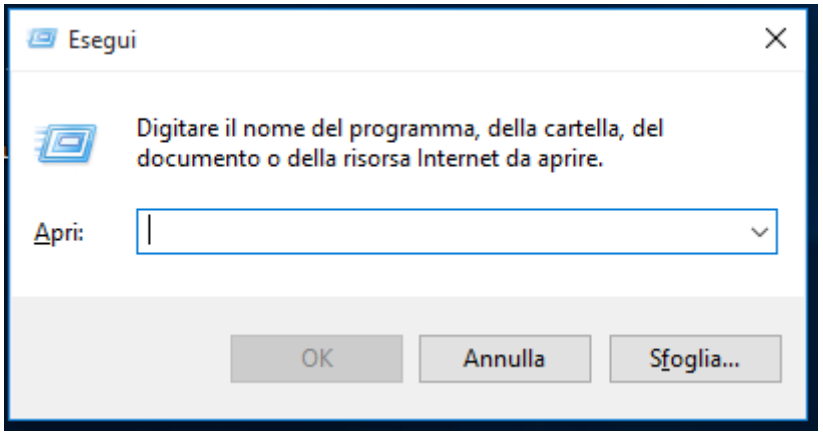
Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

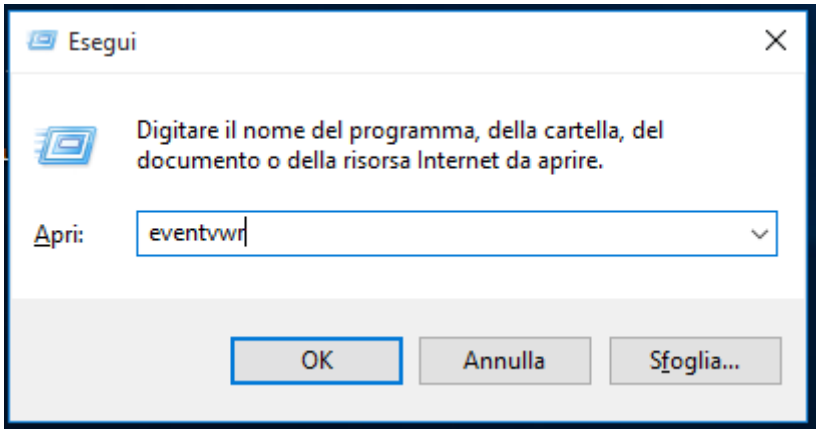
Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

Accesso al Visualizzatore Eventi

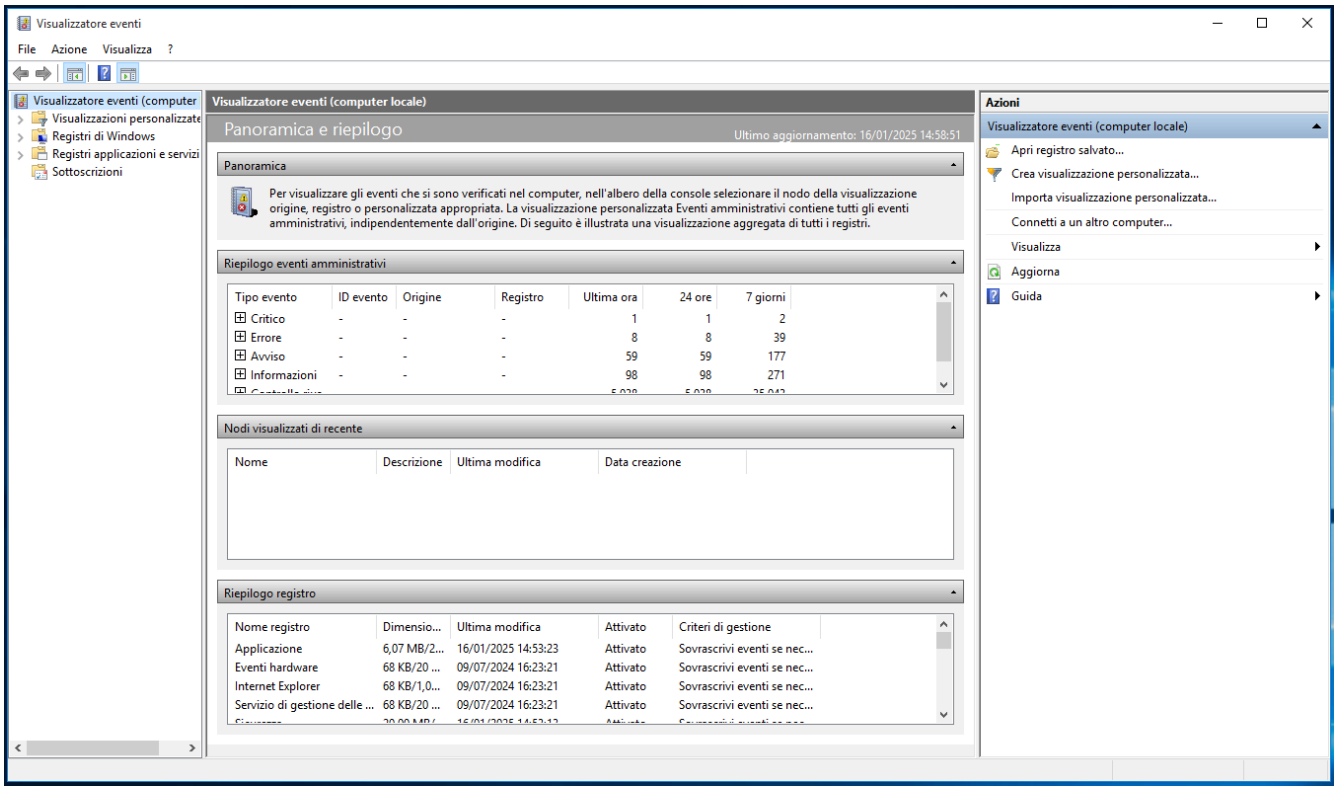
- **Premi Win + R per aprire la finestra "Esegui".**



