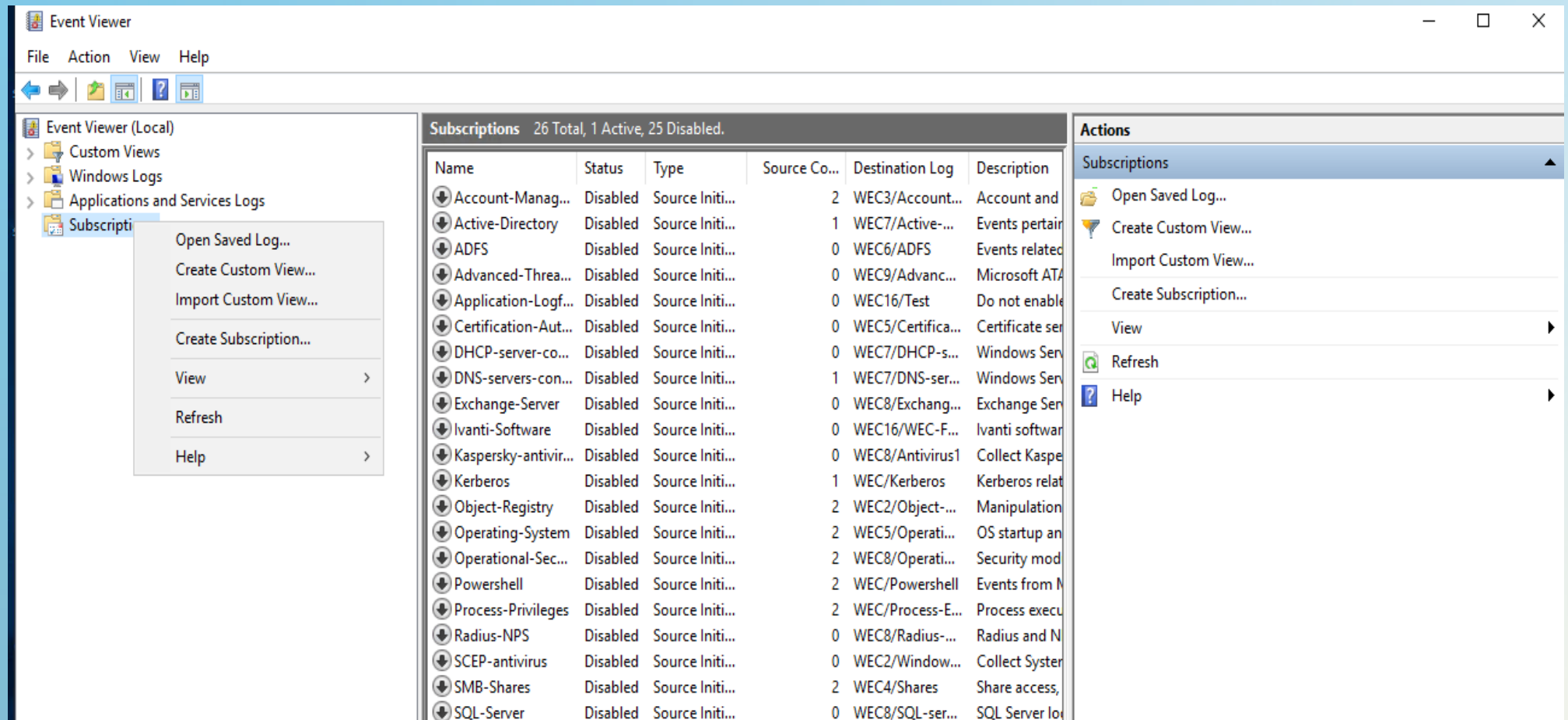
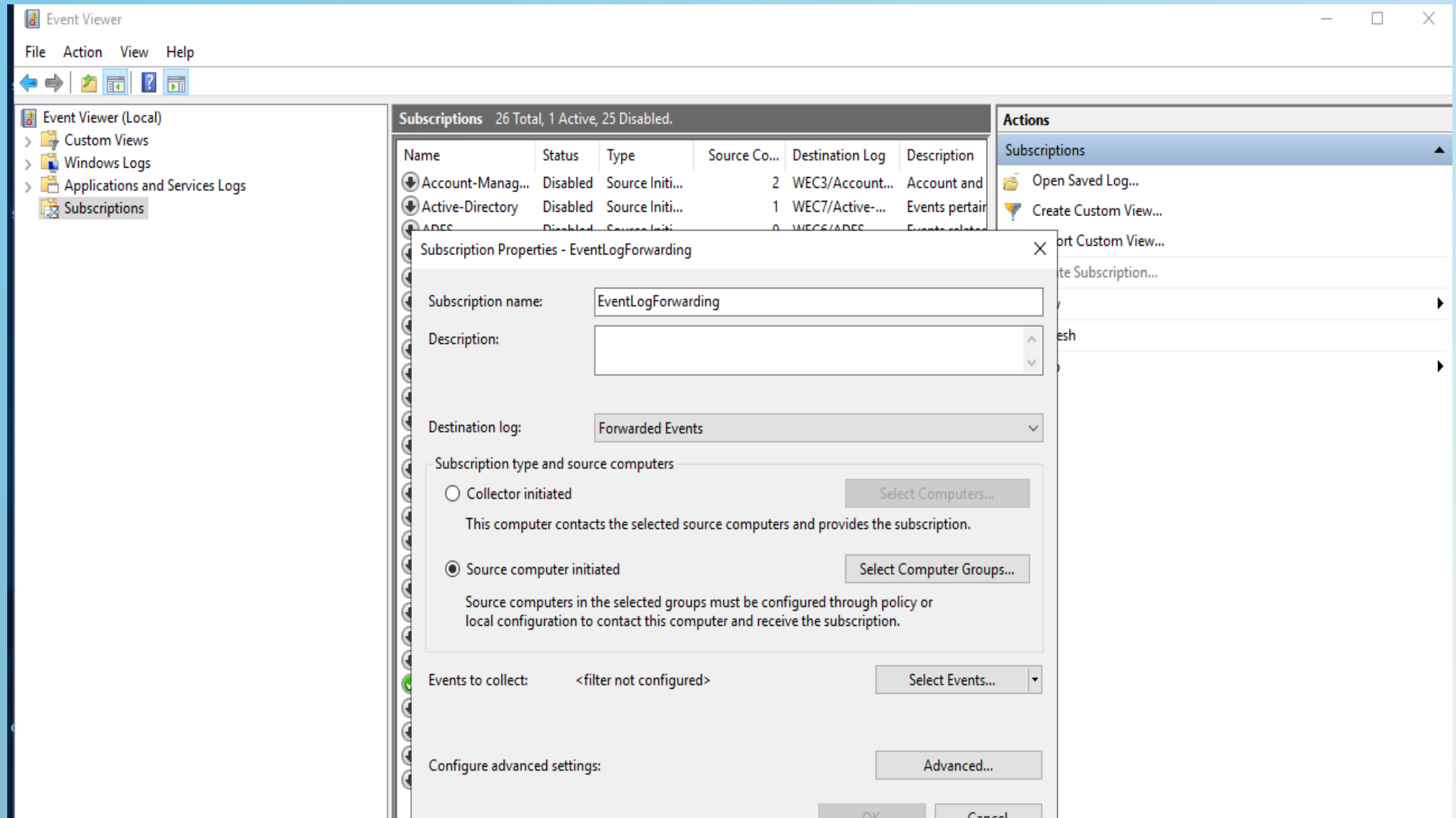
