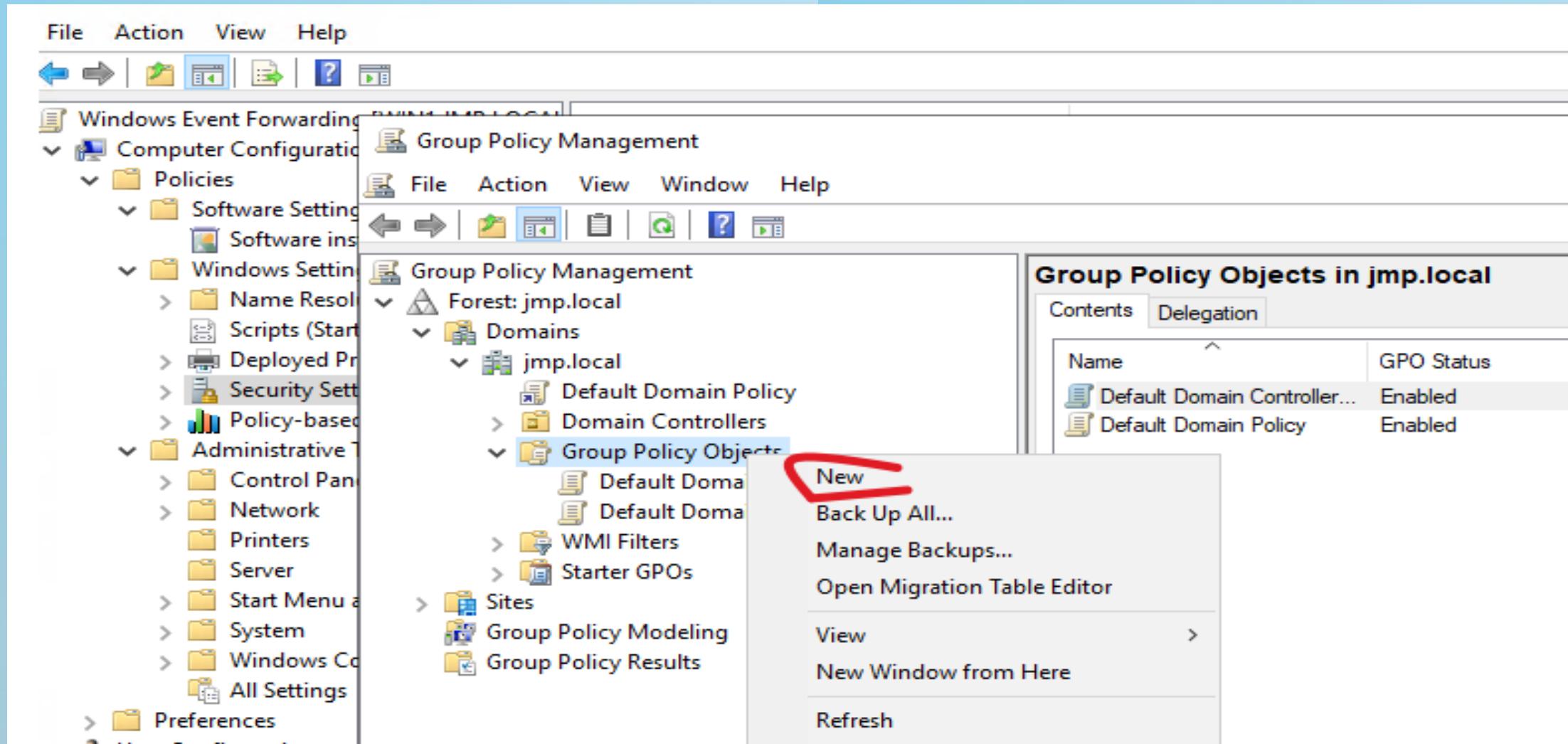


installation d'une GPO "WEF" en images

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

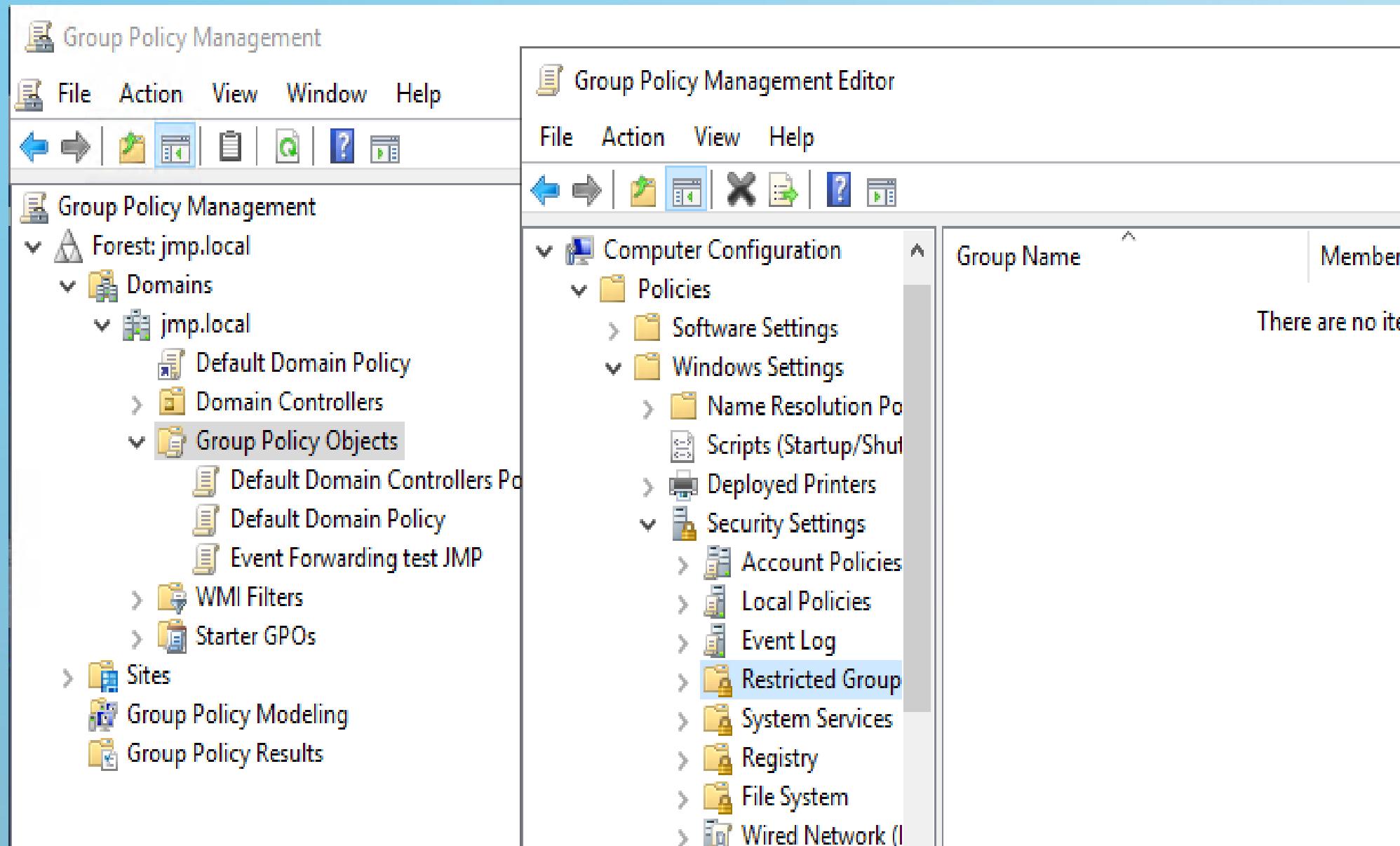


The screenshot shows the Windows Group Policy Management console. On the left, the navigation pane displays the forest and domain structure under 'Forest: jmp.local'. In the 'Group Policy Objects' section, 'GPO WEF' is selected and highlighted with a red oval. A context menu is open over this item, listing options such