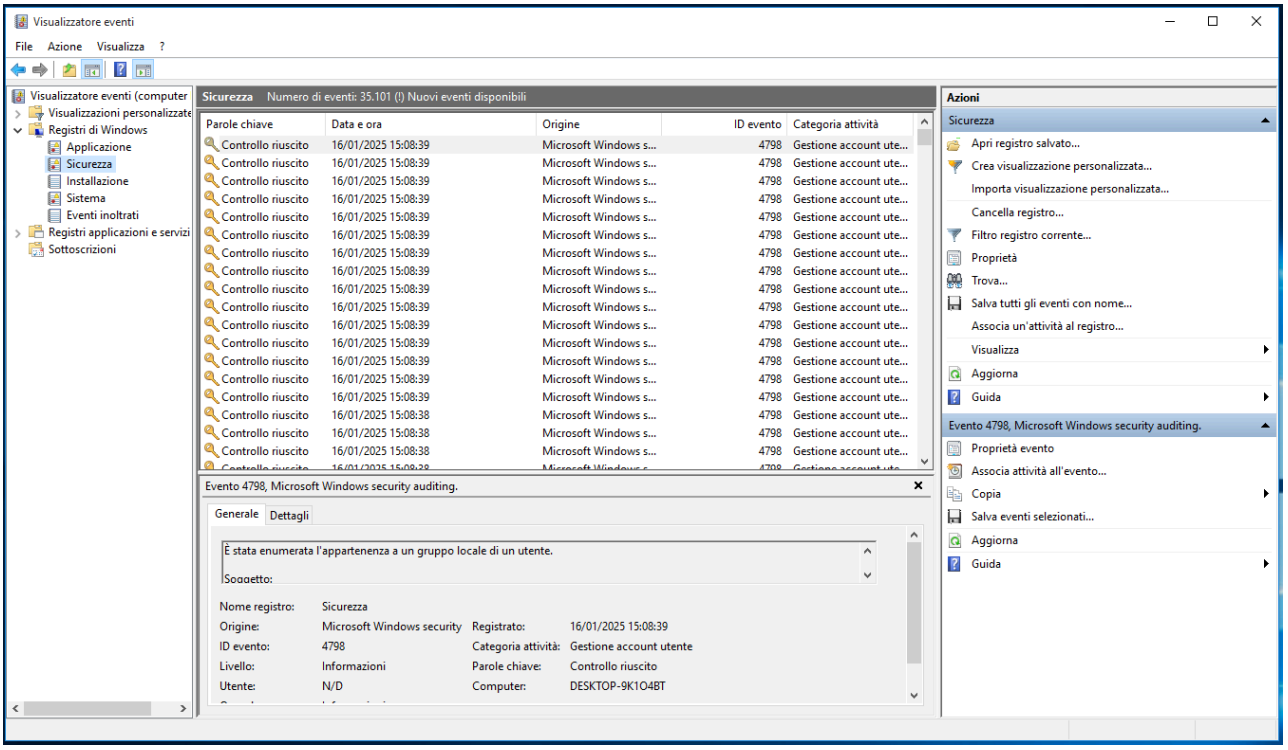
- **Digita eventvwr e premi Invio.**



- **Nel Visualizzatore eventi, nel pannello di sinistra:**

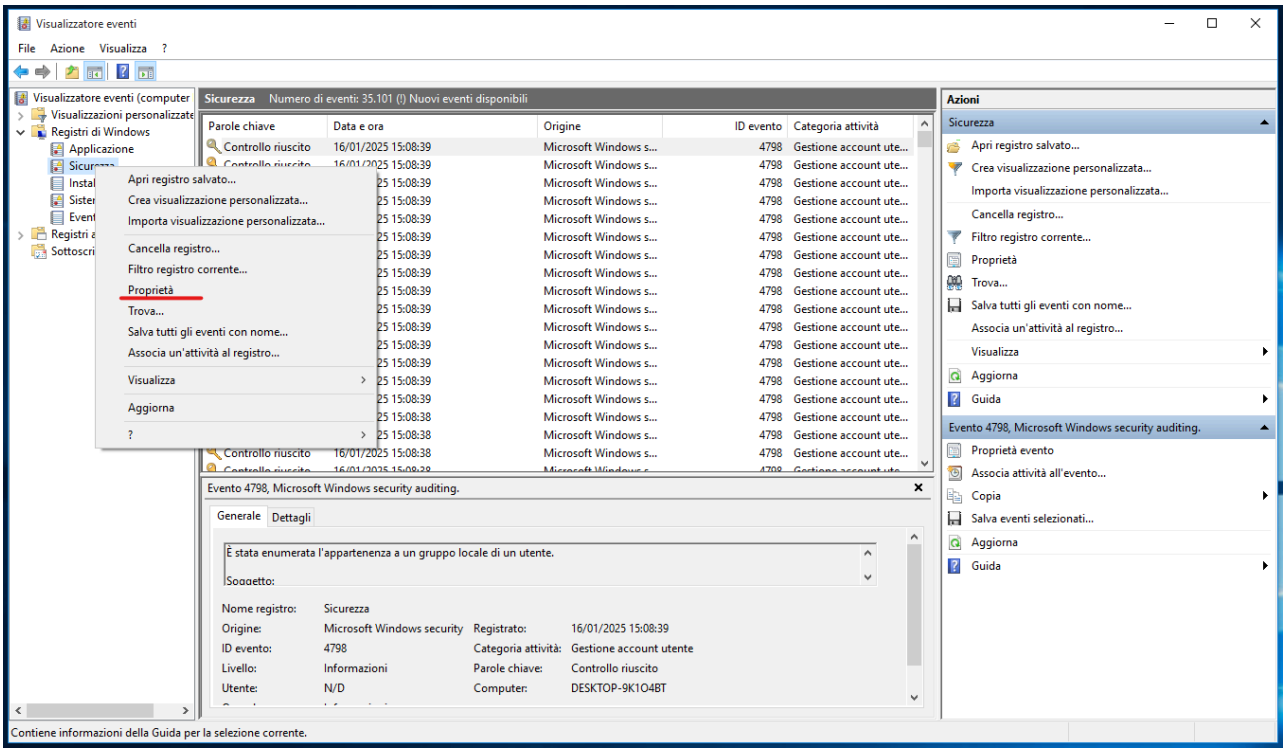


- **Espandi Registri di Windows.**
- **Seleziona Sicurezza.**

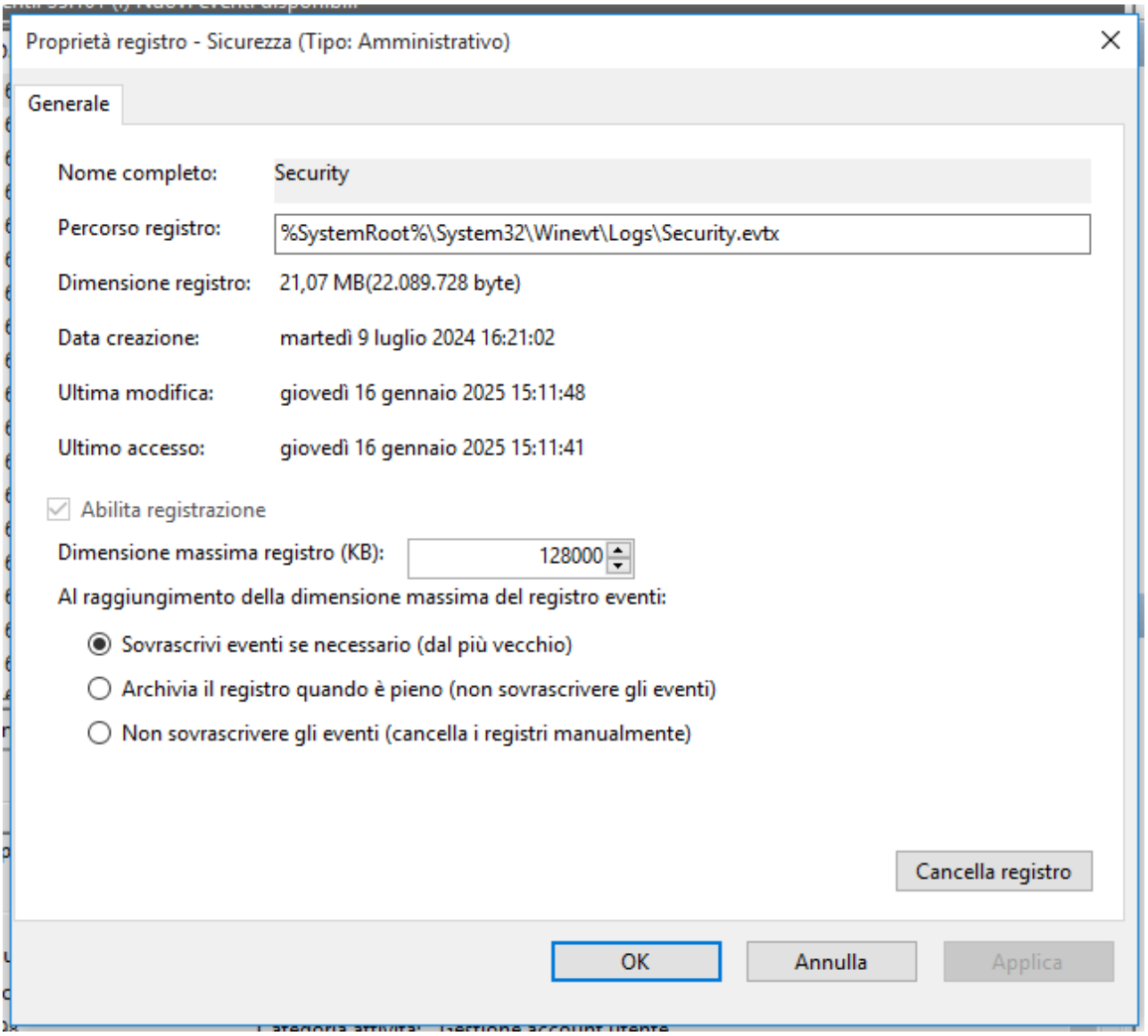


Configurazione delle Proprietà del Registro di Sicurezza

- **1. Con il registro di sicurezza selezionato:**
  - **Fai clic con il pulsante destro del mouse su Sicurezza.**
  - **Seleziona Proprietà.**



- **2. Nella finestra delle proprietà:**
  - **Configura la dimensione massima del file di log (ad esempio, 10 MB o più, in base alle necessità).**
  - **Scegli l'azione da eseguire quando il file di log è pieno:**
    - **Sovrascrivere eventi più vecchi secondo necessità.**
    - **Non sovrascrivere eventi (registro manuale).**
    - **Sovrascrivere eventi più vecchi di N giorni.**

