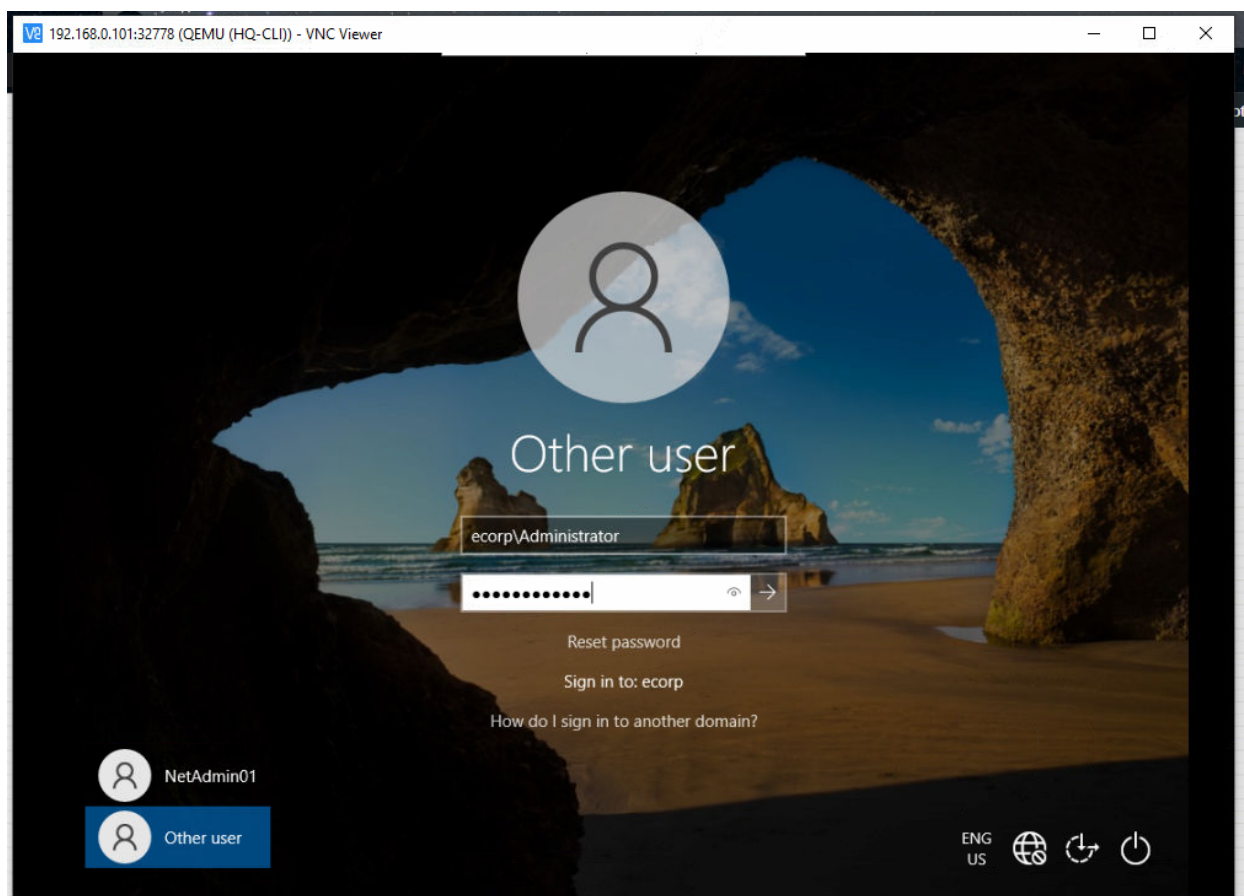




Receba os eventos de log de segurança

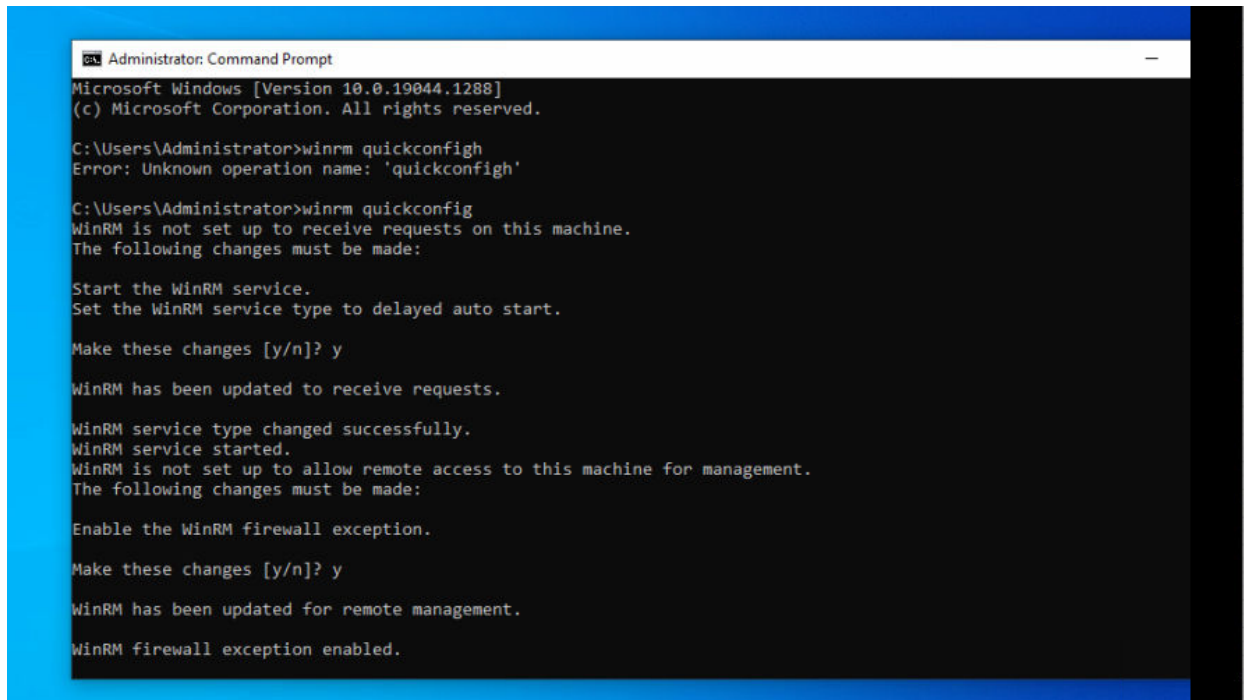
Logue no usuario de administrador



winrm quickconfig

Esse comando ira enviar da minha maquina de origem os logs para minha maquina coletora(que no caso é meu windows server)

Esse winrm seria um serviço de acesso remoto que permite o servidor acessar os logs



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>winrm quickconfig
Error: Unknown operation name: 'quickconfig'

