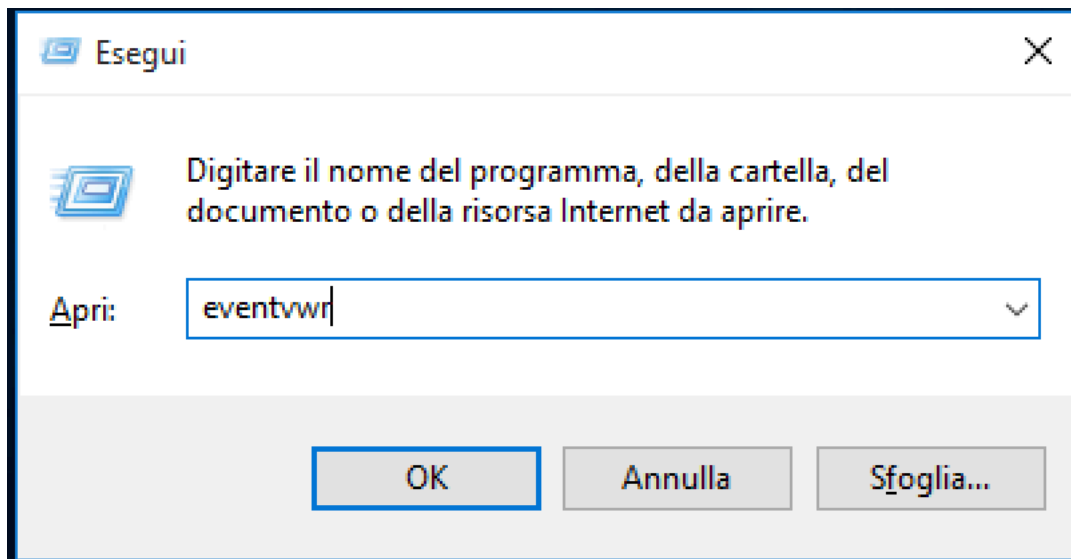


S9L4

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

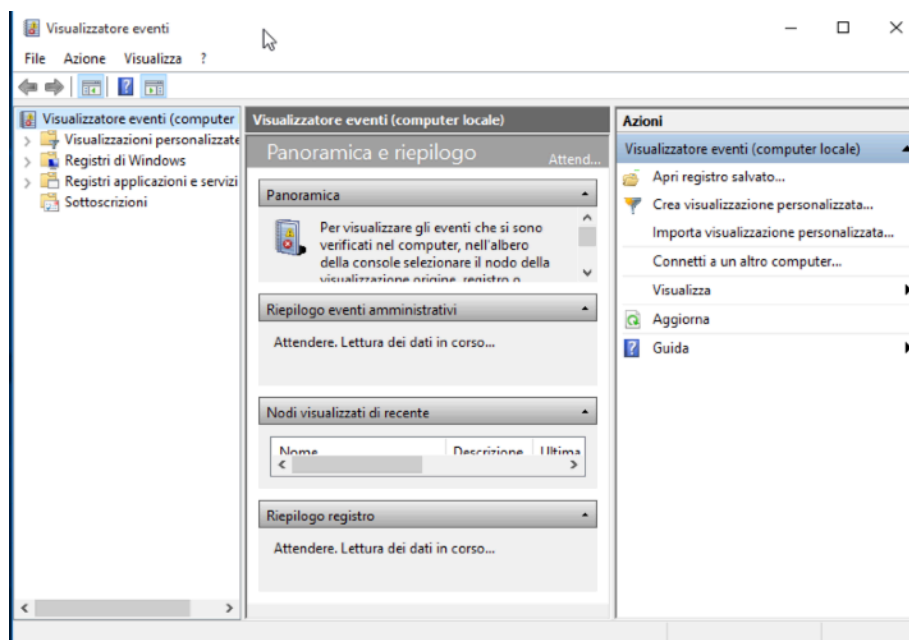
Step1.

