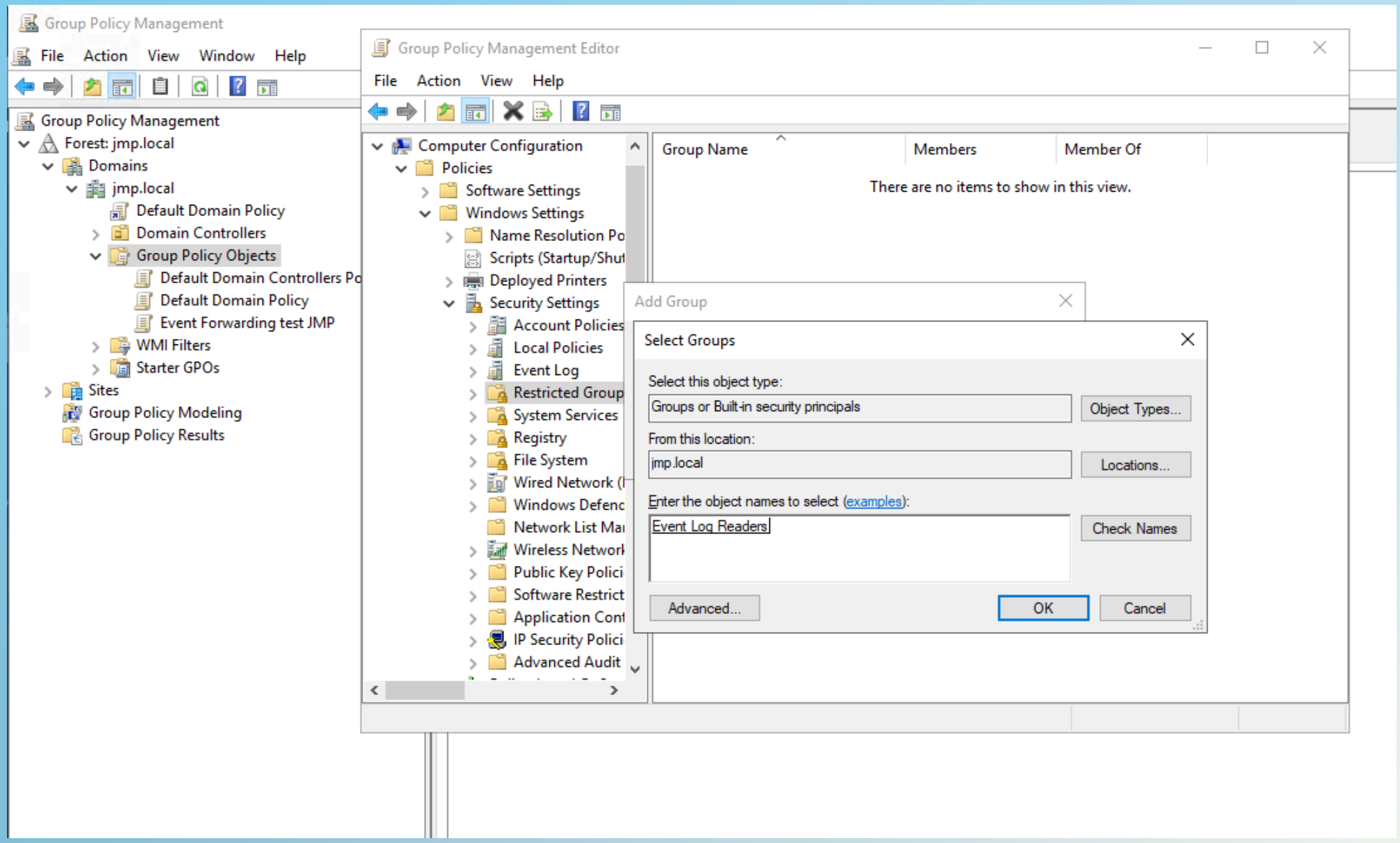


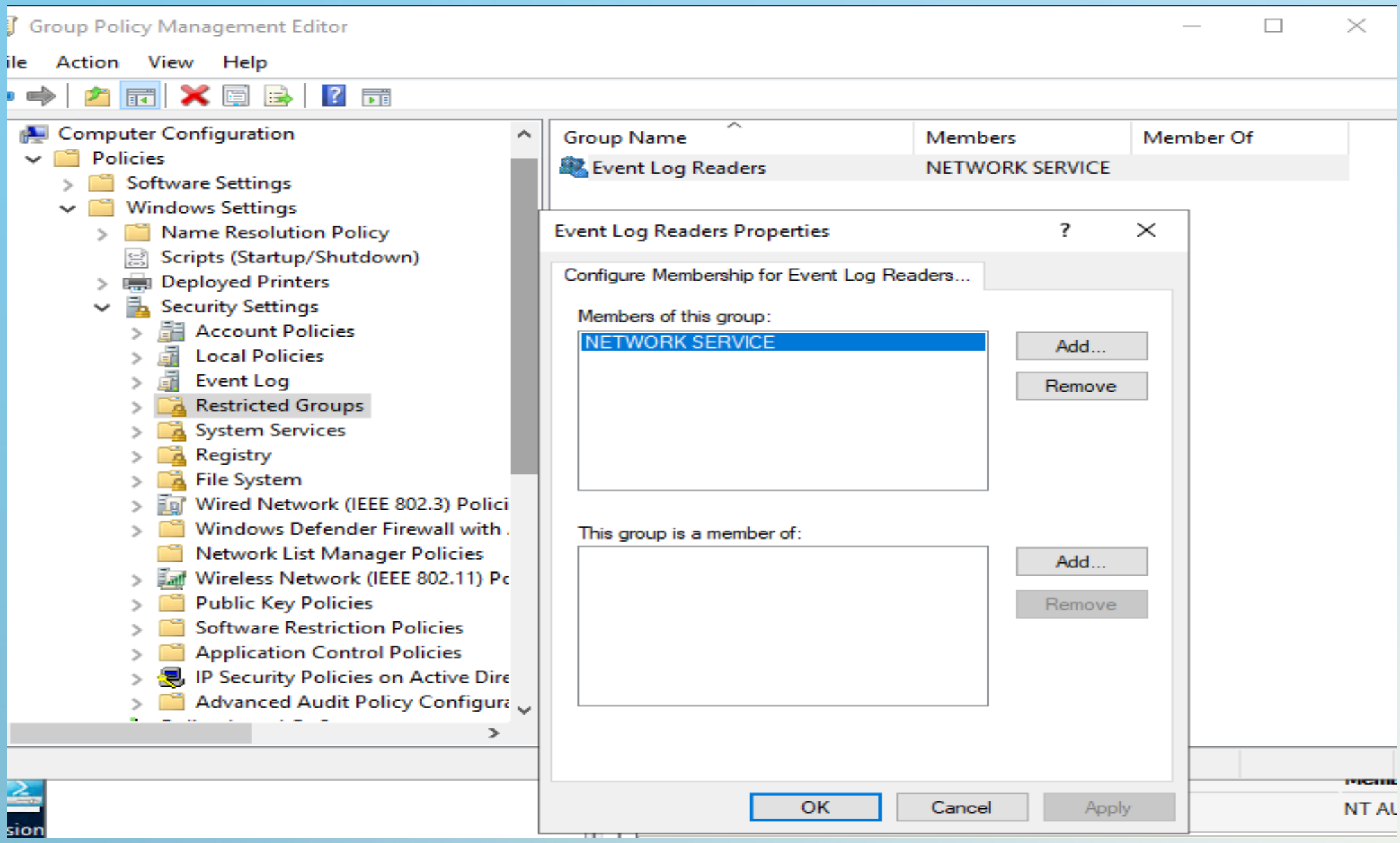

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
GPO WEF
WMI Filters
Starter GPO
Sites
Group Policy Mode
Group Policy Result
Edit...
GPO Status
Back Up...
Restore from Backup...
Import Settings...
Save Report...
View
New Window from Here
Copy
Delete
Rename
GPO WEF
Scope Details Settings Delegation Status
GPO WEF
Data collected on: 8/20/2023 3:58:50 PM
General
Details
Configuration (Enabled)
No settings defined.
No settings defined.