C:\Users\Administrator>winrm quickconfig
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Start the WinRM service.
Set the WinRM service type to delayed auto start.
Make these changes [y/n]? y

WinRM has been updated to receive requests.

WinRM service type changed successfully.
WinRM service started.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

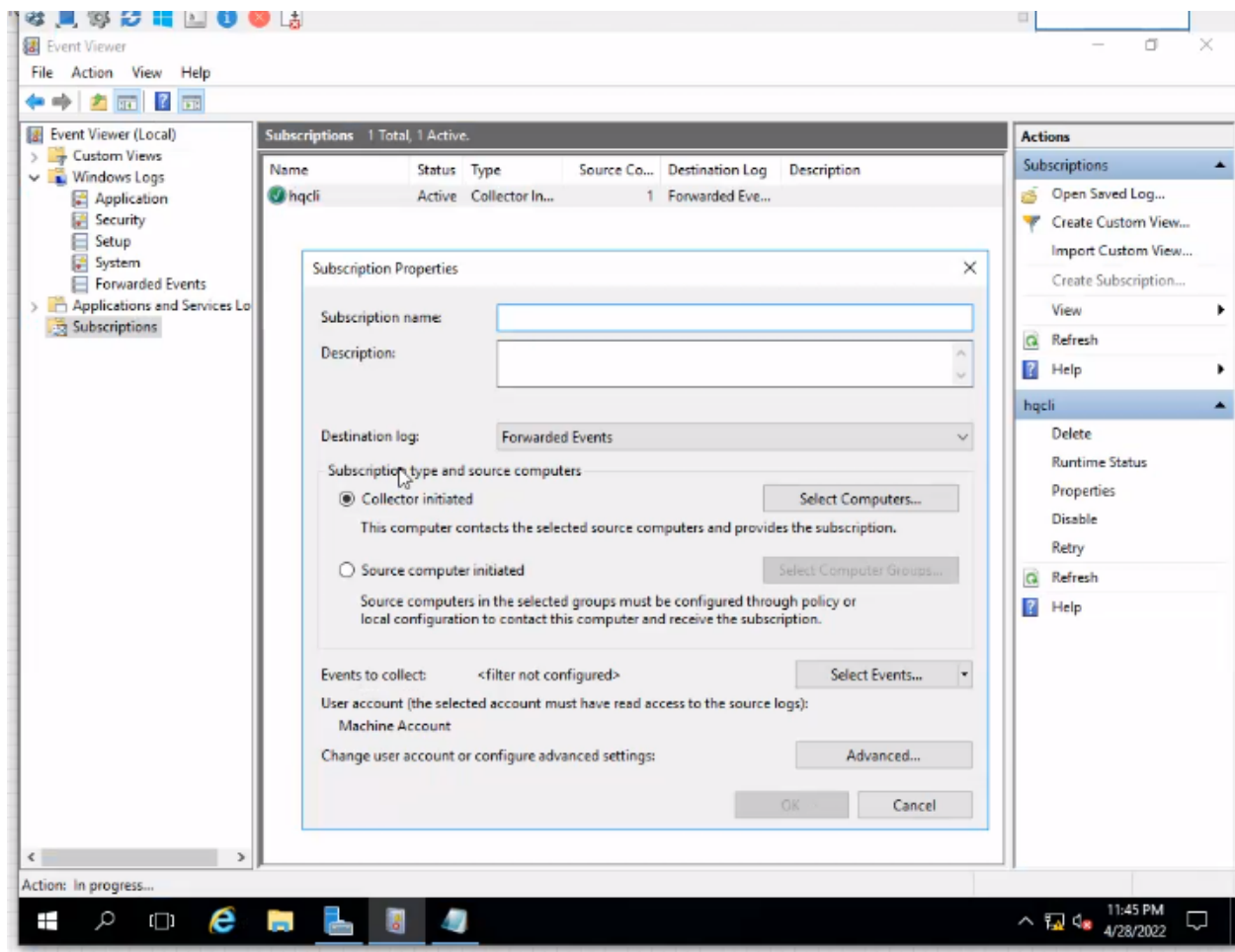
Enable the WinRM firewall exception.
Make these changes [y/n]? y

