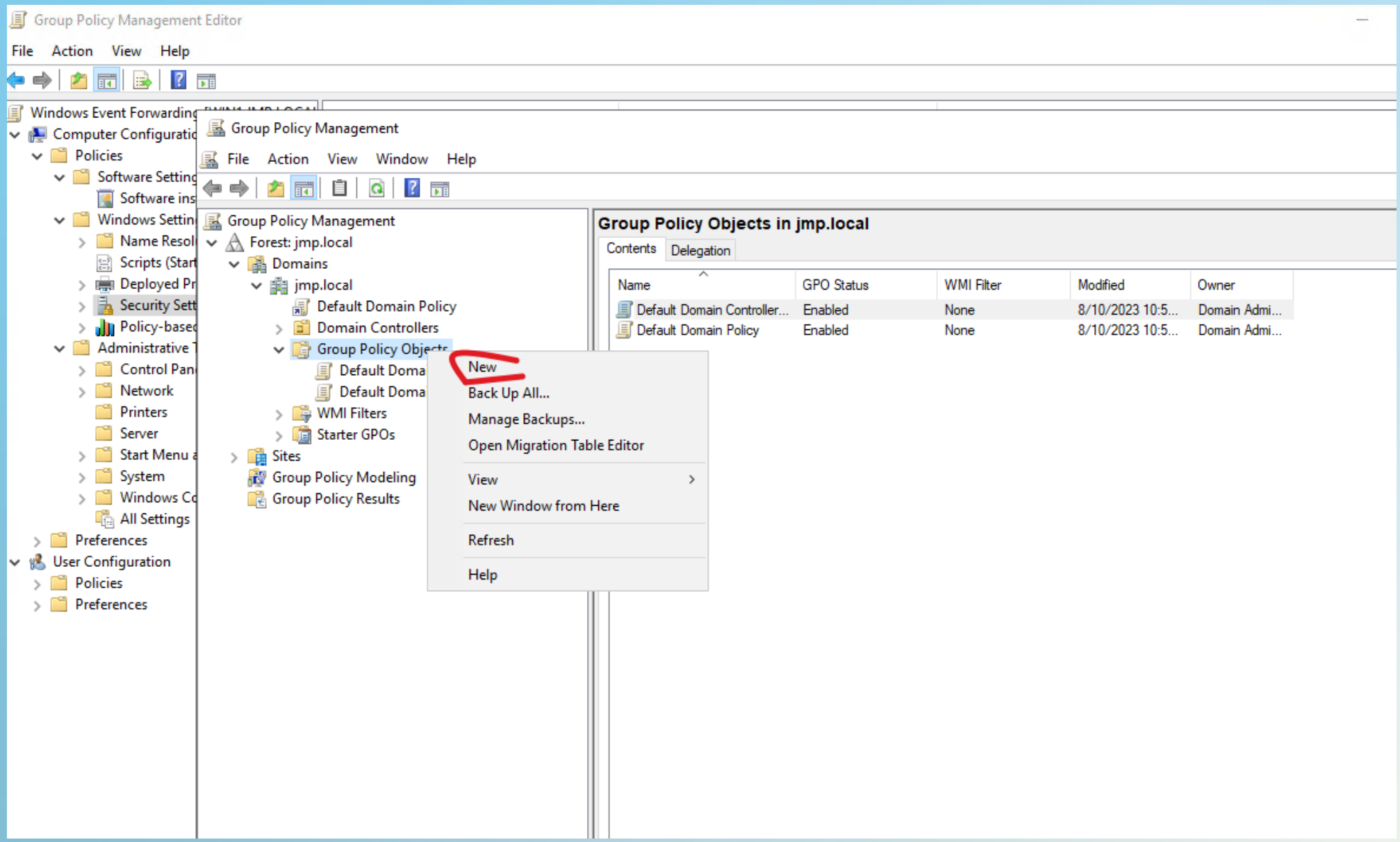
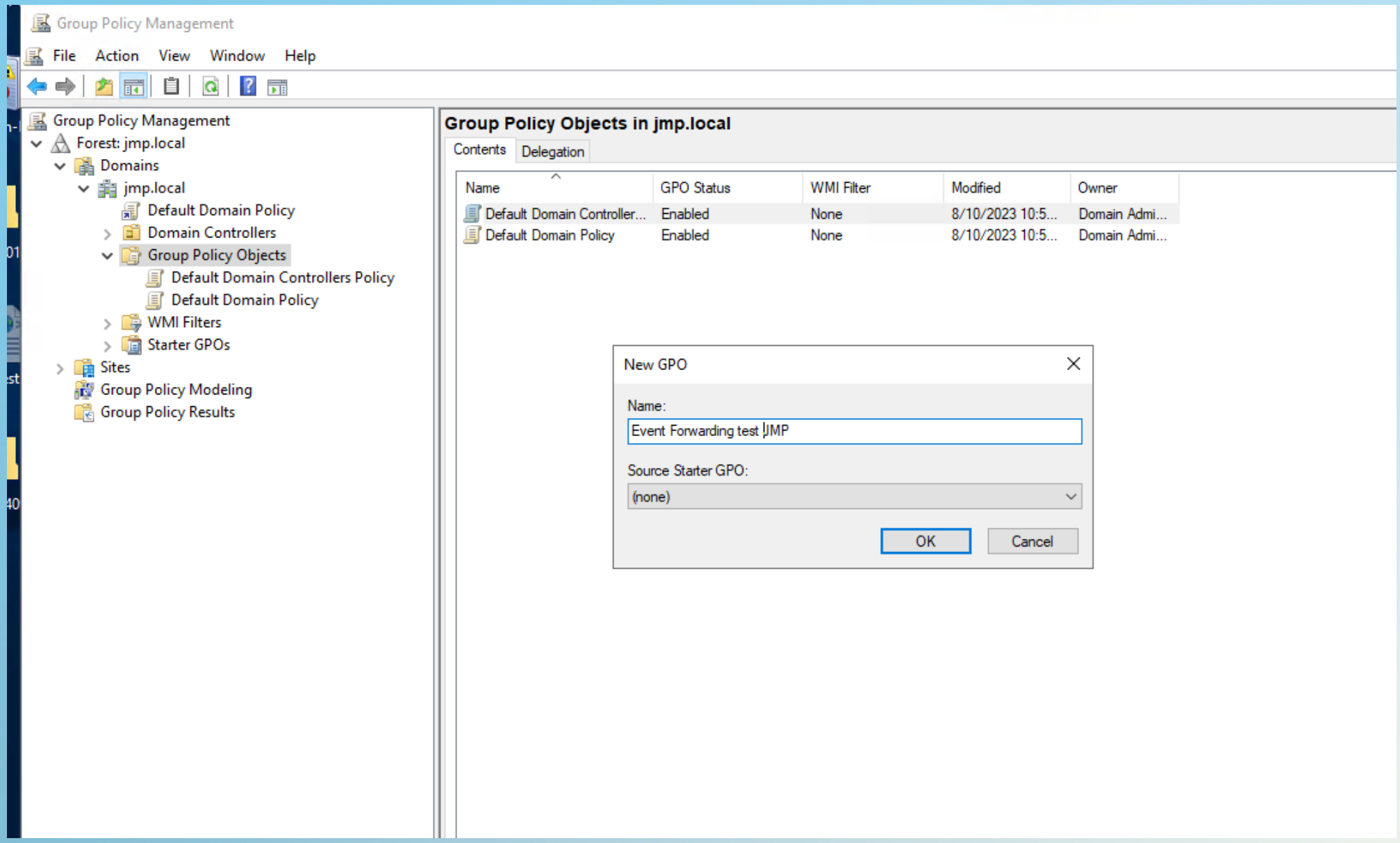