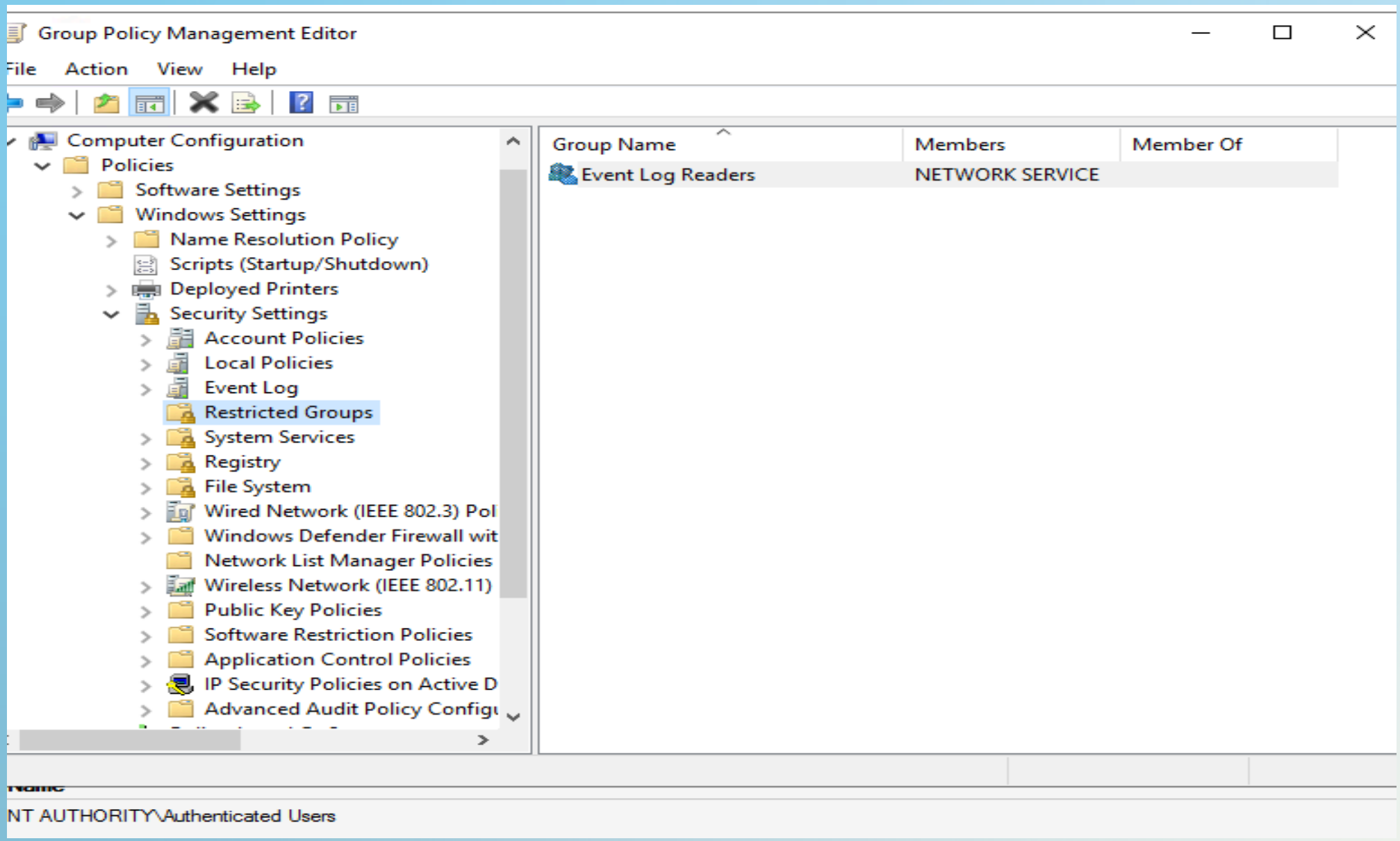
Configuration de la GPO pour les serveurs forwarders des "events logs"

- *Donner le droit de lecture aux logs (plusieurs variantes)*: Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups > Add Group > Event Log Readers > Add Members > Add > NetworkService


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Po
Scripts (Startup/Shut
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Group
System Services
Registry
File System
Wired Network (I
Group Name
Members
There are no iter