as 'Edit...', 'GPO Status', 'Back Up...', 'Restore from Backup...', 'Import Settings...', 'Save Report...', 'View', 'New Window from Here', 'Copy', 'Delete', and 'Rename'. To the right of the menu, the 'Details' tab of the 'GPO WEF' properties window is visible, showing the following details:

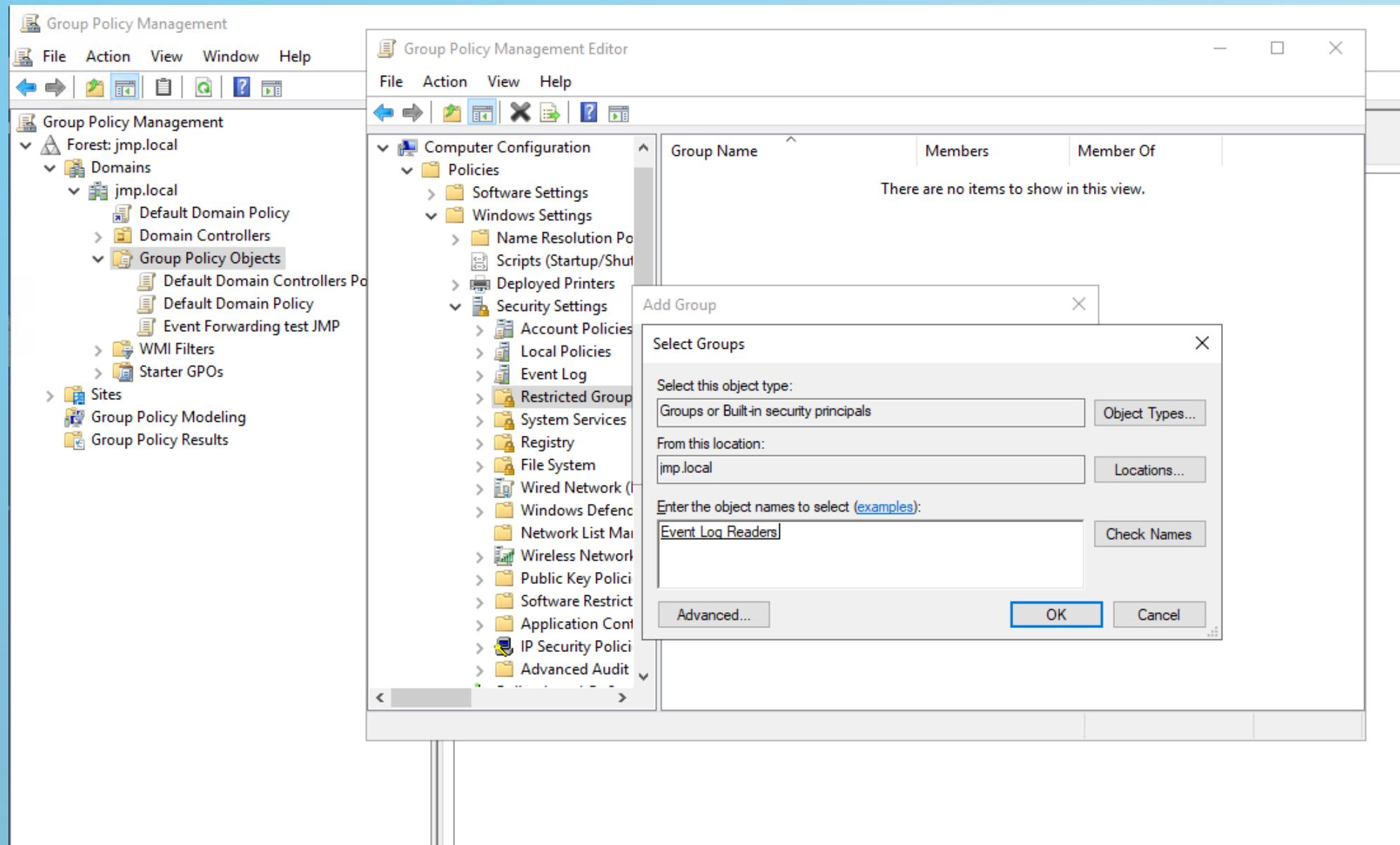
Setting	Status
Security Filtering	Configuration (Enabled)
No settings defined.	
File Replication Configuration (Enabled)	Configuration (Enabled)
No settings defined.	

