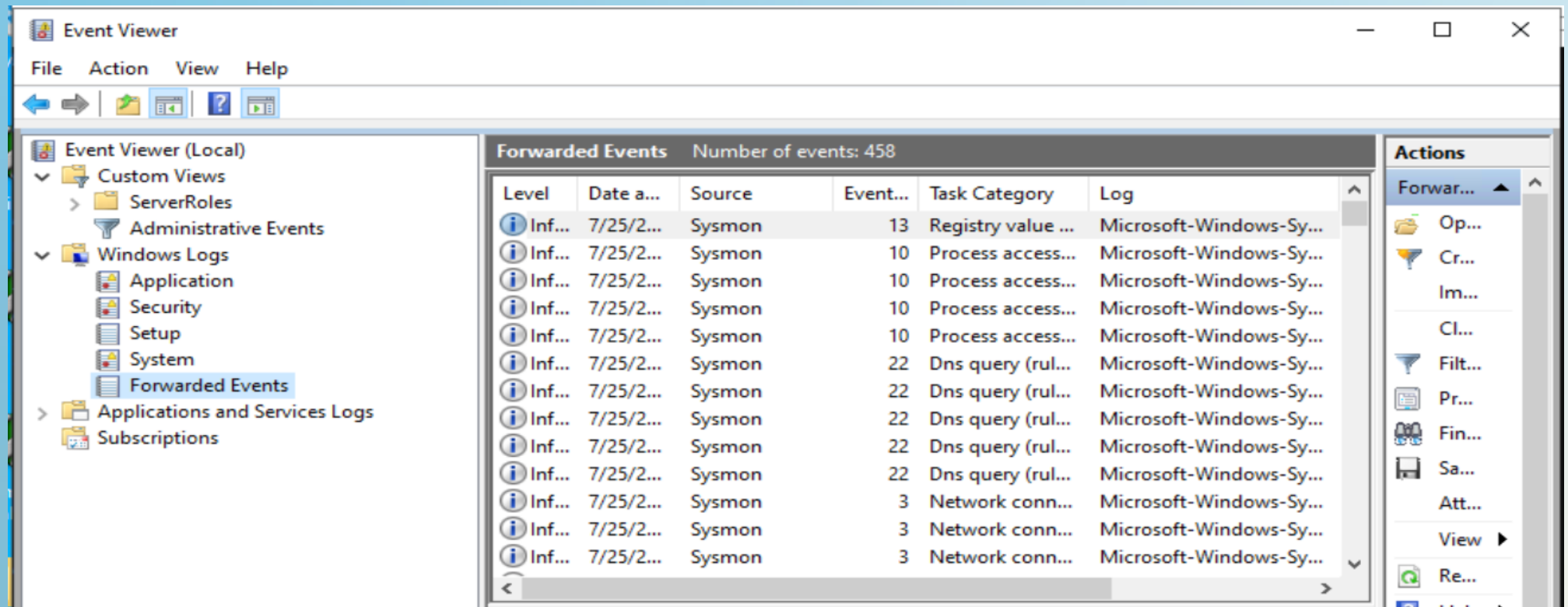
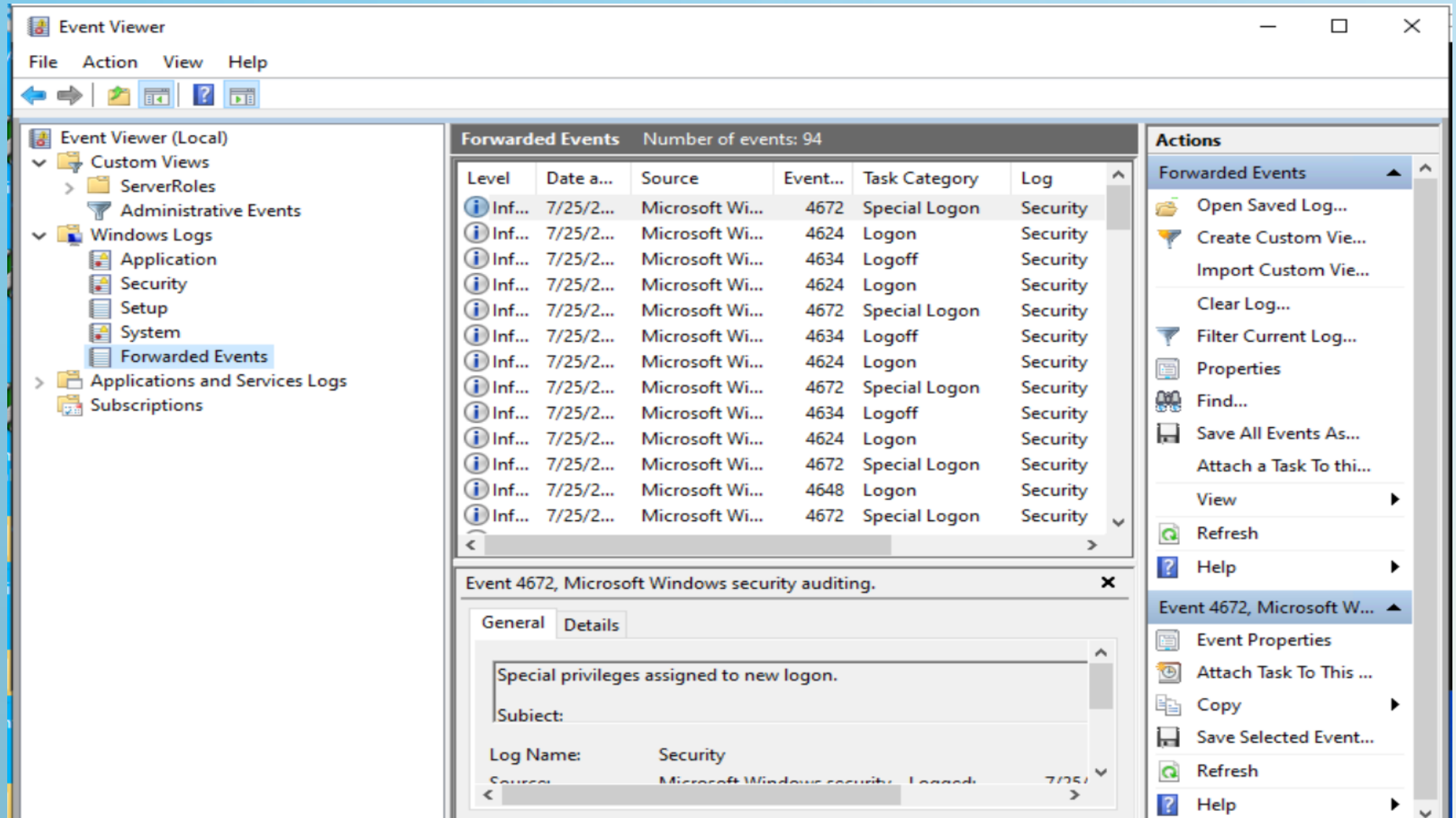
installation d'un "wec server" en images.

Résultats attendus

Recevoir les "events sysmon" d'une machine distant "windows (>=10)" sur un serveur WEC" dédié ici win-1 le DC) dans le canal "forwarded events".



Résultats attendus: recevoir aussi les "security events"