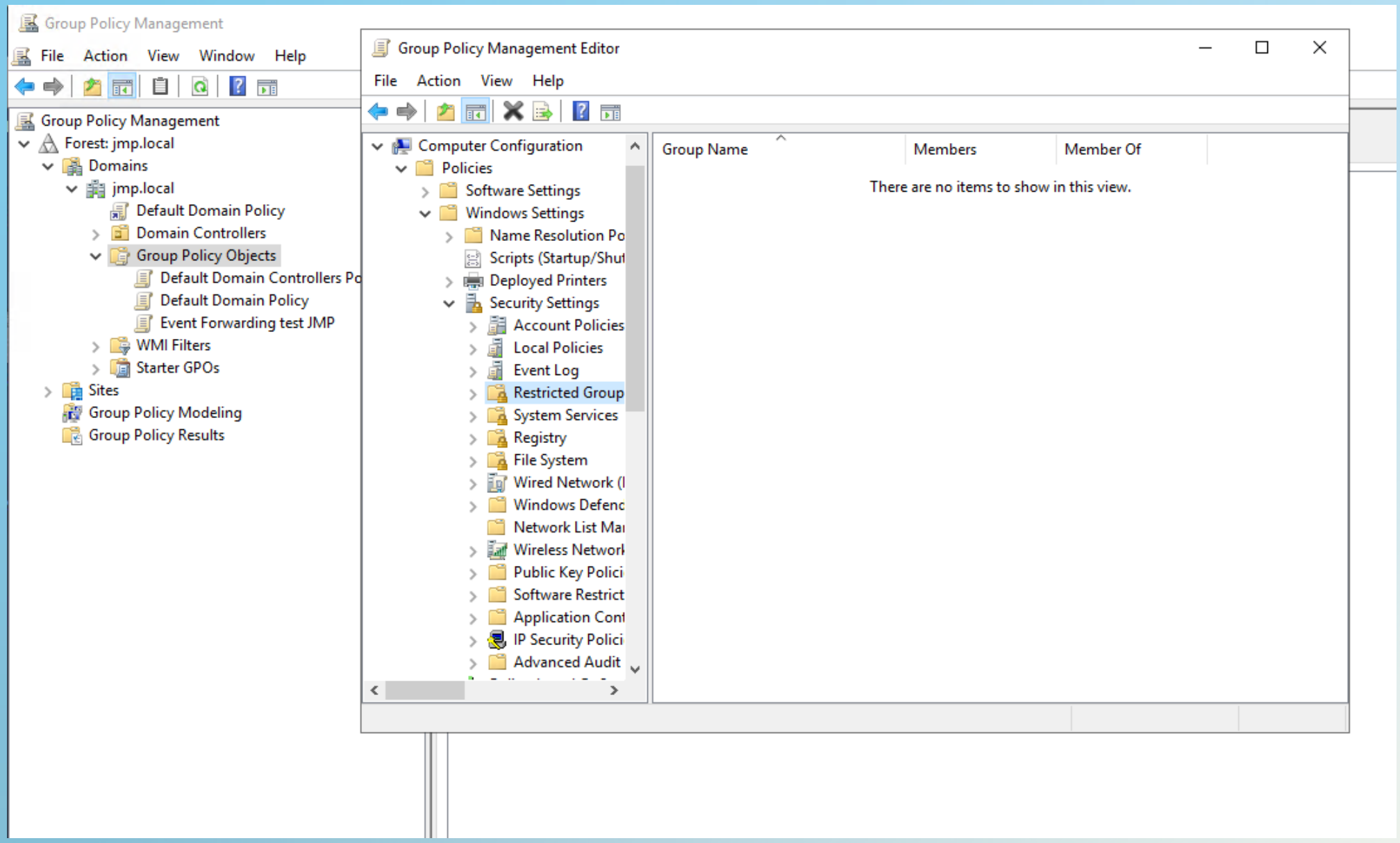
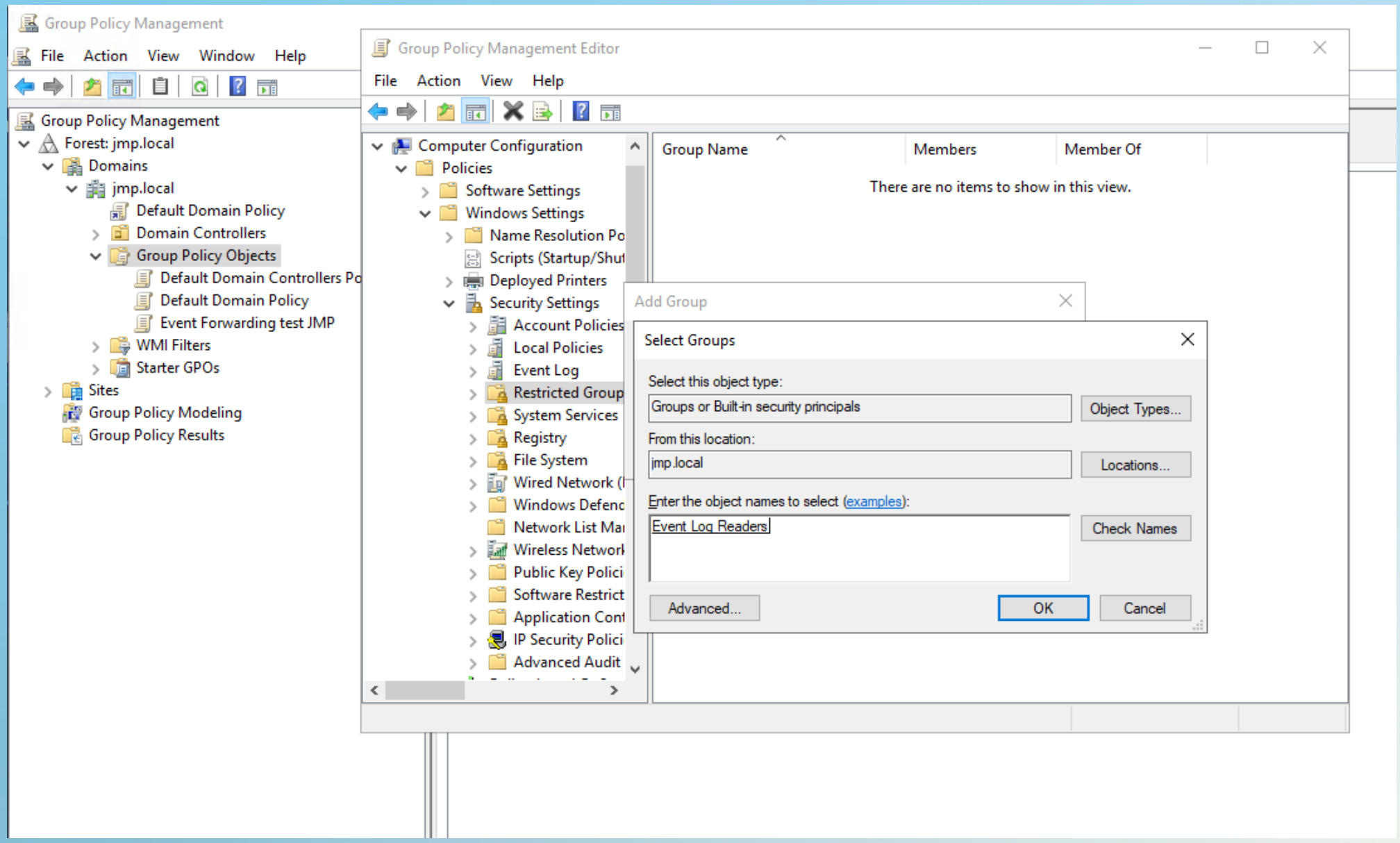
