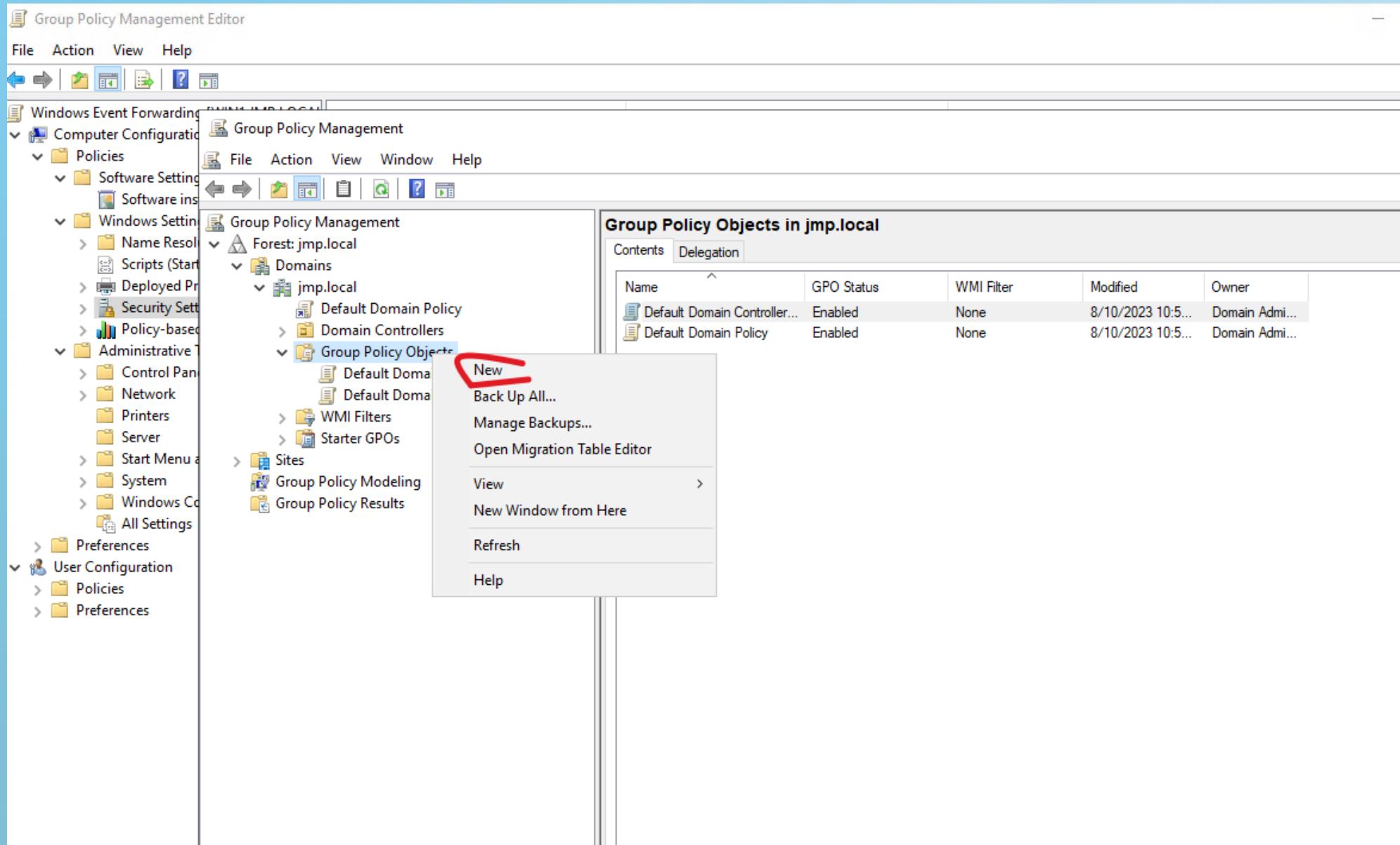
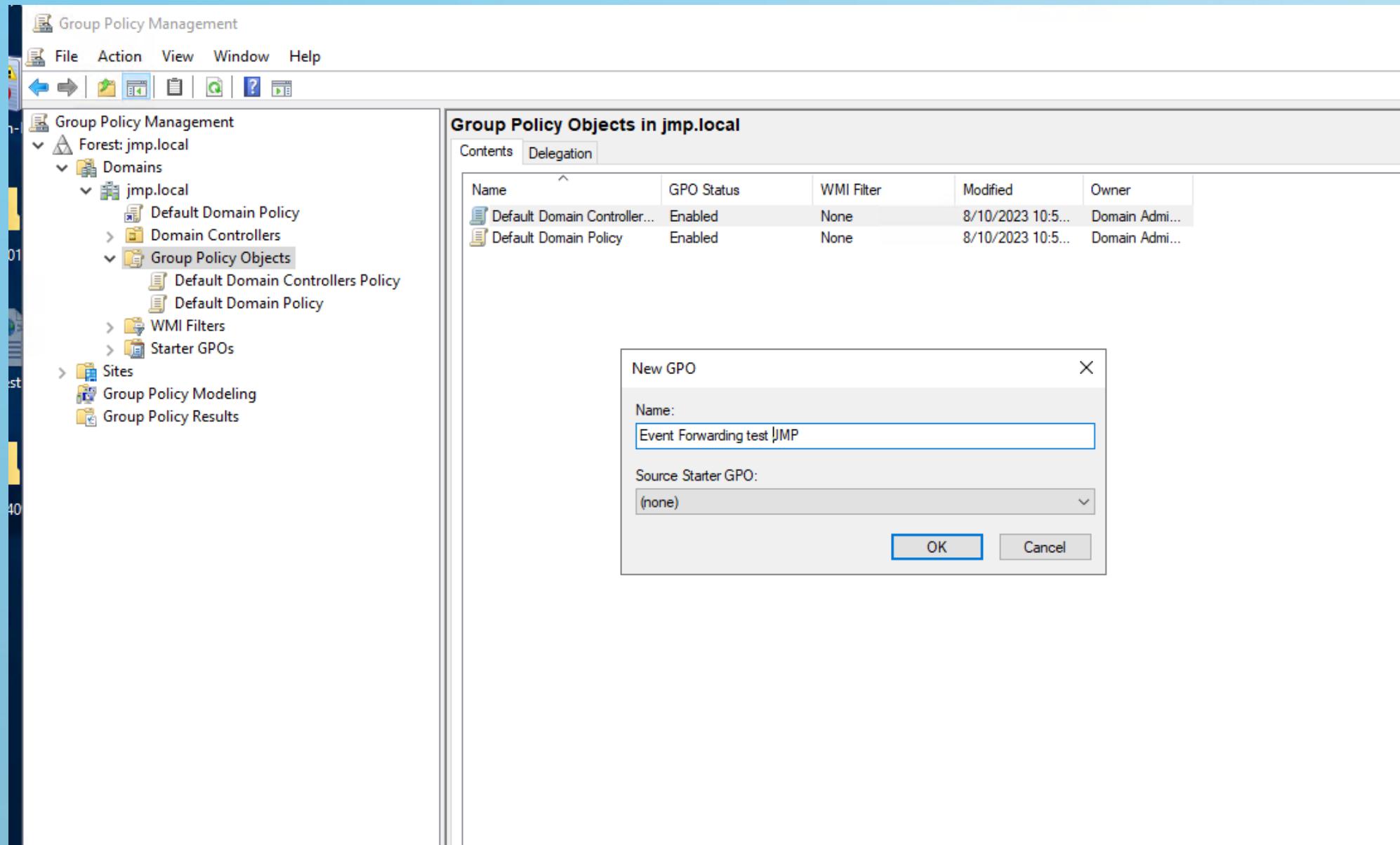


