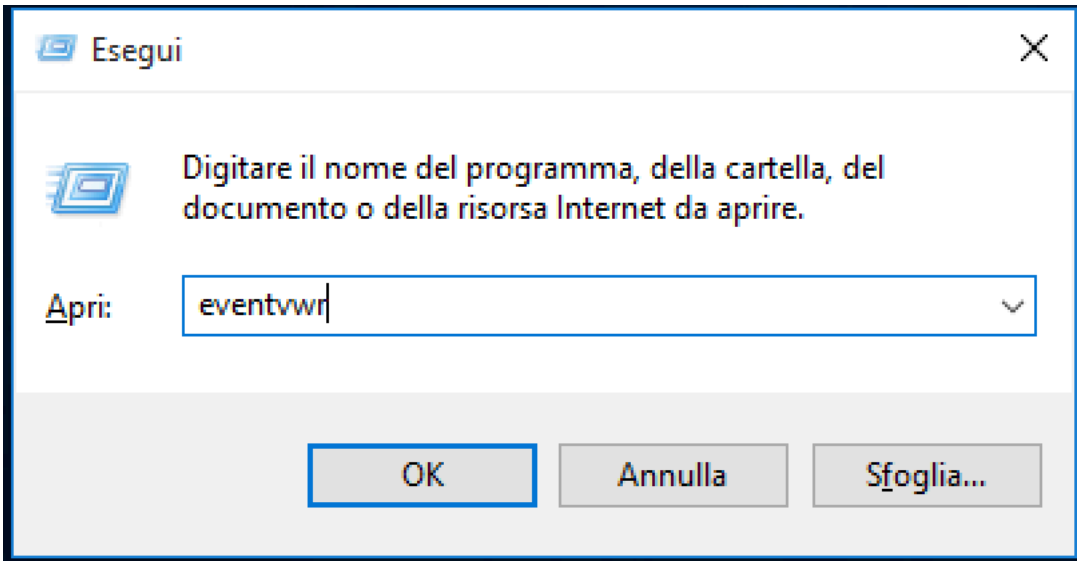
S9L4

Obiettivo: Configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows

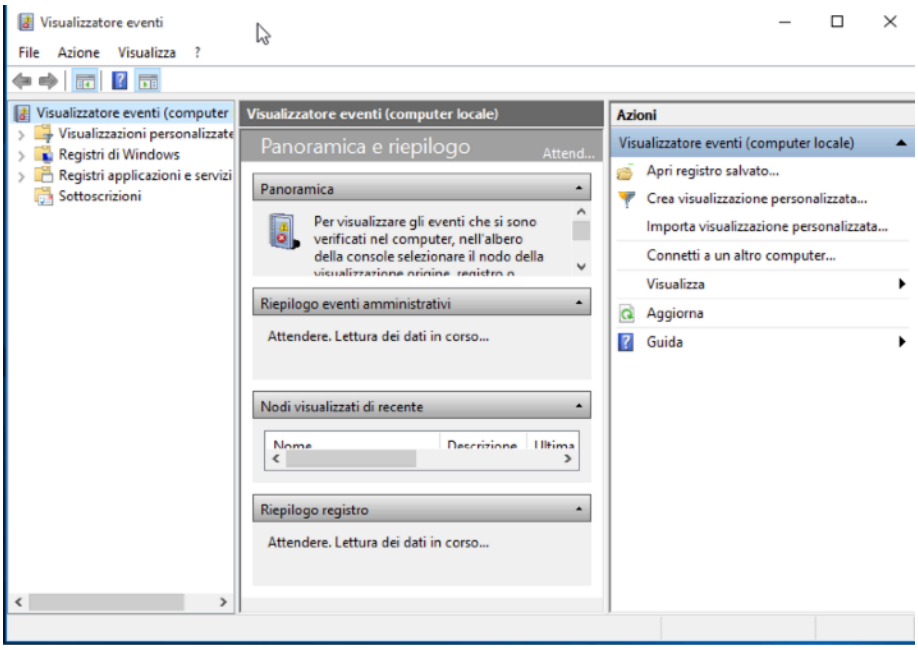
Step1.