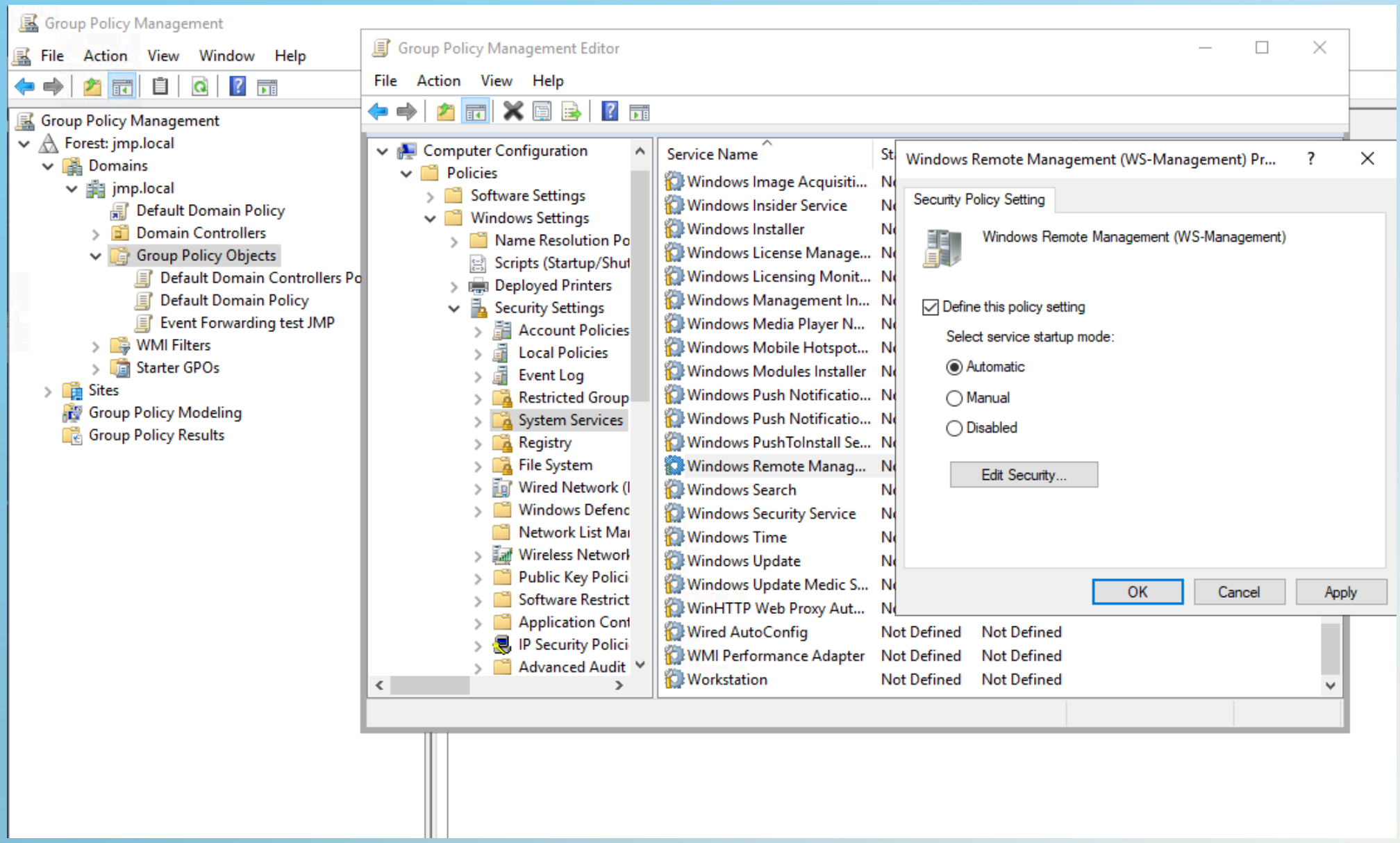

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Po
Scripts (Startup/Shut
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Group
System Services
Registry
File System
Wired Network (
Windows Defenc
Network List Mar
Wireless Network
Public Key Polici
Software Restrict
Application Cont
IP Security Polici
Advanced Audit
Group Name
Members
Member Of
There are no items to show in this view.
Add Group
Select Groups
Select this object type:
Groups or Built-in security principals
Object Types...
From this location:
jmp.local
Locations...
Enter the object names to select (examples):
Event Log Readers
Check Names
Advanced...
OK
Cancel


Group Policy Management Editor
ile Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polici
Windows Defender Firewall with
Network List Manager Policies
Wireless Network (IEEE 802.11) Pc
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Dire
Advanced Audit Policy Configura
Group Name
Members
Member Of
Event Log Readers
NETWORK SERVICE
Event Log Readers Properties
Configure Membership for Event Log Readers...
Members of this group:
NETWORK SERVICE
Add...
Remove
This group is a member of:
Add...
Remove
OK
Cancel
Apply
NT AU


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Defender Firewall wit
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Group Name
Members
Member Of
Event Log Readers
NETWORK SERVICE
NT AUTHORITY\Authenticated Users

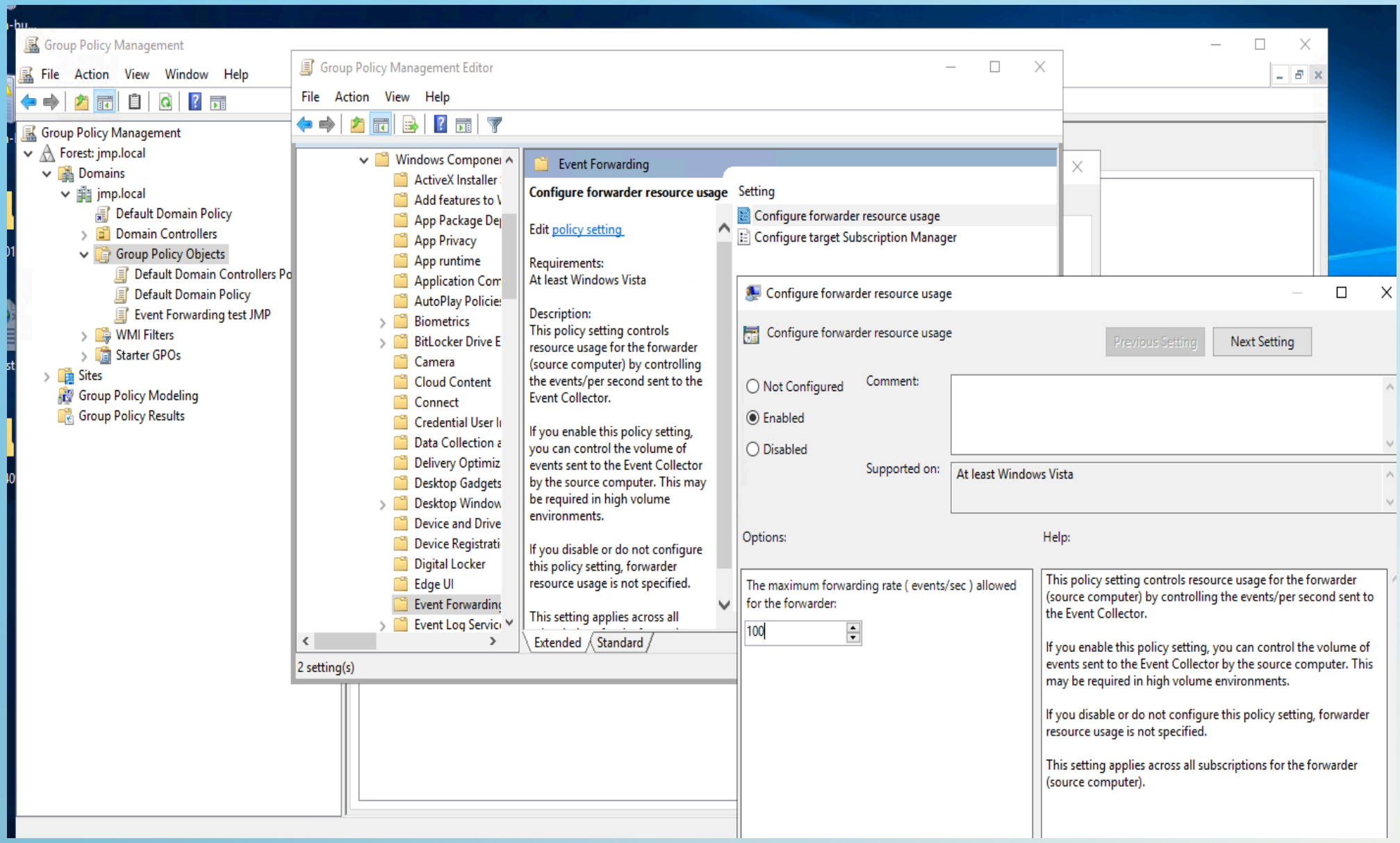
Démarrage automatique de WinRM sur les machines du domaine