installation d'une GPO "WEF" en images

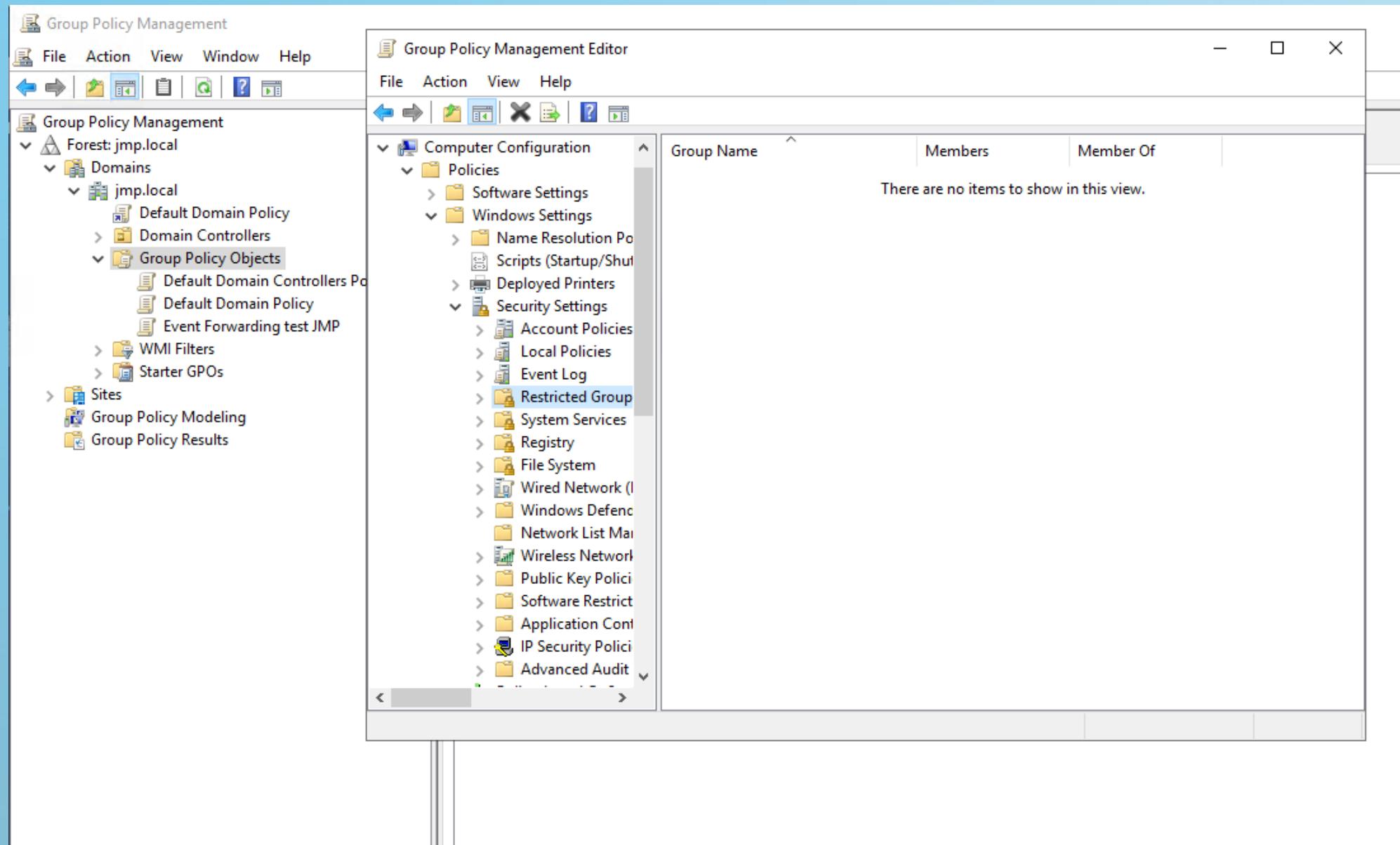
R5.cyber.11 Supervision de la sécurité



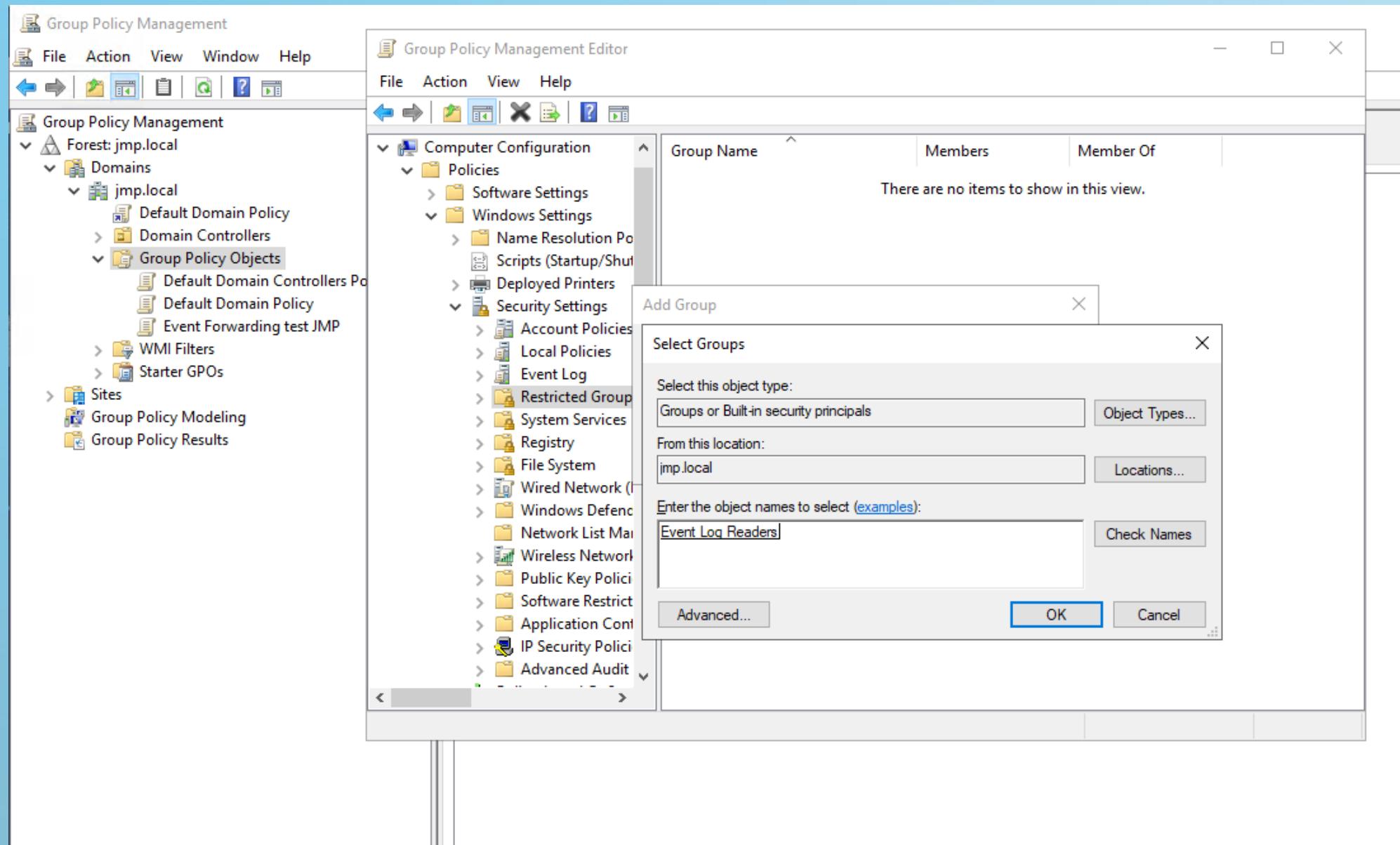