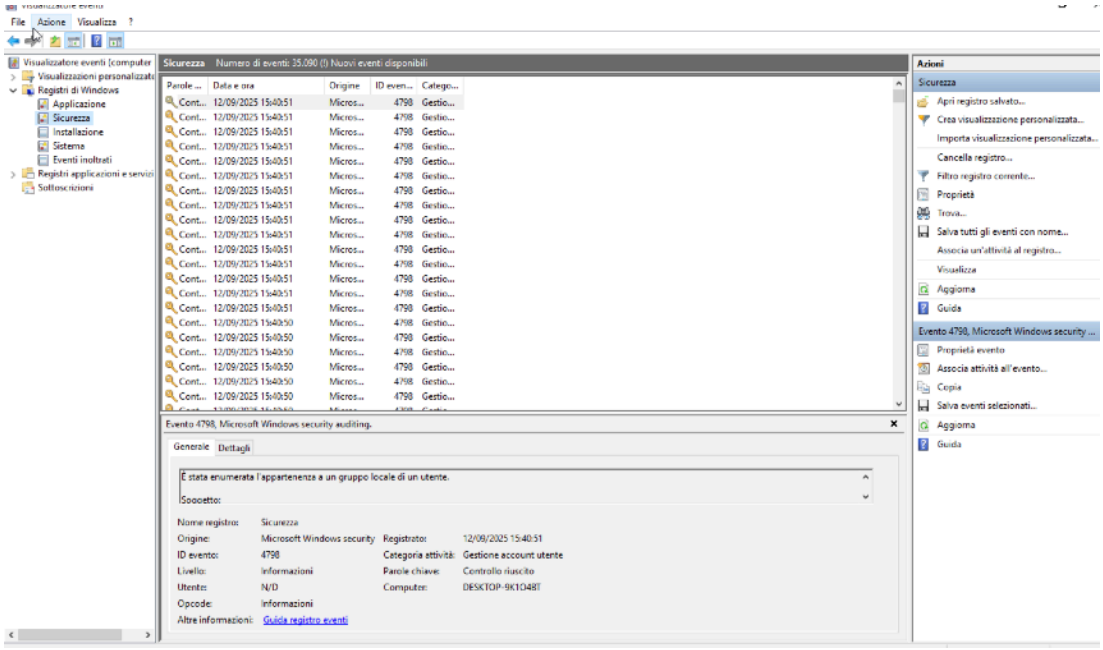
Avvio la macchina windows e con il comando win+R apro la finestra Esegui, dopo di che inserisco “eventvwr”



Step2.

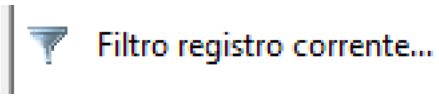
Si apre la pagina degli eventi, vado su registri windows e sicurezza



