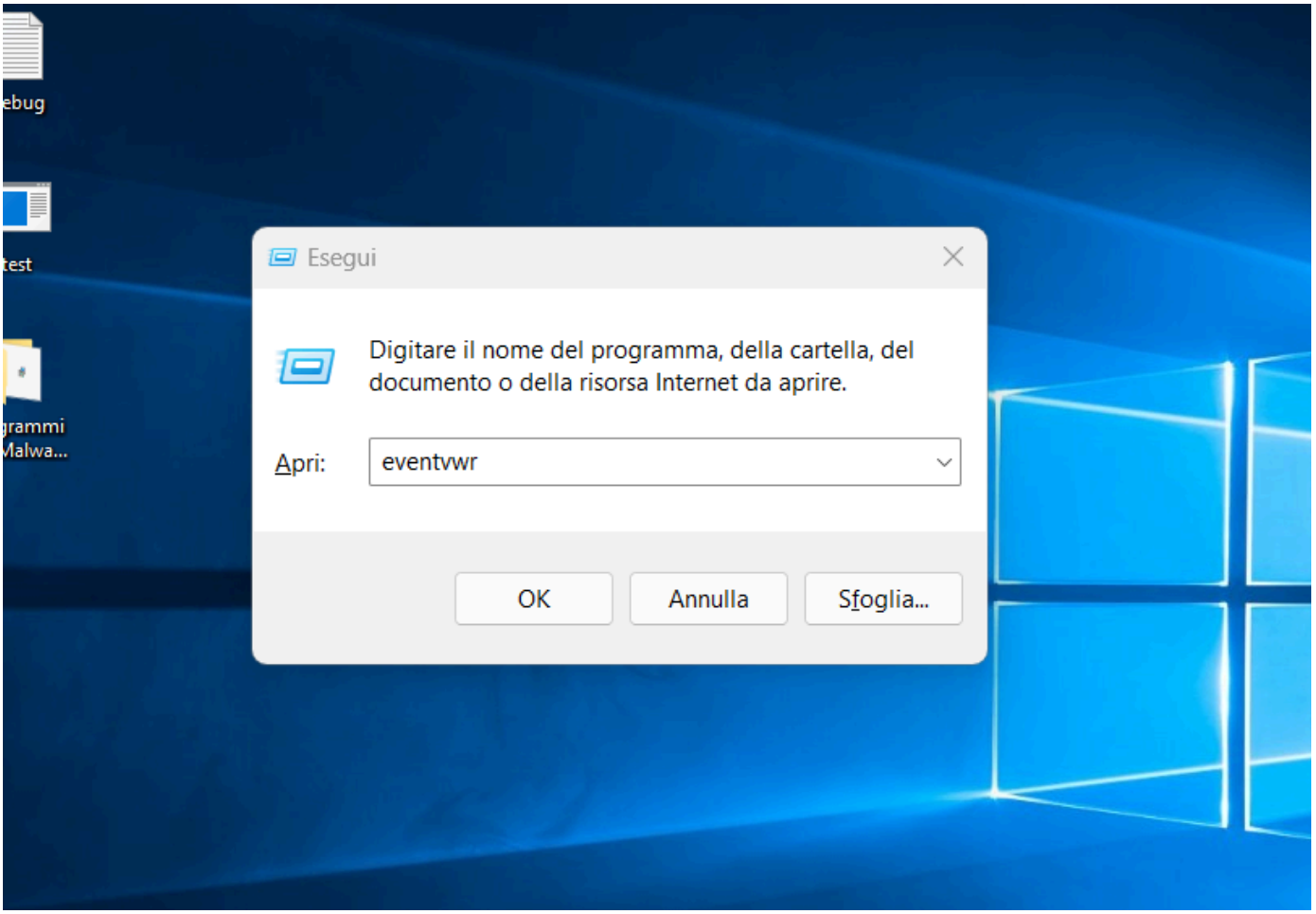
Entrare nei registri Windows

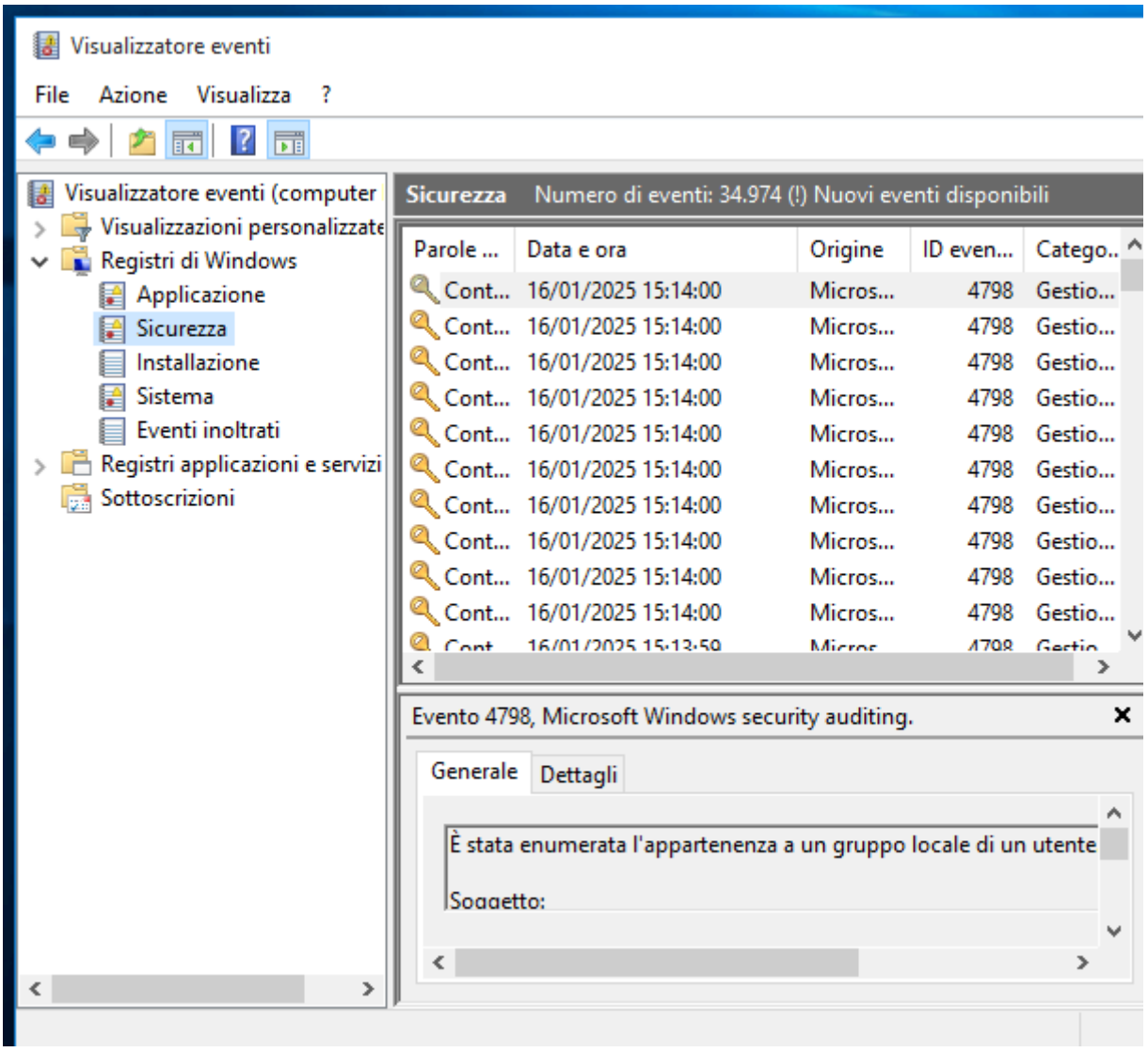
Entrare nei registri Windows

In questa breve guida spiegherò come accedere ai registri di windows per visualizzarne tutti i log.