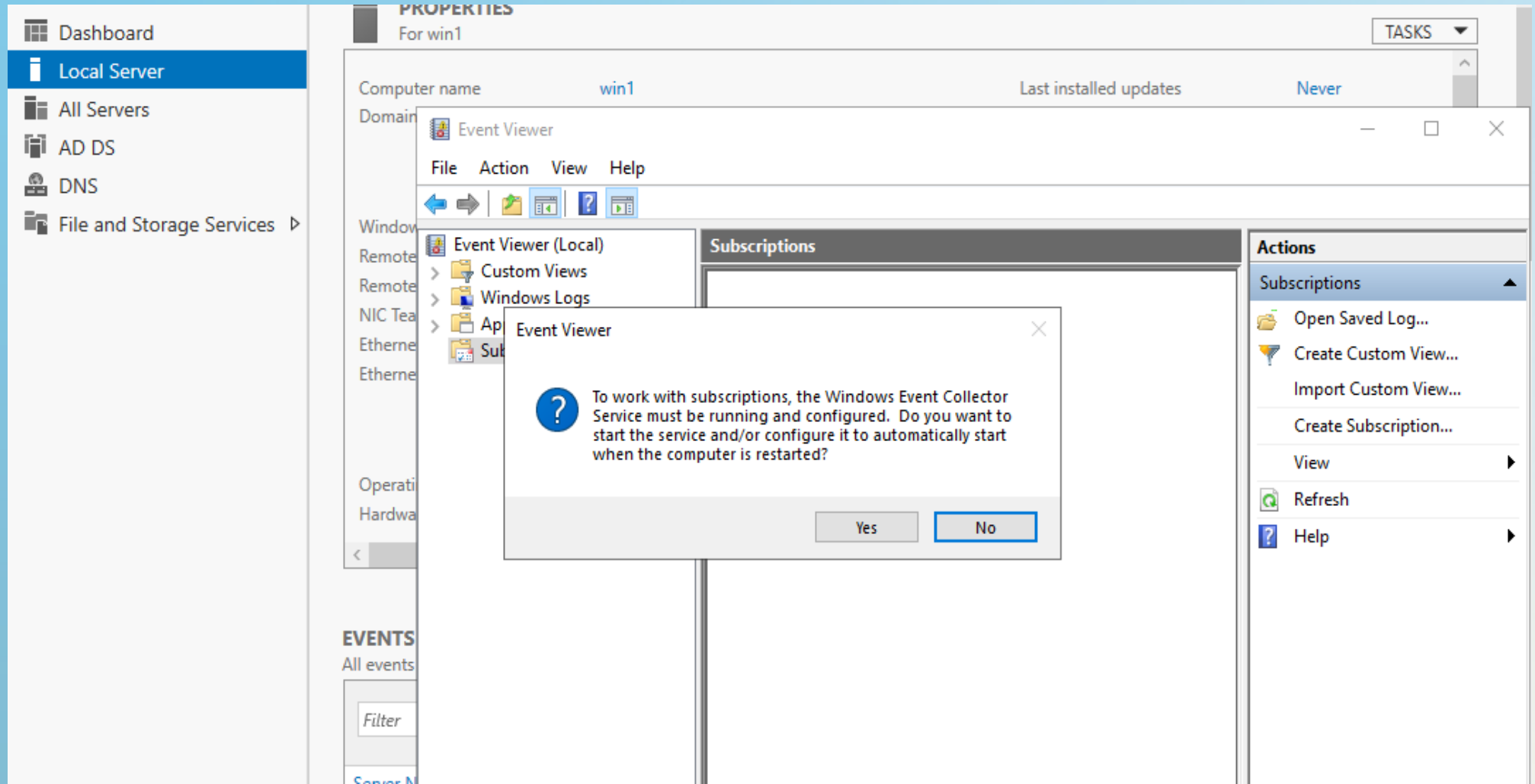


Pré-requis: le service WinRM qui assure le transport des évènements doit être démarré sur toutes les machines.

```
jmp\vagrant@WIN1 C:\Users\vagrant>sc query  winrm

SERVICE_NAME: winrm
        TYPE               : 30  WIN32
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Dans "eventviewer" de win-1 (DC) clicker sur "subscription" va démarrer le service "WEC"

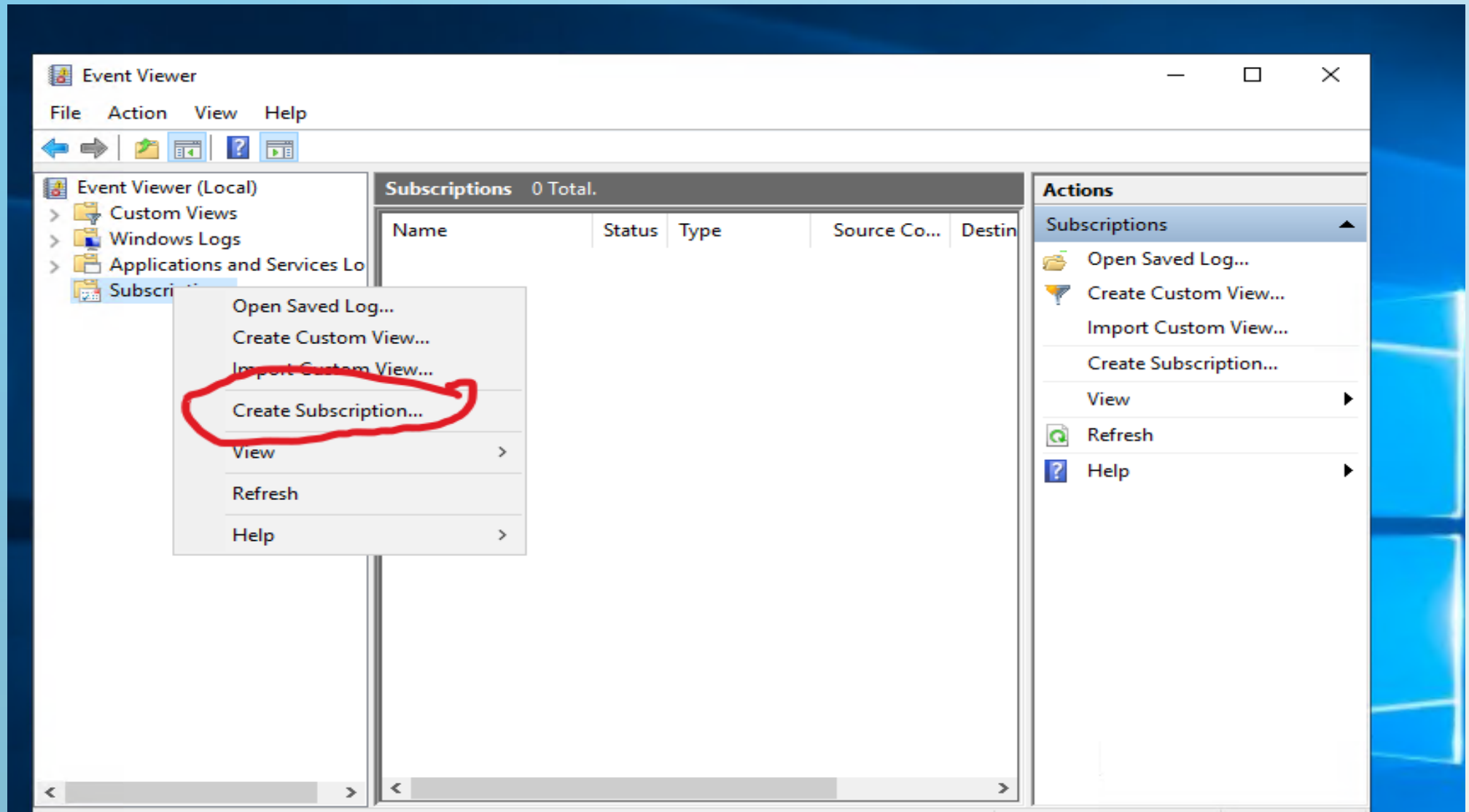


Visualisez le démarrage du service "SEC" sur le serveur "win-1" (DC)

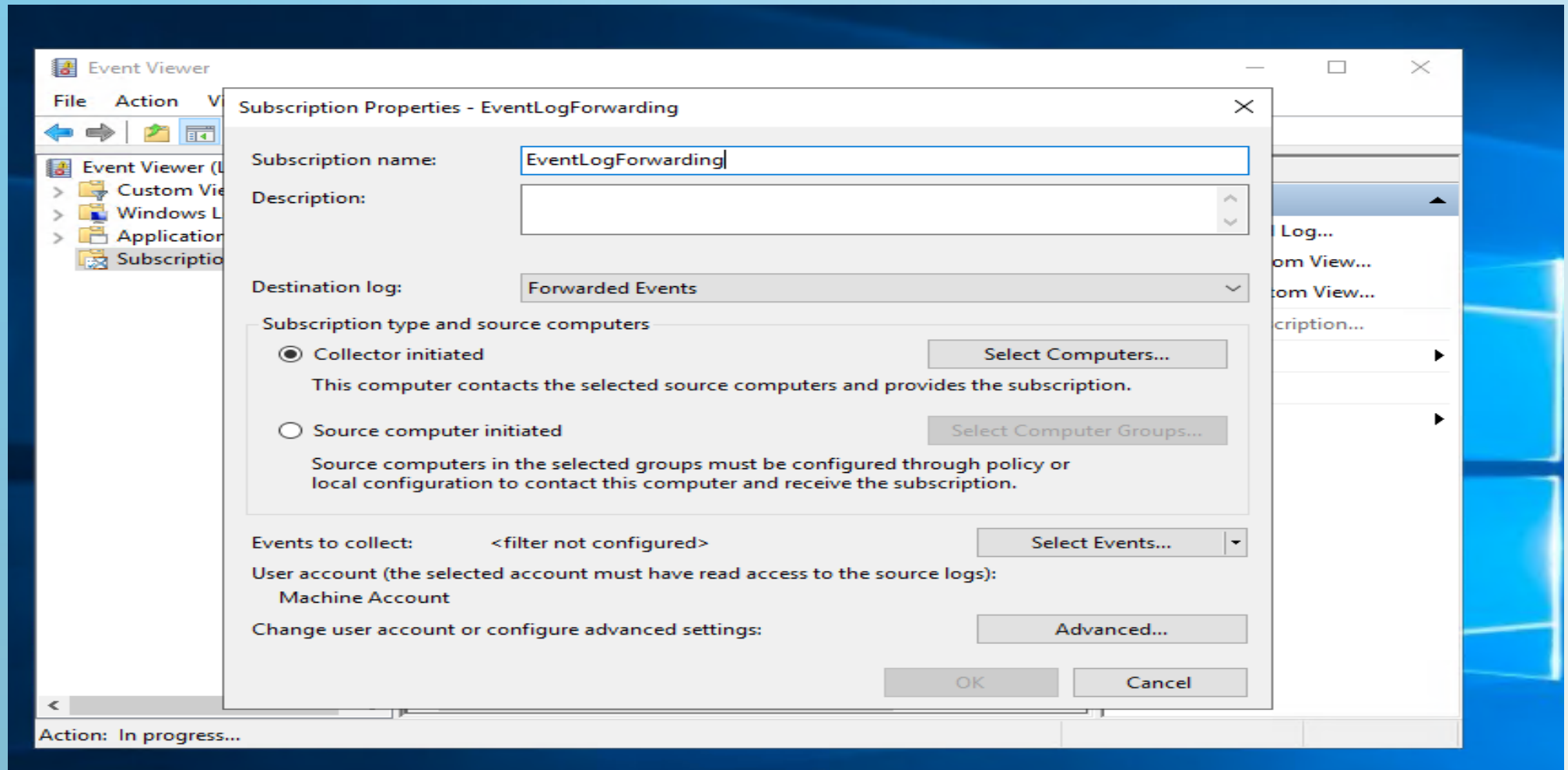
```
jmp\vagrant@WIN1 C:\Users\vagrant>sc query  wecsvc