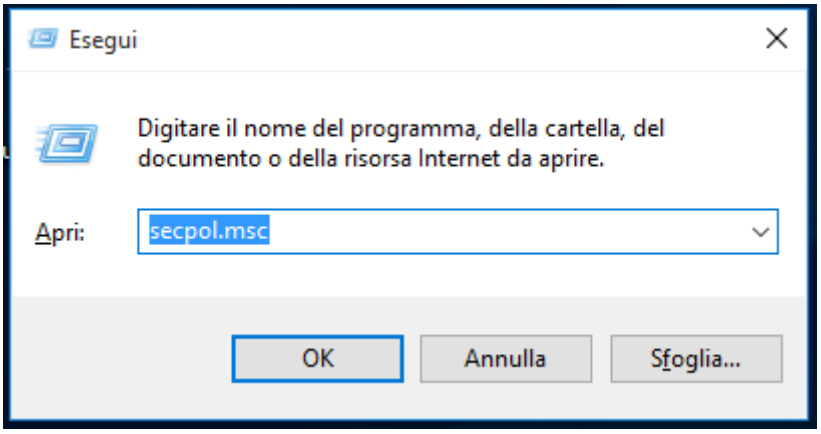


- **3. Applica le modifiche e chiudi la finestra.**

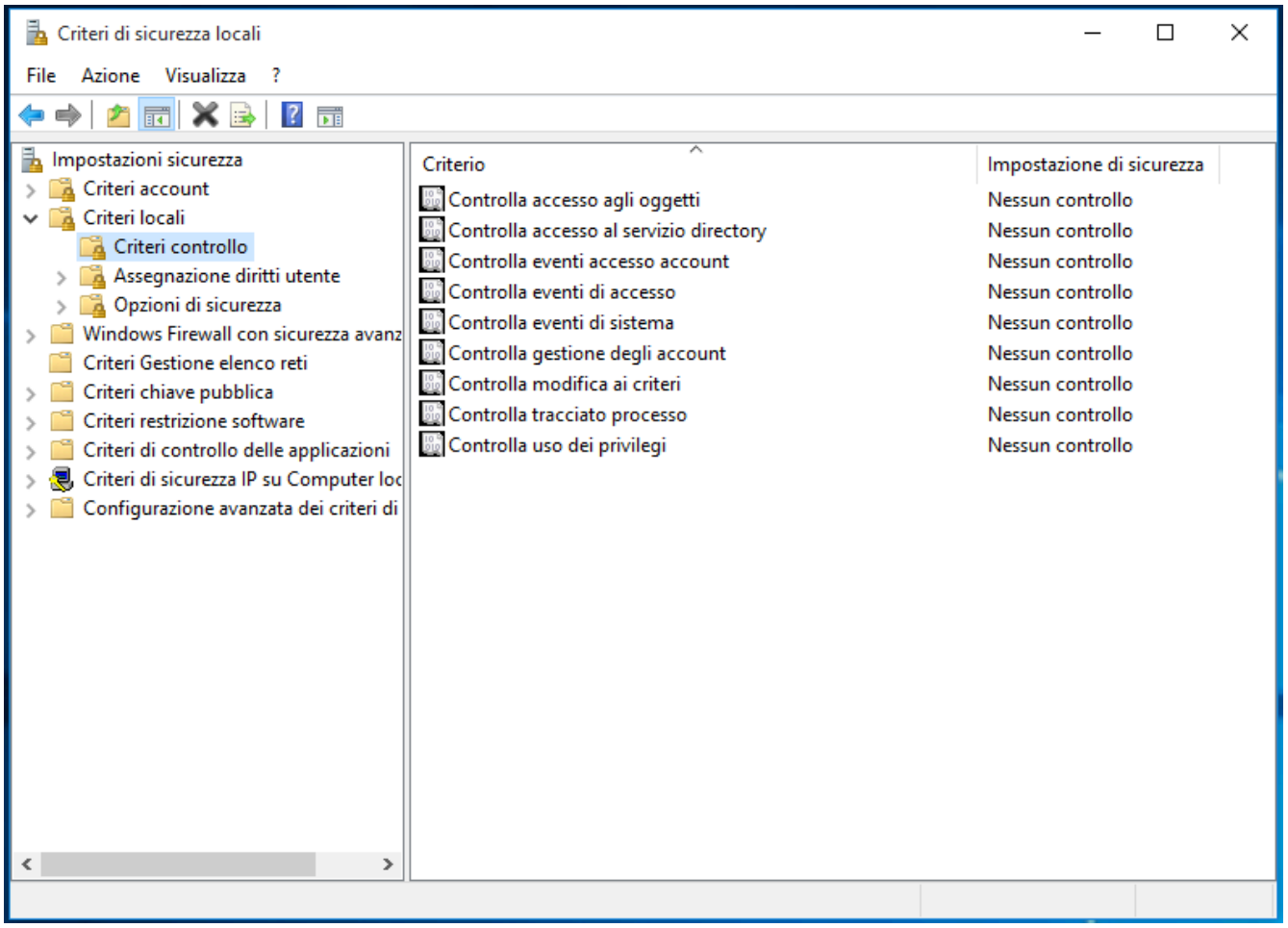
Abilitazione della Registrazione degli Eventi di Sicurezza

Per garantire che gli eventi di sicurezza siano registrati:

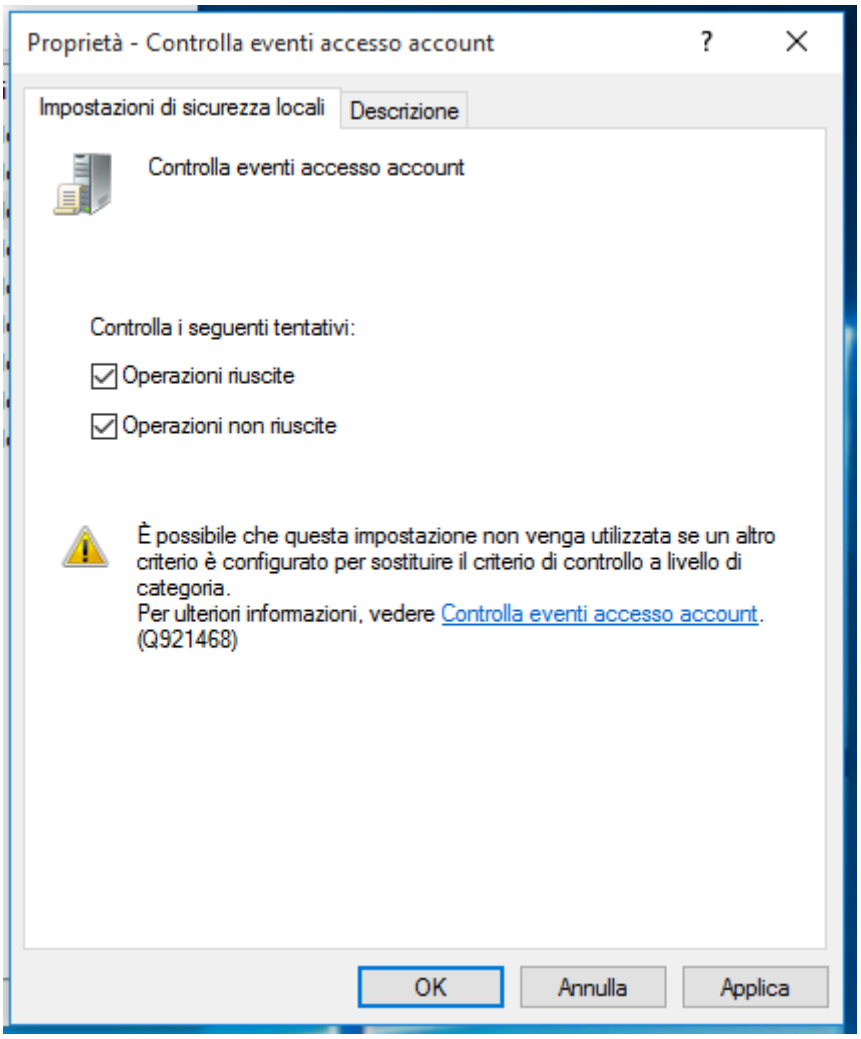
- **1. Apri Criteri di sicurezza locali:**
  - **Premi Win + R, digita secpol.msc e premi Invio.**



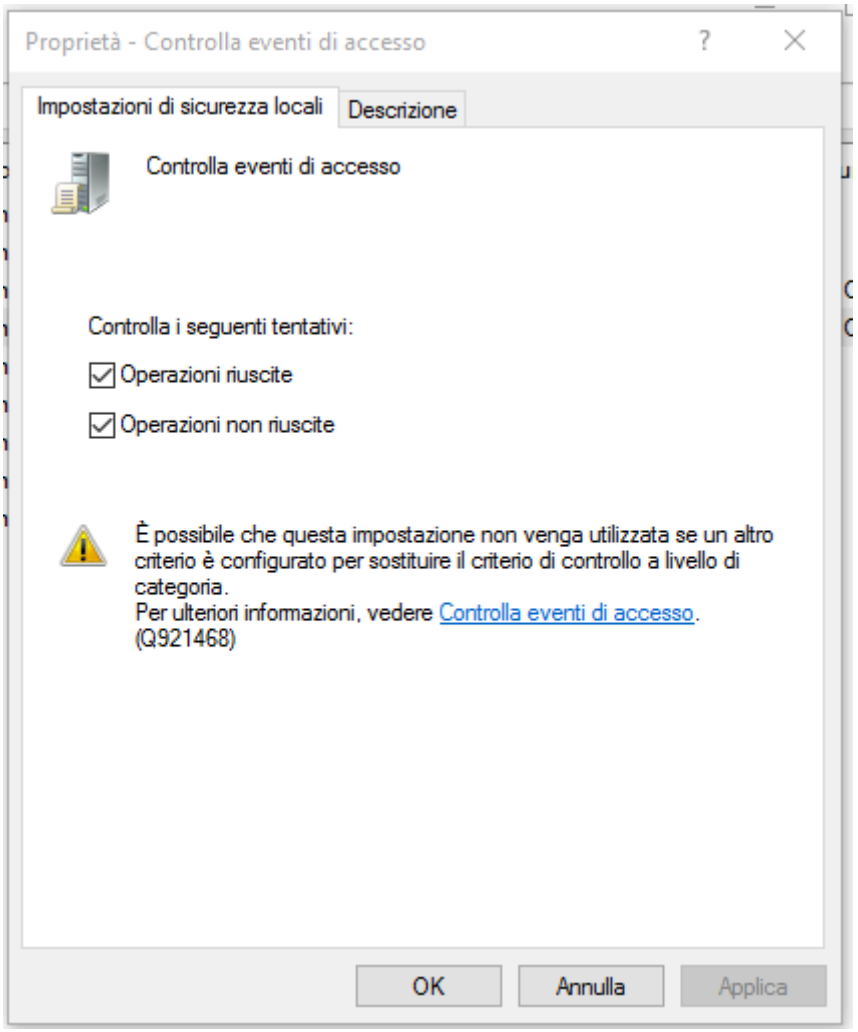
- **2. Espandi Criteri locali > Criteri di controllo.**