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

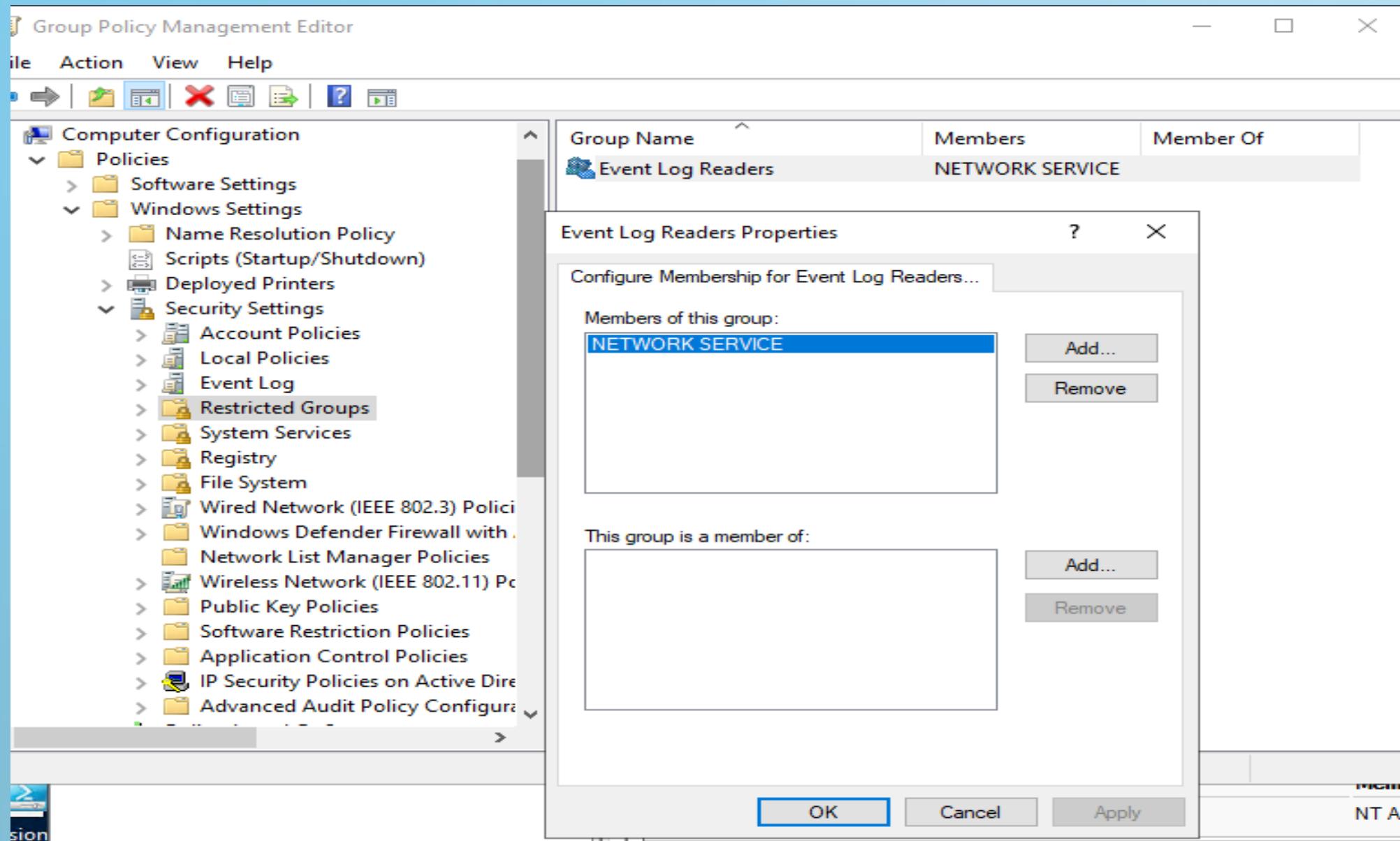
- *Donner le droit de lecture aux logs (plusieurs variantes):* Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups > Add Group > Event Log Readers > Add Members > Add > NetworkService



R5.cyber.11 Supervision de la sécurité



R5.cyber.11 Supervision de la sécurité



R5.cyber.11 Supervision de la sécurité

The screenshot shows the Group Policy Management Editor window. The left pane displays a tree view of policy settings under 'Computer Configuration' > 'Policies' > 'Security Settings'. The 'Restricted Groups' node is selected and highlighted in blue. The right pane contains a table titled 'Event Log Readers' with one row. The table has columns for 'Group Name', 'Members', and 'Member Of'. The single entry is 'Event Log Readers' with 'NETWORK SERVICE' listed under 'Members' and 'Member Of'.