WinRM has been updated for remote management.
WinRM firewall exception enabled.
```

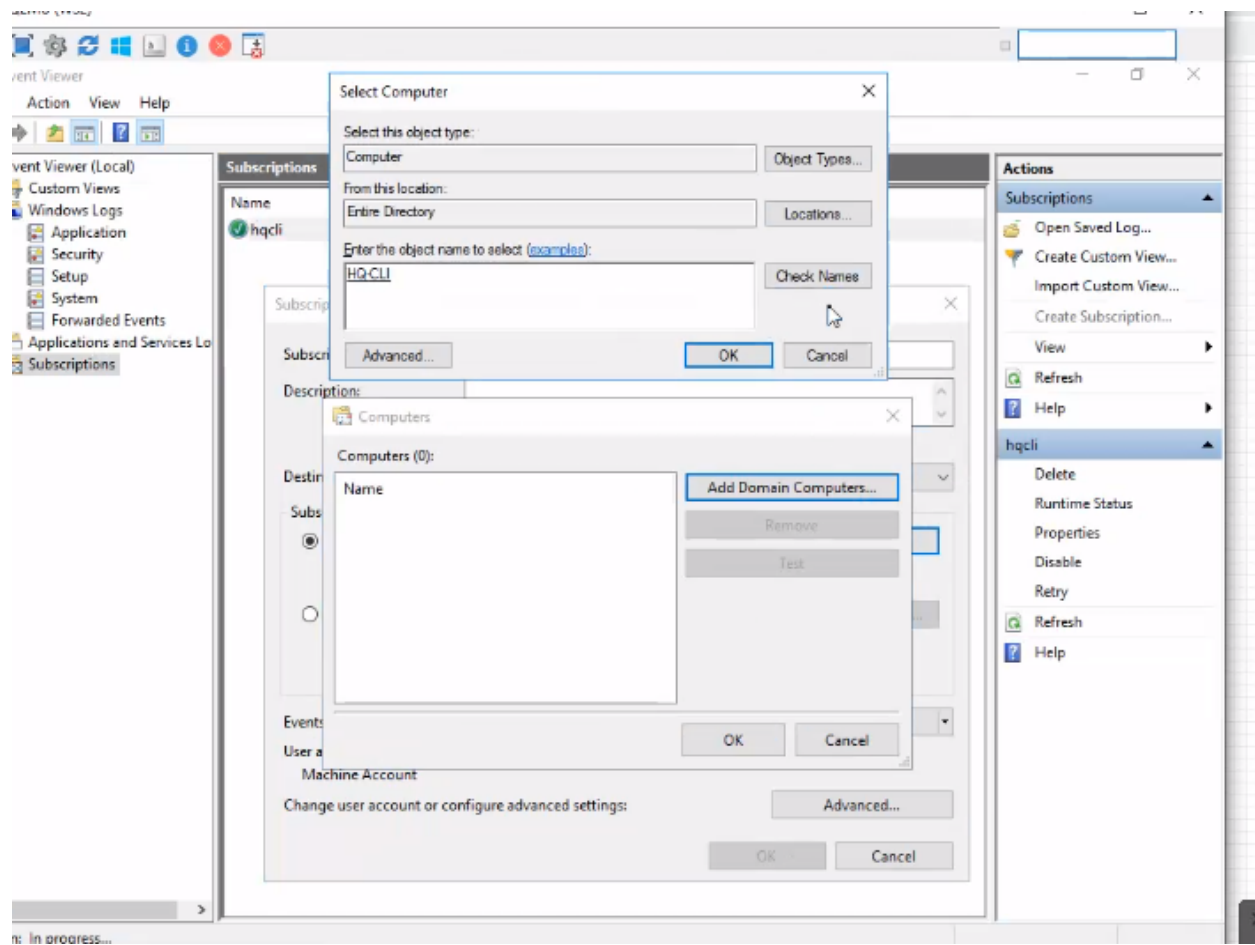
para entrar nesse event viewer e so digitar o nome dele no iniciari

Event viewer

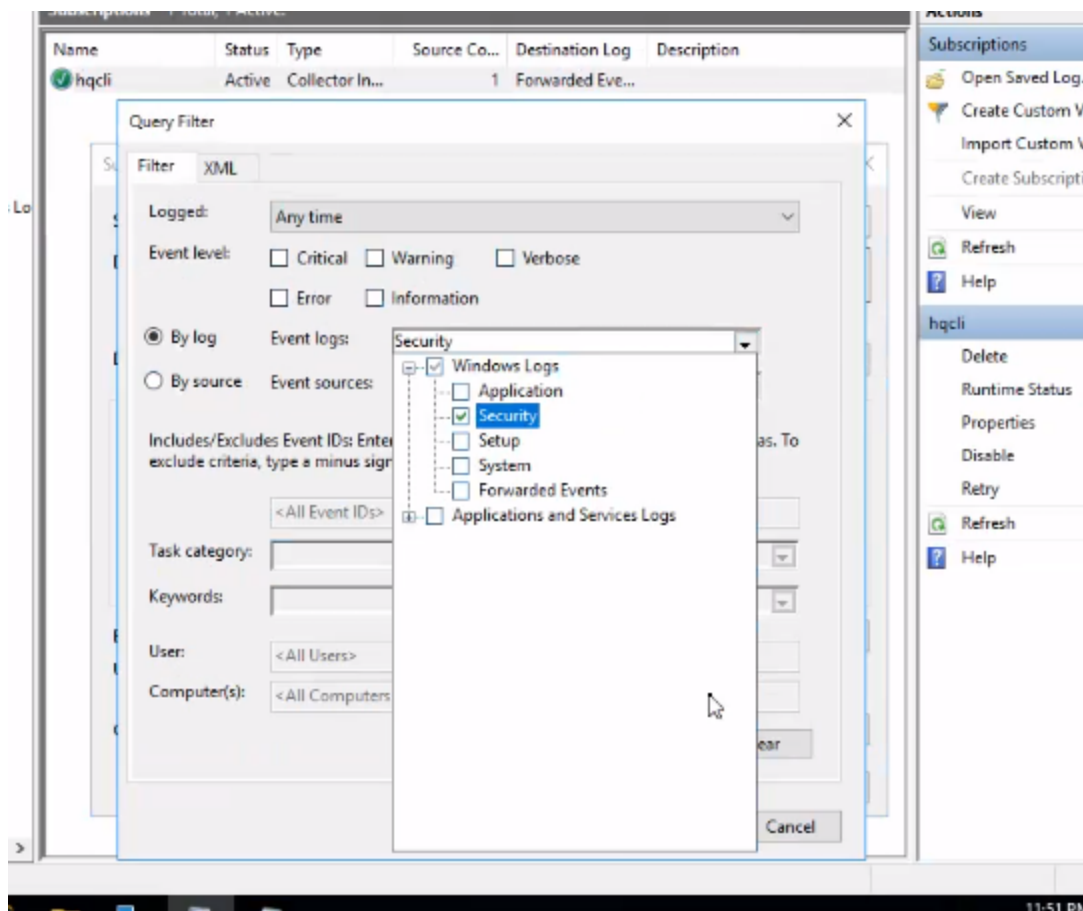
Vai clicar em, create subscription



Iremos em select computer, para adicionar o computador de origem



Depois iremos em select event, e selecionaremos os eventos



Ai depois fomos em advanced para adicionar a conta do usuario que tem acesso a esses logs(no caso o administrador)