SERVICE_NAME: wecsvc
        TYPE               : 30  WIN32
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Créez une nouvelle "subscription"

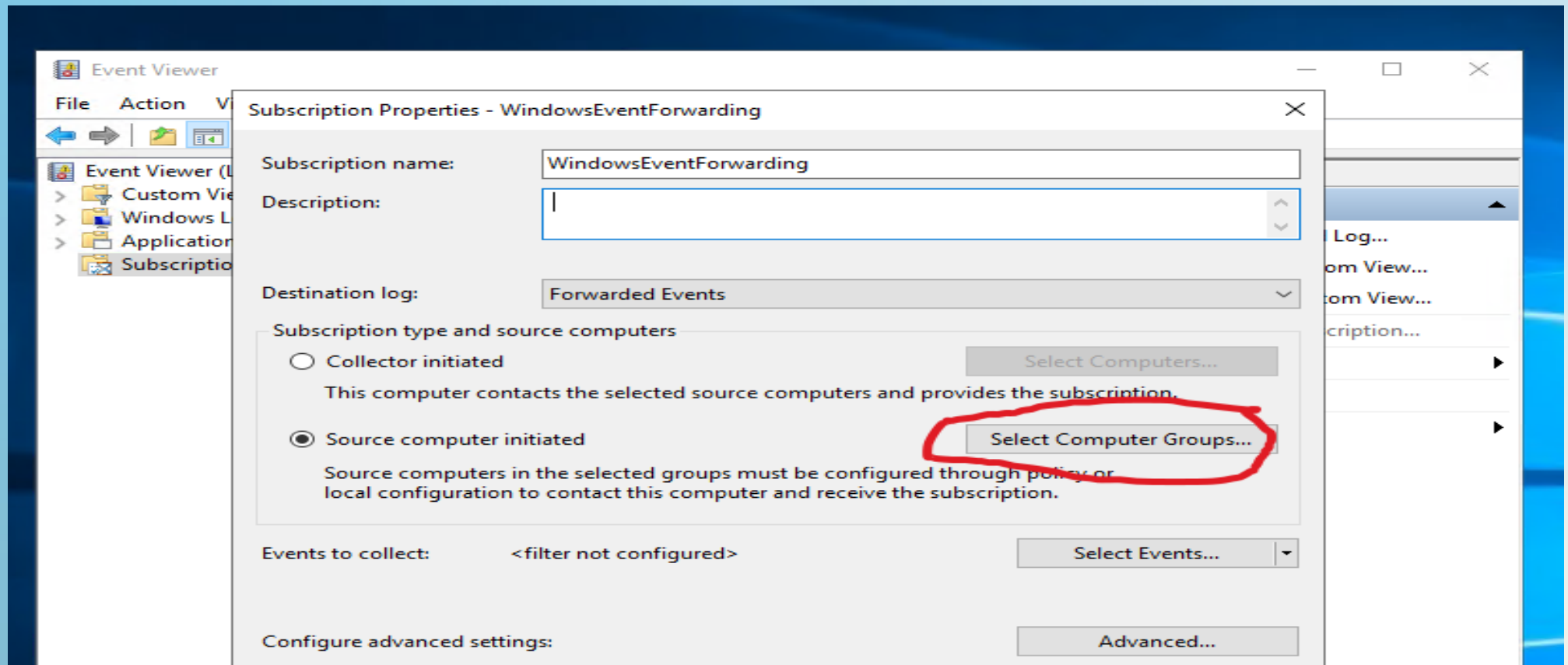


Créez une nouvelle "subscription" nommée EventLogforwarding

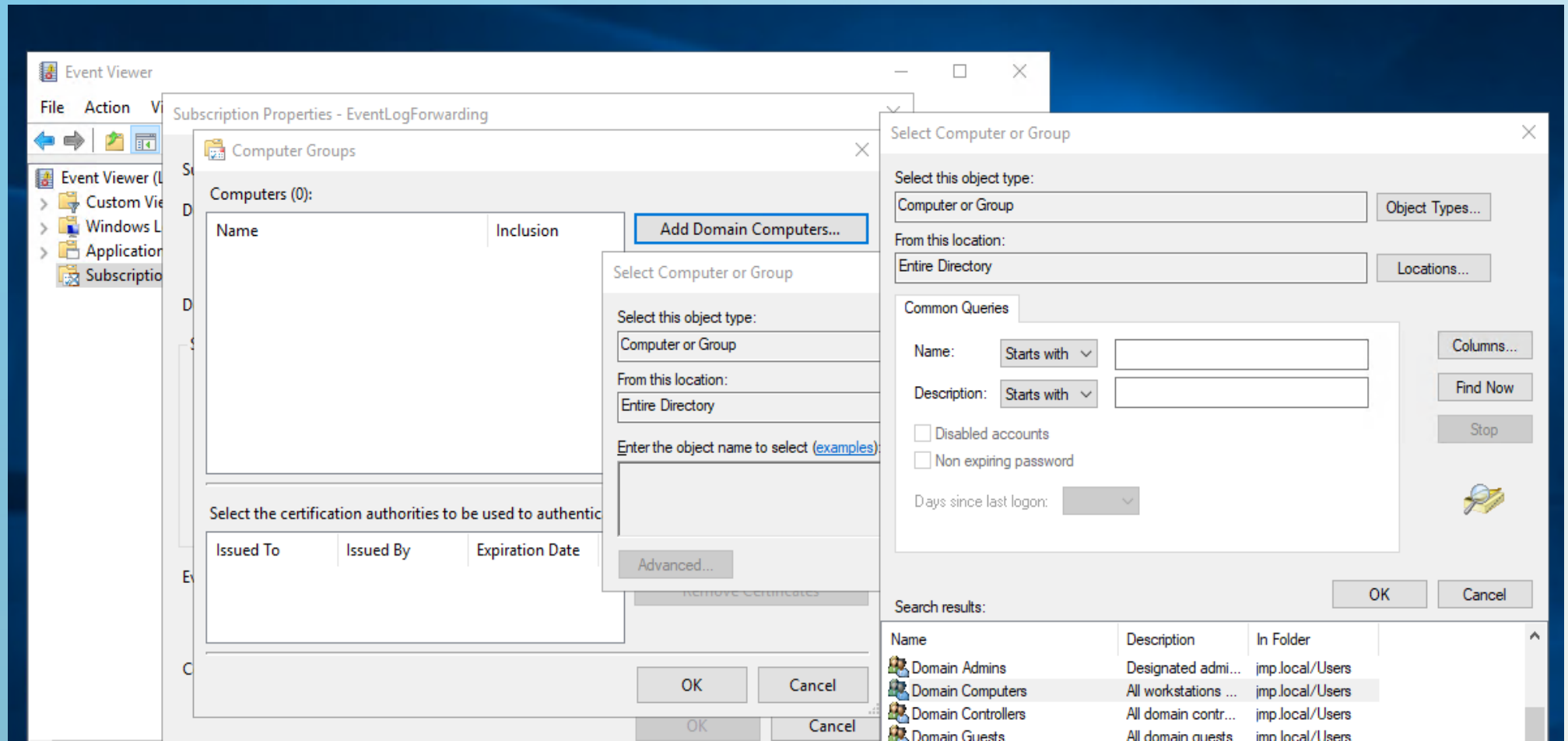


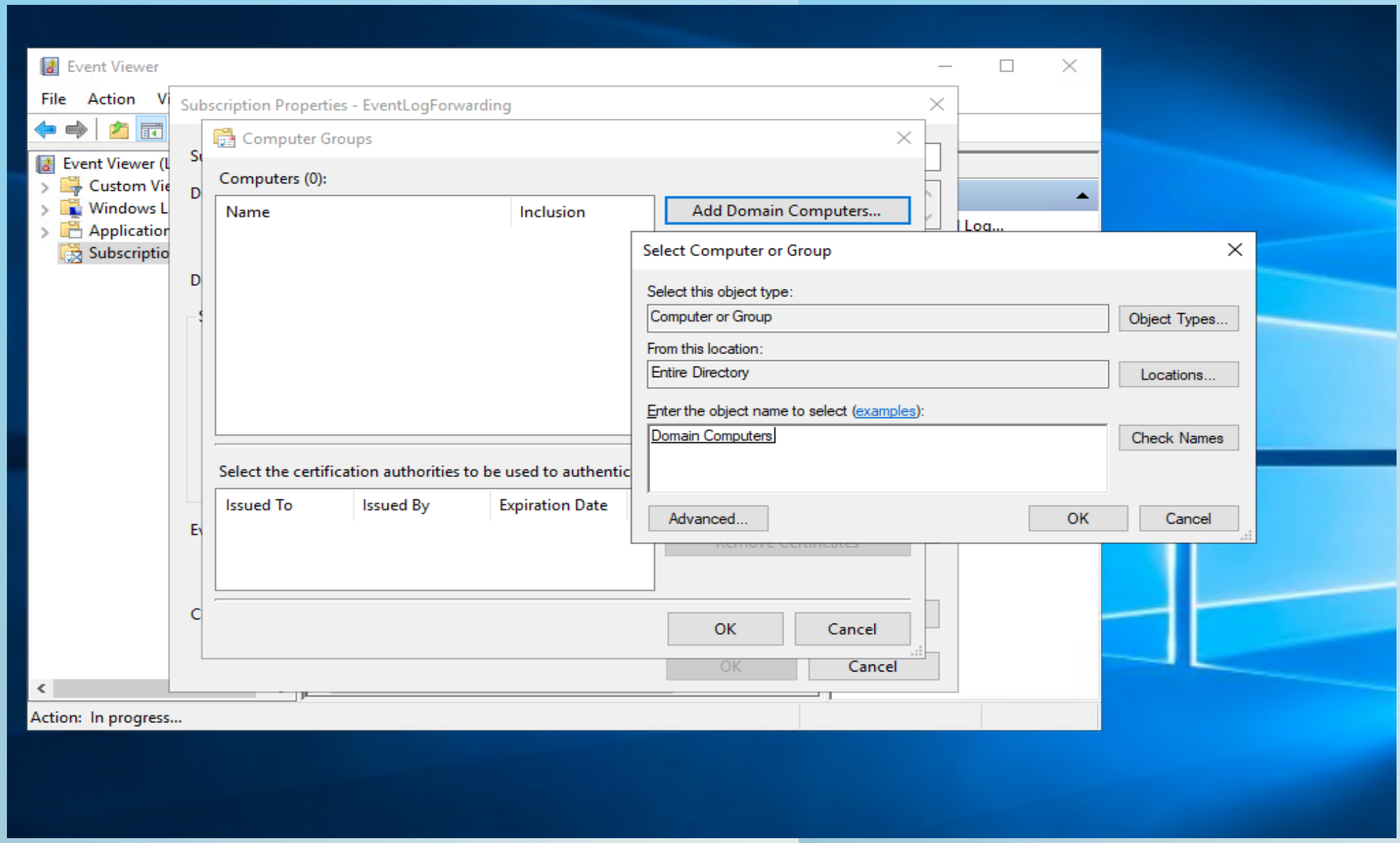