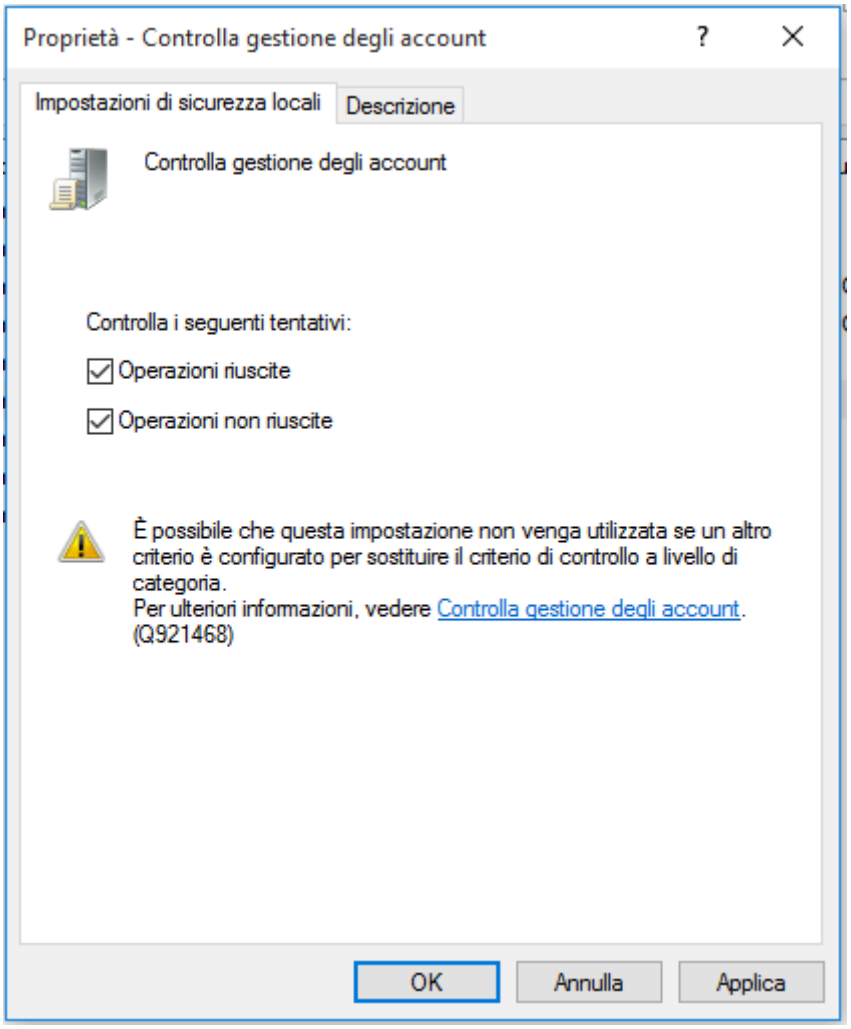
- **3. Configura le seguenti voci (doppio clic per modificare):**
  - **Accesso degli account.**



