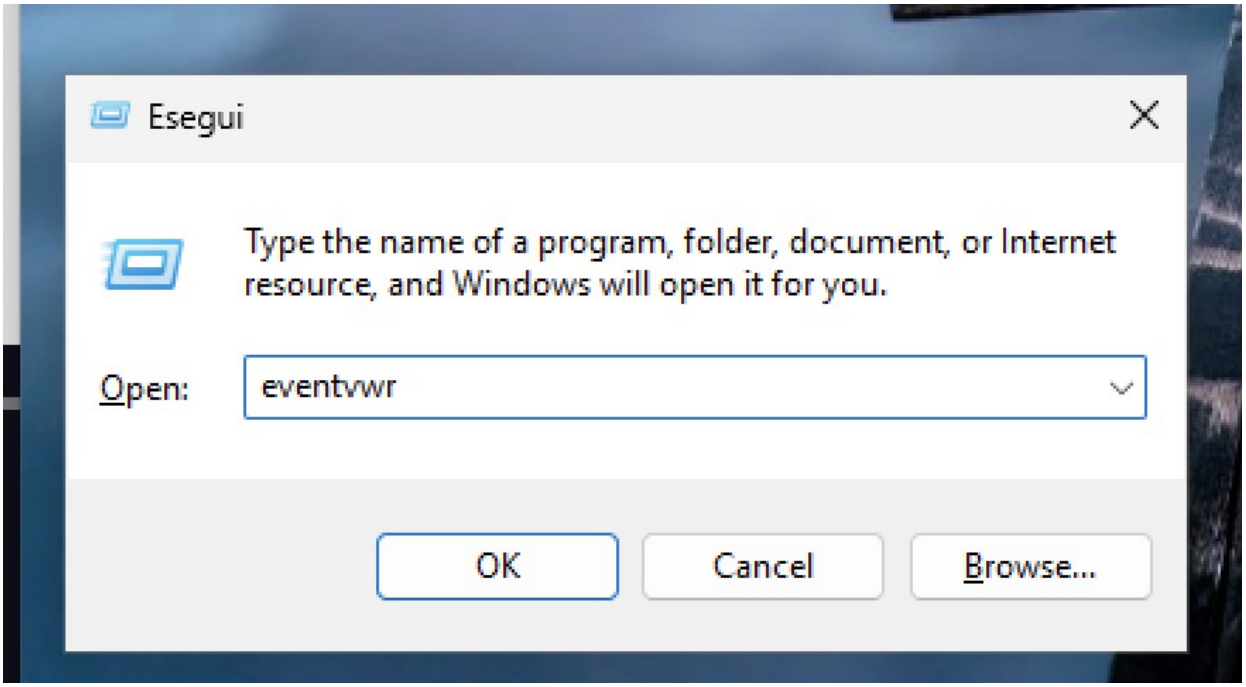
Obiettivo:
Configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows.

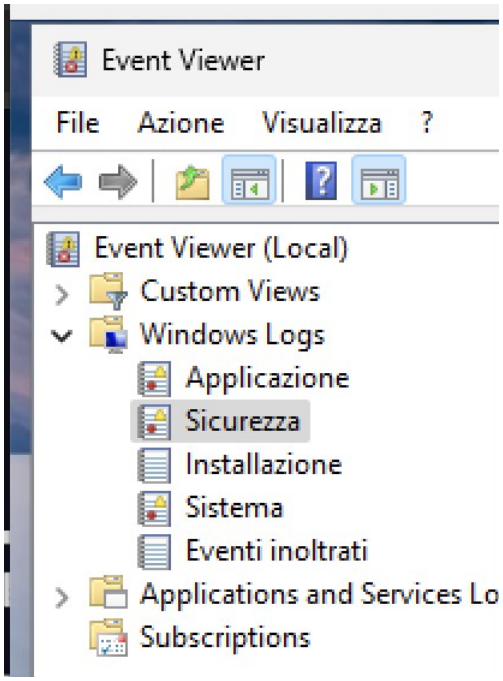
Istruzioni:
1 Accedere al Visualizzatore Eventi:

- Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
- Digita eventvwr e premi Invio.