R5.cyber.11 Supervision de la sécurité



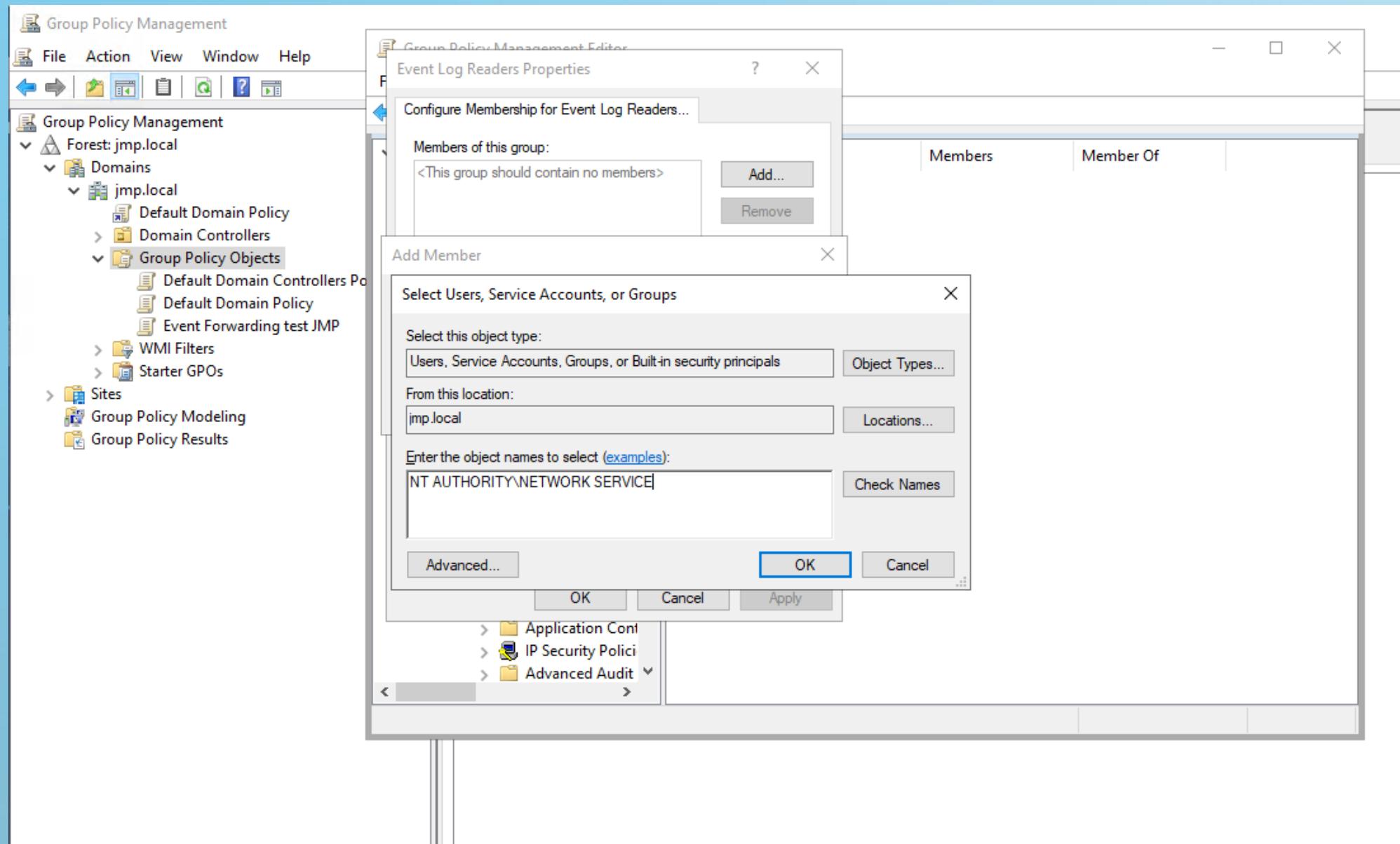
R5.cyber.11 Supervision de la sécurité



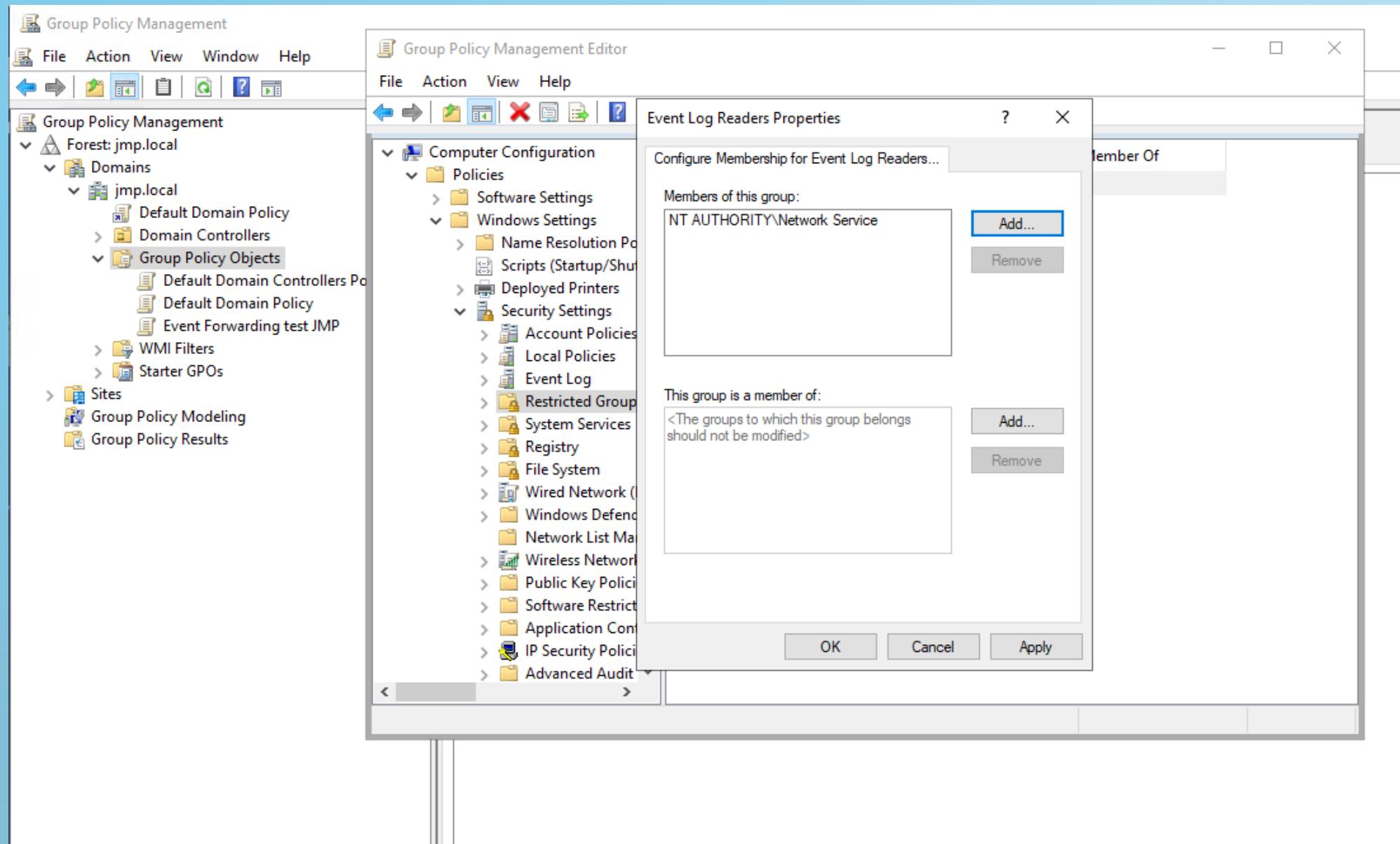