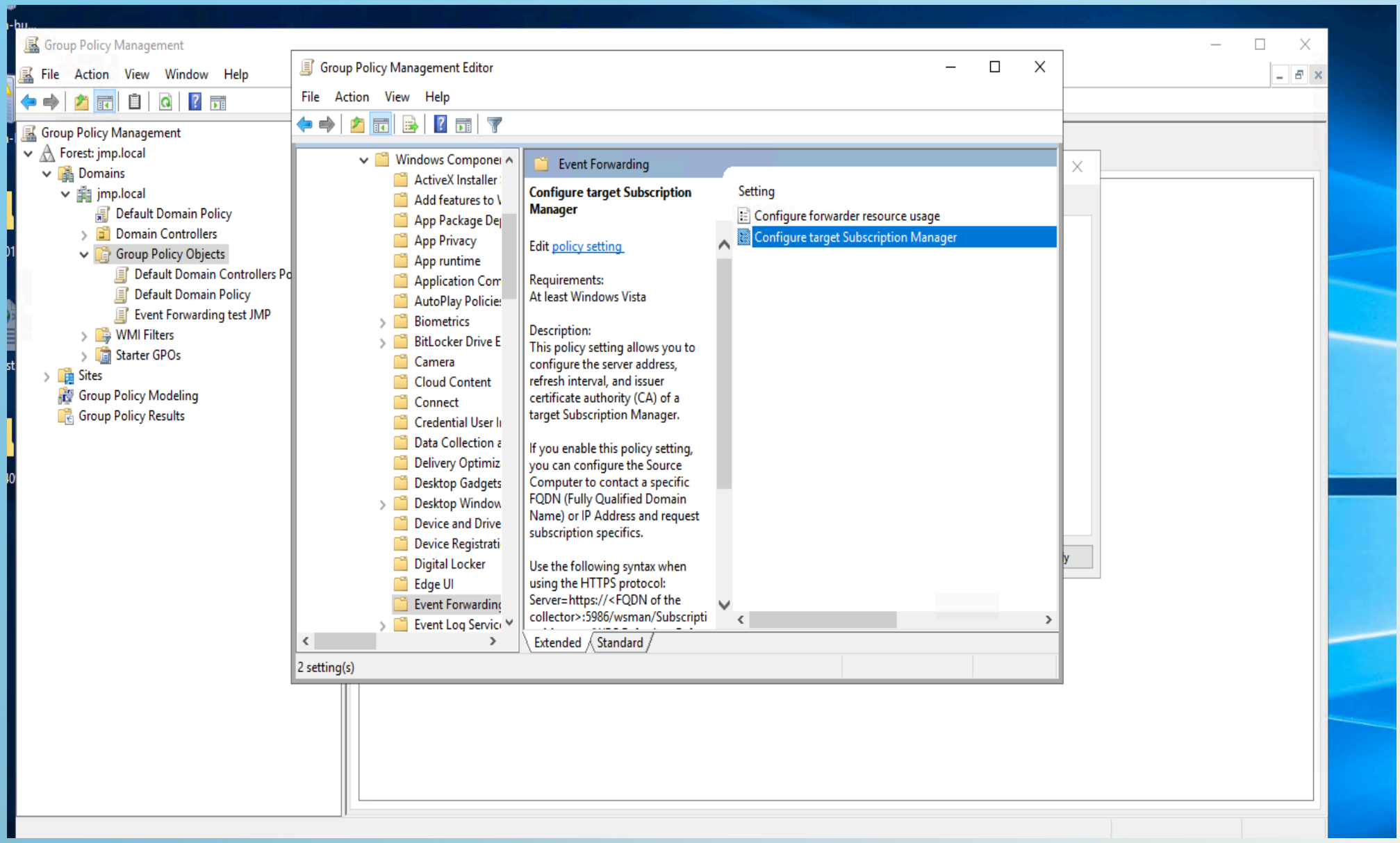
- *Démarrer le service WinRM sur les machines du domaine*: Computer Configuration > Policies > Windows Settings > Security Settings > System Services > Windows Remote Management (WS-Management) > Startup Mode > Automatic

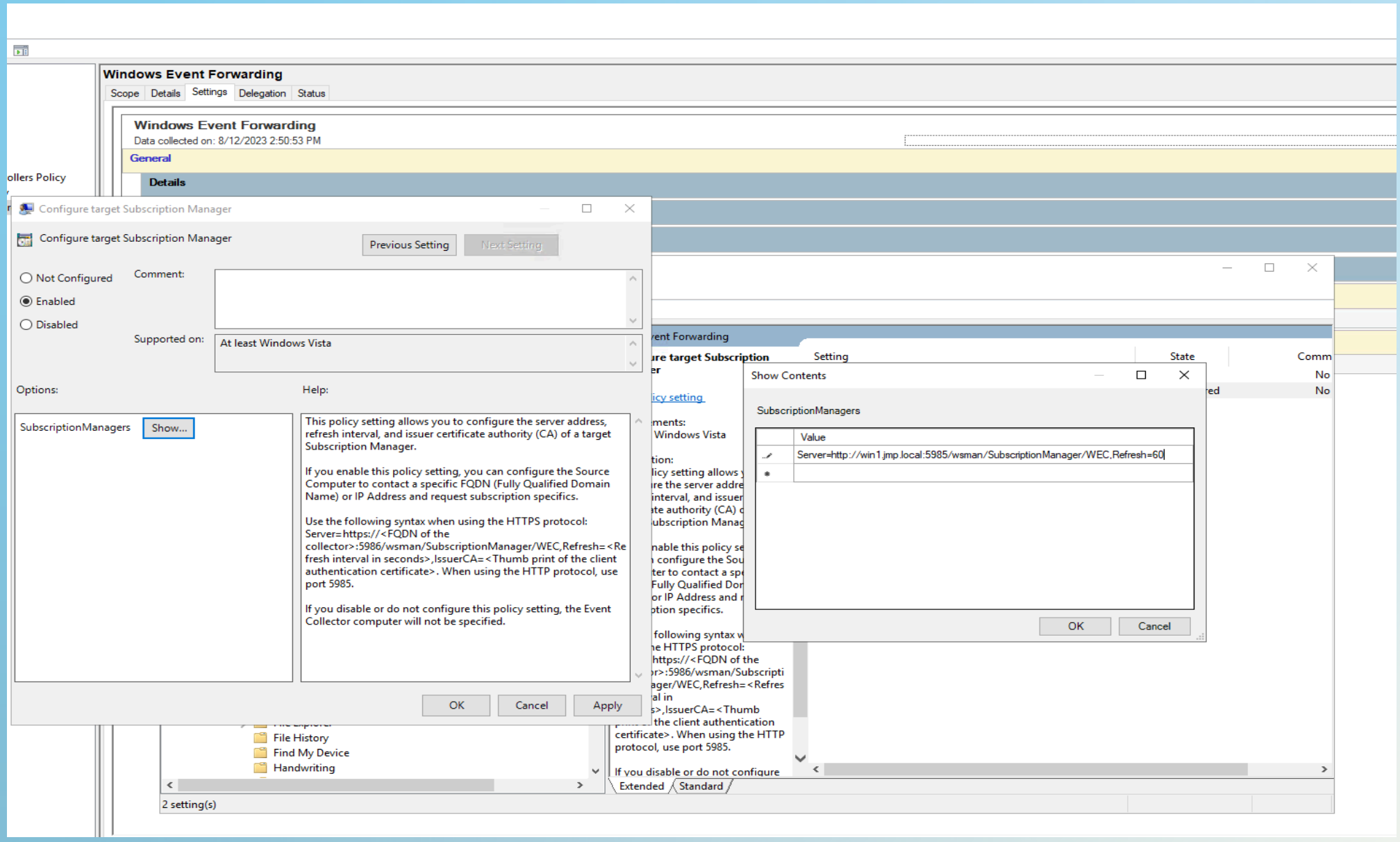

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Po
Scripts (Startup/Shut
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Group
System Services
Registry
File System
Wired Network (I
Windows Defenc
Network List Mar
Wireless Network
Public Key Polici
Software Restrict
Application Cont
IP Security Polici
Advanced Audit
Service Name
Windows Image Acquisiti...
Windows Insider Service
Windows Installer
Windows License Manage...
Windows Licensing Monit...
Windows Management In...
Windows Media Player N...
Windows Mobile Hotspot...
Windows Modules Installer
Windows Push Notificatio...
Windows Push Notificatio...
Windows PushToInstall Se...
Windows Remote Manag...
Windows Search
Windows Security Service
Windows Time
Windows Update
Windows Update Medic S...
WinHTTP Web Proxy Aut...
Wired AutoConfig Not Defined Not Defined
WMI Performance Adapter Not Defined Not Defined
Workstation Not Defined Not Defined
Windows Remote Management (WS-Management) Pr...
Security Policy Setting
Windows Remote Management (WS-Management)
Define this policy setting
Select service startup mode:
Automatic
Manual
Disabled
Edit Security...
OK
Cancel
Apply