- **Logon/logoff.**



- **Gestione account.**

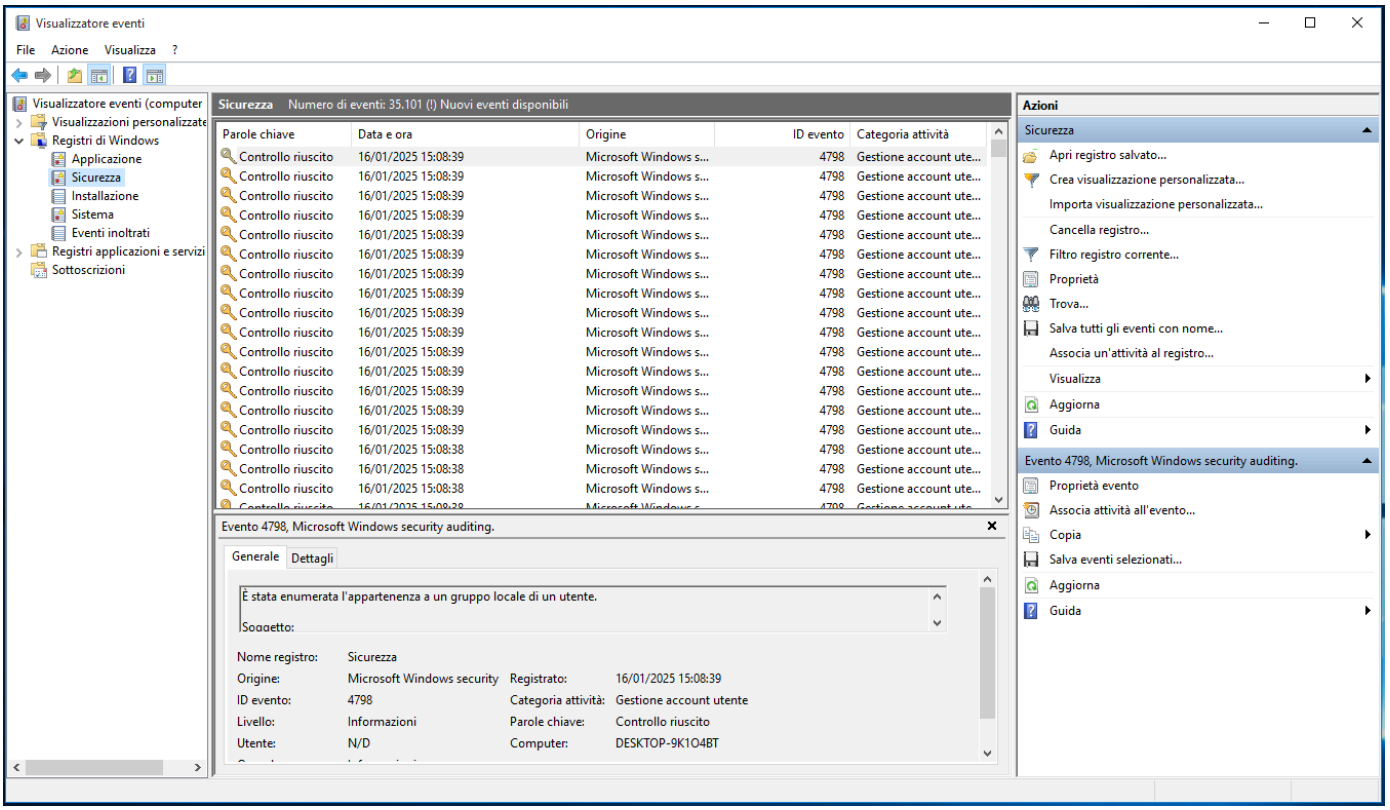


- **Altri criteri rilevanti per il tuo scenario.**

- **4. Attiva l'opzione Successo e/o Insuccesso secondo necessità.**
- **5. Applica e chiudi.**

Verifica dei Log di Sicurezza

- **1. Torna al Visualizzatore eventi.**



- **2. Fai doppio clic su un evento nella categoria Sicurezza per visualizzarne i dettagli.**
- **3. Usa i filtri per trovare eventi specifici:**
  - **Fai clic con il pulsante destro su Sicurezza > Filtra registro corrente.**
  - **Imposta criteri specifici (ID eventi, livello, parola chiave, ecc.).**

Risultato

- **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
  - **TimeCreated**
    [**SystemTime**] 2025-01-16T14:23:03.022245700Z
  EventRecordID 652172
  - **Correlation**
    [**ActivityID**] {B4471EDC-6821-0000-E91E-47B42168DB01}
  - **Execution**
    [**ProcessID**] 552
    [**ThreadID**] 844
  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 0x808
  CallerProcessName C:\Windows\System32\wbem\WmiPrvSE.exe

Descrizione

L'evento indica che un processo o un'entità ha richiesto informazioni sui gruppi locali a cui un utente appartiene. È comune durante le operazioni di gestione di account o verifiche di sicurezza.

Dettagli del Registro