R5.cyber.11 Supervision de la sécurité



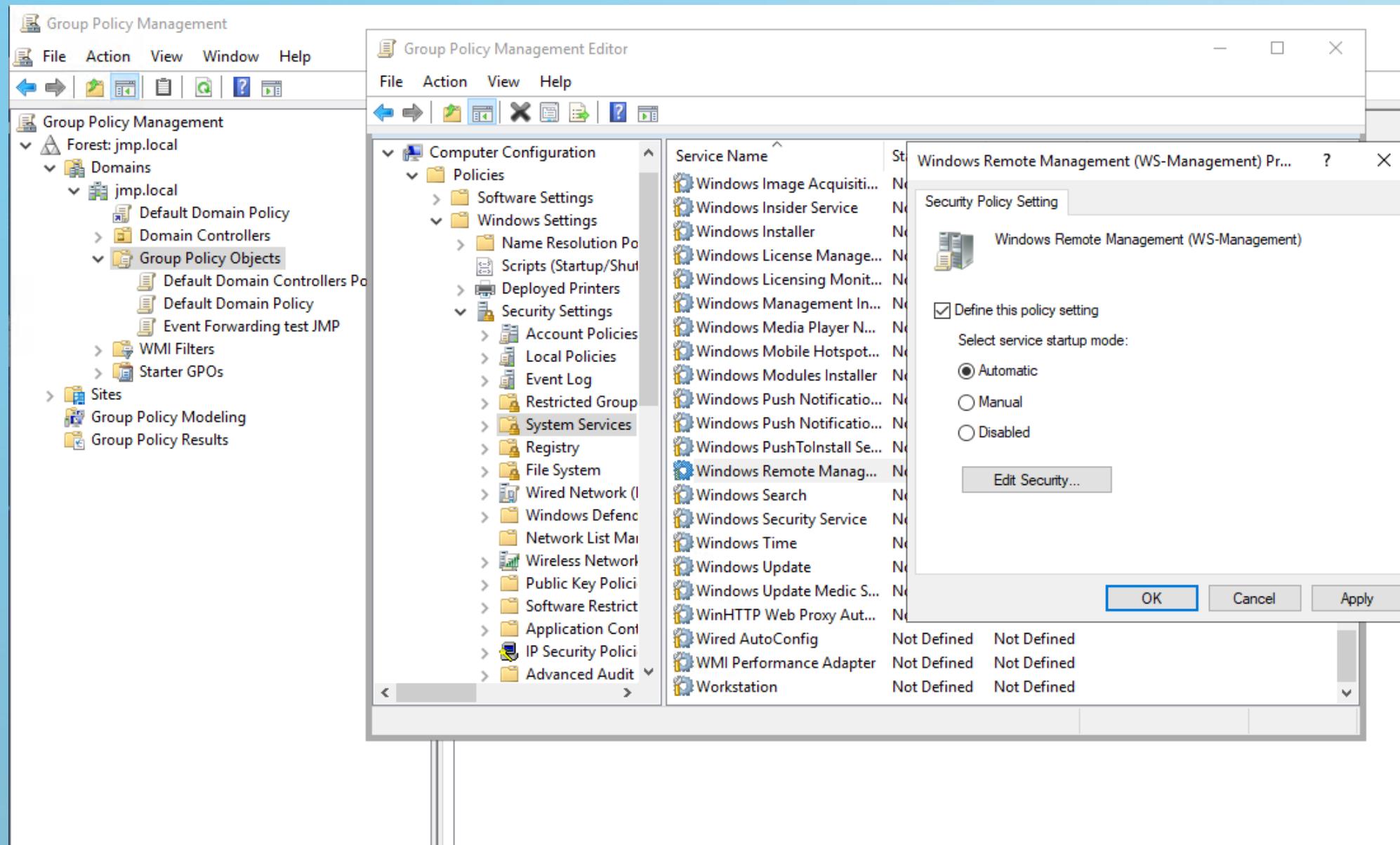
R5.cyber.11 Supervision de la sécurité



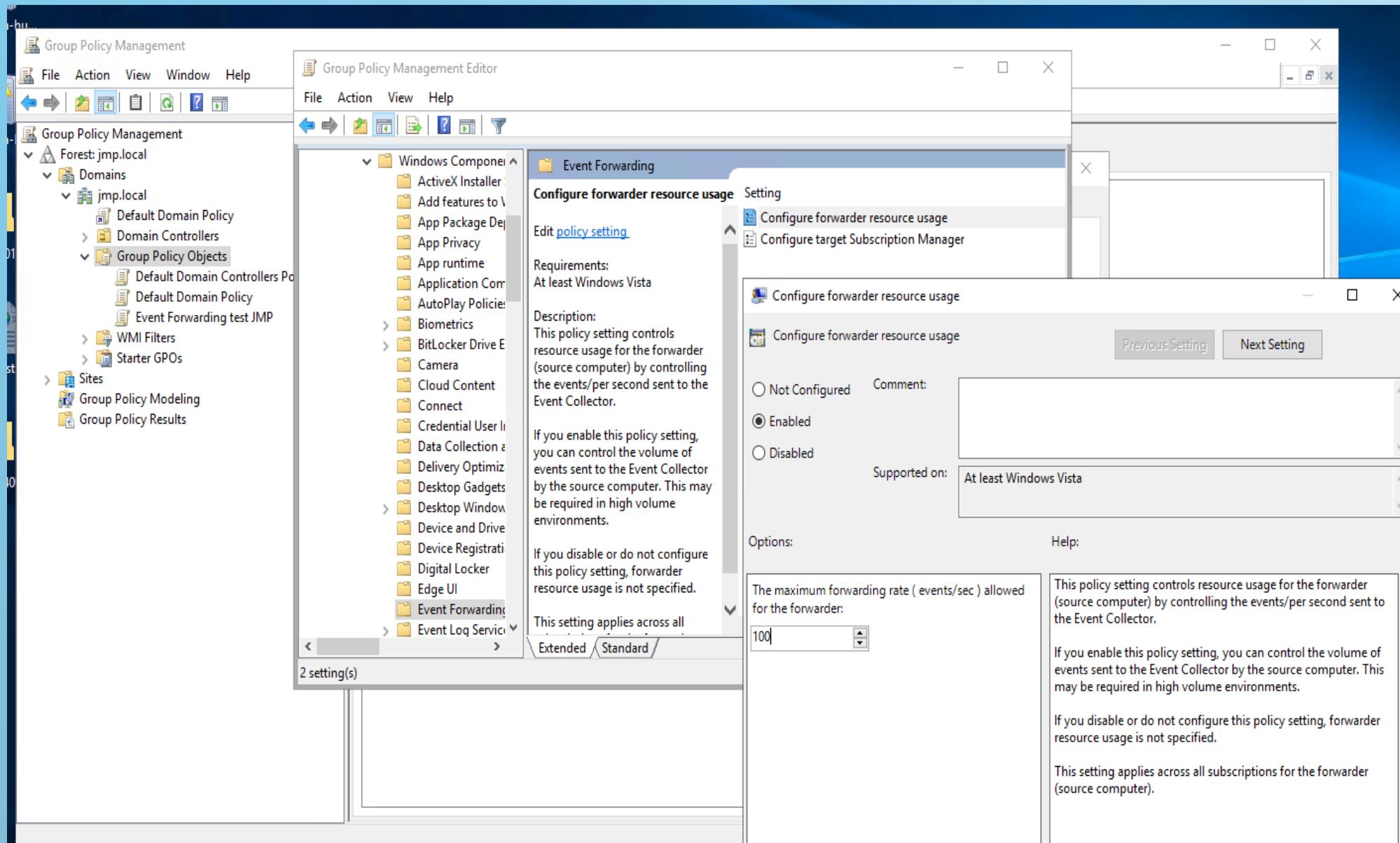