La subscription est pilotée par le client WEC

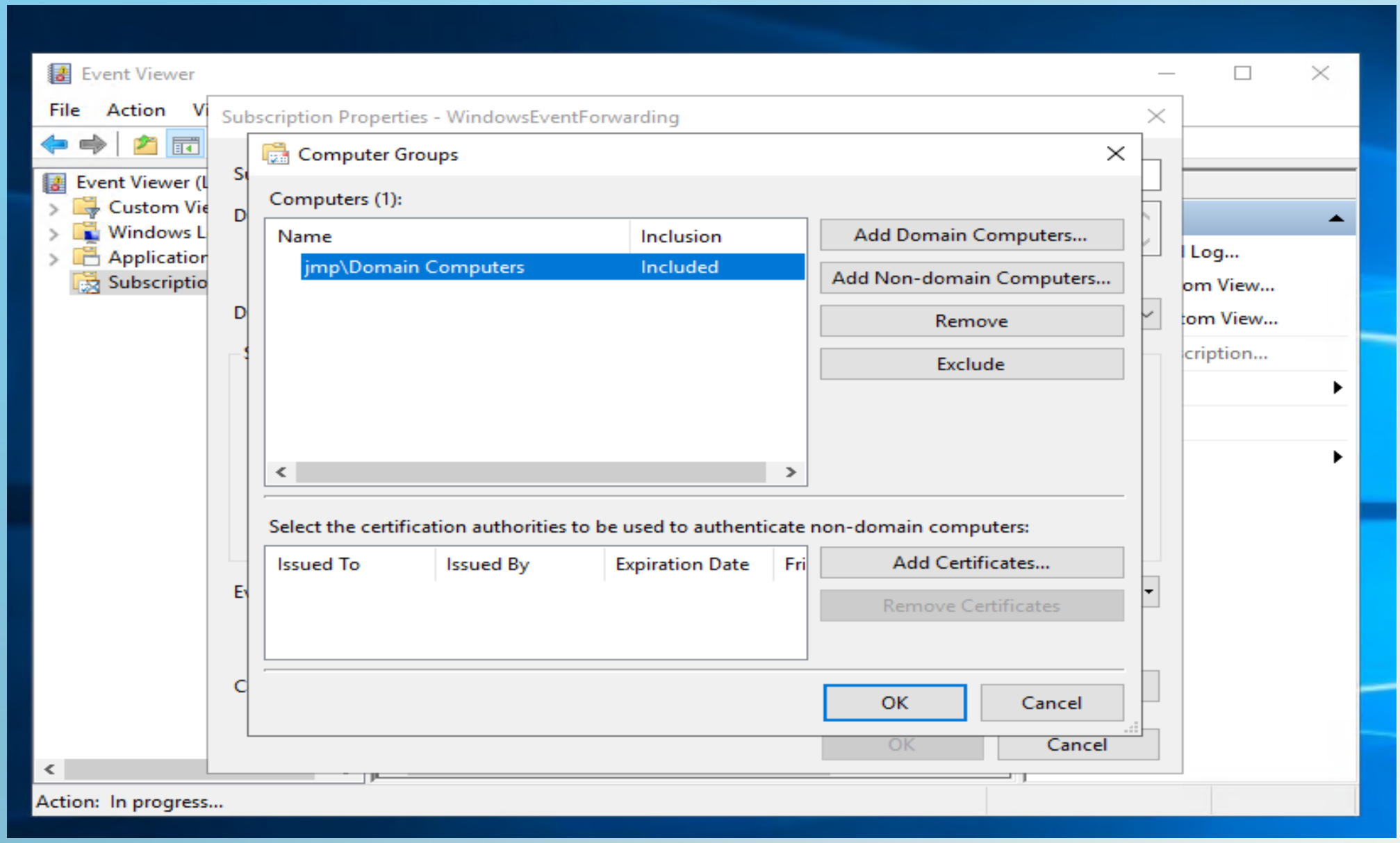
Choisissez "source computer initiated" et clickez sur "Select Computer Groups"



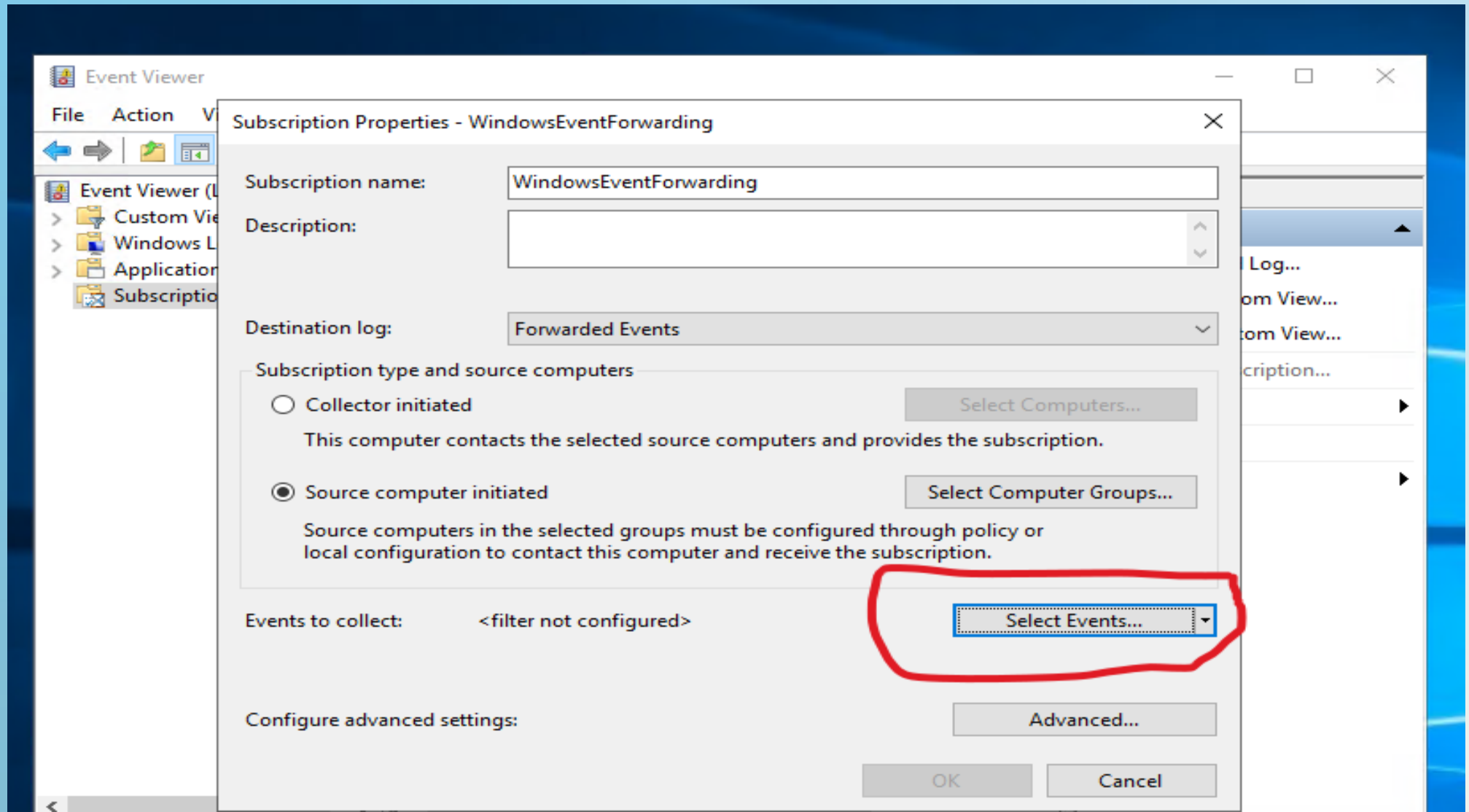
On ajoute le groupe "domain computers" pour que tous les ordinateurs du domaine envoient leurs logs vers le serveur WEC (win-1).