1. **Origine**:
   - **Microsoft-Windows-Security-Auditing**: Proviene dal sistema di auditing di Windows, utilizzato per monitorare eventi di sicurezza.
2. **Soggetto**:

- **ID sicurezza**: `SYSTEM`, il sistema operativo ha eseguito l'operazione.
- **Nome account**: `DESKTOP-9K1O4BT$`, il nome del computer che ha effettuato la richiesta.
  -** ID accesso**: `0x3E7`, rappresenta l'accesso al sistema come account LocalSystem.

3. **Utente**:
   -** ID sicurezza**: `S-1-5-21-...`, l'identificatore di sicurezza dell'utente WmsControl.
   - **Nome account**: `WmsControl`, l'utente il cui gruppo è stato enumerato.
   - **Dominio account**: `DESKTOP-9K1O4BT`, indica che si tratta di un account locale sul computer.
4. **Informazioni sul processo**:
   - **ID processo**: `0x808`, identifica il processo che ha eseguito l'azione.
   - **Nome processo**: `C:\Windows\System32\wbem\WmiPrvSE.exe`, il processo WMI Provider Host, utilizzato spesso per attività di gestione del sistema e interrogazioni WMI.

Significato dell'Evento

- Questo evento è normale e indica che il sistema o un'applicazione ha richiesto informazioni sull'appartenenza ai gruppi locali dell'utente WmsControl.
- È spesso associato a operazioni amministrative, script di gestione o software di monitoraggio.