R5.cyber.11 Supervision de la sécurité



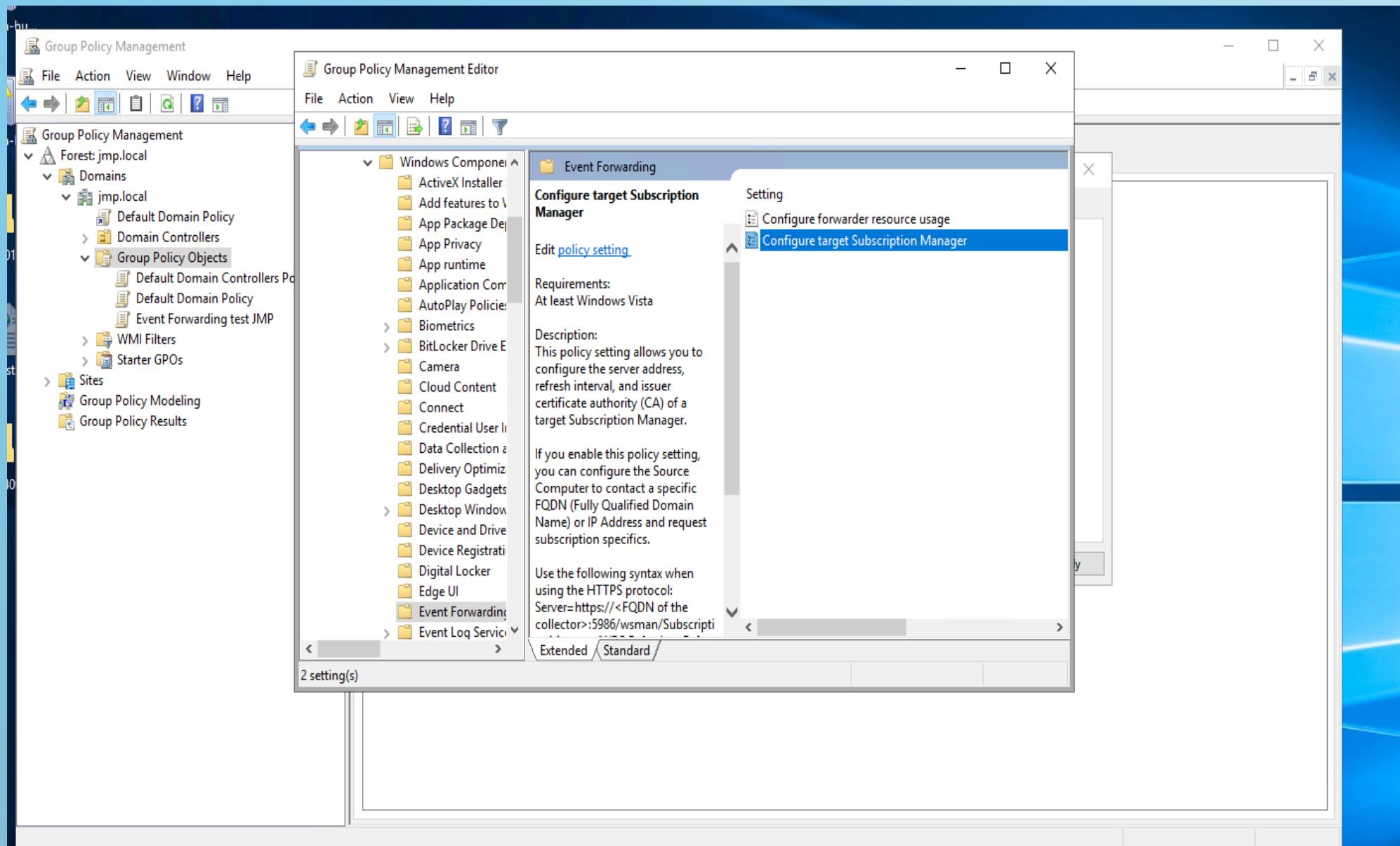
R5.cyber.11 Supervision de la sécurité



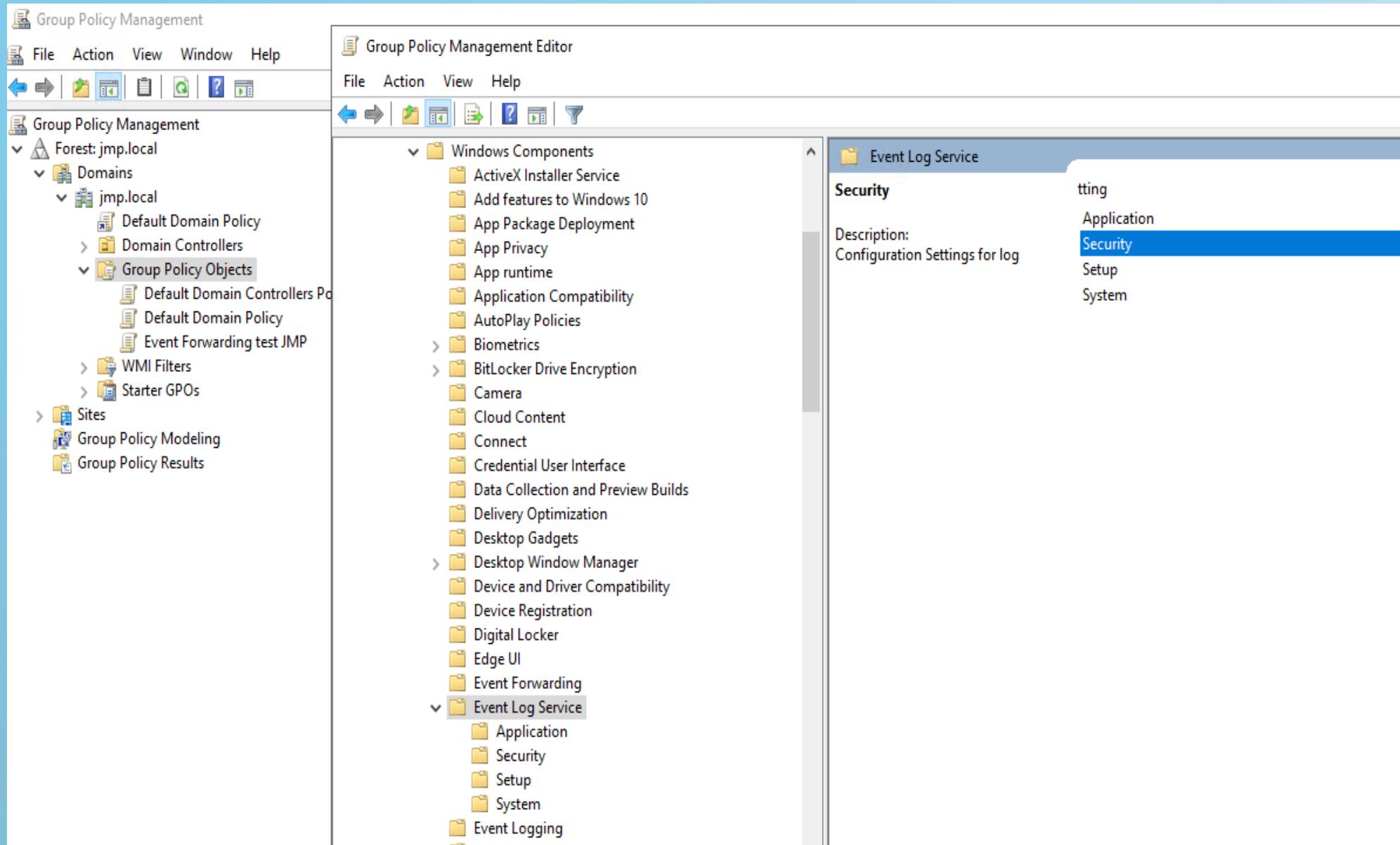
R5.cyber.11 Supervision de la sécurité



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 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 'Event Logging' folder. The menu is titled 'Security' and contains several options under 'Configure log access': '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.