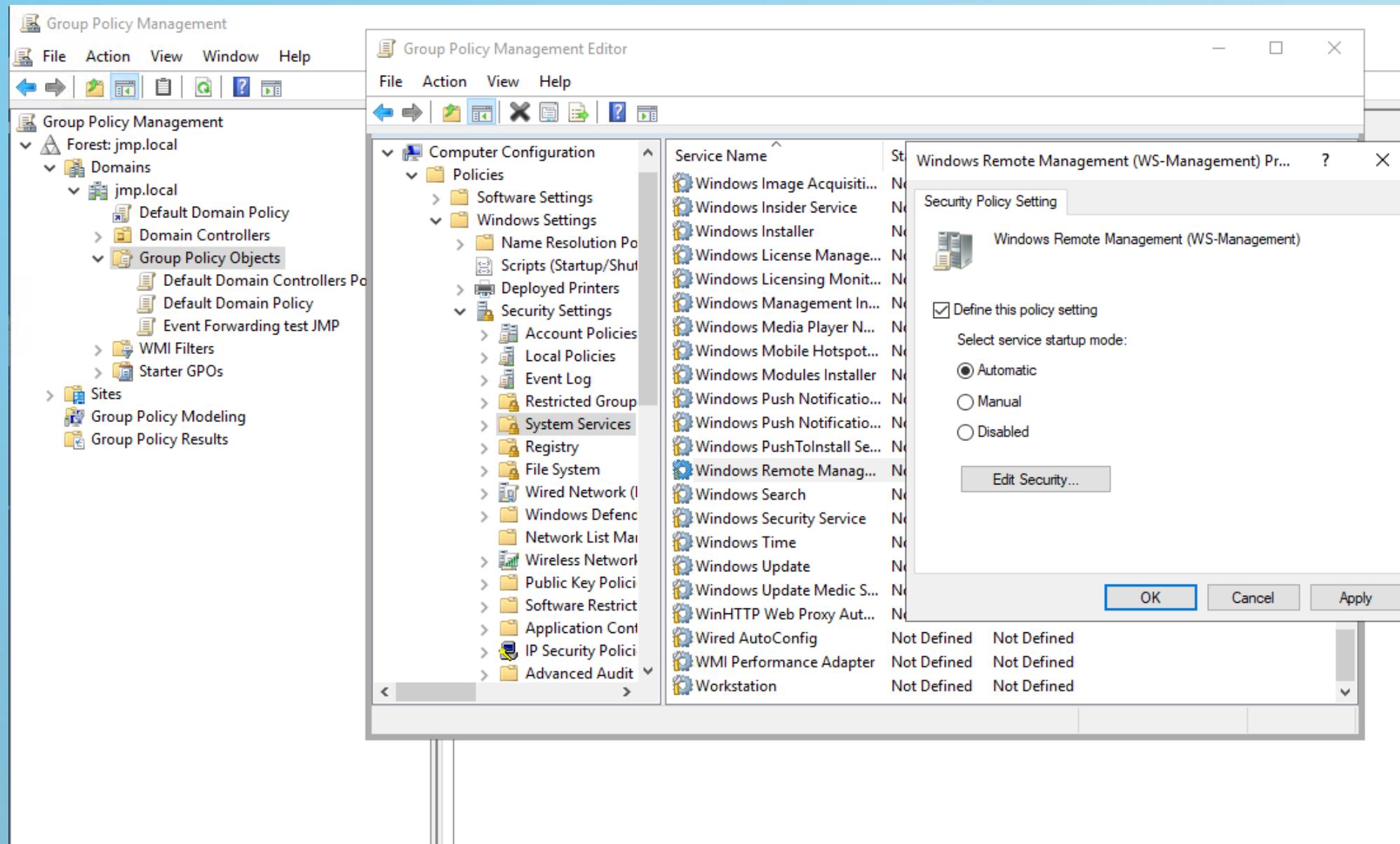
Group Name	Members	Member Of
Event Log Readers	NETWORK SERVICE	