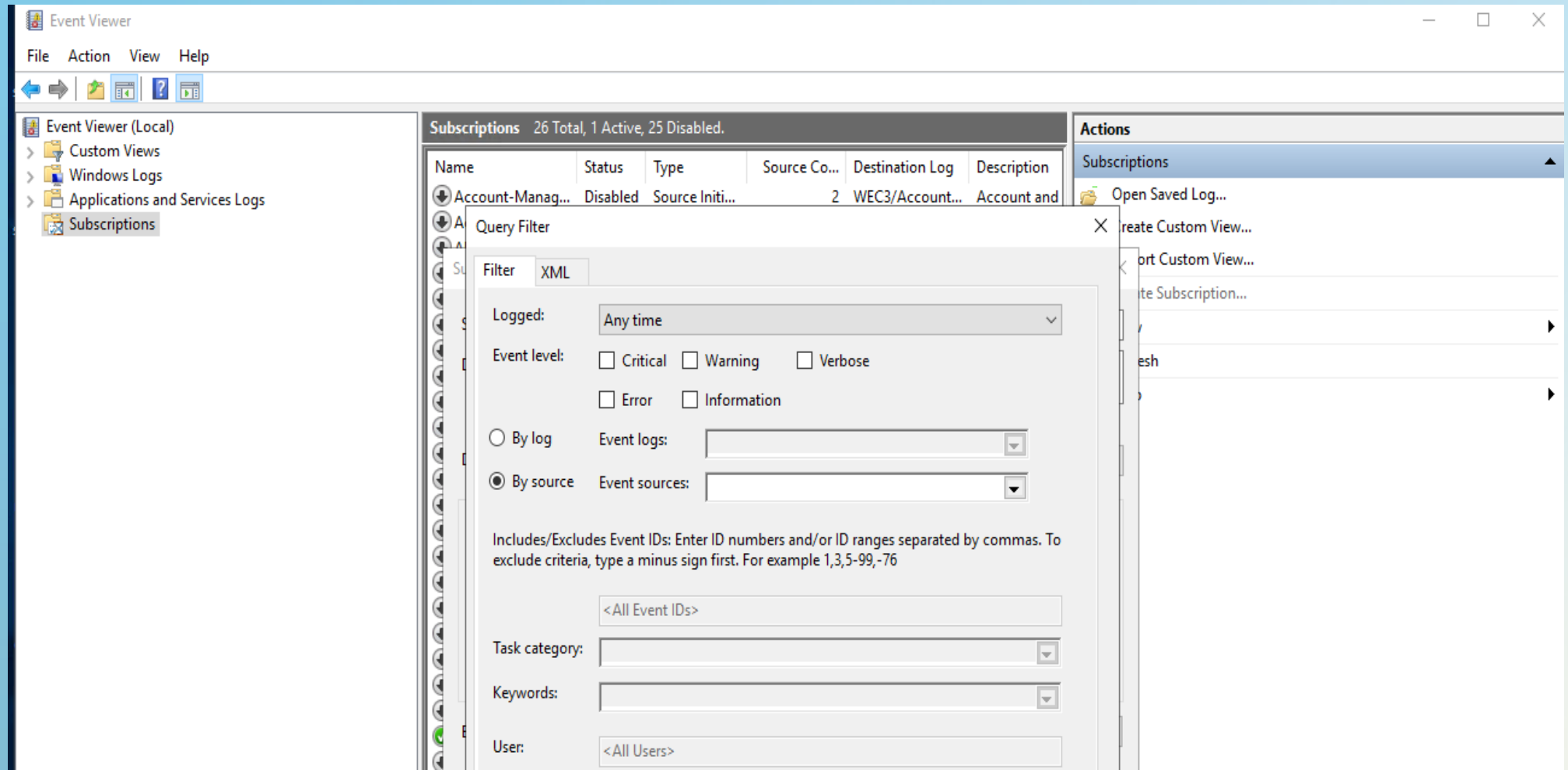

Event Viewer
File
Action
Subscription Properties - EventLogForwarding
Computer Groups
Computers (0):
Name
Inclusion
Add Domain Computers...
Select the certification authorities to be used to authentic
Issued To
Issued By
Expiration Date
OK
Cancel
Select Computer or Group
Select this object type:
Computer or Group
Object Types...
From this location:
Entire Directory
Locations...
Enter the object name to select (examples):
Domain Computers
Check Names
Advanced...
OK
Cancel
Action: In progress...


Event Viewer
File
Action
Subscription Properties - WindowsEventForwarding
Computer Groups
Computers (1):
Name
Inclusion
jmp\Domain Computers
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
Add Certificates...
Remove Certificates
OK
Cancel
Action: In progress...

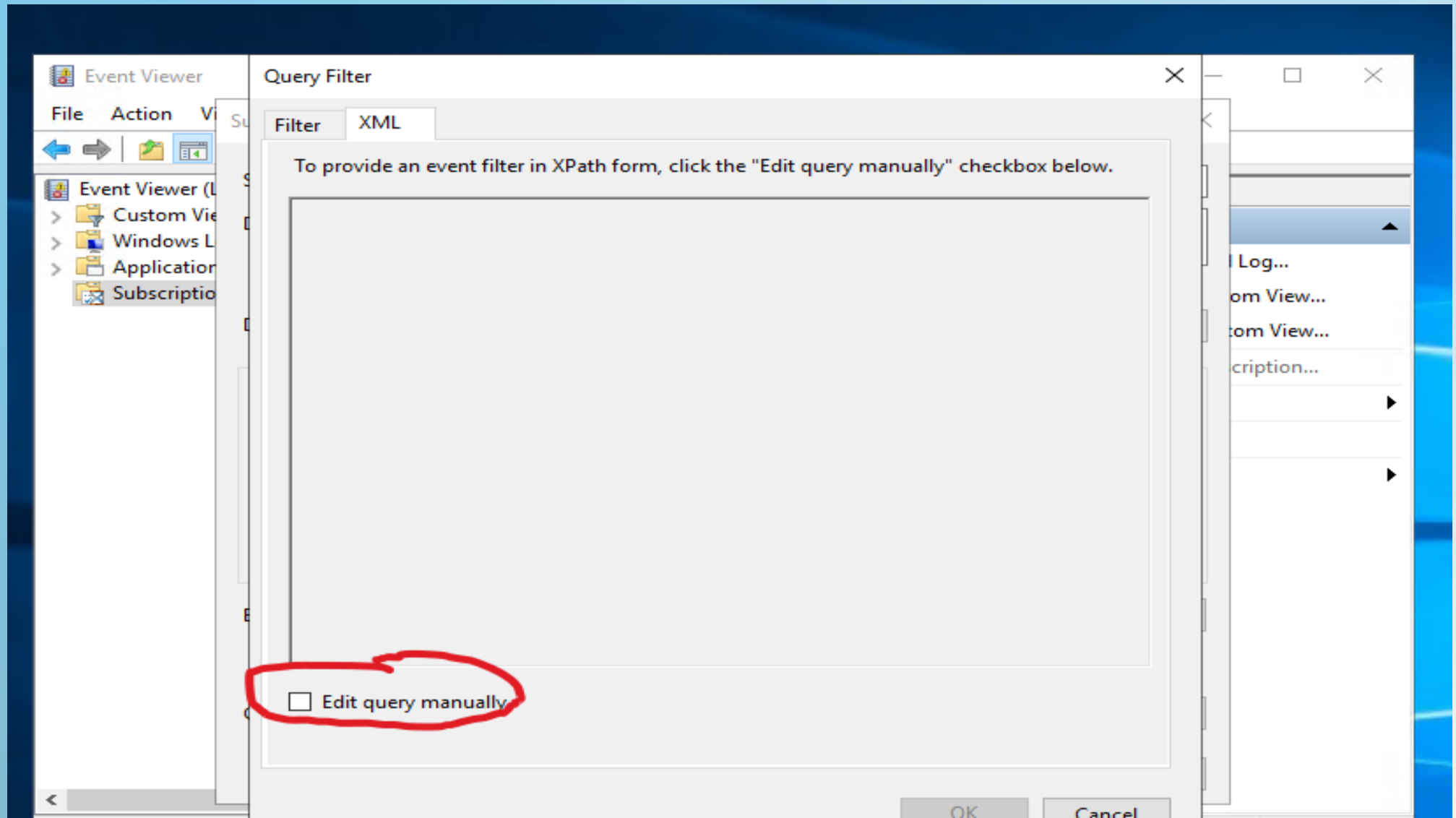
On va sélectionner les évènements à transférer