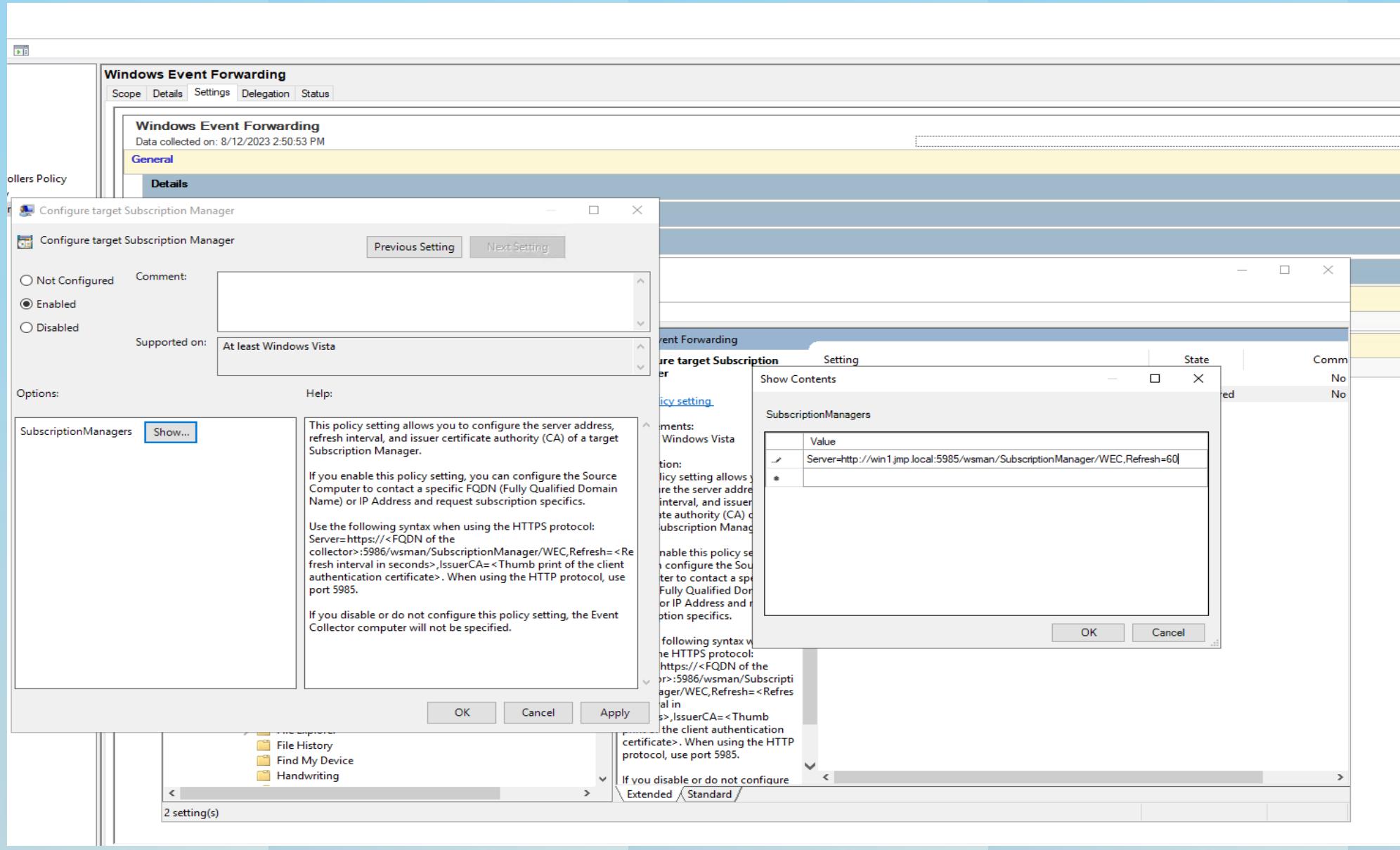
If you disable or do not configure this policy setting, only system software and administrators can read or clear this log.

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.

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 console interface. The left pane displays a tree structure for 'Forest: jmp.local' under 'Group Policy Management'. The 'Windows Event Forwarding' node is selected in the 'Default Domain Policy' section. The right pane shows the 'Windows Event Forwarding' configuration details.

Windows Event Forwarding

Scope: jmp:vagrant

Details: Computer Configuration (Enabled)

Delegation: No

Status: No

Windows Settings

Security Settings

Restricted Groups

Group	Members	Member of
BUILTIN\Event Log Readers	NT AUTHORITY\NETWORK SERVICE	

System Services

Windows Remote Management (WS-Management) (Startup Mode: Automatic)

Permissions: No permissions specified

Auditing: No auditing specified

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Event Forwarding

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

Windows Components/Event Log Service/Security

Policy	Setting	Comment
Configure log access	Enabled	Log Access O:BAG:SYD:(A;;0x0007::SY)(A;;0x7..BA)(A;;0x1::BO)(A;;0x1::SO)(A;;0x1::S-1-5-32-573)(A;;0x1::NS)

User Configuration (Enabled)