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

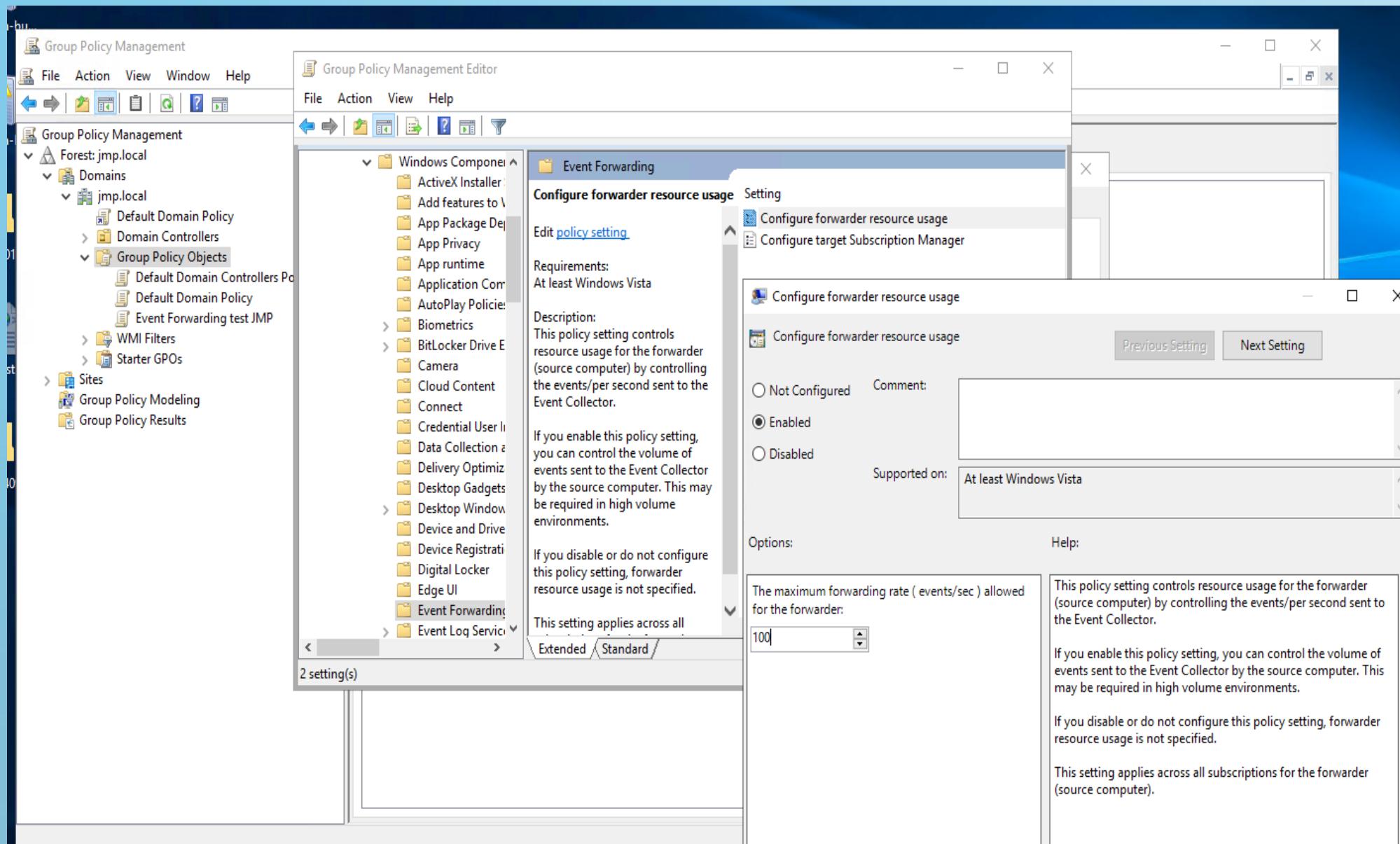
R5.cyber.11 Supervision de la sécurité



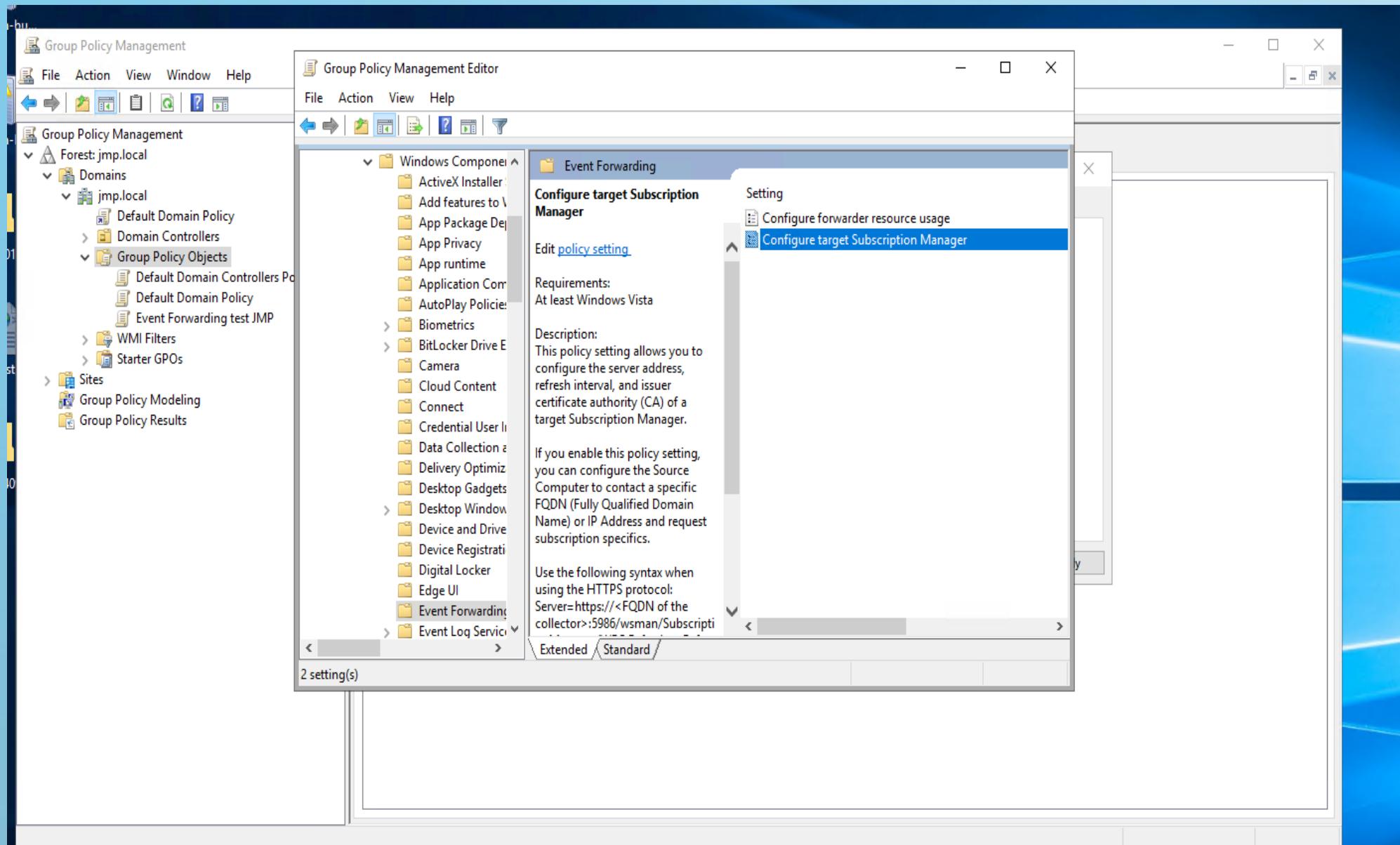
- *Configurer les ressources* : Computer Configuration > Policies > Administrative Templates > Windows Components > Event Forwarding > Configure Forwarder Ressource Usage