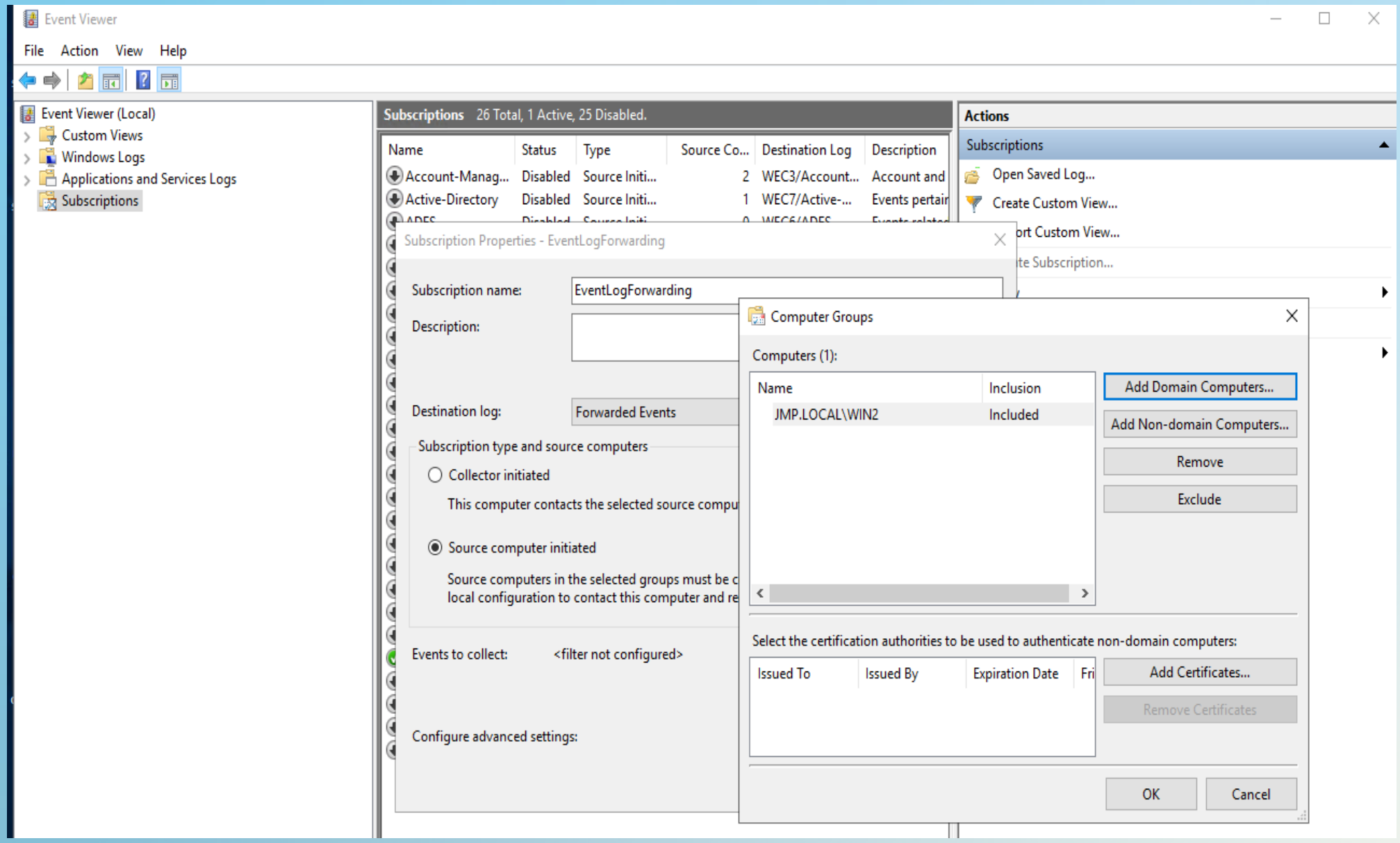
installation d'un "wec server" en images.