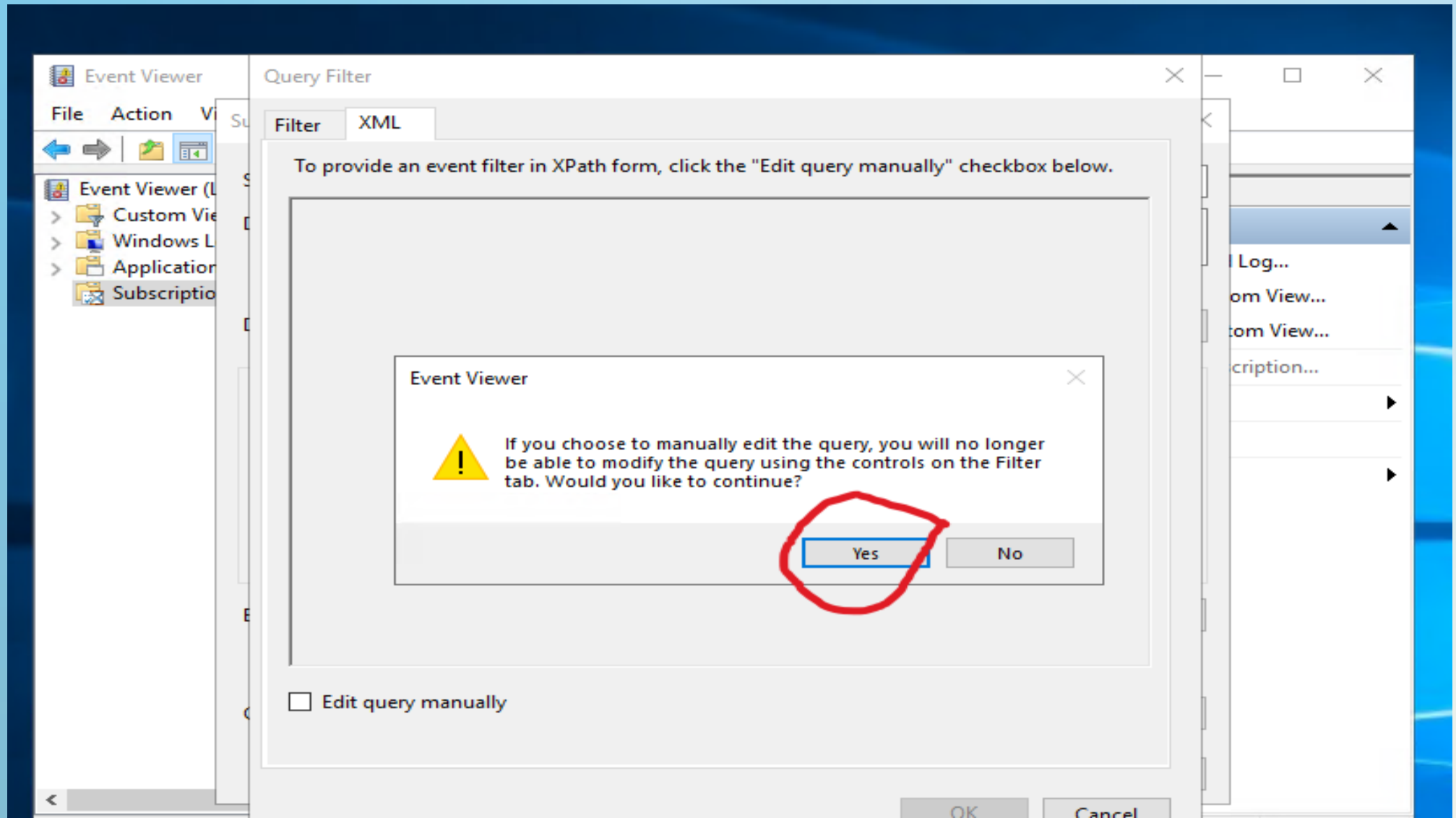
On sélectionne les sources d'évènements à transférer



On configure manuellement la requête XPATH



On configure manuellement la requête XPATH



L'ANSSI recommande cette configuration

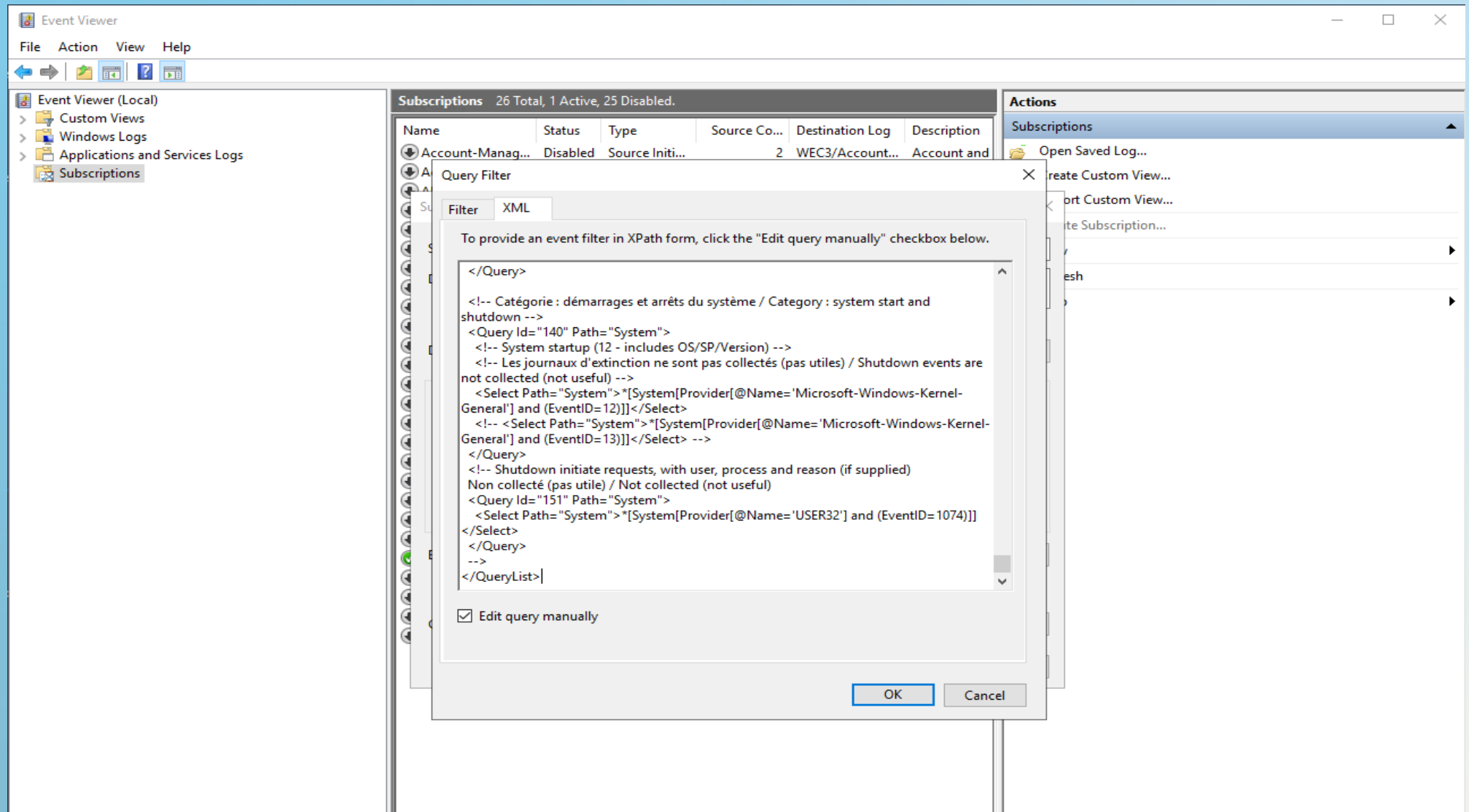
https://raw.githubusercontent.com/ANSSI-FR/guide-journalisation-microsoft/main/Standard_WEC_query.xml