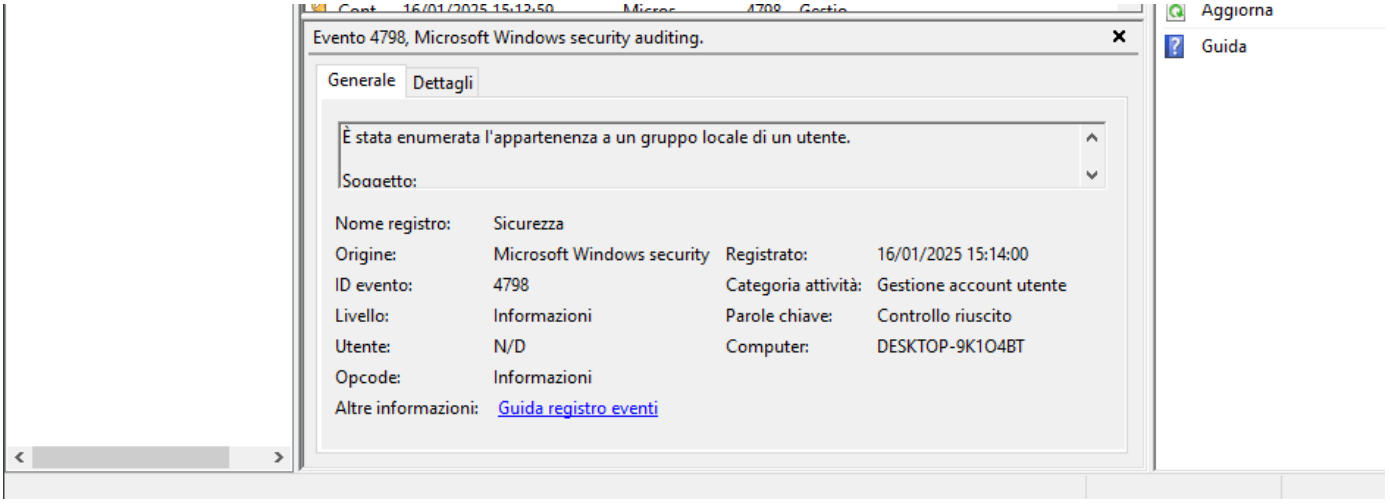
- Step 1: Premere il tasto Windows + R per aprire la barra dell'esegui.
- Step 2: Digitare `eventvwr` e mandare invio.