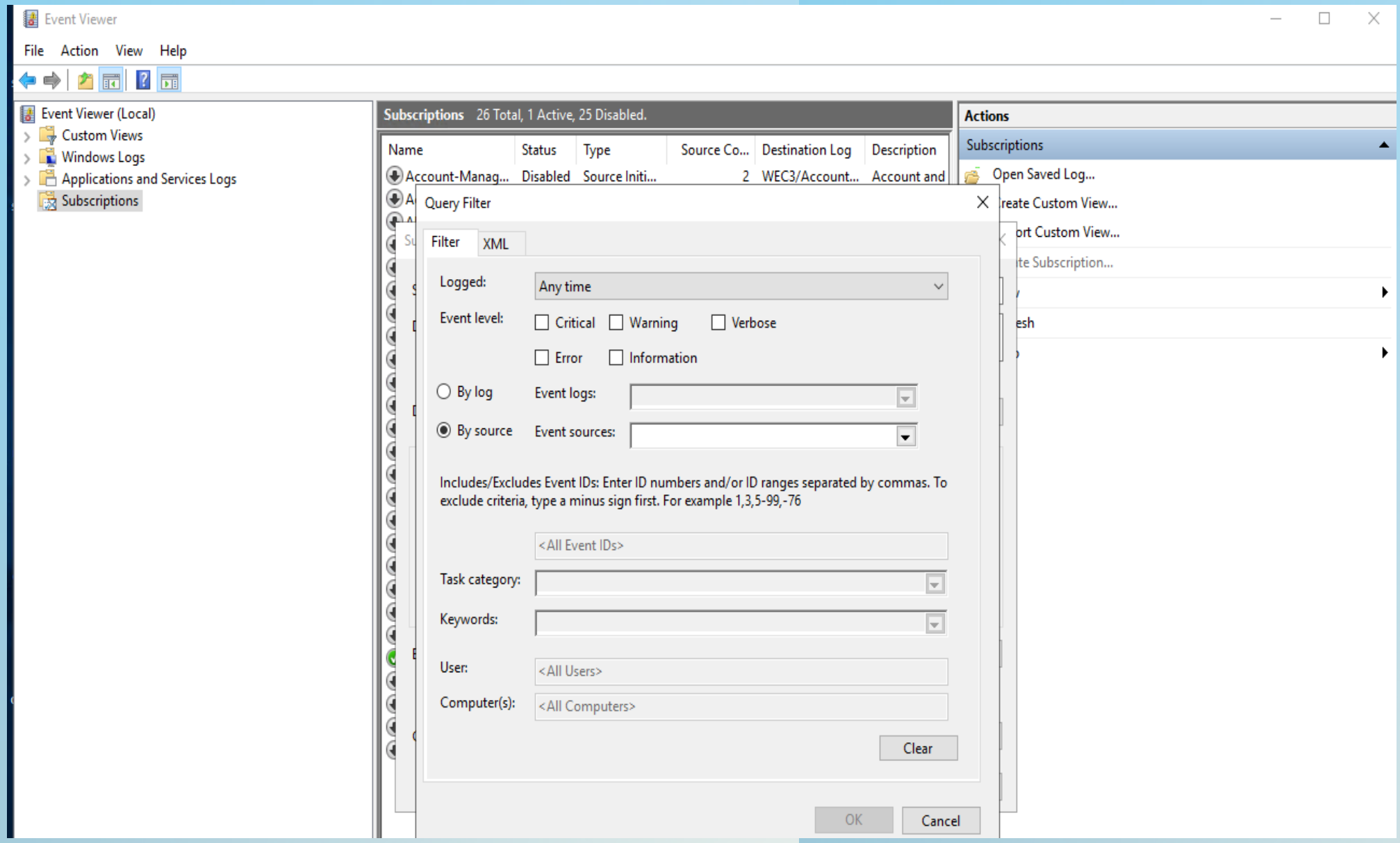
Buts: recevoir les "events sysmon" d'un "windows (>=10)" sur une machine ("wec server" dédié) dans "forwarded events"