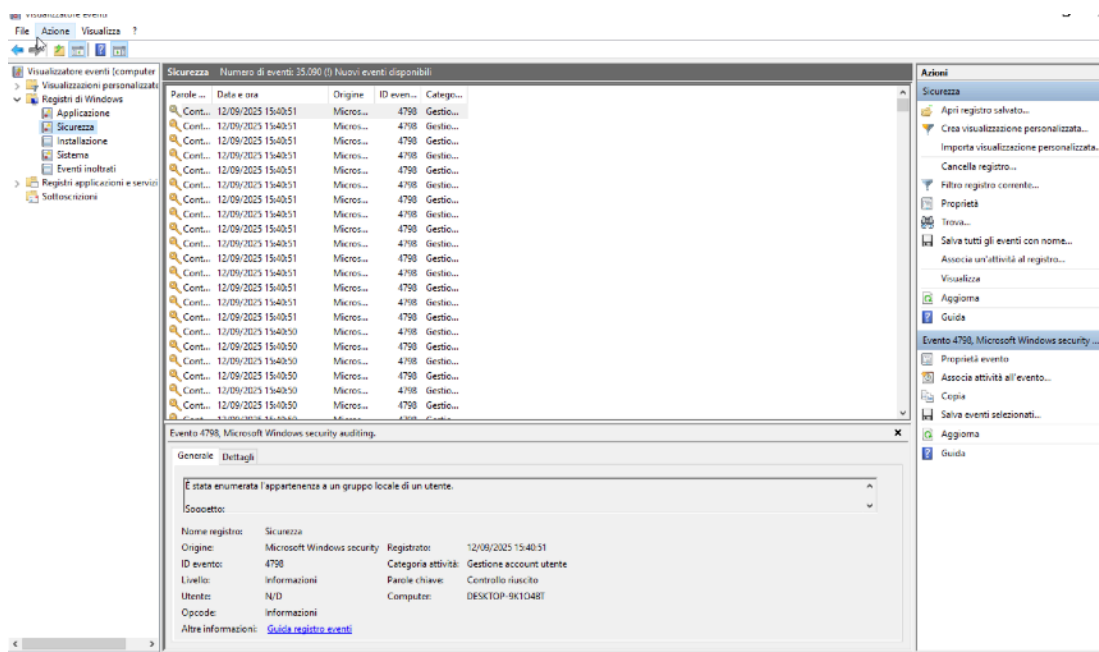
Avvio la macchina windows e con il comando win+R apro la finestra Esegui, dopo di che inserisco “eventvwr”



Step2.

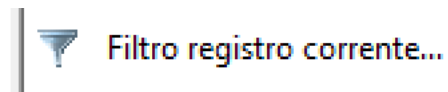
Si apre la pagina degli eventi, vado su registri windows e sicurezza





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)

Filtro registro corrente

Filtro XML

Registrato: In qualsiasi momento

Livello evento: ☐ Critico ☐ Avviso ☐ Dettagliato
☐ Errore ☐ Informazioni

☒ Per registro Registri eventi: Sicurezza

☐ Per origine Origine eventi:

Includi/Escludi ID evento. Immettere numeri di ID e/o intervalli di ID separati da virgole. Per escludere un criterio, anteporvi un segno meno. Ad esempio: 1,3,5-99,-76

4624,4634

Categoria attività:

Parole chiave:

Utente: <Tutti gli utenti>

Computer: <Tutti i computer>

Cancella

OK Annulla

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

Sicurezza - Numero di eventi: 55/152

Filtrati: Registro: Security; Origine: ; ID evento: 4624,4634. Numero di eventi: 8

Parole ...	Data e ora	Origine	ID even...	Catego...
Cont...	12/09/2025 15:41:45	Micros...	4624	Accesso
Cont...	12/09/2025 15:39:26	Micros...	4624	Accesso
Cont...	12/09/2025 15:38:49	Micros...	4624	Accesso
Cont...	12/09/2025 15:38:49	Micros...	4624	Accesso
Cont...	09/09/2025 13:56:17	Micros...	4634	Discon...
Cont...	09/09/2025 13:56:17	Micros...	4634	Discon...
Cont...	09/09/2025 13:56:10	Micros...	4624	Accesso
Cont...	09/09/2025 13:56:10	Micros...	4624	Accesso

Cliccando su uno di questi si possono avere più informazioni

Proprietà evento - Evento 4634, Microsoft Windows security auditing.

Generale Dettagli

Un account è stato disconnesso.

Soggetto:

ID sicurezza:	Window Manager\DWM-3
Nome account:	DWM-3
Dominio account:	Window Manager
ID accesso:	0x374973

Nome registro: Sicurezza

Origine:	Microsoft Windows security	Registrato:	09/09/2025 13:56:17
ID evento:	4634	Categoria attività:	Disconnessione
Livello:	Informazioni	Parole chiave:	Controllo riuscito
Utente:	N/D	Computer:	DESKTOP-9K1O4BT
Opcode:	Informazioni		

Altre informazioni: [Guida registro eventi](#)