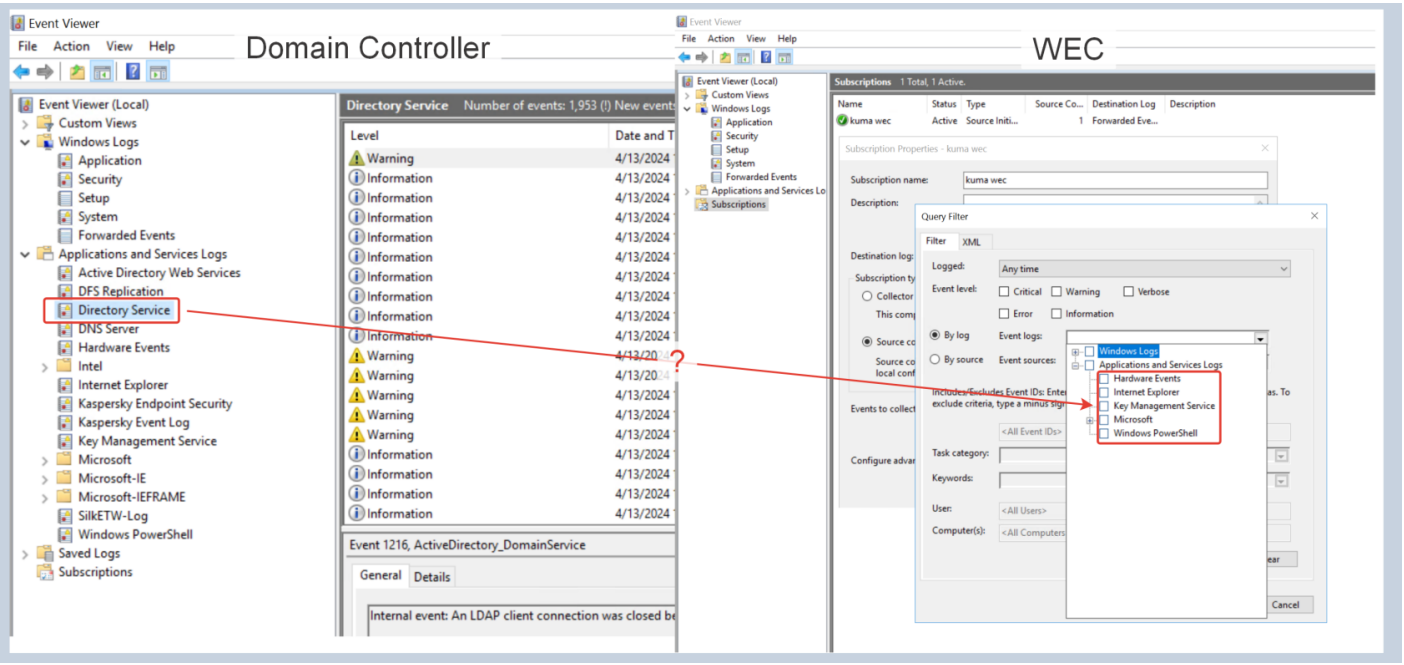
Настройка подписки WEC с использованием XML фильтра

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

При настройке подписки WEC через графический интерфейс не получится выбрать нужные для сбора журналы, если на сервере с WEC не установлены соответствующие роли Windows Server или ПО.

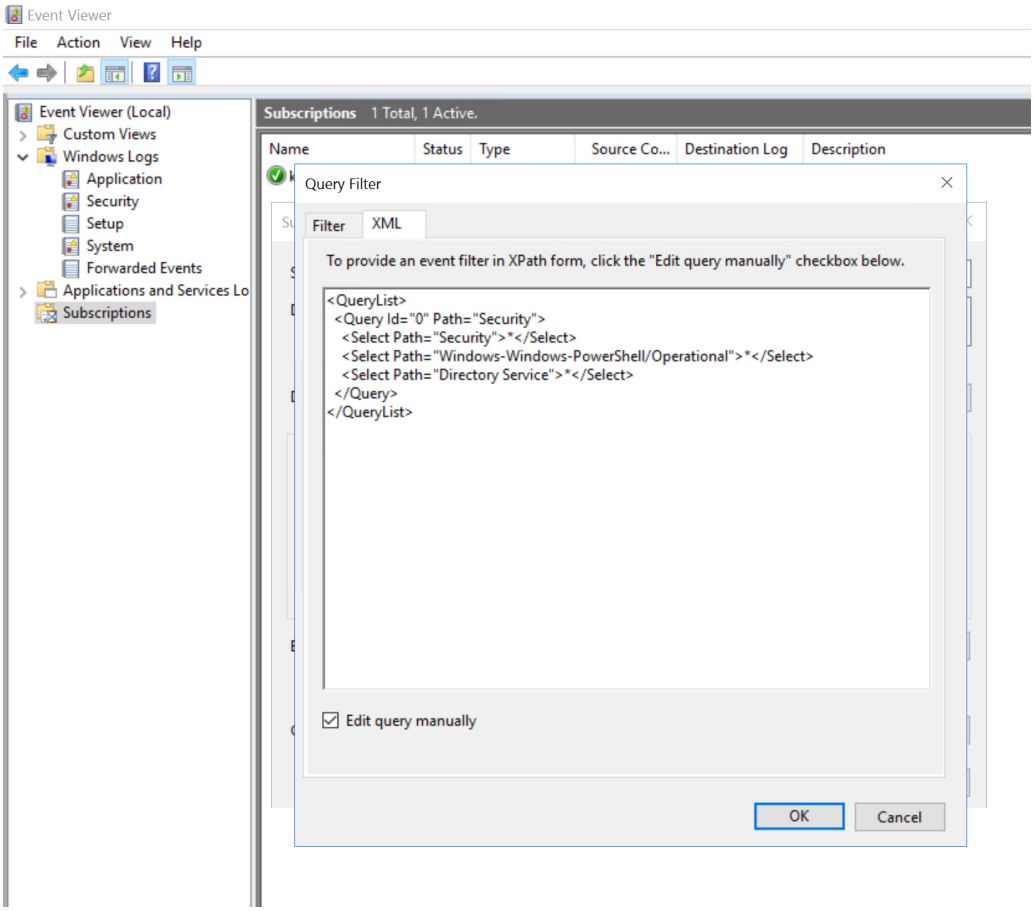


Чтобы выбрать журналы, которые фактически присутствуют на удаленном сервере, но не доступны для выбора на WEC, можно воспользоваться XML фильтром.

Ниже приведен пример XML фильтра для сбора событий из стандартного журнала Security, а также из журнала, который присущ только контроллеру домена - Directory Service.

```
<QueryList>
  <Query Id="0" Path="Security">
```

```
    <Select Path="Security">*</Select>
    <Select Path="Windows-Windows-PowerShell/Operational">*</Select>
    <Select Path="Directory Service">*</Select>
  </Query>
</QueryList>
```



В результате данной настройки WEC начнет собирать события из журнала контроллера домена Directory Service.

Аналогичном образом можно настроить сбор событий из других специфических журналов, а также использовать XML фильтры, если требуется выполнить настройку большого количества подписок WEC.

Revision #3
Created 13 April 2024 10:08:49 by kmssrv
Updated 18 December 2024 10:16:52 by Boris Rzr