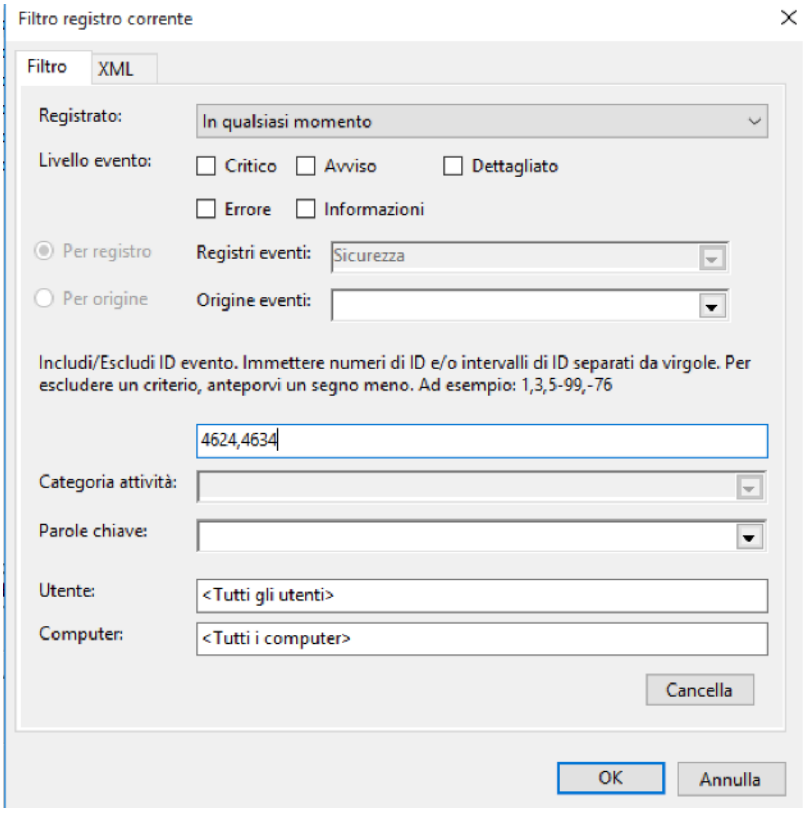


Step3

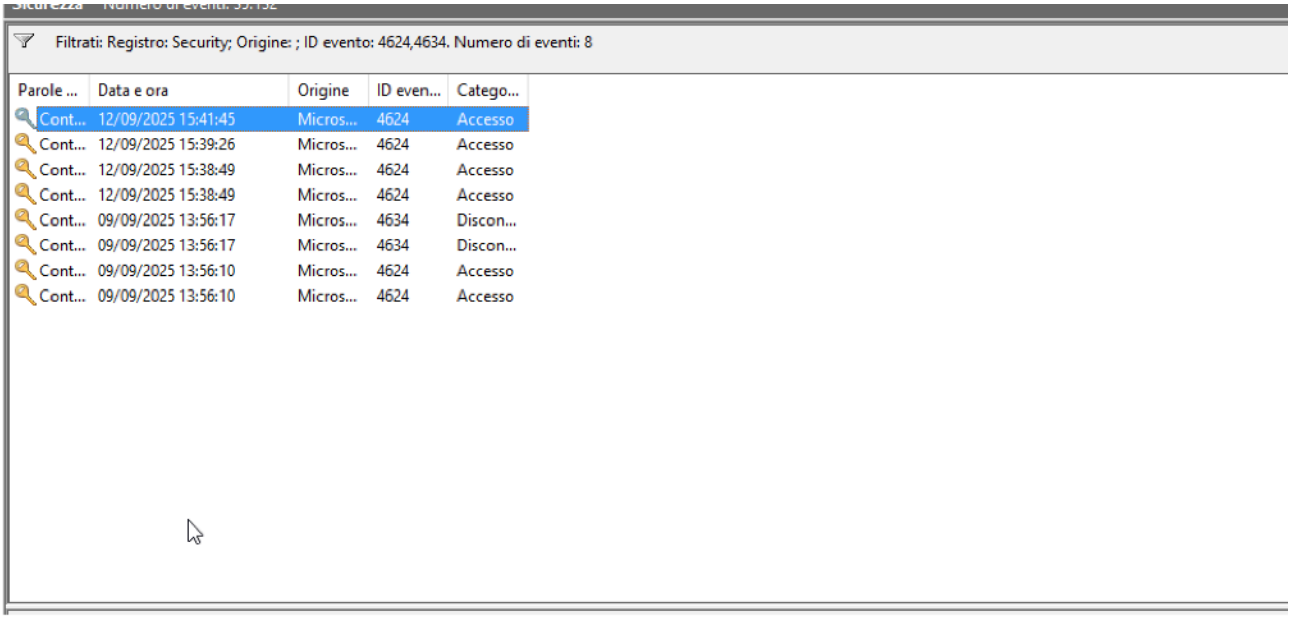
Ora per visualizzare e filtrare i Log dei login/logout vado su “filtro registro corrente” in alto a destra



Inserisco l ID che identifica i login e logout ovvero 4624(login) 4634(logout)



Premo ok e posso vedere che sono stati filtrati i Log richiesti



Cliccando su uno di questi si possono avere più informazioni