- *Configurer le subscription Manager* : Computer Configuration > Policies > Administrative Templates > Windows Components > Event 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
```

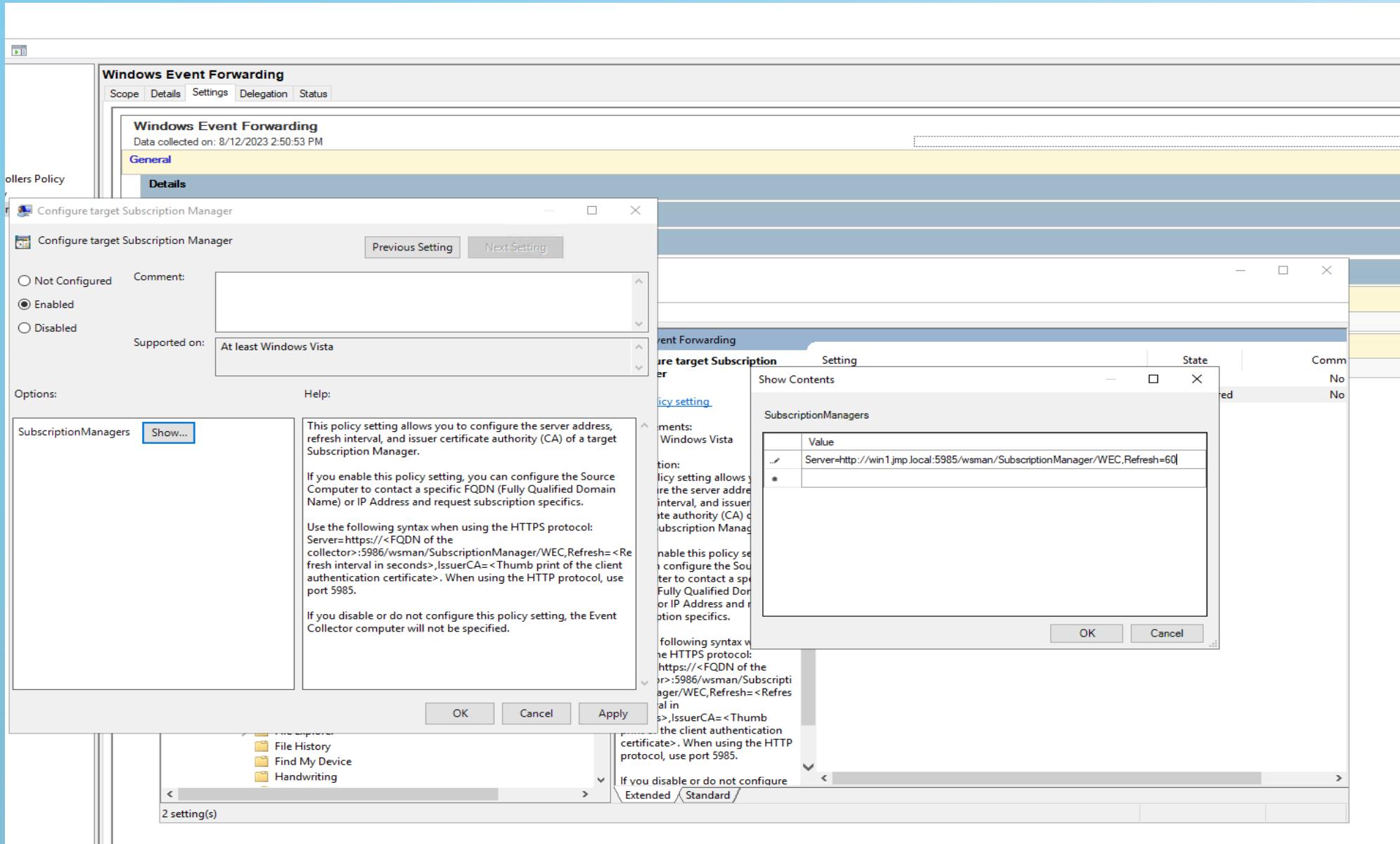
R5.cyber.11 Supervision de la sécurité

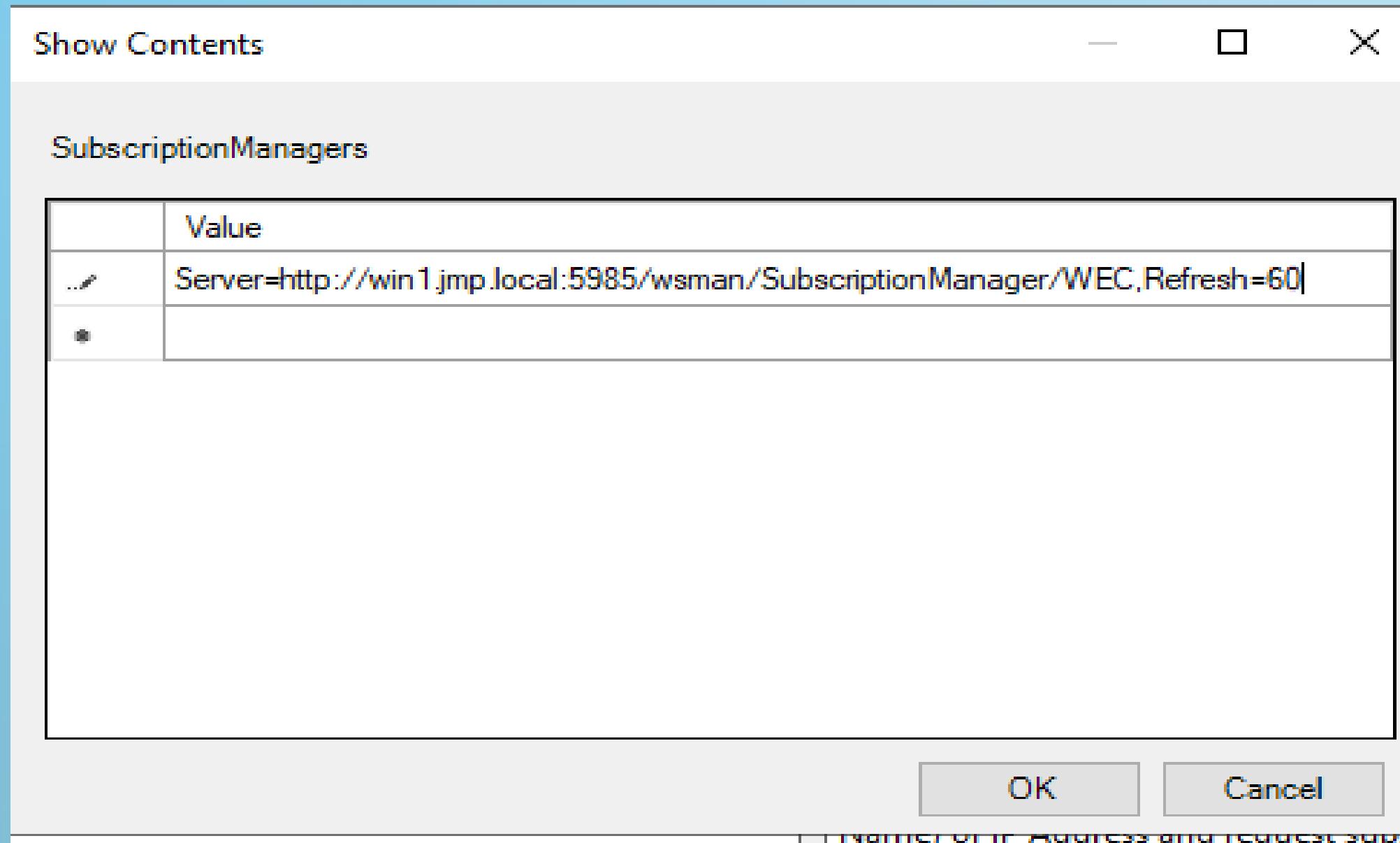


R5.cyber.11 Supervision de la sécurité



R5.cyber.11 Supervision de la sécurité