Buts: idem pour les "security events"



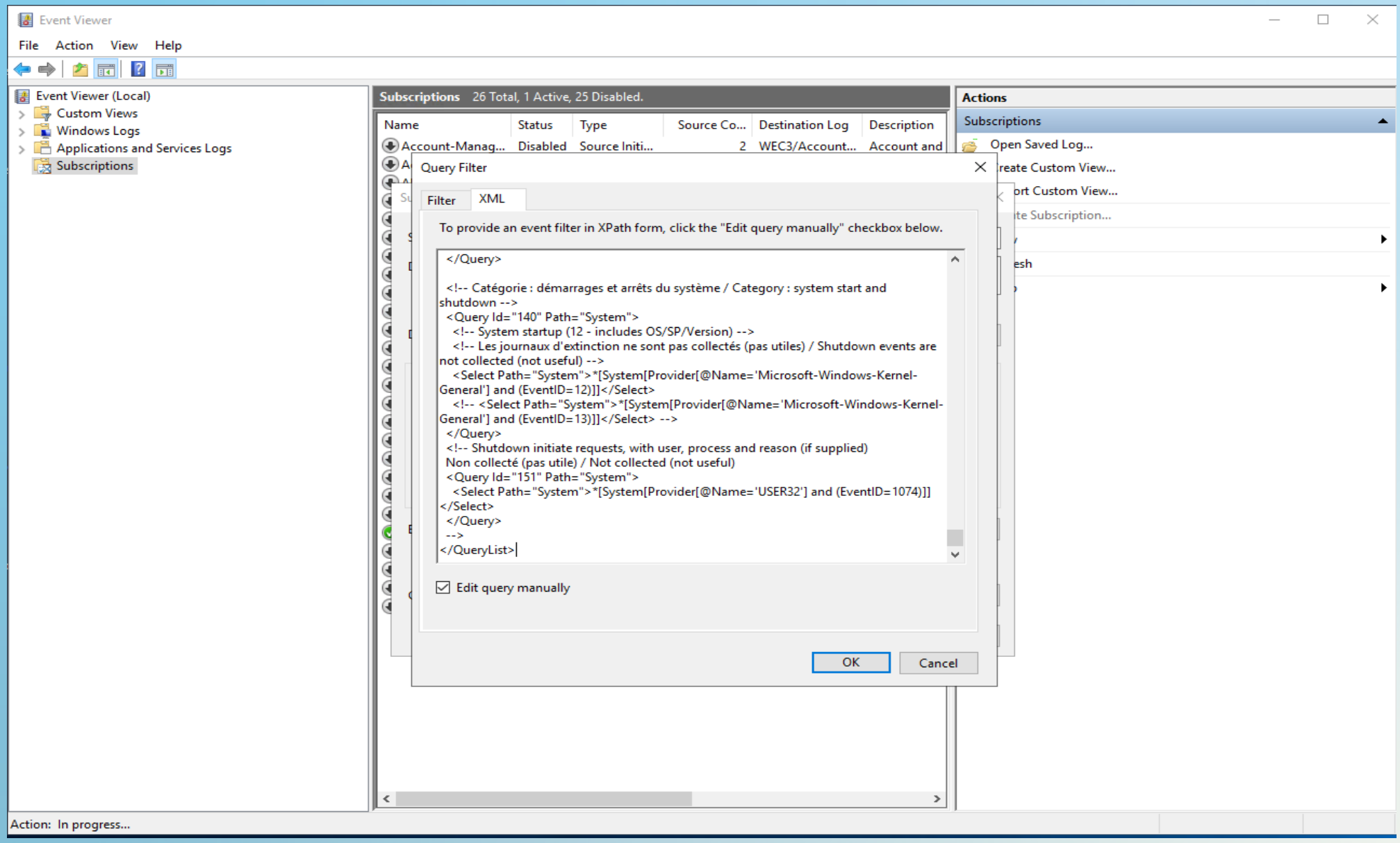

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Subscriptions 26 Total, 1 Active, 25 Disabled.
Name Status Type Source Co... Destination Log Description
Account-Manag... Disabled Source Initi... 2 WEC3/Account... Account and
Active-Directory Disabled Source Initi... 1 WEC7/Active-... Events pertair
Subscription Properties - EventLogForwarding
Subscription name: EventLogForwarding
Description:
Destination log: Forwarded Events
Subscription type and source computers
Collector initiated
This computer contacts the selected source compu
Source computer initiated
Source computers in the selected groups must be c
local configuration to contact this computer and re
Events to collect: <filter not configured>
Configure advanced settings:
Actions
Subscriptions
Open Saved Log...
Create Custom View...
ort Custom View...
te Subscription...
Computer Groups
Computers (1):
Name Inclusion
JMP.LOCAL\WIN2 Included
Add Domain Computers...
Add Non-domain Computers...
Remove
Exclude
Select the certification authorities to be used to authenticate non-domain computers:
Issued To Issued By Expiration Date Fri
Add Certificates...
Remove Certificates
OK
Cancel