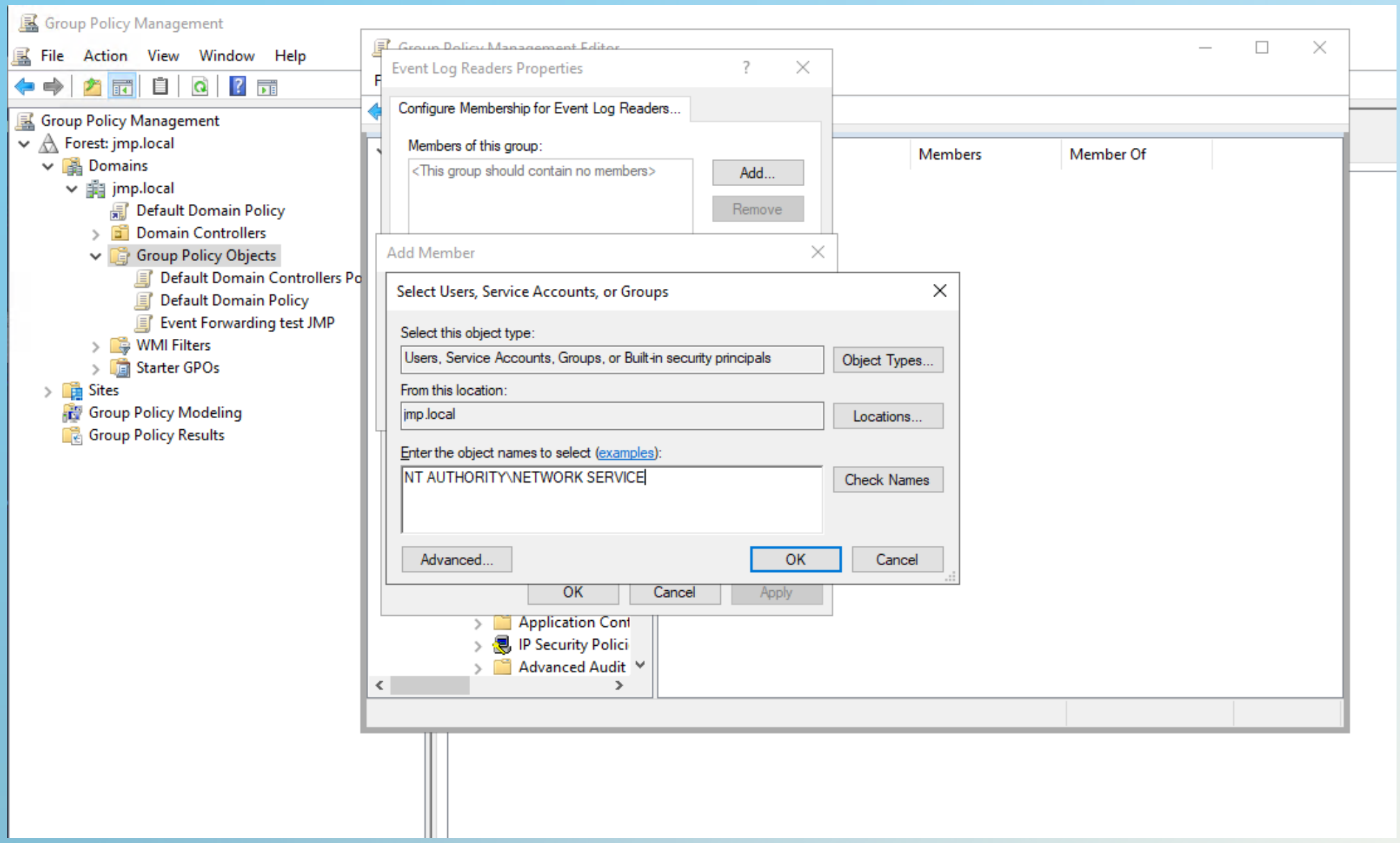
installation d'une GPO "WEF" en images