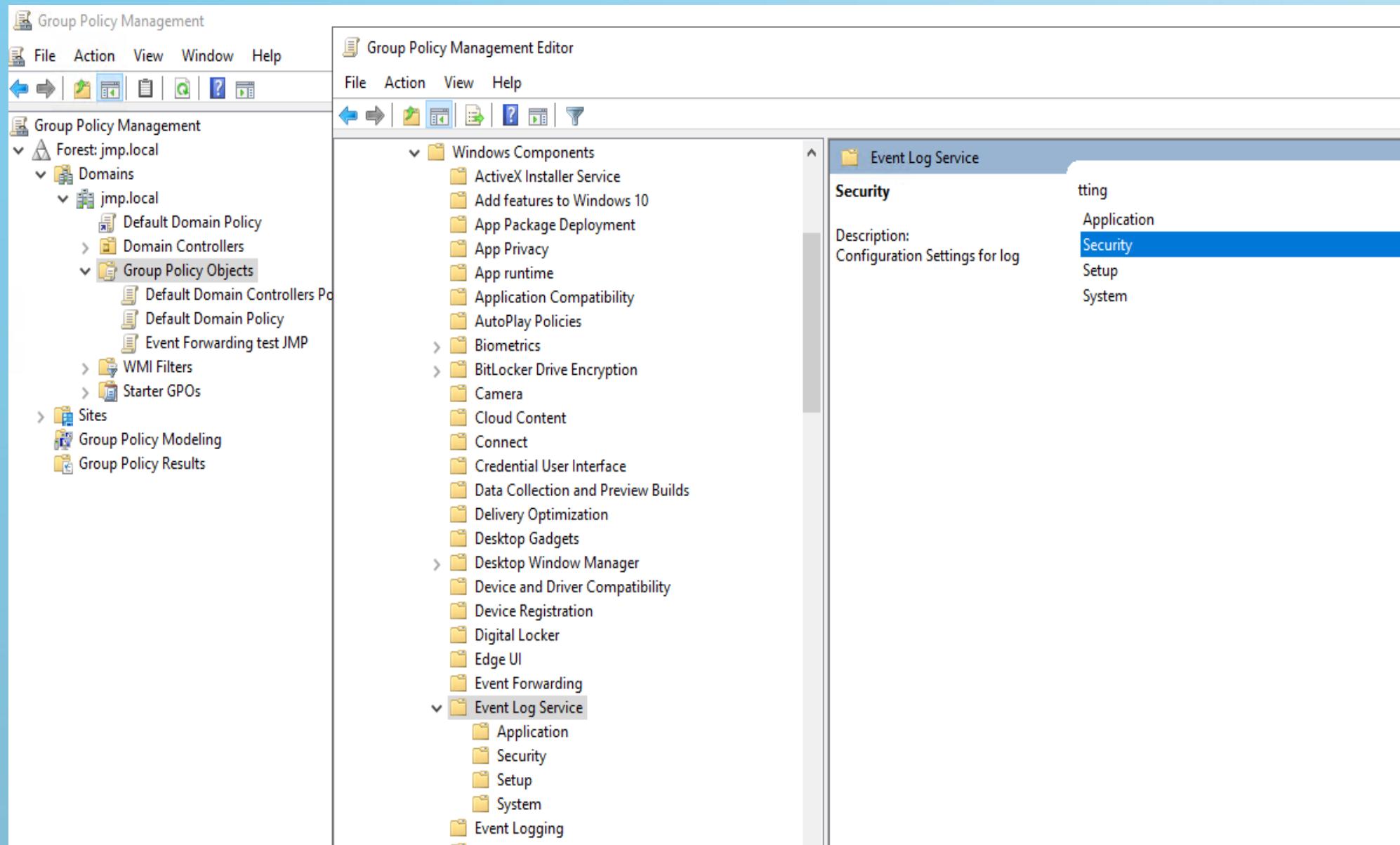
- *On donne maintenant les droits sur chaque channel de log à l'utilisateur "EventLogReader" et à "NetworkService" pour pouvoir lire les logs : Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service > Security*

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.

R5.cyber.11 Supervision de la sécurité