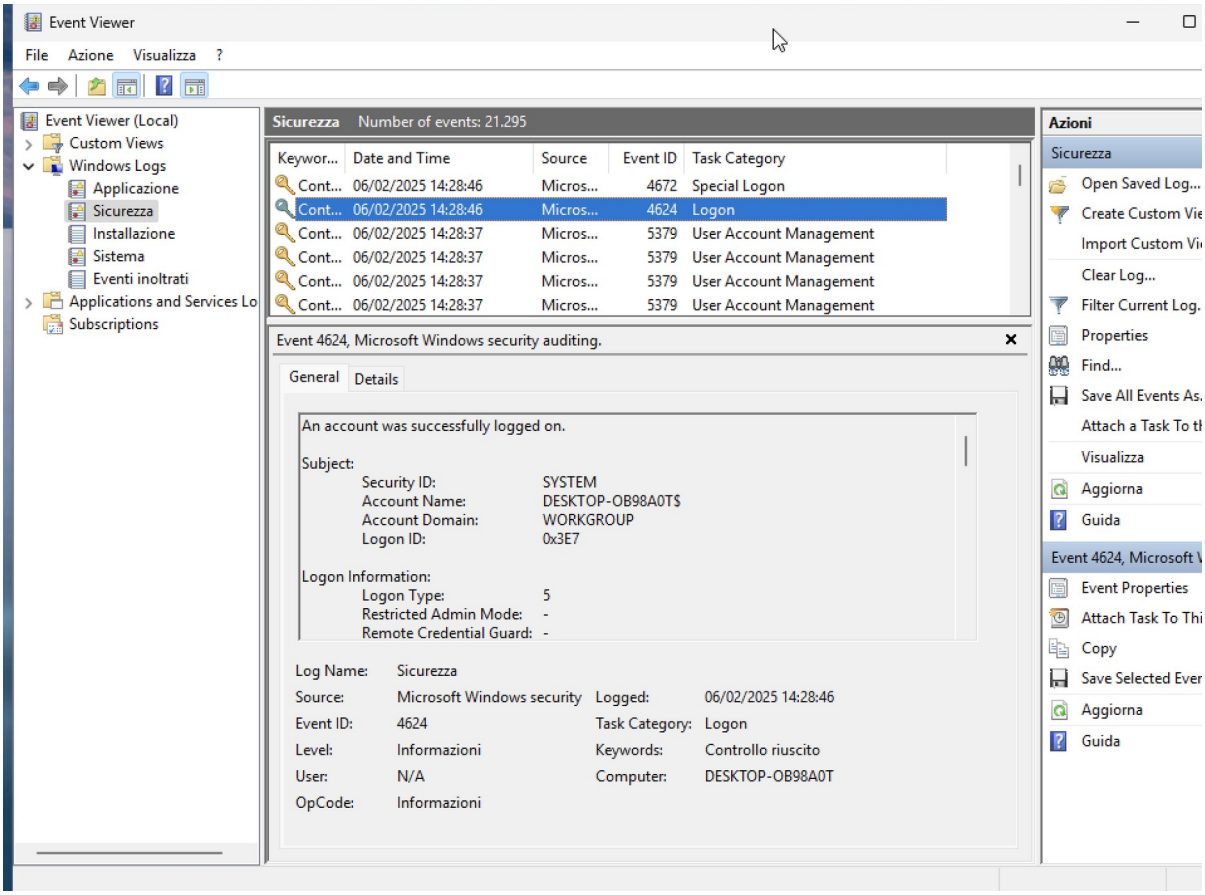


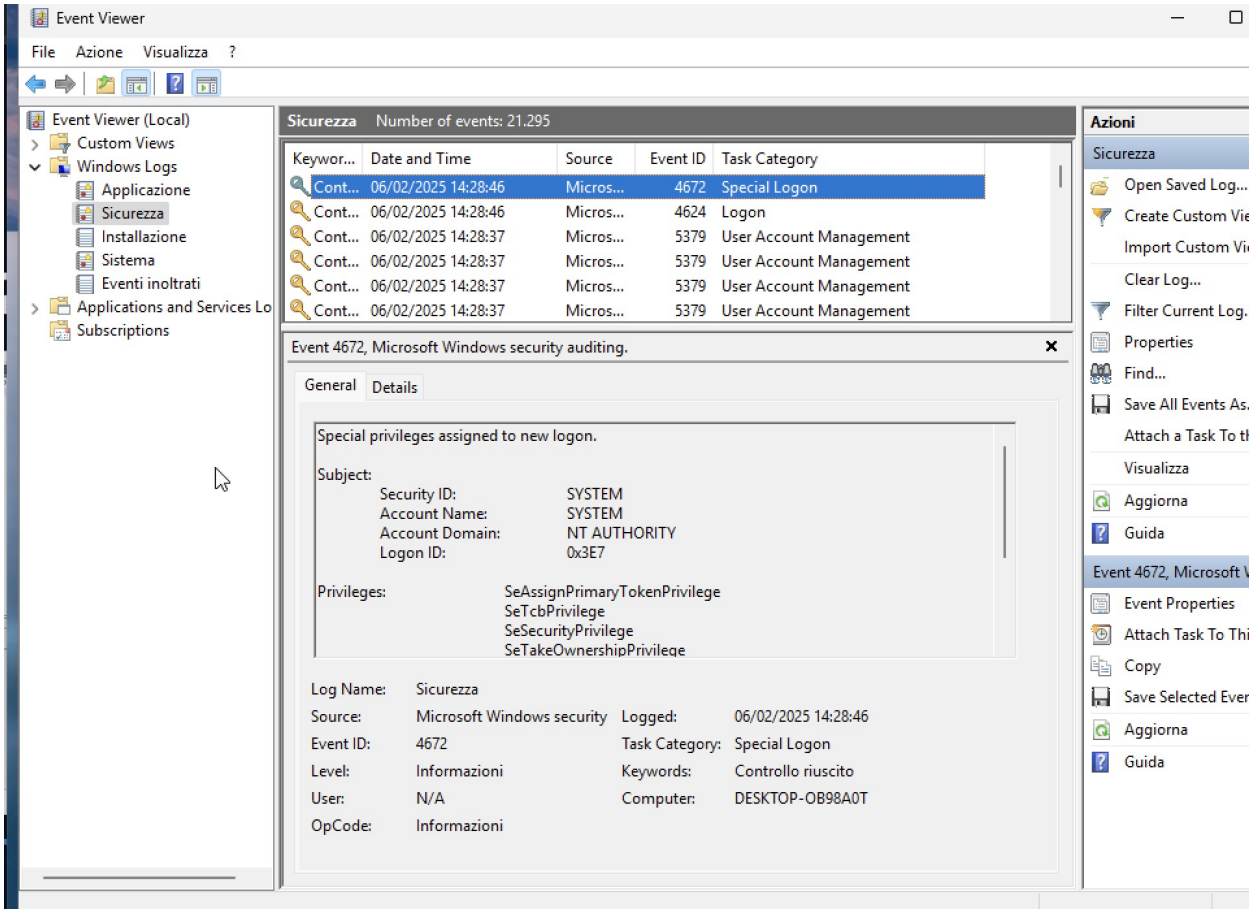
Configurare le Proprietà del Registro di Sicurezza:

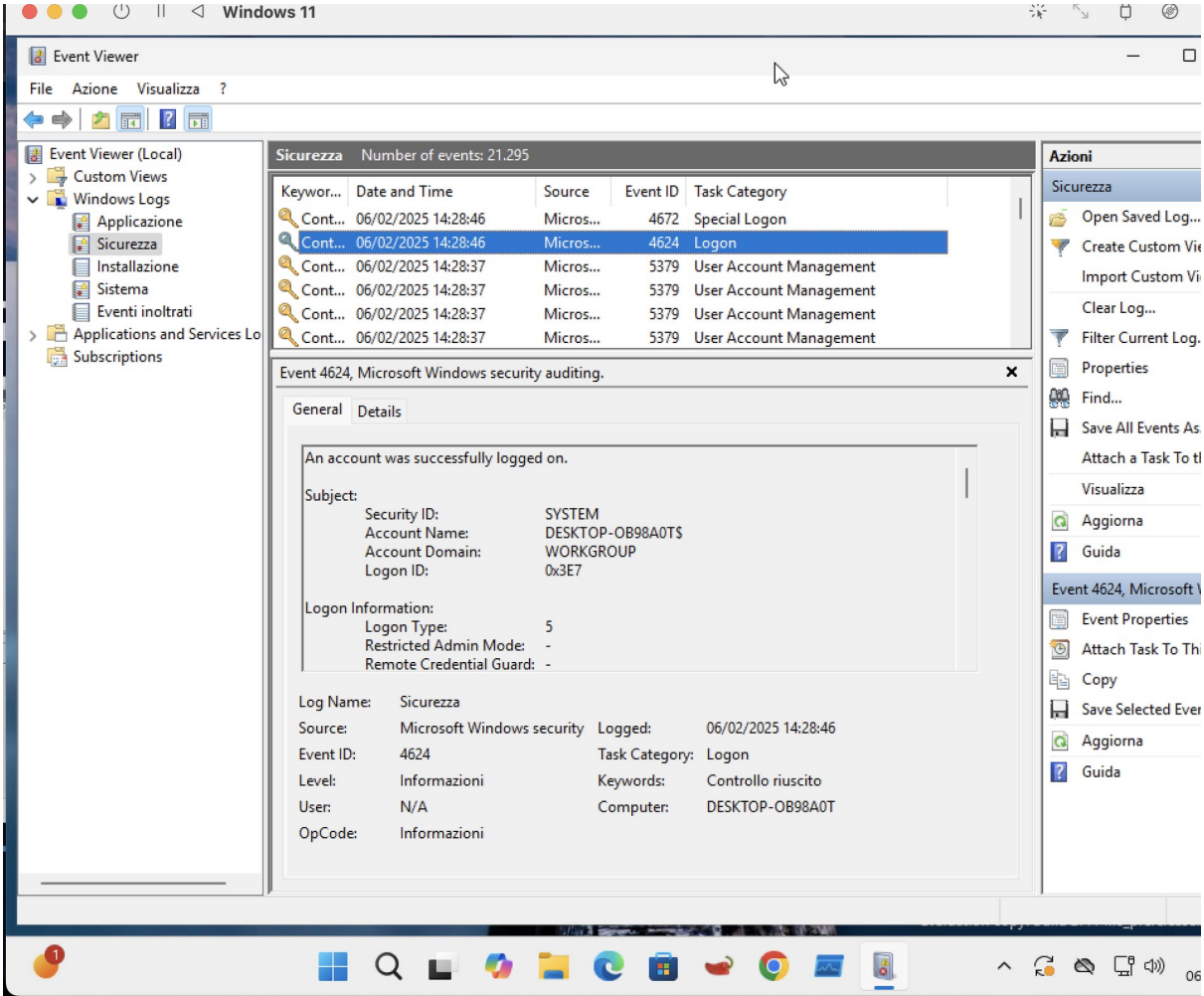
- Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".



3. Analizzare gli eventi con Categoria Attività Logon e Special Logon






Windows 11
Event Viewer
File Azione Visualizza ?
Event Viewer (Local)
Custom Views
Windows Logs
Applicazione
Sicurezza
Installazione
Sistema
Eventi inoltrati
Applications and Services Lo
Subscriptions
Sicurezza Number of events: 21.295
Keywor... Date and Time Source Event ID Task Category
Cont... 06/02/2025 14:28:46 Micros... 4672 Special Logon
Cont... 06/02/2025 14:28:46 Micros... 4624 Logon
Cont... 06/02/2025 14:28:37 Micros... 5379 User Account Management
Cont... 06/02/2025 14:28:37 Micros... 5379 User Account Management
Cont... 06/02/2025 14:28:37 Micros... 5379 User Account Management
Cont... 06/02/2025 14:28:37 Micros... 5379 User Account Management
Event 4624, Microsoft Windows security auditing.
General Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: DESKTOP-OB98A0T$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Logon Information:
Logon Type: 5
Restricted Admin Mode: -
Remote Credential Guard: -
Log Name: Sicurezza
Source: Microsoft Windows security
Logged: 06/02/2025 14:28:46
Event ID: 4624
Task Category: Logon
Level: Informazioni
Keywords: Controllo riuscito
User: N/A
Computer: DESKTOP-OB98A0T
OpCode: Informazioni
Azioni
Sicurezza
Open Saved Log...
Create Custom Vie
Import Custom Vi
Clear Log...
Filter Current Log.
Properties
Find...
Save All Events As
Attach a Task To t
Visualizza
Aggiorna
Guida
Event 4624, Microsoft
Event Properties
Attach Task To Th
Copy
Save Selected Ever
Aggiorna
Guida