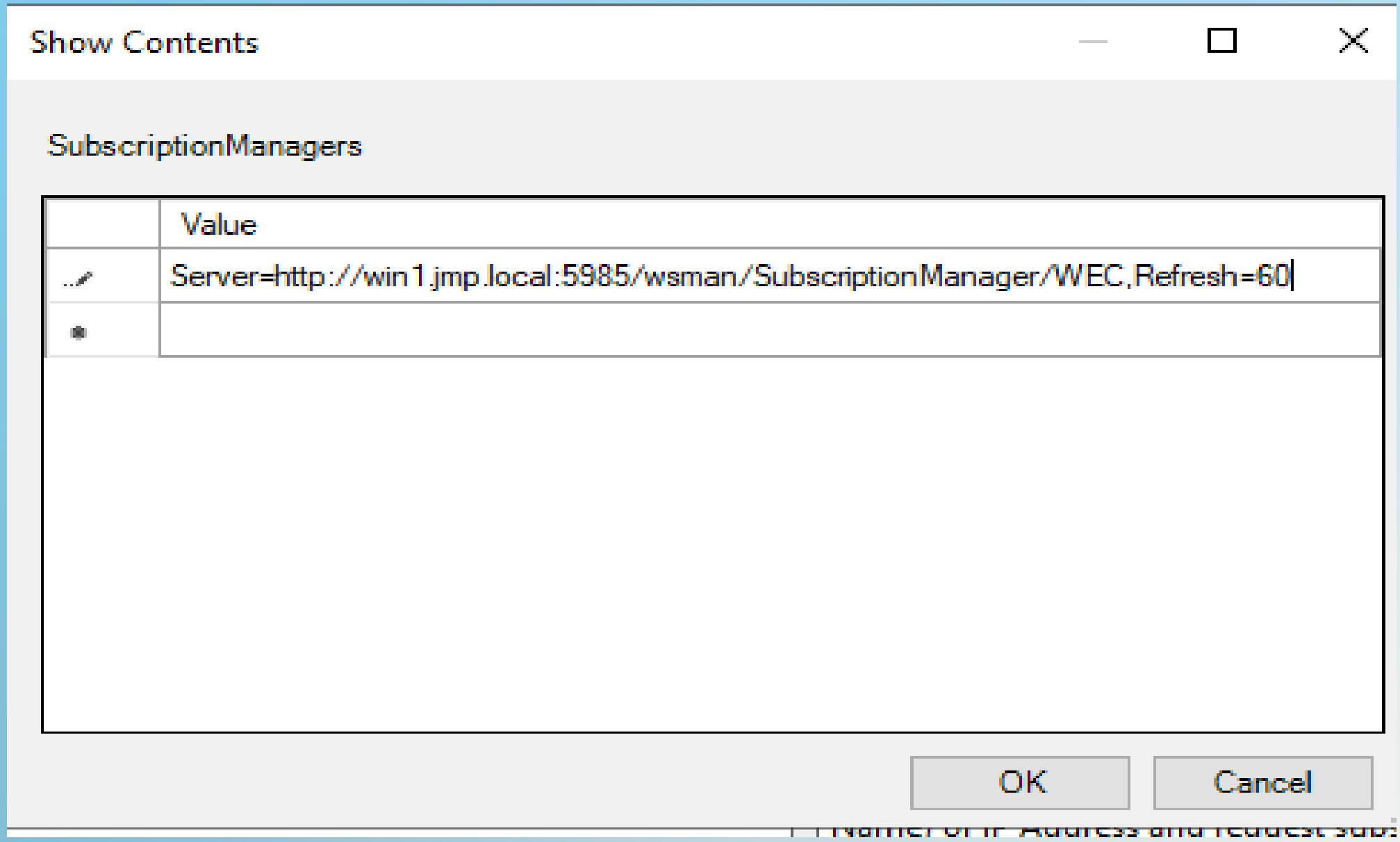
- *Configurer les ressources* : Computer Configuration > Policies > Administrative Templates > Windows Components > Event Forwarding > Configure Forwarder Ressource Usage
- *Configurer le subscription Manager* : Computer Configuration > Policies > Administrative Templates > Windows Components > Event Forwarding > Configure Subscription Manager -> enabled -> saisir le nom du serveur WEC (win-1) et le port 5985 (c 'est ce qui permet au forwardeur WEC de trouver son ou ses serveur)

```
Server=http://win1.jmp.local:5985/wsman/SubscriptionManager/WEC,Refresh=60
```


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Windows Compone
ActiveX Installer
Add features to V
App Package De
App Privacy
App runtime
Application Com
AutoPlay Policies
Biometrics
BitLocker Drive E
Camera
Cloud Content
Connect
Credential User I
Data Collection a
Delivery Optimiz
Desktop Gadgets
Desktop Window
Device and Drive
Device Registrati
Digital Locker
Edge UI
Event Forwardin
Event Log Servic
Event Forwarding
Configure forwarder resource usage
Edit policy setting
Requirements:
At least Windows Vista
Description:
This policy setting controls resource usage for the forwarder (source computer) by controlling the events/per second sent to the Event Collector.
If you enable this policy setting, you can control the volume of events sent to the Event Collector by the source computer. This may be required in high volume environments.
If you disable or do not configure this policy setting, forwarder resource usage is not specified.
This setting applies across all
Setting
Configure forwarder resource usage
Configure target Subscription Manager
Extended Standard
2 setting(s)
Configure forwarder resource usage
Configure forwarder resource usage
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
The maximum forwarding rate (events/sec) allowed for the forwarder:
100
This policy setting controls resource usage for the forwarder (source computer) by controlling the events/per second sent to the Event Collector.
If you enable this policy setting, you can control the volume of events sent to the Event Collector by the source computer. This may be required in high volume environments.
If you disable or do not configure this policy setting, forwarder resource usage is not specified.
This setting applies across all subscriptions for the forwarder (source computer).


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Windows Compone
ActiveX Installer
Add features to V
App Package De
App Privacy
App runtime
Application Com
AutoPlay Policies
Biometrics
BitLocker Drive E
Camera
Cloud Content
Connect
Credential User I
Data Collection a
Delivery Optimiz
Desktop Gadgets
Desktop Window
Device and Drive
Device Registrati
Digital Locker
Edge UI
Event Forwardin
Event Log Servic
Event Forwarding
Configure target Subscription Manager
Edit policy setting
Requirements:
At least Windows Vista
Description:
This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.
If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.
Use the following syntax when using the HTTPS protocol:
Server=https://<FQDN of the collector>:5986/wsman/Subscripti
Setting
Configure forwarder resource usage
Configure target Subscription Manager
Extended
Standard
2 setting(s)