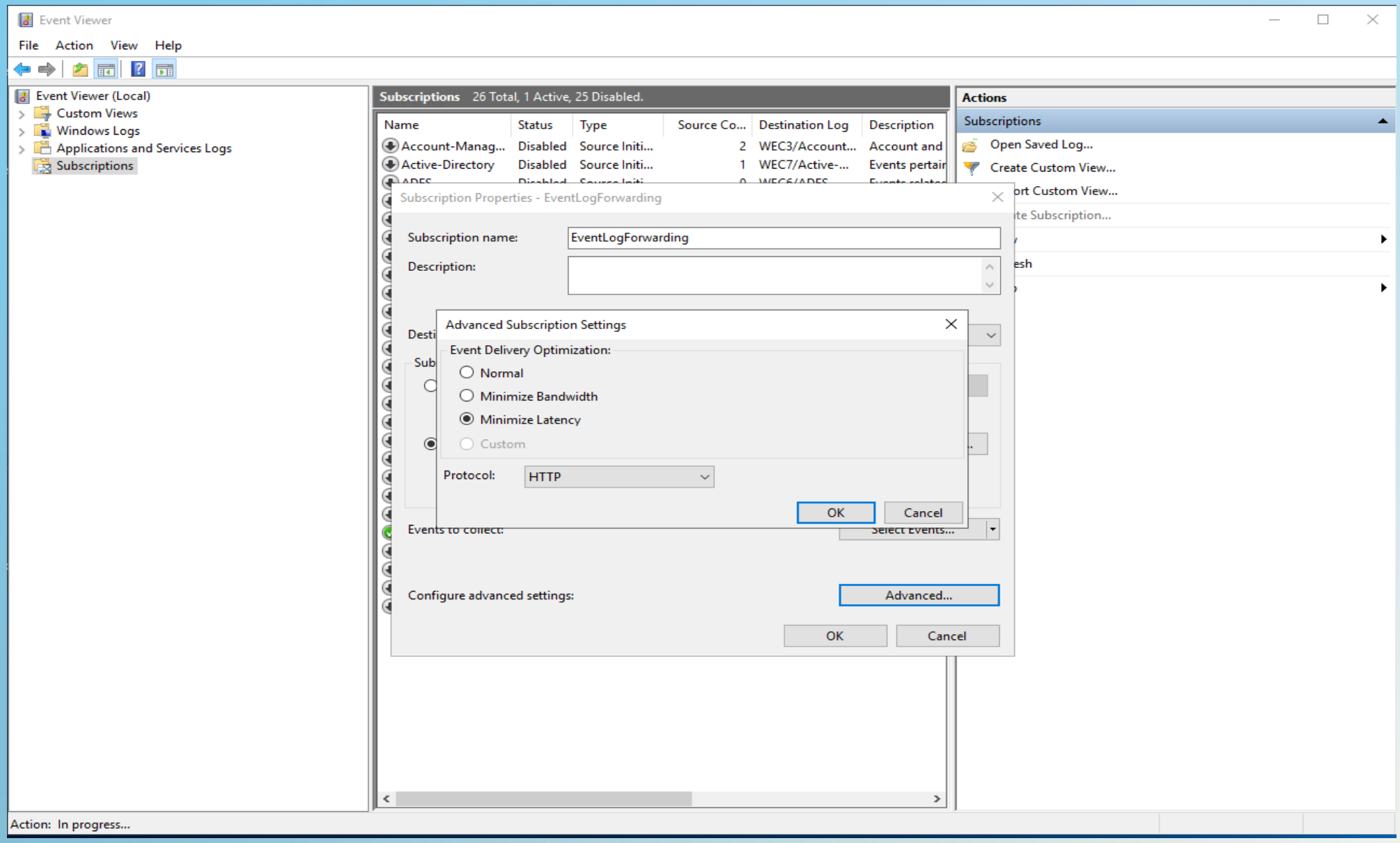

Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Subscriptions 26 Total, 1 Active, 25 Disabled.
Name Status Type Source Co... Destination Log Description
Account-Manag... Disabled Source Initi... 2 WEC3/Account... Account and
Actions
Subscriptions
Open Saved Log...
Query Filter
Filter XML
Logged: Any time
Event level: Critical Warning Verbose
Error Information
By log Event logs:
By source Event sources:
Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76
<All Event IDs>
Task category:
Keywords:
User: <All Users>
Computer(s): <All Computers>
Clear
OK
Cancel