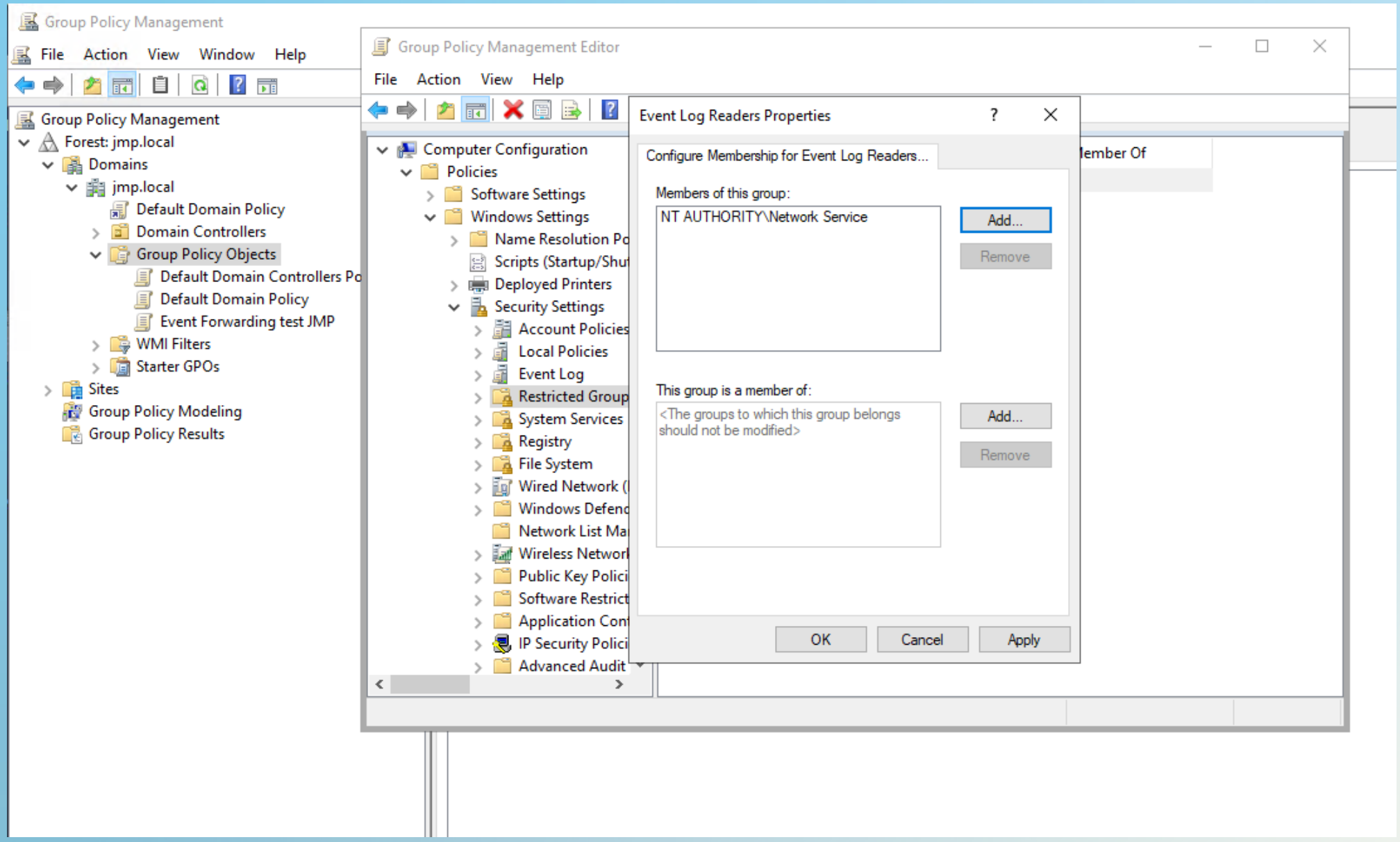

Group Policy Management Editor
File Action View Help
Windows Event Forwarding
Computer Configuratio
Policies
Software Setting
Software ins
Windows Settin
Name Resol
Scripts (Start
Deployed Pr
Security Sett
Policy-based
Administrative T
Control Pan
Network
Printers
Server
Start Menu a
System
Windows Co
All Settings
Preferences
User Configuration
Policies
Preferences
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 Doma
Default Doma
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
New
Back Up All...
Manage Backups...
Open Migration Table Editor
View
New Window from Here
Refresh
Help
Group Policy Objects in jmp.local
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Owner
Default Domain Controller...
Enabled
None
8/10/2023 10:5...
Domain Admi...
Default Domain Policy
Enabled
None
8/10/2023 10:5...
Domain Admi...