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

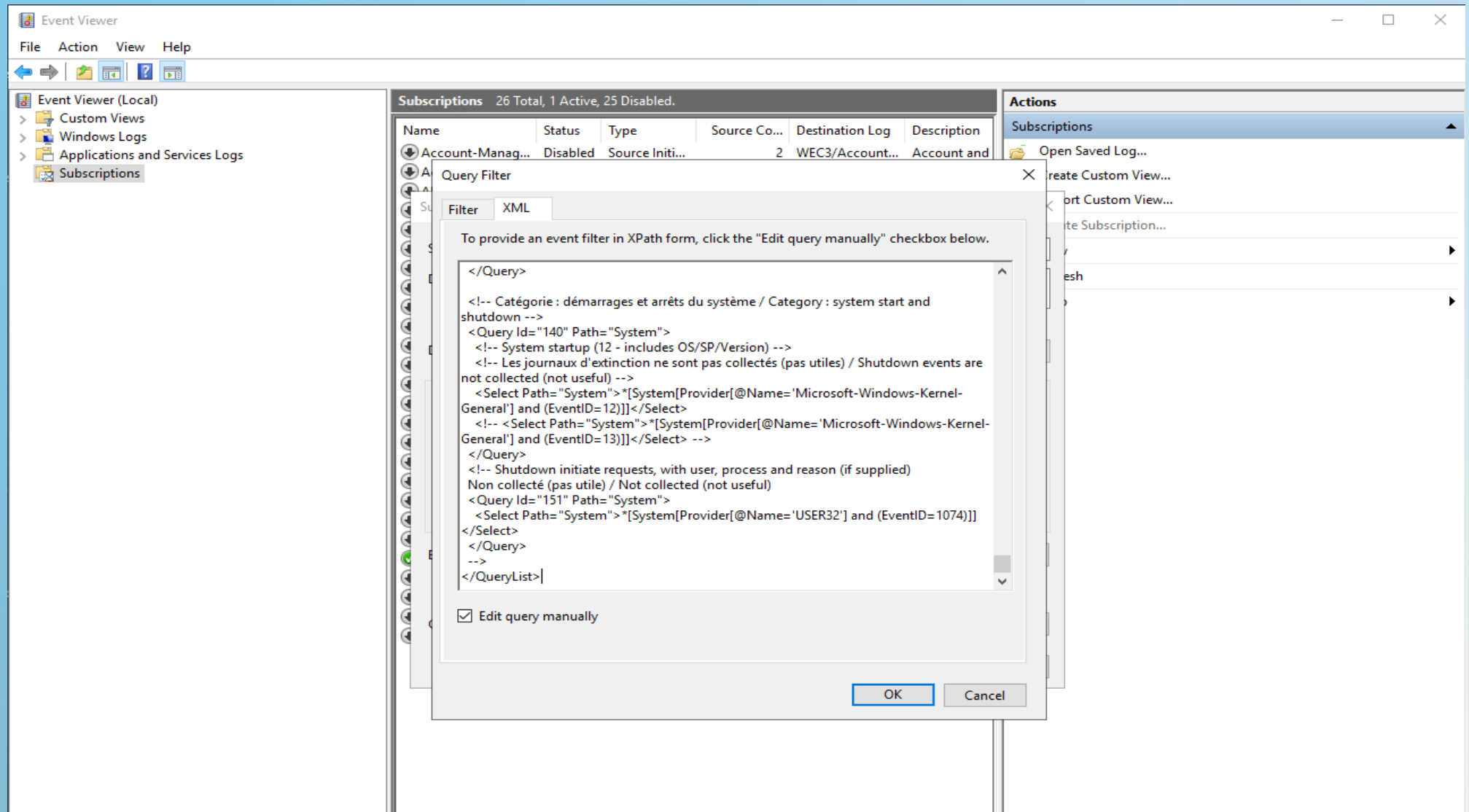
```
<!-- Version 20210902_1600 -->
<QueryList>
  <!--
    Cette requête WEC est basée sur celles proposées par Microsoft dans cet article : / This WEC query is based on what Microsoft proposed in this article :
    https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
    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">
```

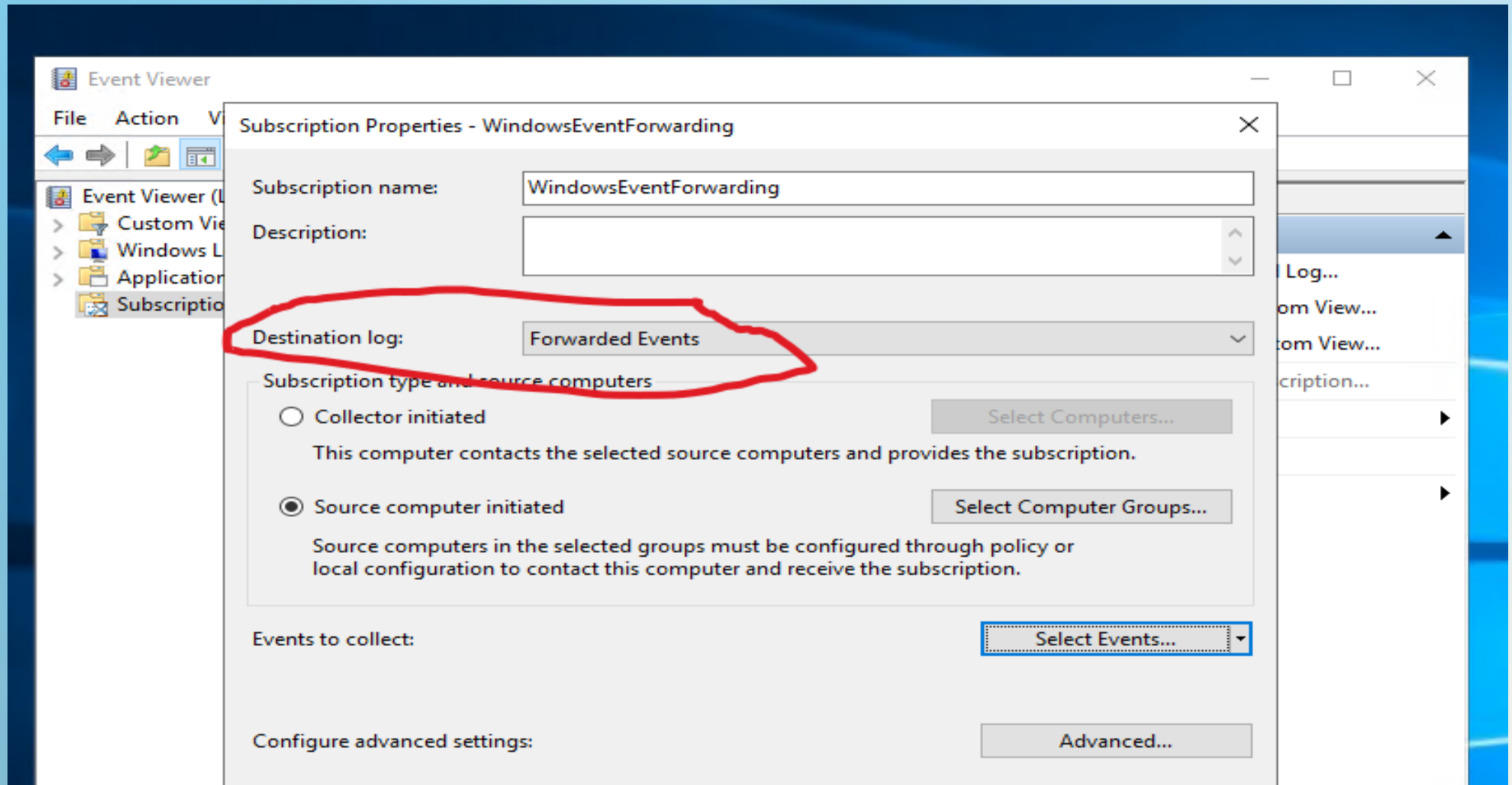
Copiez la configuration recommandée par l'ANSSI



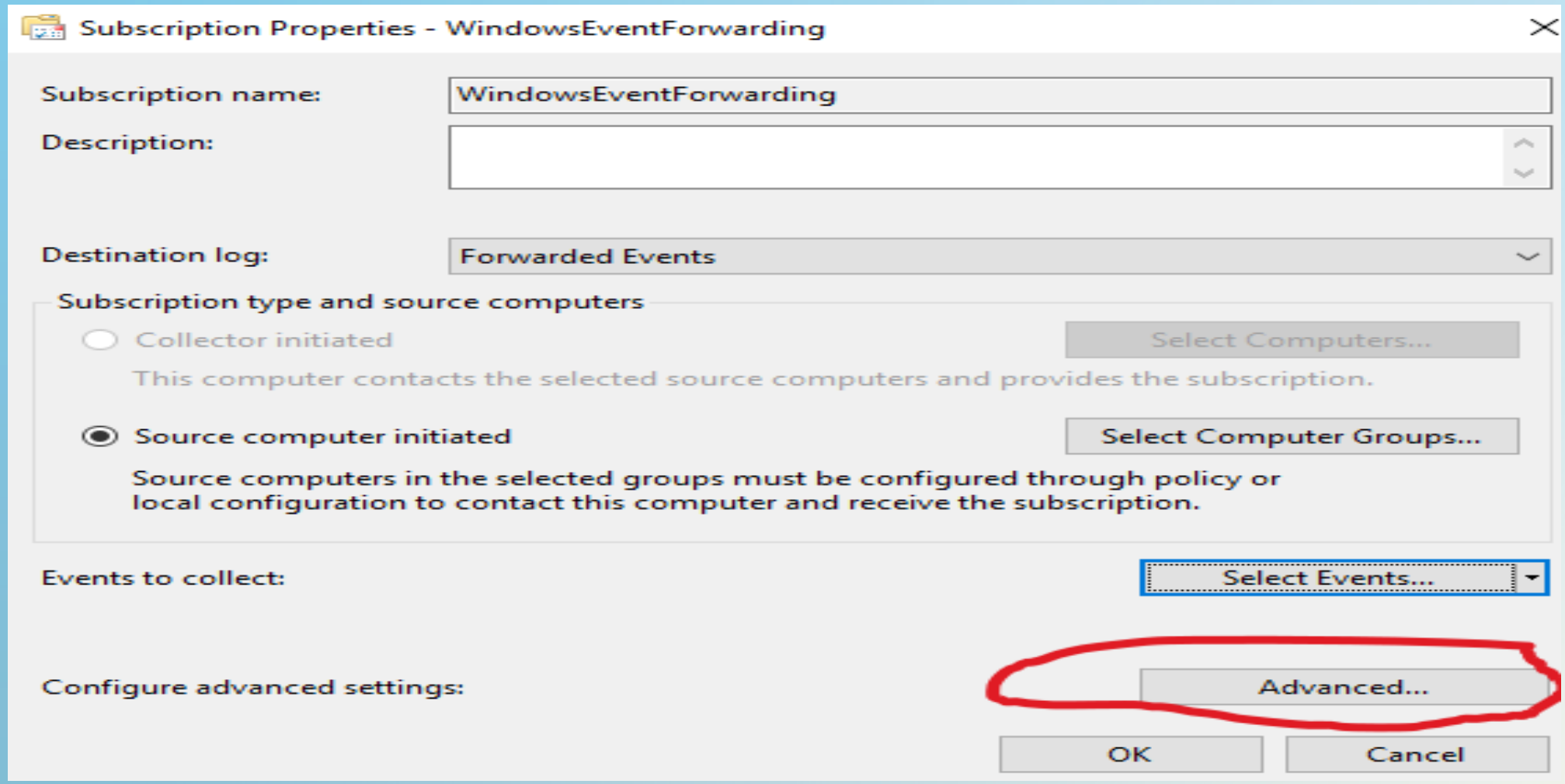
Copiez la configuration recommandée par l'ANSSI