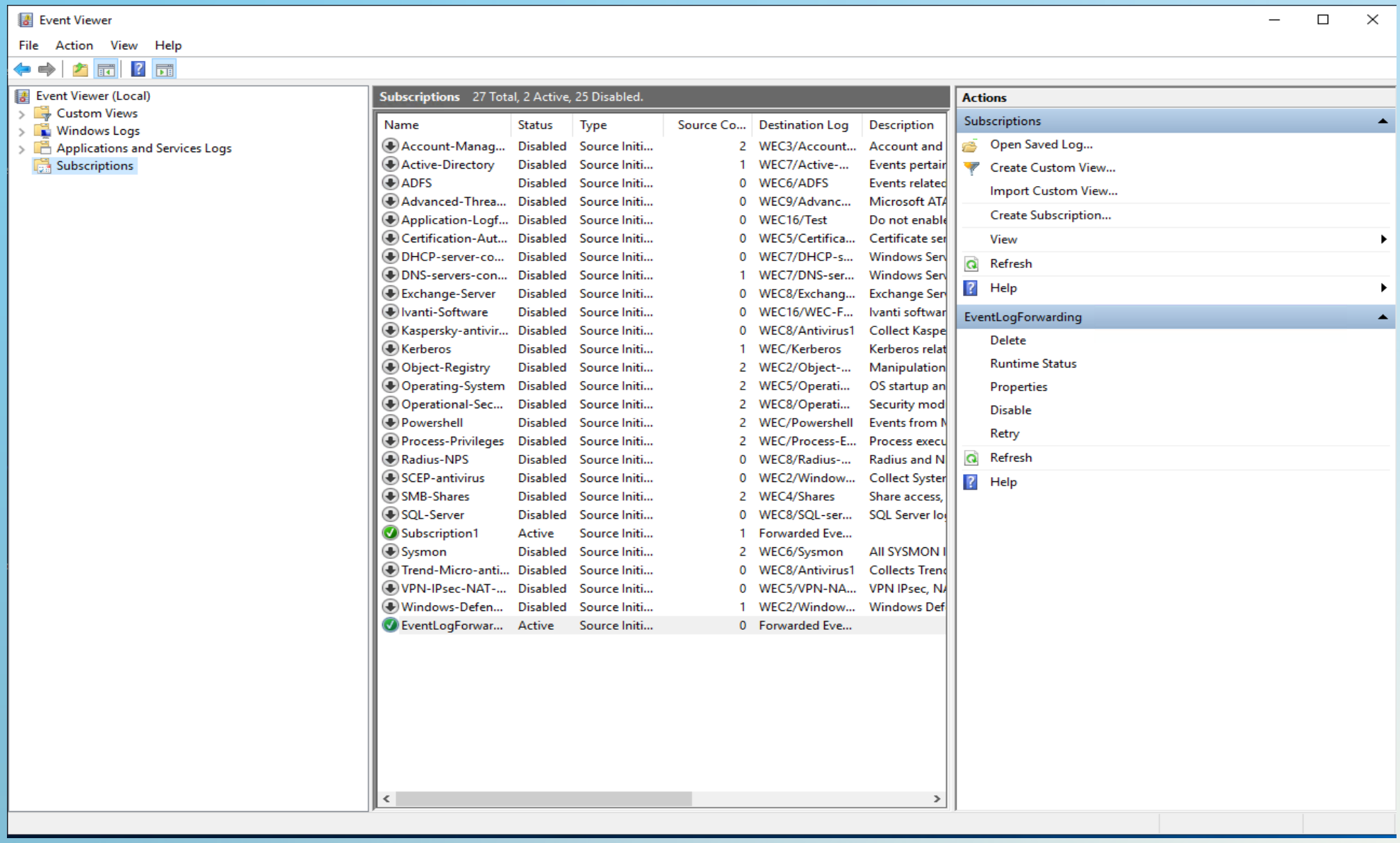
R5.cyber.11 Supervision de la sécurité

https://raw.githubusercontent.com/ANSSI-FR/guide-journalisation-microsoft/main/Standard_WEC_query.xml

```
<!-- Version 20210902_1600 -->
<QueryList>
  <!--
    Cette requête WEC est basée sur celles proposées par Microsoft dans cet article : / This WEC query is based on what Microsoft proposed in this article :
    https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
    Ce fichier contient les annotations originales de Microsoft en anglais, non traduites / This file contains original Microsoft's annotations in english with no french translation
    Les annotations ajoutées par l'ANSSI sont en français et en anglais / Annotations added by the ANSSI are in french and english
    Certaines selections d'évènements ont été désactivées (commentées) lorsqu'elles concernent des produits trop spécifiques et peuvent être décommentées au besoin / Some event selections have been disabled (commented) when they concern too specific products but they can be
uncommented if necessary
    D'autres selections ont été désactivées (commentées) lorsqu'elles sont jugées peu utiles à collecter / Other event selections have been disabled (commented) when they have been considered not very interesting to collect
  -->

  <!-- Catégorie : stratégies de restriction logicielle diverses / category : various software restriction strategies -->
  <!-- SRP : utile uniquement si des règles SRP ont été déployées / Only useful if SRP rules have been deployed -->
  <Query Id="0" Path="Application">
    <Select Path="Application">*[System[(EventID='866')]]</Select>
  </Query>
  <!-- AppLocker EXE events : utile uniquement si des règles d'exécutables pour Applocker ont été déployées / Only useful if applocker EXE rules have been deployed -->
  <Query Id="1" Path="Microsoft-Windows-AppLocker/EXE and DLL">
    <Select Path="Microsoft-Windows-AppLocker/EXE and DLL">*[UserData[RuleAndFileData[PolicyName="EXE"]]]</Select>
  </Query>
  <!-- AppLocker script events : utile uniquement si des règles de MSI ou de script pour Applocker ont été déployées / Only useful if applocker MSI or script rules have been deployed -->
  <Query Id="2" Path="Microsoft-Windows-AppLocker/MSI and Script">
    <Select Path="Microsoft-Windows-AppLocker/MSI and Script">*</Select>
  </Query>
  <!-- AppLocker packaged (Modern UI) app execution -->
  <Query Id="3" Path="Microsoft-Windows-AppLocker/Packaged app-Execution">
    <Select Path="Microsoft-Windows-AppLocker/Packaged app-Execution">*</Select>
  </Query>
  <!-- AppLocker packaged (Modern UI) app installation -->
  <Query Id="4" Path="Microsoft-Windows-AppLocker/Packaged app-Deployment">
    <Select Path="Microsoft-Windows-AppLocker/Packaged app-Deployment">*</Select>
  </Query>
  <!-- CodeIntegrity (WDAC) : utile uniquement si des politiques de Code Integrity (WDAC) ont été déployées en mode enforced ou audit / Only useful if WDAC policies have been deployed in enforced or audit mode -->
  <!-- Nombreux faux positifs sont journalisés, il est préférable de les filtrer pour réduire le bruit / A lot of false positive events are logged, they should be filtered to cut down noise -->
  <!--
  <Query Id="5" Path="Microsoft-Windows-CodeIntegrity/Operational">
    <Select Path="Microsoft-Windows-CodeIntegrity/Operational">*[System[(EventID=3001 or EventID=3023 or EventID=3064 or EventID=3076 or EventID=3077 or EventID=3080 or EventID=3082 or EventID=3089)]]</Select>
  </Query>
  -->


  <!-- Catégorie : stratégies Anti Malwares / Category : anti Malware strategies -->
  <Query Id="10" Path="Microsoft-Windows-Windows Defender/Operational">
    <!-- Modern Windows Defender event provider Detection events (1006-1009) and (1116-1119) -->
    <Select Path="Microsoft-Windows-Windows Defender/Operational">*[System[( (EventID &gt;= 1006 and EventID &lt;= 1009) )]]</Select>
    <Select Path="Microsoft-Windows-Windows Defender/Operational">*[System[( (EventID &gt;= 1116 and EventID &lt;= 1119) )]]</Select>
    <!-- Evènement 1120 si ThreatFileHashLogging a été activé via le registre / Event 1120 if ThreatFileHashLogging has been enabled through registry -->
    <Select Path="Microsoft-Windows-Windows Defender/Operational">*[System[(EventID=1120)]]</Select>
  </Query>
  <!-- Anti-malware *old* events, but only detect events (cuts down noise)
  Utile seulement sur les systèmes obsolètes / Useful only on obsolete systems
  <Query Id="11" Path="System">
    <Select Path="System">*[System[Provider[@Name='Microsoft Antimalware'] and (EventID &gt;= 1116 and EventID &lt;= 1119)]]</Select>
  </Query>
  -->
  <!-- EMET events
  Utile uniquement si EMET (qui n'est plus supporté par Microsoft) est toujours utilisé sur certains systèmes / Only if EMET (which is not supported anymore by Microsoft) is still installed on some systems
  <Query Id="12" Path="Application">
    <Select Path="Application">*[System[Provider[@Name='EMET']]]</Select>
  </Query>
  -->

  <!-- Catégorie : processus / Category : processes -->
  <Query Id="20" Path="Security">
    <!-- Process Create (4688) -->
    <Select Path="Security">*[System[EventID=4688]]</Select>
  </Query>
  <Query Id="21" Path="Security">
```