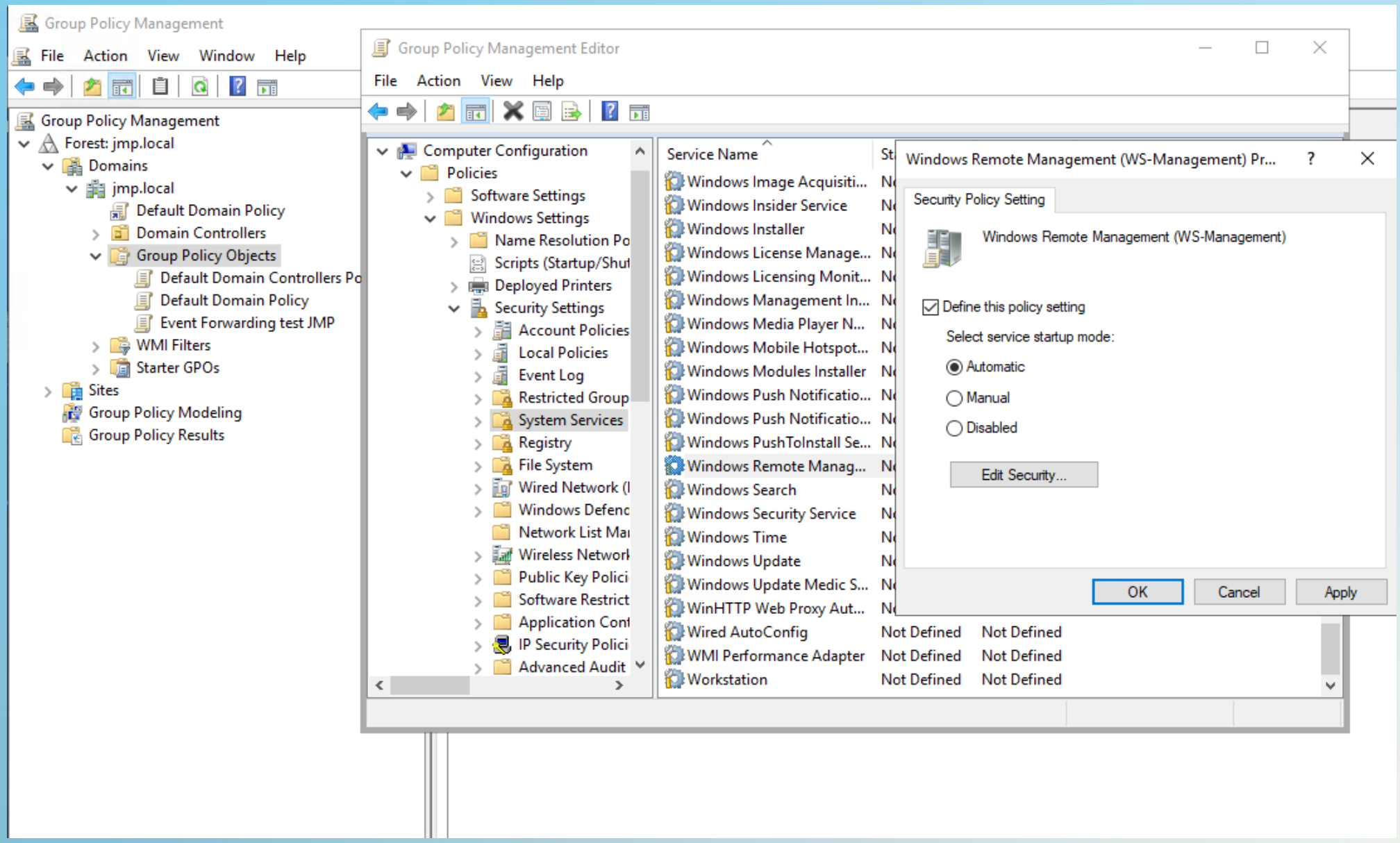

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in jmp.local
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Owner
Default Domain Controller...
Enabled
None
8/10/2023 10:5...
Domain Admi...
Default Domain Policy
Enabled
None
8/10/2023 10:5...
Domain Admi...
New GPO
Name:
Event Forwarding test JMP
Source Starter GPO:
(none)
OK
Cancel

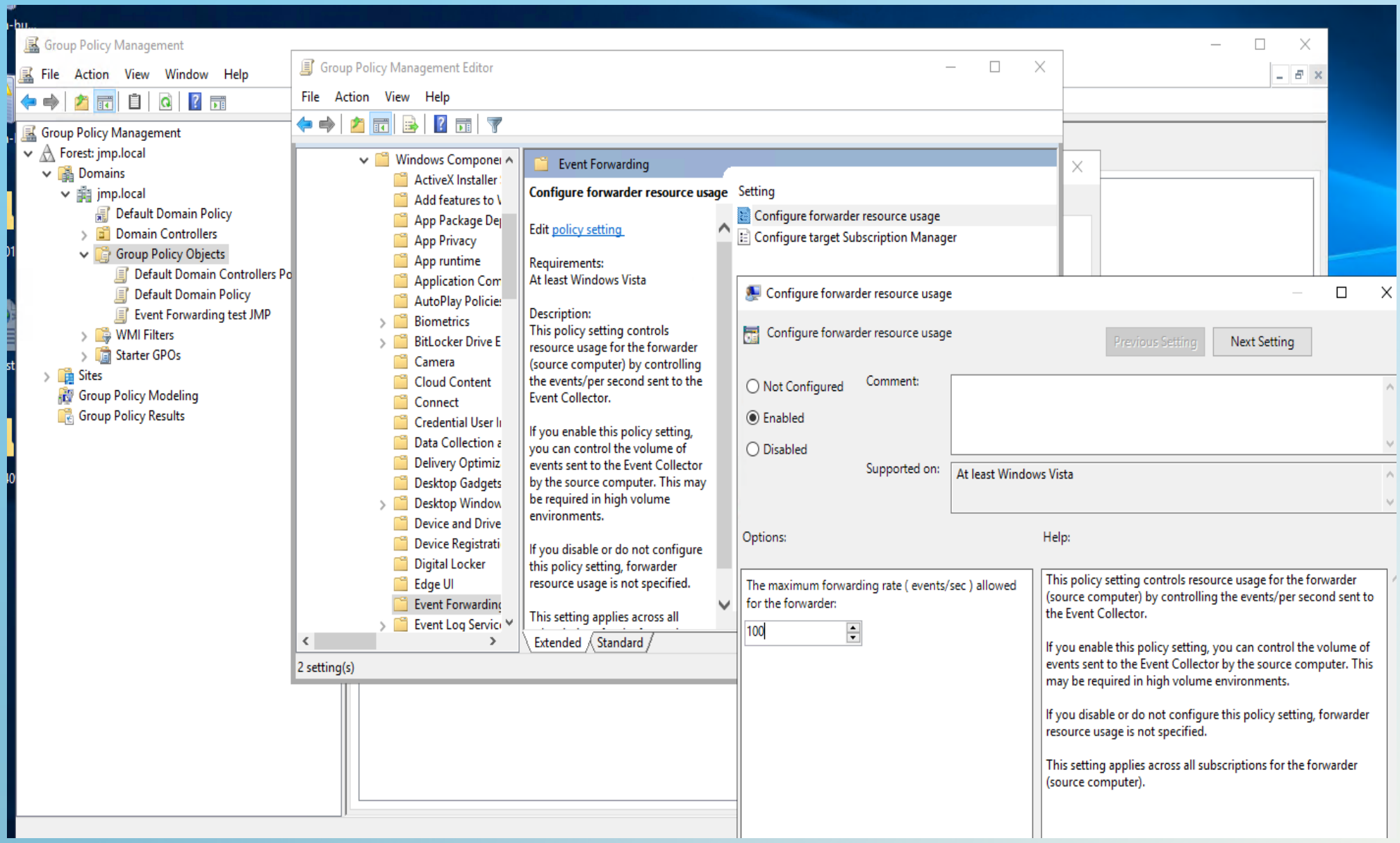

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
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 Networ
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.