```
jmp\vagrant@WIN1 C:\Users\vagrant\Desktop>wevtutil gl Security
name: Security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: 0:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x1;;;B0)(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
```

R5.cyber.11 Supervision de la sécurité



R5.cyber.11 Supervision de la sécurité

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays the Group Policy Management tree under 'Forest: jmp.local'. The 'Group Policy Objects' node is expanded, showing various GPOs like 'Default Domain Policy', 'Event Forwarding test JMP', and 'Starter GPOs'. The main pane shows the 'Windows Components' section of the Group Policy Management Editor. A context menu is open over the 'Event Log Service' node, specifically over the 'Security' folder. The menu is titled 'Configure log access' and lists several options: 'Control the location of the log file', 'Specify the maximum log file size (KB)', 'Back up log automatically when full', 'Configure log access' (which is highlighted in blue), 'Configure log access (legacy)', and 'Control Event Log behavior when the log file reaches'. The 'Configure log access' option is described as follows:

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.

 Configure log access

 Configure log access

[Previous Setting](#) [Next Setting](#)

Not Configured Comment:

Enabled

Disabled

Supported on:

At least Windows Vista

Options:

Log Access :1::SO)(A;;0x1::S-1-5-32-573)(A;;0x1::NS)

Help:

This policy setting specifies the Security Definition Language (SDI) definition for both "configure log access" and "audit log access" security tools.

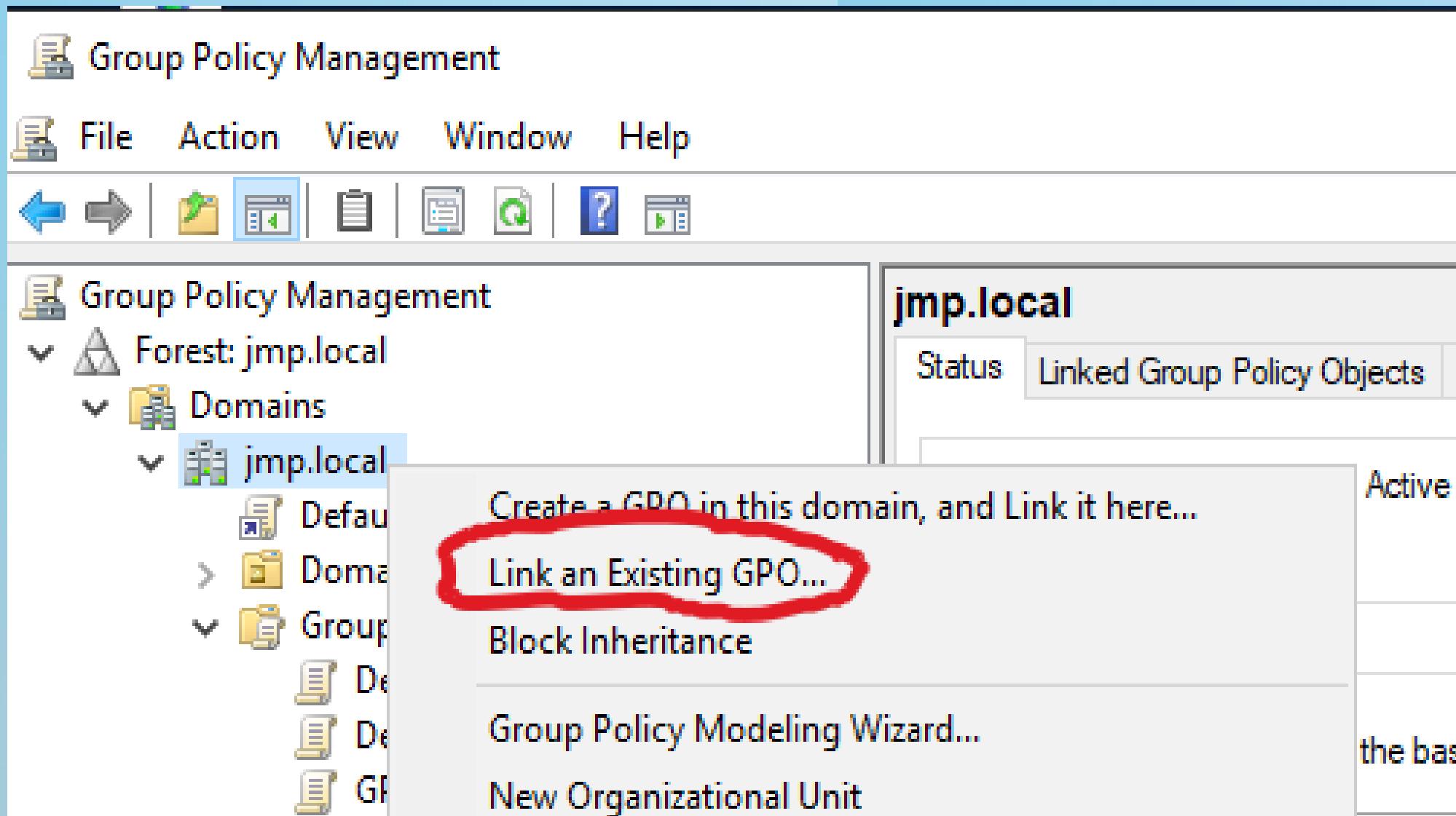
If you enable this policy setting, the system will use the specified SDI definition for both tools.

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

The screenshot shows the Group Policy Management console interface. On the left, the navigation pane displays the forest and domain structure, with the 'Event Forwarding test JMP' GPO selected under 'Group Policy Objects'. The main pane shows the 'Settings' tab for this GPO. The 'Delegation' section lists permissions for various groups and users. The 'Computer Configuration (Enabled)' section contains policy definitions for Windows Settings, Security Settings, and Restricted Groups. Under 'Administrative Templates', there are sections for Windows Components/Event Forwarding and Windows Components/Event Forwarding. The 'Event Forwarding' table in the 'Windows Components/Event Forwarding' section shows the configuration for 'Configure forwarder resource usage' (Setting: Enabled, Comment: The maximum forwarding rate (events/sec) allowed for the forwarder: 100) and 'Configure target Subscription Manager' (Setting: Enabled). The 'SubscriptionManagers' table shows the subscription manager configuration with the URL 'Server=http://win1jmp.local:5985/wsman/subscriptionManager/WEC,Refresh=60'.

Policy	Setting	Comment
Configure forwarder resource usage	Enabled	The maximum forwarding rate (events/sec) allowed for the forwarder: 100
Configure target Subscription Manager	Enabled	SubscriptionManagers Server=http://win1jmp.local:5985/wsman/subscriptionManager/WEC,Refresh=60

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>
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
```