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Subscriptions 26 Total, 1 Active, 25 Disabled.
Name Status Type Source Co... Destination Log Description
Account-Manag... Disabled Source Initi... 2 WEC3/Account... Account and
Actions
Subscriptions
Open Saved Log...
Query Filter
Filter XML
To provide an event filter in XPath form, click the "Edit query manually" checkbox below.
</Query>
<!-- Catégorie : démarrages et arrêts du système / Category : system start and shutdown -->
<Query Id="140" Path="System">
<!-- System startup (12 - includes OS/SP/Version) -->
<!-- Les journaux d'extinction ne sont pas collectés (pas utiles) / Shutdown events are not collected (not useful) -->
<Select Path="System">*[System[Provider[@Name='Microsoft-Windows-Kernel-General'] and (EventID=12)]]</Select>
<!-- <Select Path="System">*[System[Provider[@Name='Microsoft-Windows-Kernel-General'] and (EventID=13)]]</Select> -->
</Query>
<!-- Shutdown initiate requests, with user, process and reason (if supplied)
Non collecté (pas utile) / Not collected (not useful)
<Query Id="151" Path="System">
<Select Path="System">*[System[Provider[@Name='USER32'] and (EventID=1074)]]
</Select>
</Query>
-->
</QueryList>
Edit query manually
OK
Cancel
Action: In progress...


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Subscriptions 26 Total, 1 Active, 25 Disabled.
Name Status Type Source Co... Destination Log Description
Account-Manag... Disabled Source Initi... 2 WEC3/Account... Account and
Active-Directory Disabled Source Initi... 1 WEC7/Active-... Events pertair
Subscription Properties - EventLogForwarding
Subscription name: EventLogForwarding
Description:
Advanced Subscription Settings
Event Delivery Optimization:
Normal
Minimize Bandwidth
Minimize Latency
Custom
Protocol: HTTP
OK
Cancel
Events to collect:
Configure advanced settings:
Advanced...
OK
Cancel
Actions
Subscriptions
Open Saved Log...
Create Custom View...
Action: In progress...


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Subscriptions 27 Total, 2 Active, 25 Disabled.
Name Status Type Source Co... Destination Log Description
Account-Manag... Disabled Source Initi... 2 WEC3/Account... Account and
Active-Directory Disabled Source Initi... 1 WEC7/Active-... Events pertair
ADFS Disabled Source Initi... 0 WEC6/ADFS Events relatec
Advanced-Threa... Disabled Source Initi... 0 WEC9/Advanc... Microsoft ATA
Application-Logf... Disabled Source Initi... 0 WEC16/Test Do not enable
Certification-Aut... Disabled Source Initi... 0 WEC5/Certifica... Certificate ser
DHCP-server-co... Disabled Source Initi... 0 WEC7/DHCP-s... Windows Serv
DNS-servers-con... Disabled Source Initi... 1 WEC7/DNS-ser... Windows Serv
Exchange-Server Disabled Source Initi... 0 WEC8/Exchang... Exchange Ser
Ivanti-Software Disabled Source Initi... 0 WEC16/WEC-F... Ivanti softwar
Kaspersky-antivir... Disabled Source Initi... 0 WEC8/Antivirus1 Collect Kaspe
Kerberos Disabled Source Initi... 1 WEC/Kerberos Kerberos relat
Object-Registry Disabled Source Initi... 2 WEC2/Object-... Manipulation
Operating-System Disabled Source Initi... 2 WEC5/Operati... OS startup an
Operational-Sec... Disabled Source Initi... 2 WEC8/Operati... Security mod
Powershell Disabled Source Initi... 2 WEC/Powershell Events from M
Process-Privileges Disabled Source Initi... 2 WEC/Process-E... Process execu
Radius-NPS Disabled Source Initi... 0 WEC8/Radius-... Radius and N
SCEP-antivirus Disabled Source Initi... 0 WEC2/Window... Collect Syster
SMB-Shares Disabled Source Initi... 2 WEC4/Shares Share access,
SQL-Server Disabled Source Initi... 0 WEC8/SQL-ser... SQL Server lo
Subscription1 Active Source Initi... 1 Forwarded Eve...
Sysmon Disabled Source Initi... 2 WEC6/Sysmon All SYSMON I
Trend-Micro-anti... Disabled Source Initi... 0 WEC8/Antivirus1 Collects Trenc
VPN-IPsec-NAT-... Disabled Source Initi... 0 WEC5/VPN-NA... VPN IPsec, NA
Windows-Defen... Disabled Source Initi... 1 WEC2/Window... Windows Def
EventLogForwar... Active Source Initi... 0 Forwarded Eve...
Actions
Subscriptions
Open Saved Log...
Create Custom View...
Import Custom View...
Create Subscription...
View
Refresh
Help
EventLogForwarding
Delete
Runtime Status
Properties
Disable
Retry
Refresh
Help

```
C:\Windows\system32>netsh http show urlacl url=http://+:5985/wsman/

URL Reservations:
-----------------

    Reserved URL            : http://+:5985/wsman/
        User: NT SERVICE\WinRM
            Listen: Yes
            Delegate: No
        User: NT SERVICE\Wecsvc
            Listen: Yes
            Delegate: No
            SDDL: D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)
```

https://learn.microsoft.com/en-us/troubleshoot/windows-server/admin-development/events-not-forwarded-by-windows-server-collector

Windows Remote Management service (WinRM) use these URLs. However, the default access control lists (ACLs) for these URLs allow access for only the svchost process that runs WinRM. In the default configuration of Windows Server 2016, a single svchost process runs both WinRM and WecSvc. Because the process has access, both services function correctly. However, if you change the configuration so that the services run on separate host processes, WecSvc no longer has access and event forwarding no longer functions.