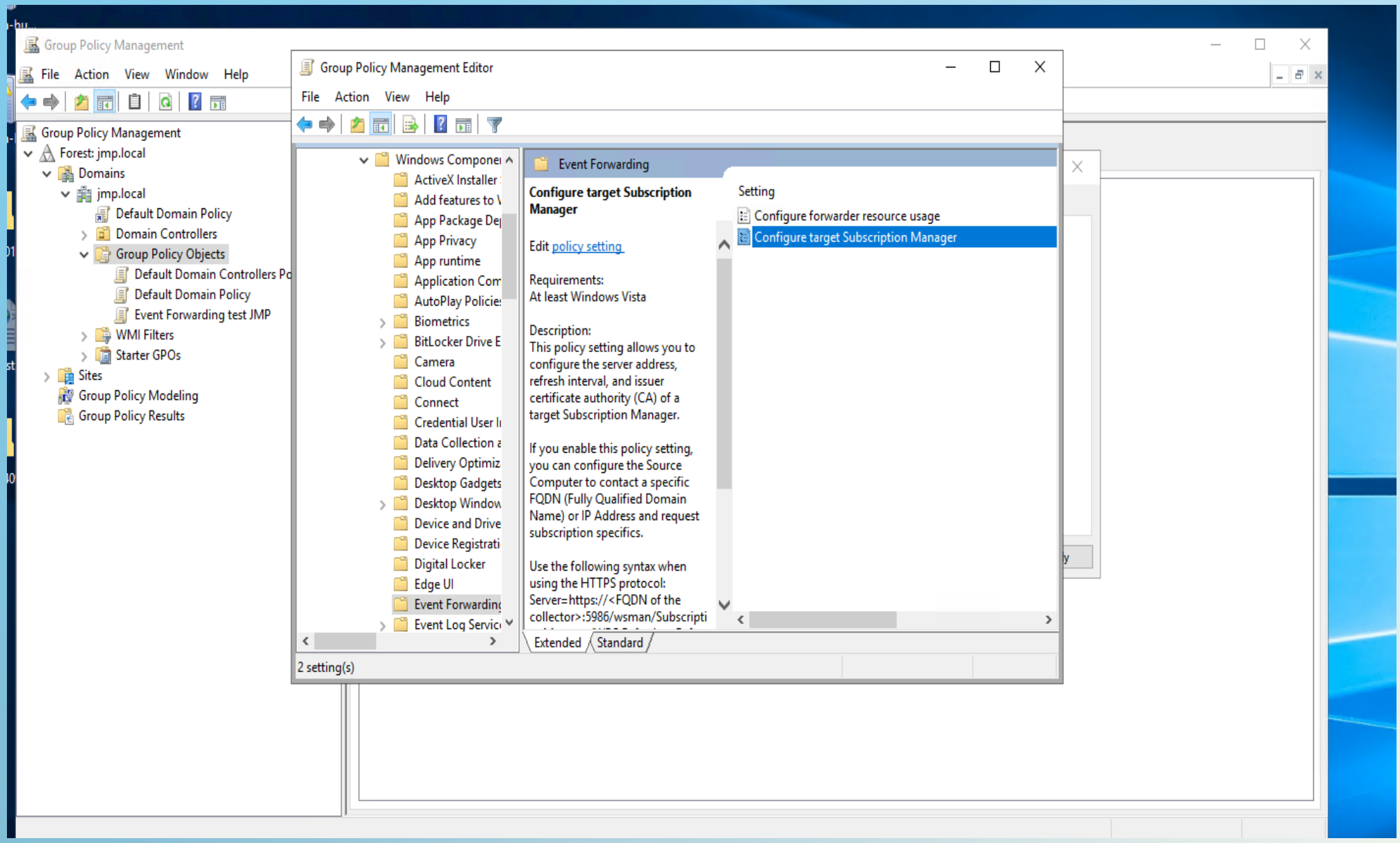

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
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

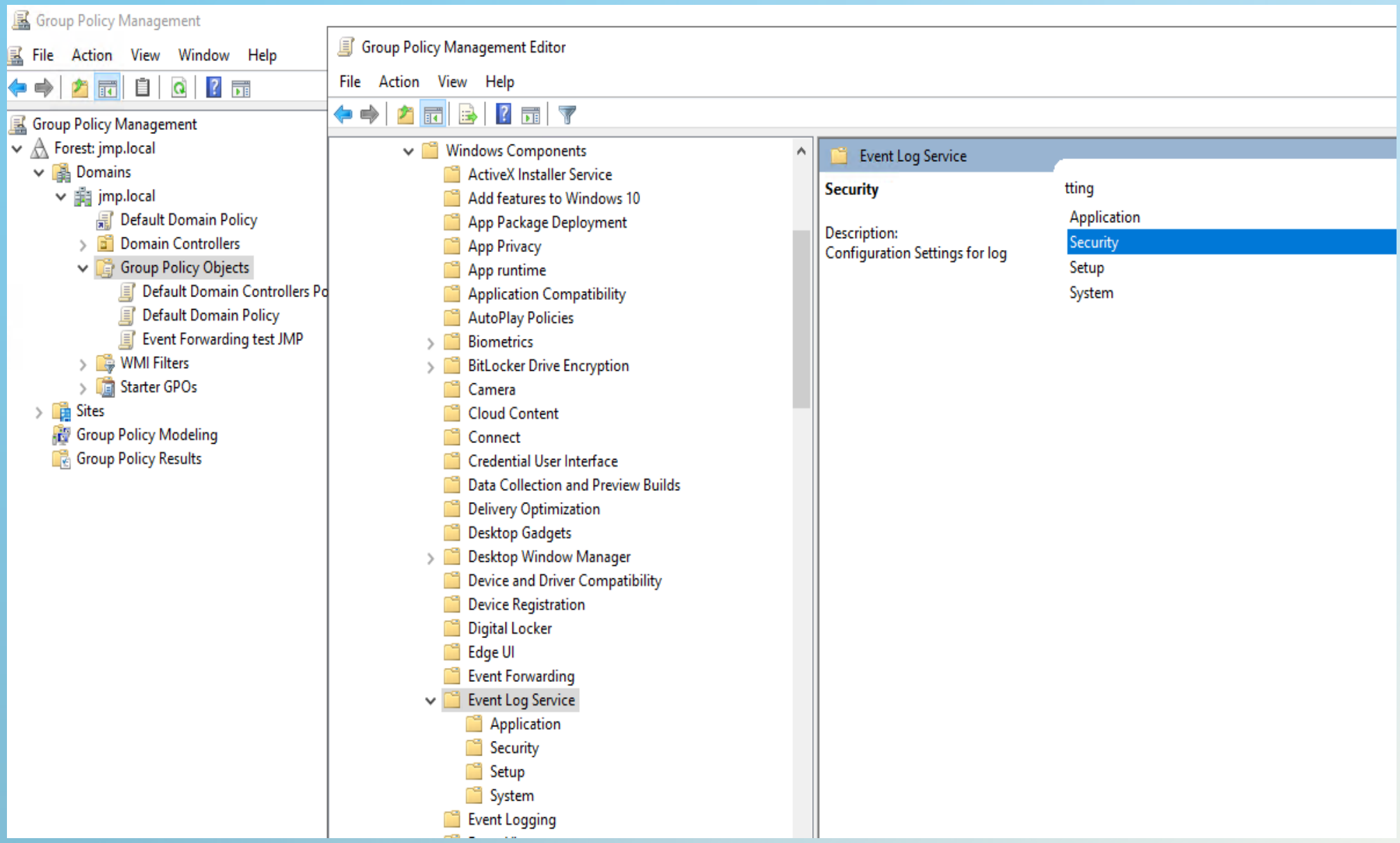

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Event Log Readers Properties
Configure Membership for Event Log Readers...
Members of this group:
<This group should contain no members>
Add...
Remove
Add Member
Select Users, Service Accounts, or Groups
Select this object type:
Users, Service Accounts, Groups, or Built-in security principals
Object Types...
From this location:
jmp.local
Locations...
Enter the object names to select (examples):
NT AUTHORITY\NETWORK SERVICE
Check Names
Advanced...
OK
Cancel
OK
Cancel
Apply
Members
Member Of
Application Cont
IP Security Polici
Advanced Audit