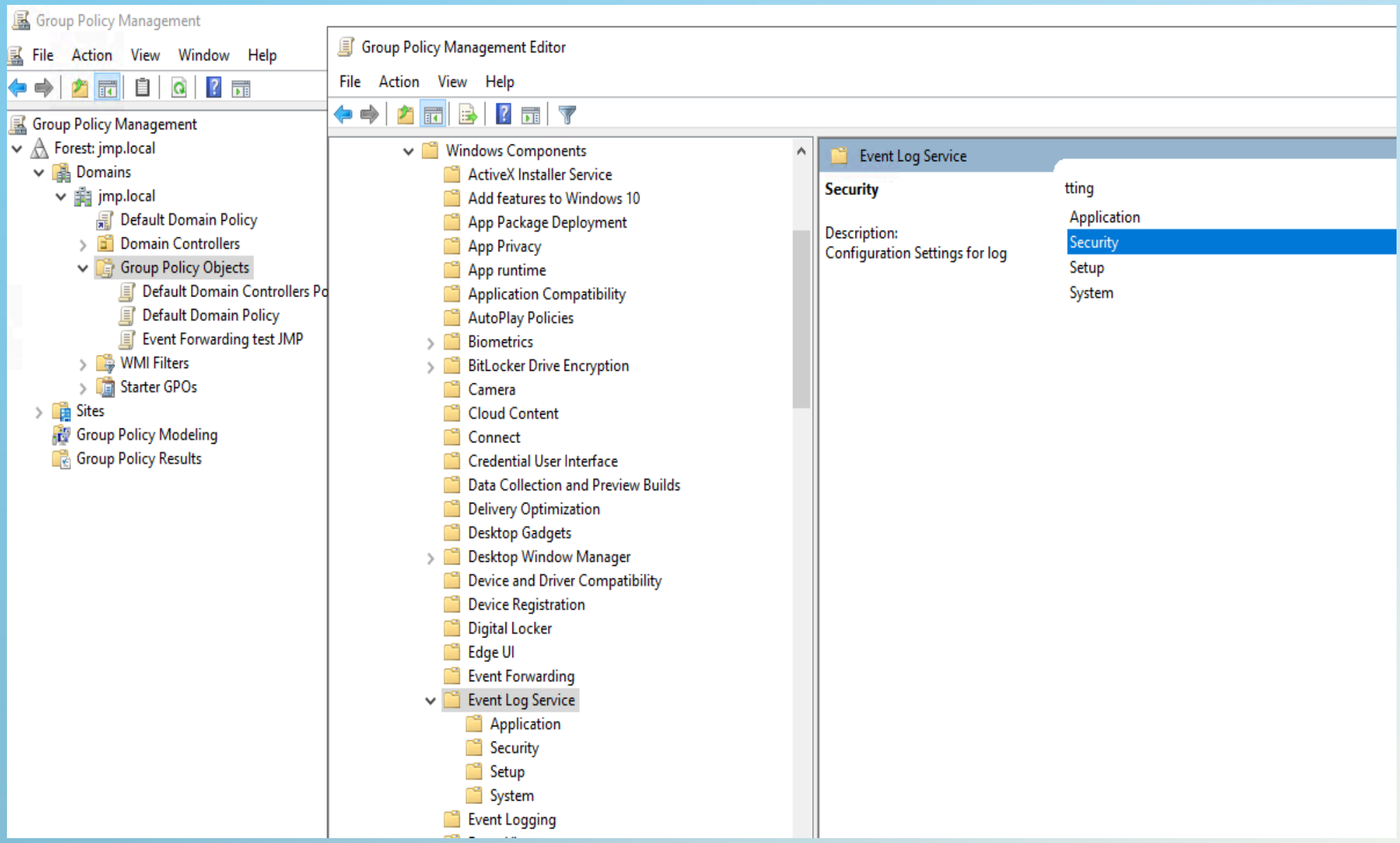

Windows Event Forwarding
Scope
Details
Settings
Delegation
Status
Windows Event Forwarding
Data collected on: 8/12/2023 2:50:53 PM
General
Details
Configure target Subscription Manager
Configure target Subscription Manager
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
SubscriptionManagers
Show...
This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.
If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.
Use the following syntax when using the HTTPS protocol: Server=https://<FQDN of the collector>:5986/wsman/SubscriptionManager/WEC,Refresh=<Refresh interval in seconds>,IssuerCA=<Thumb print of the client authentication certificate>. When using the HTTP protocol, use port 5985.
If you disable or do not configure this policy setting, the Event Collector computer will not be specified.
OK
Cancel
Apply
Show Contents
SubscriptionManagers
Value
Server=http://win1.jmp.local:5985/wsman/SubscriptionManager/WEC,Refresh=60
OK
Cancel
Setting
State
Comm
No
No
File History
Find My Device
Handwriting
Extended
Standard
2 setting(s)

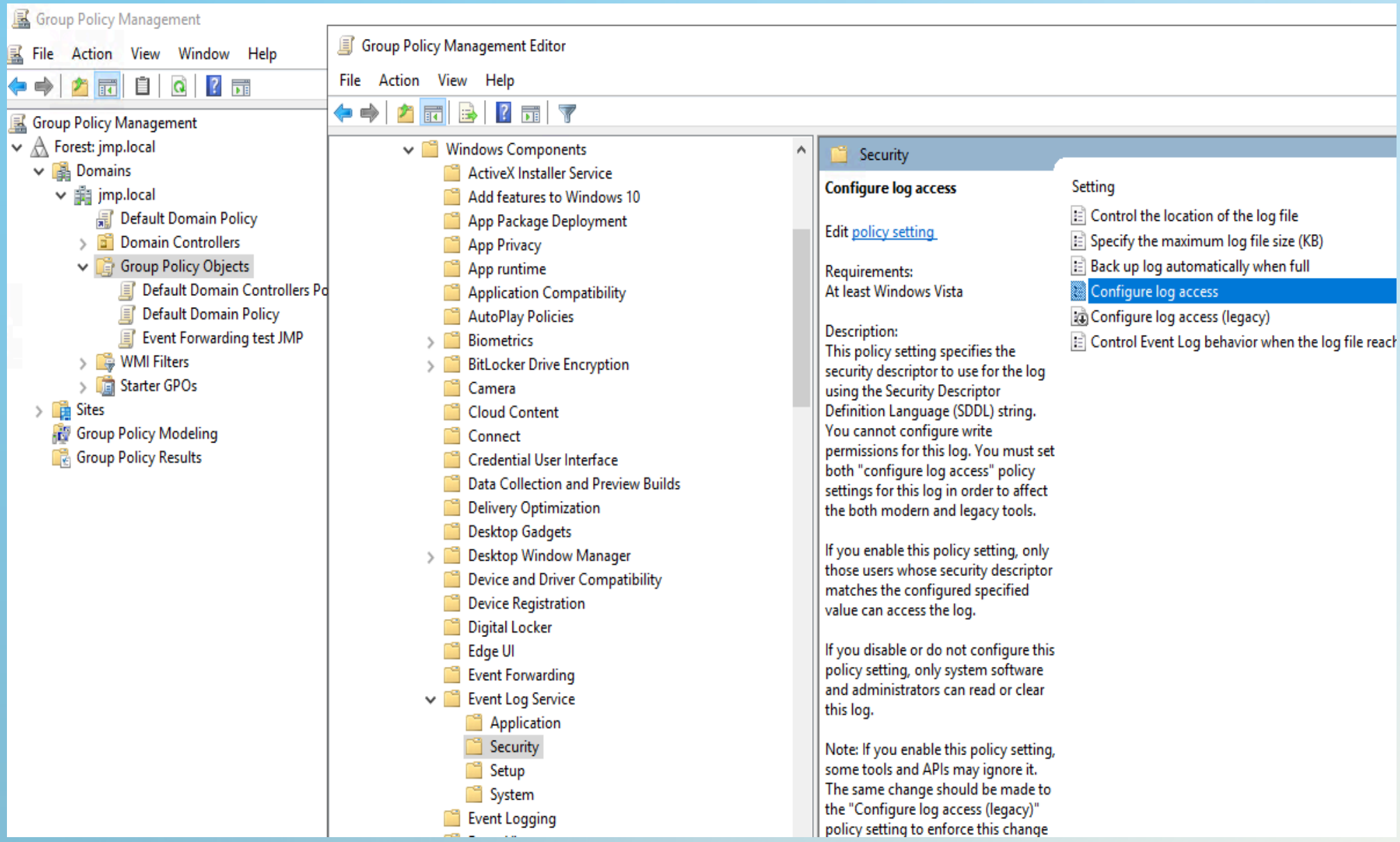

Show Contents
SubscriptionManagers
Value
Server=http://win1.jmp.local:5985/wsman/SubscriptionManager/WEC,Refresh=60
OK
Cancel