The services function differently in Windows Server 2019. If a Windows Server 2019 computer has more than 3.5 GB of RAM, separate svchost processes run WinRM and WecSvc. Because of this change, event forwarding may not function correctly in the default configuration. For more information about the service changes, see Changes to Service Host grouping in Windows 10.

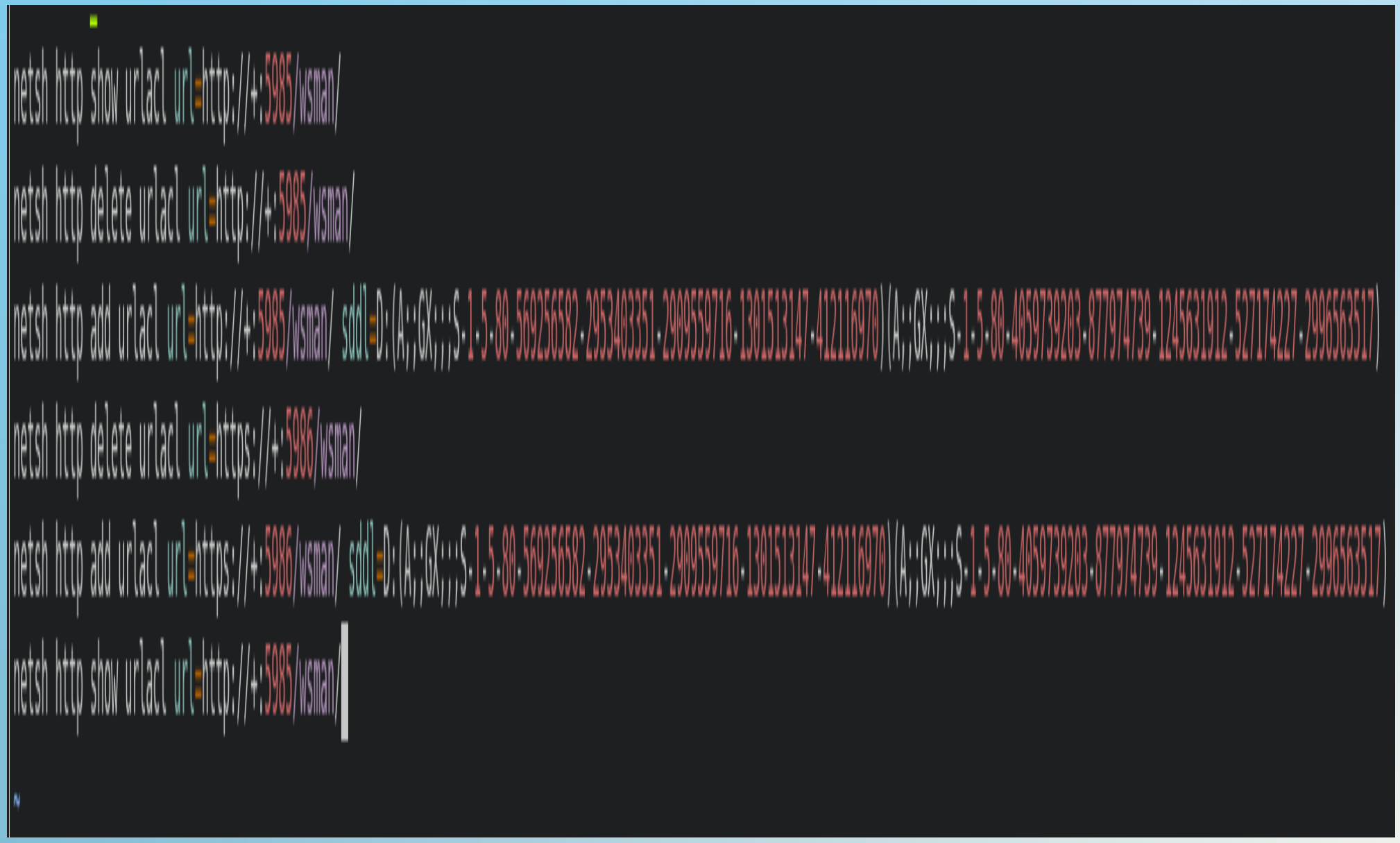
Resolution

To view the URL permissions, open an elevated Command Prompt window and run the command `netsh http show urlacl`.

To fix the URL permissions, use the elevated Command Prompt window and run the following commands:

Windows Command Prompt — Copy

```
netsh http delete urlacl url=http://+:5985/wsman/
netsh http add urlacl url=http://+:5985/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2
netsh http delete urlacl url=https://+:5986/wsman/
netsh http add urlacl url=https://+:5986/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-
```


netsh http show urlacl url=http://+:5985/wsman/
netsh http delete urlacl url=http://+:5985/wsman/
netsh http add urlacl url=http://+:5985/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)
netsh http delete urlacl url=https://+:5986/wsman/
netsh http add urlacl url=https://+:5986/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)
netsh http show urlacl url=http://+:5985/wsman/