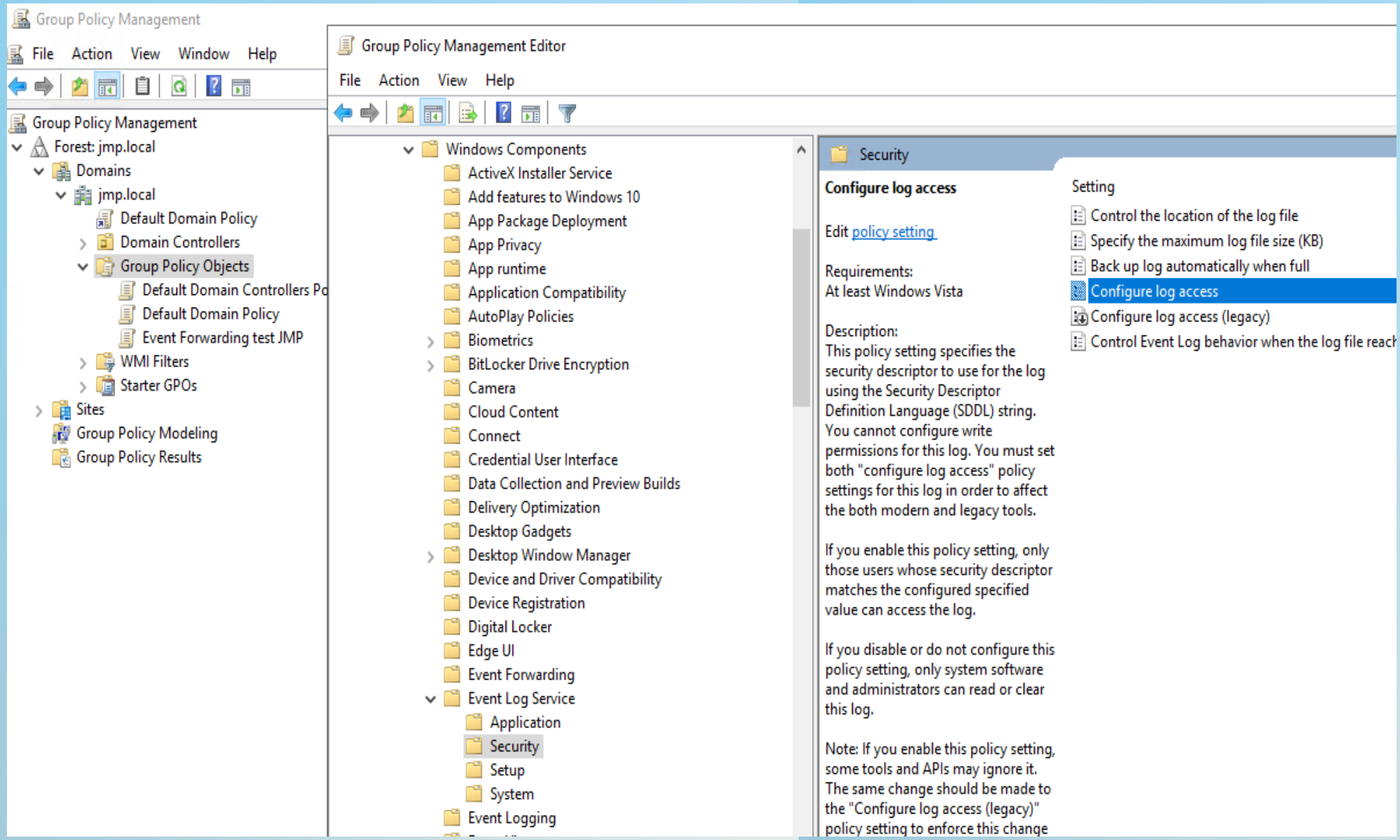

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
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 Ma
Wireless Networ
Public Key Polici
Software Restrict
Application Cont
IP Security Polici
Advanced Audit
Event Log Readers Properties
Configure Membership for Event Log Readers...
Members of this group:
NT AUTHORITY\Network Service
Add...
Remove
This group is a member of:
<The groups to which this group belongs should not be modified>
Add...
Remove
OK
Cancel
Apply