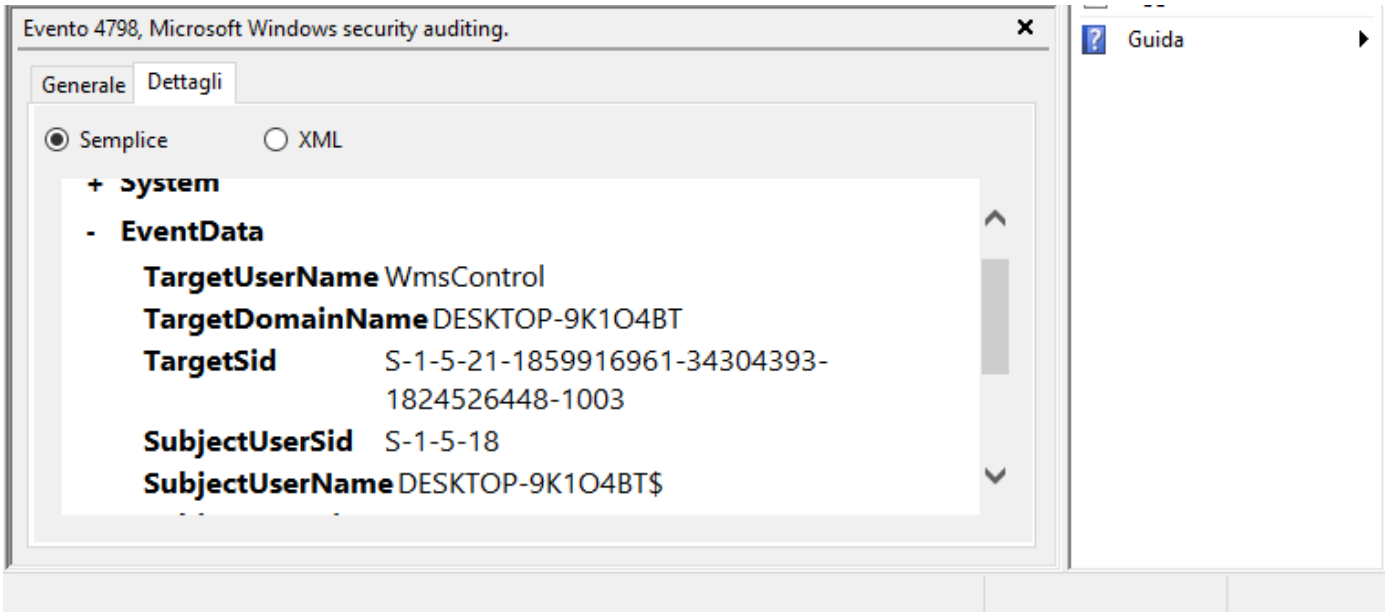


- Step 3: Nella colonna di sinistra comparirà "Registri di Windows".
- Step 4: Dopodichè sempre a sinistra apparirà la voce "sicurezza".



Con un seplice doppio click sull'evento avremo accesso a tutte le informazioni che ci servono.





Qui incollo il risultato completo:
+System

-Provider

[Name] Microsoft-Windows-Security-Auditing
[Guid] {54849625-5478-4994-A5BA-3E3B0328C30D}

EventID 4798

Version 0

Level 0

Task 13824

Opcode 0

Keywords 0x8020000000000000

-imeCreated

[SystemTime] 2025-01-16T14:14:00.290581200Z

EventRecordID 1007573

-Correlation

[ActivityID] {1E4FC35E-681F-0000-64C3-4F1E1F68DB01}

-Execution

[ProcessID] 564
[ThreadID] 604

Channel Security

Computer DESKTOP-9K1O4BT

Security

-EventData

TargetUserName WmsControl
TargetDomainName DESKTOP-9K1O4BT
TargetSid S-1-5-21-1859916961-34304393-1824526448-1003
SubjectUserSid S-1-5-18
SubjectUserName DESKTOP-9K1O4BT$
SubjectDomainName WORKGROUP
SubjectLogonId 0x3e7
CallerProcessId 0xe80
CallerProcessName C:\Windows\System32\wbem\WmiPrvSE.exe

Ora spieghiamo passo passo il log:

Analisi dell'evento 4798 - Enumerazione dei gruppi di un utente

Elementi principali dell'evento

1. **Provider**
   - **Name**: Microsoft-Windows-Security-Auditing
     L'evento è generato dal sottosistema di auditing della sicurezza di Windows.
   - **EventID**: 4798
     Identifica l'enumerazione dei gruppi di un utente.
2. **TimeCreated**
   - L'evento è stato registrato il **16 gennaio 2025, alle 14:14:00 UTC**.
3. **TargetUserName**
   - **WmsControl**
     L'utente per cui sono stati interrogati i gruppi è **WmsControl**.
4. **TargetDomainName**
   - **DESKTOP-9K1O4BT**
     Specifica il dominio o il computer a cui appartiene l'utente. In questo caso, si tratta del nome del computer locale.
5. **TargetSid**

- **S-1-5-21-1859916961-34304393-1824526448-1003**
  Indica l'identificatore di sicurezza (SID) dell'utente **WmsControl**.

6. **SubjectUserSid**
   - **S-1-5-18**
     Questo SID rappresenta l'**account del sistema locale** (LocalSystem), che ha effettuato l'operazione.
7. **SubjectUserName**
   - **DESKTOP-9K1O4BT**
     Indica che l'azione è stata effettuata dal computer stesso, identificato come **DESKTOP-9K1O4BT$**.
8. **SubjectDomainName**
   - **WORKGROUP**
     Specifica che il computer fa parte di un **gruppo di lavoro** e non di un dominio Active Directory.
9. **SubjectLogonId**
   - **0x3e7**
     Questo valore rappresenta una sessione di accesso del **sistema locale** (LocalSystem).
10. **CallerProcessName**
    - **C:\Windows\System32\wbem\WmiPrvSE.exe**
      Indica che il processo che ha interrogato i gruppi è **WmiPrvSE.exe**, ovvero il provider WMI (Windows Management Instrumentation). Questo processo è spesso utilizzato per monitorare e raccogliere informazioni sul sistema.