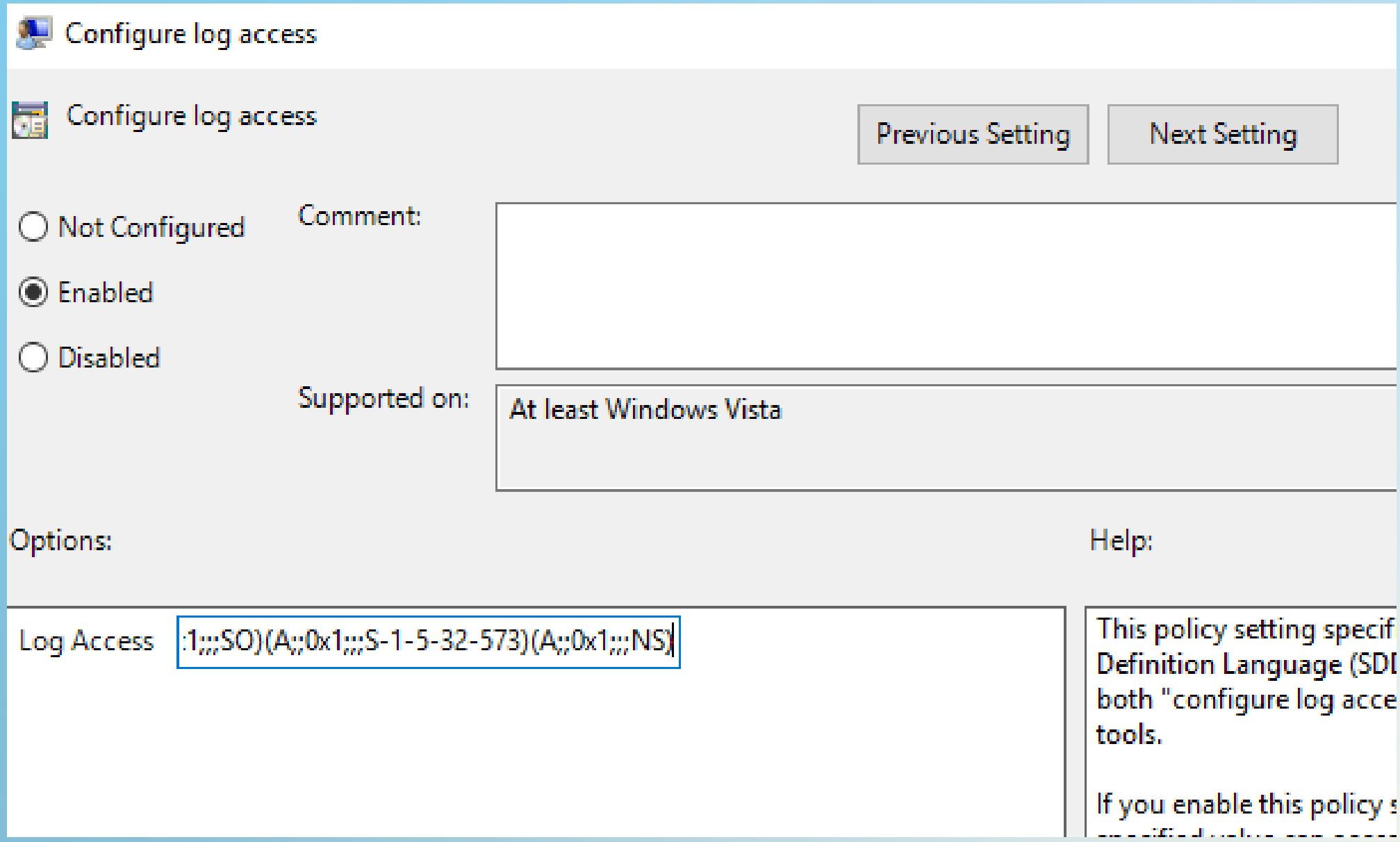
- *On donne maintenant les droits sur chaque channel de log à l'utilisateur "EventLogReader" et à "NetworkService" pour pouvoir lire les logs* : Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > Security

La valeur à mettre est constituée par le SDDL de base (A;;0x3;;;S-1-5-20) auquel on rajoute le SDDL de l'utilisateur EventLogReader (A;;0x1;;;NS) . Utilisez la commande "**wevtutil gl security**" pour obtenir le SDDL de base et demander à chatGPT de vous l'expliquer.

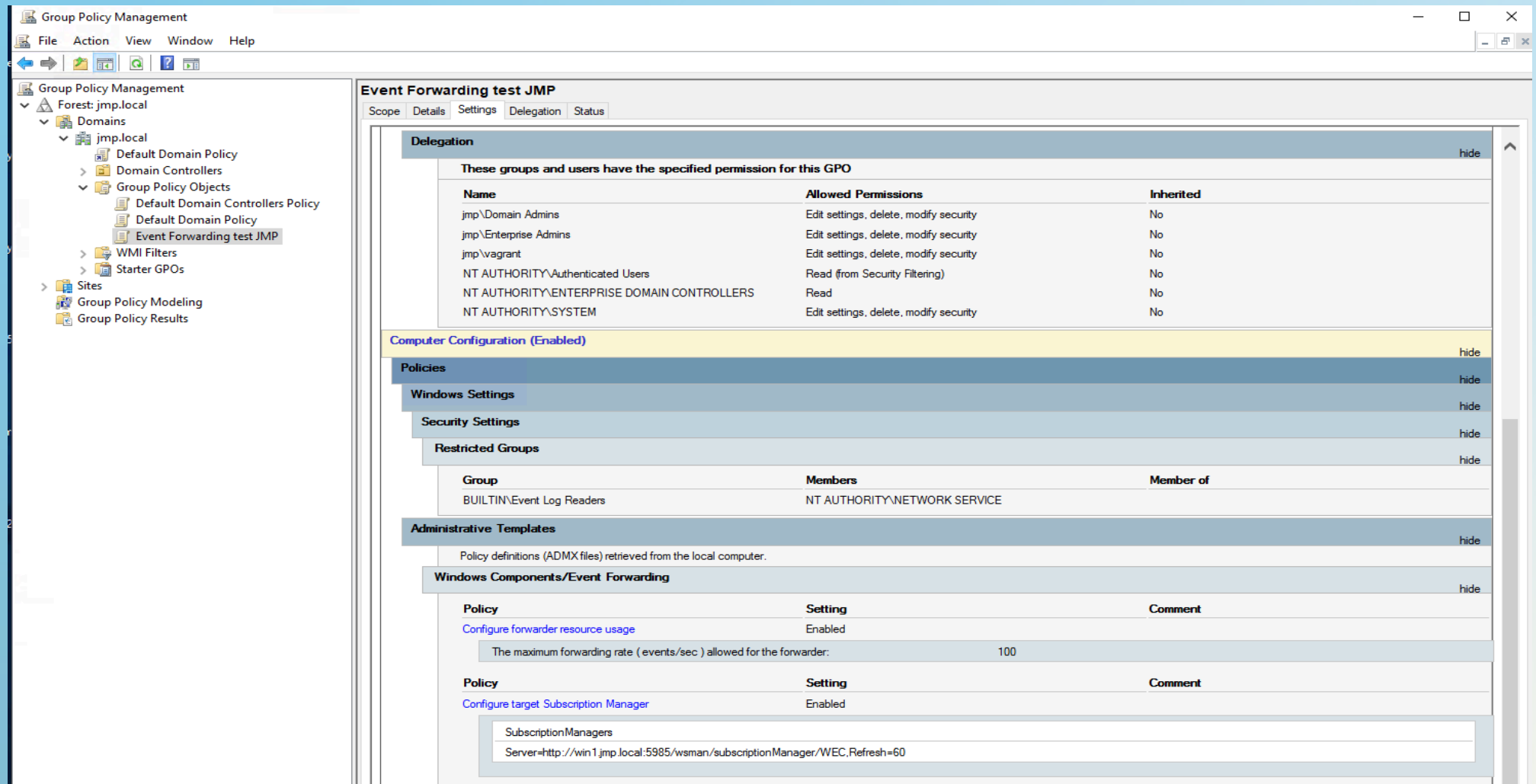
```
jmp\vagrant@WIN1 C:\Users\vagrant\Desktop>wevtutil gl Security
name: Security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x1;;;BO)(A;;0x1;;;SO)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Security.evtx
  retention: false
  autoBackup: false
  maxSize: 1073741824
publishing:
  fileMax: 1
```