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

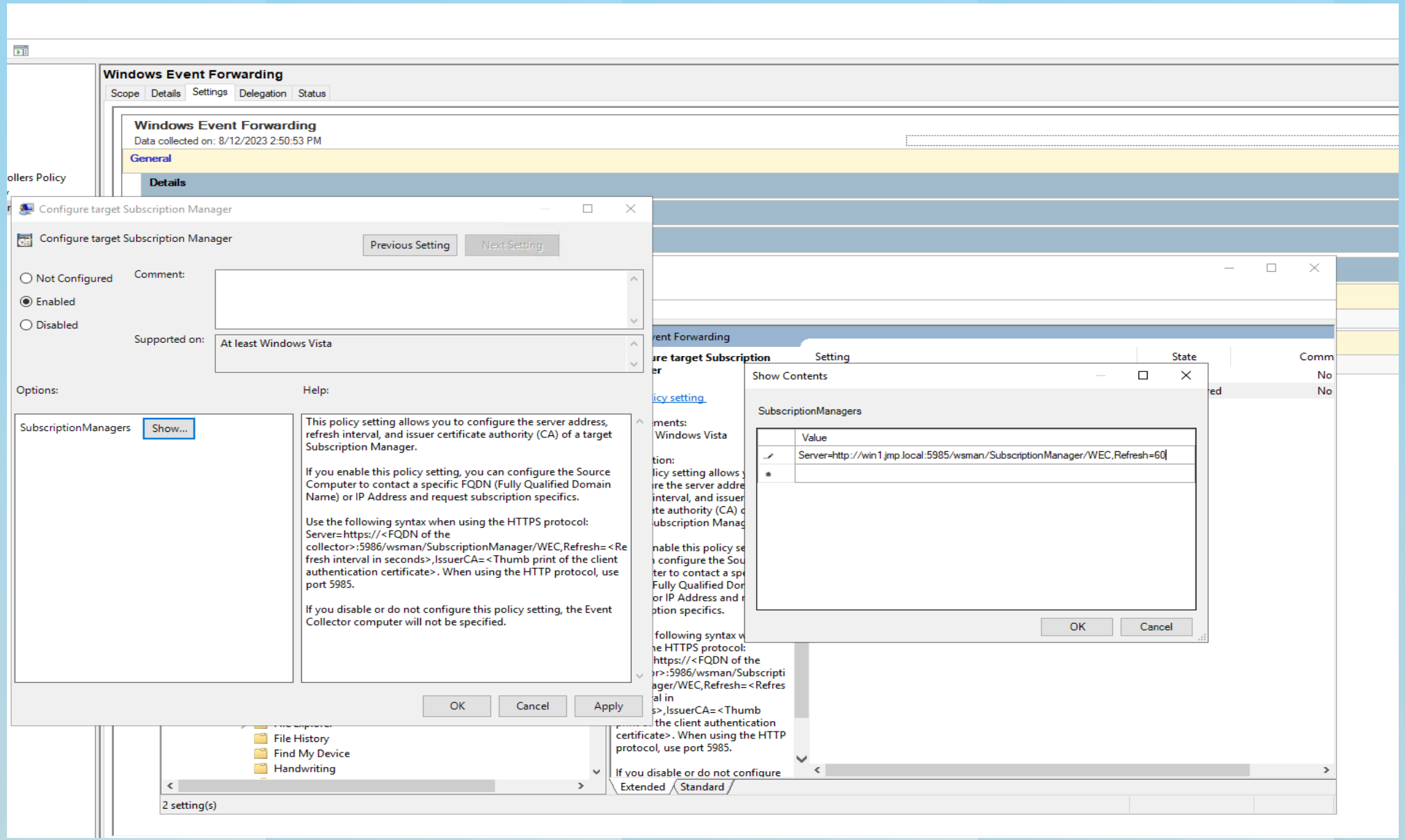

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
Windows Compone
ActiveX Installer
Add features to
App Package De
App Privacy
App runtime
Application Com
AutoPlay Policie
Biometrics
BitLocker Drive E
Camera
Cloud Content
Connect
Credential User I
Data Collection a
Delivery Optimiz
Desktop Gadgets
Desktop Windov
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).

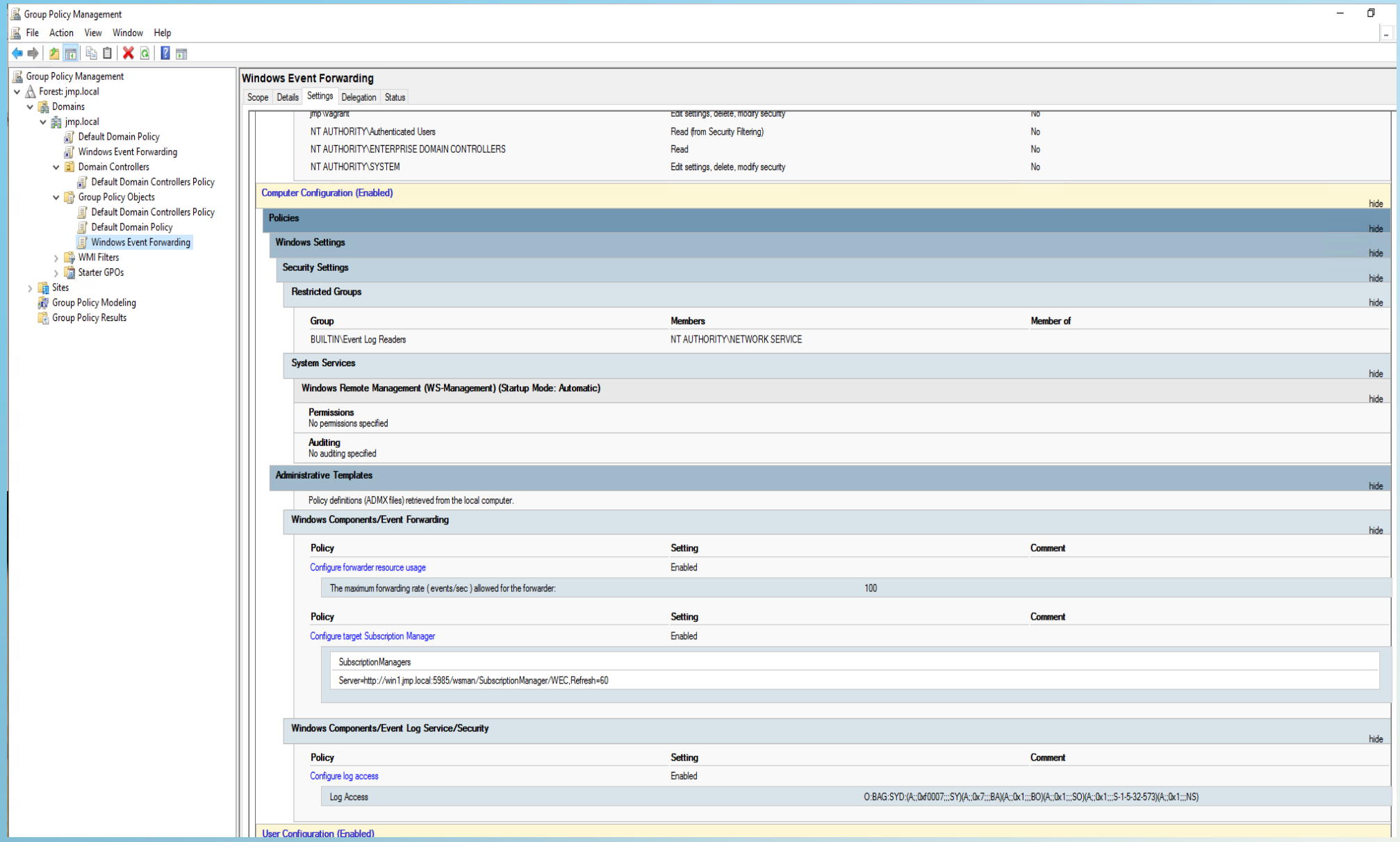

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Po
Default Domain Policy
Event Forwarding test JMP
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
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 Forwarding
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)


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

```
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
```


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)


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Windows Event Forwarding
Domain Controllers
Default Domain Controllers Policy
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
Windows Event Forwarding
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Windows Event Forwarding
Scope Details Settings Delegation Status
NT AUTHORITY\Authenticated Users Read (from Security Filtering) No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS Read No
NT AUTHORITY\SYSTEM Edit settings, delete, modify security No
Computer Configuration (Enabled)
hide
Policies
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
Policy Setting Comment
Configure target Subscription Manager Enabled
SubscriptionManagers
Server=http://win1.jmp.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;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x1;;;BO)(A;;0x1;;;SO)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
User Configuration (Enabled)