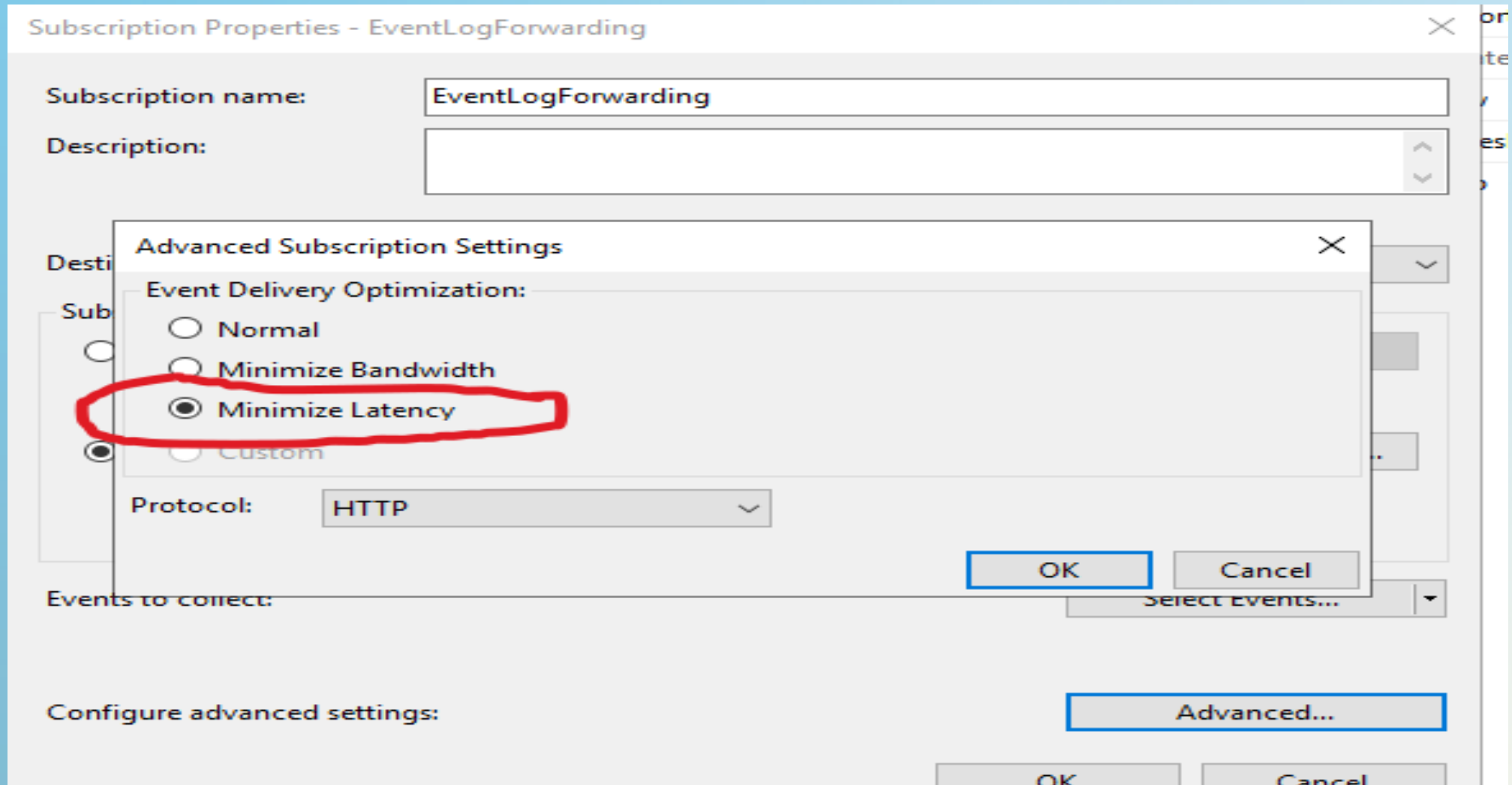
Sélectionnez le canal de destination "ForwardedEvents" (visible dans "eventviewer")



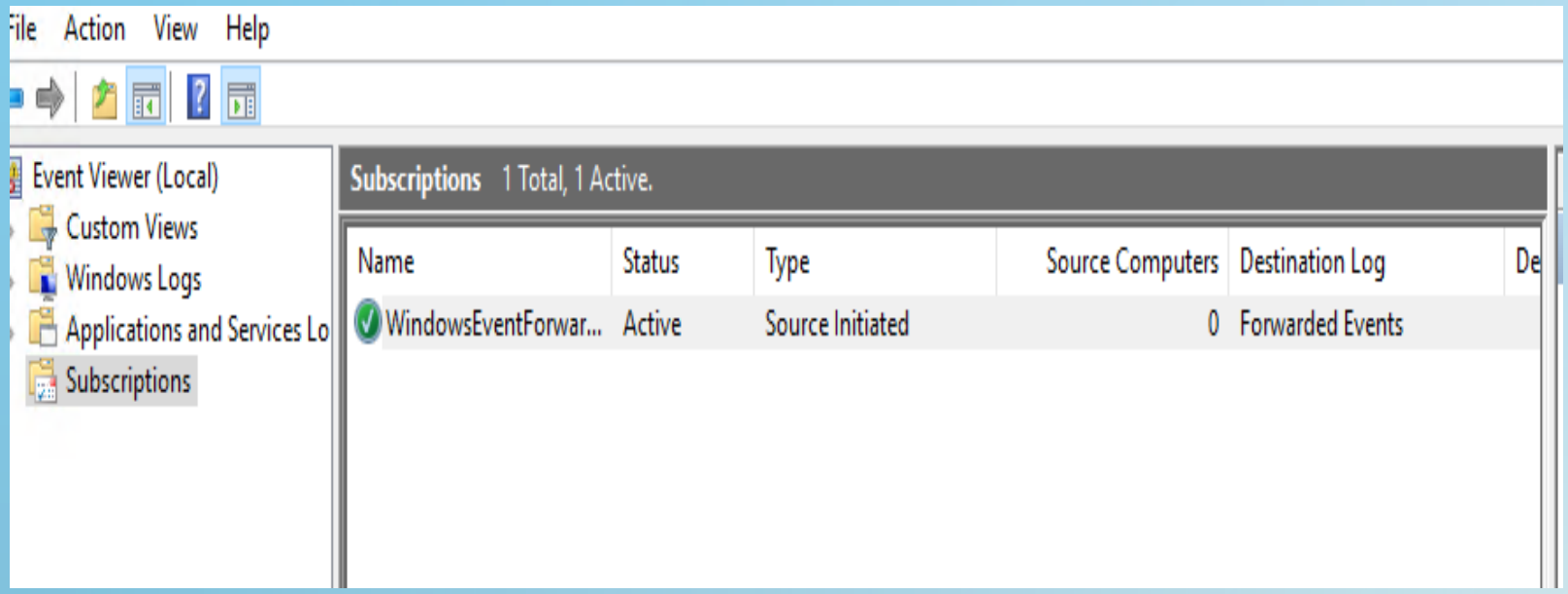
Configuration avancée pour le TP afin de recevoir les évènements au plus vite)



Configuration avancée pour le TP afin de recevoir les évènements au plus vite)



Subscription créée !



Avec windows 2016 et supérieur il faut corriger les permissions sur le protocole WS-Management avec les commandes suivantes sur le serveur WEC (win-1)

```
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)œ
~
```

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

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-
```