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Windows Components
ActiveX Installer Service
Add features to Windows 10
App Package Deployment
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview Builds
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Application
Security
Setup
System
Event Logging
Event Log Service
Security
tting
Description:
Configuration Settings for log
Application
Security
Setup
System

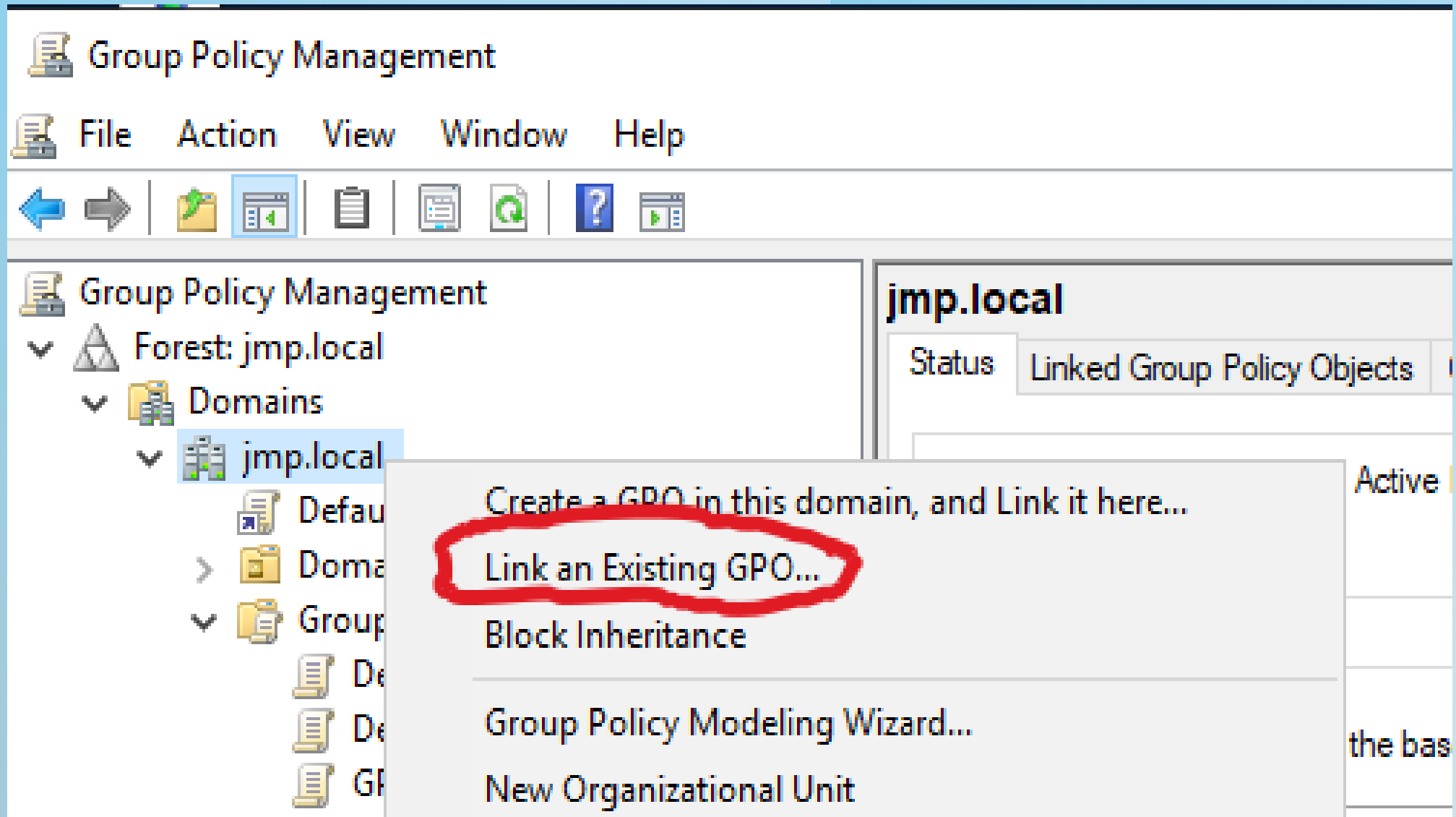

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Windows Components
ActiveX Installer Service
Add features to Windows 10
App Package Deployment
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview Builds
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Application
Security
Setup
System
Event Logging
Security
Configure log access
Edit policy setting
Requirements:
At least Windows Vista
Description:
This policy setting specifies the security descriptor to use for the log using the Security Descriptor Definition Language (SDDL) string. You cannot configure write permissions for this log. You must set both "configure log access" policy settings for this log in order to affect the both modern and legacy tools.
If you enable this policy setting, only those users whose security descriptor matches the configured specified value can access the log.
If you disable or do not configure this policy setting, only system software and administrators can read or clear this log.
Note: If you enable this policy setting, some tools and APIs may ignore it. The same change should be made to the "Configure log access (legacy)" policy setting to enforce this change
Setting
Control the location of the log file
Specify the maximum log file size (KB)
Back up log automatically when full
Configure log access
Configure log access (legacy)
Control Event Log behavior when the log file reach


Configure log access
Configure log access
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
Log Access
:1;;;SO)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
This policy setting specif
Definition Language (SDI
both "configure log acce
tools.
If you enable this policy s

Au final vous pouvez vérifier sur l'onglet "settings" de la GPO que tout est bien configuré



On lie la GPO au domaine maintenant



Propagation forcée de la GPO sur les serveurs forwarders

```
jmp\vagrant@WIN1 C:\Users\vagrant\Desktop>gpupdate /Force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Vérification de la bonne propagation de la GPO sur le serveur forwarder (win-2) Ca peut mettre un peu de temps à se propager...

```
vagrant@WIN2 C:\Users\vagrant>gpresult /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2018 Microsoft Corporation. All rights reserved.

Created on 8/12/2023 at 3:19:45 PM


RSOP data for WIN2\vagrant on WIN2 : Logging Mode
-------------------------------------------------

OS Configuration:            Member Server
OS Version:                  10.0.17763
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\vagrant
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=WIN2,CN=Computers,DC=jmp,DC=local
    Last time Group Policy was applied: 8/12/2023 at 3:18:55 PM
```