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

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

Istruzioni:

1) Accedere al Visualizzatore Eventi:
   a) Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
   b) Digita eventvwr e premi Invio.
2) Configurare le Proprietà del Registro di Sicurezza:
   a) Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".
3) Provate a impostare il log dei Login/Logoff

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

1. Obiettivo

L'obiettivo dell'esercizio è configurare e gestire i **file di log della sicurezza** utilizzando il **Visualizzatore eventi di Windows** e i criteri di sicurezza locali, al fine di monitorare gli accessi, i logon, i logoff e le eventuali anomalie di sicurezza.

2. Strumenti Utilizzati

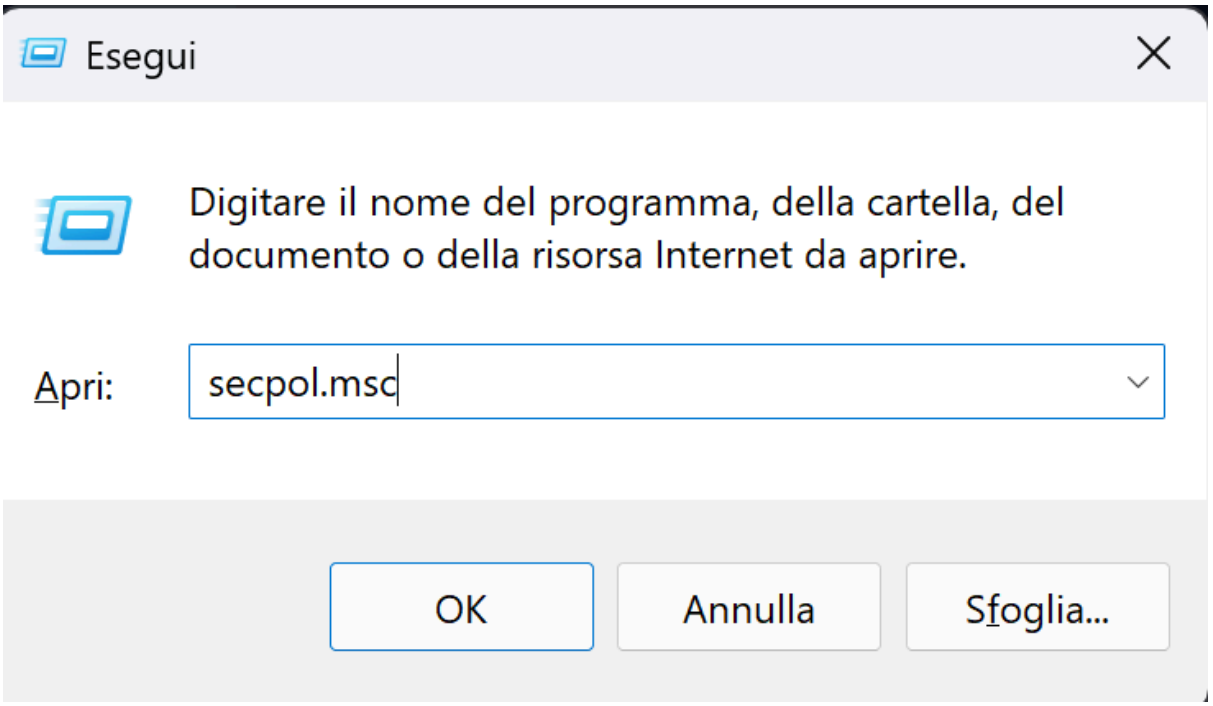
- **Sistema operativo:** Windows
- **Strumenti di configurazione:**
  - `eventvwr.msc` → per accedere al Visualizzatore Eventi
  - `secpol.msc` → per configurare le criteri di sicurezza locali
- **Sezioni coinvolte:**
  - Registri di Windows → Sicurezza
  - Criteri di controllo di sistema
  - Accesso / Fine sessione
  - Controllo Accesso

---

3. Procedura

3.1 Accesso ai Criteri di Sicurezza Locali

1. Premere **Win + R** per aprire la finestra **Esegui**.
2. Digitare `secpol.msc` e premere **Invio**.
3. Si aprirà la finestra dei **Criteri di sicurezza locali**.



3.3 Configurazione del Controllo Accesso

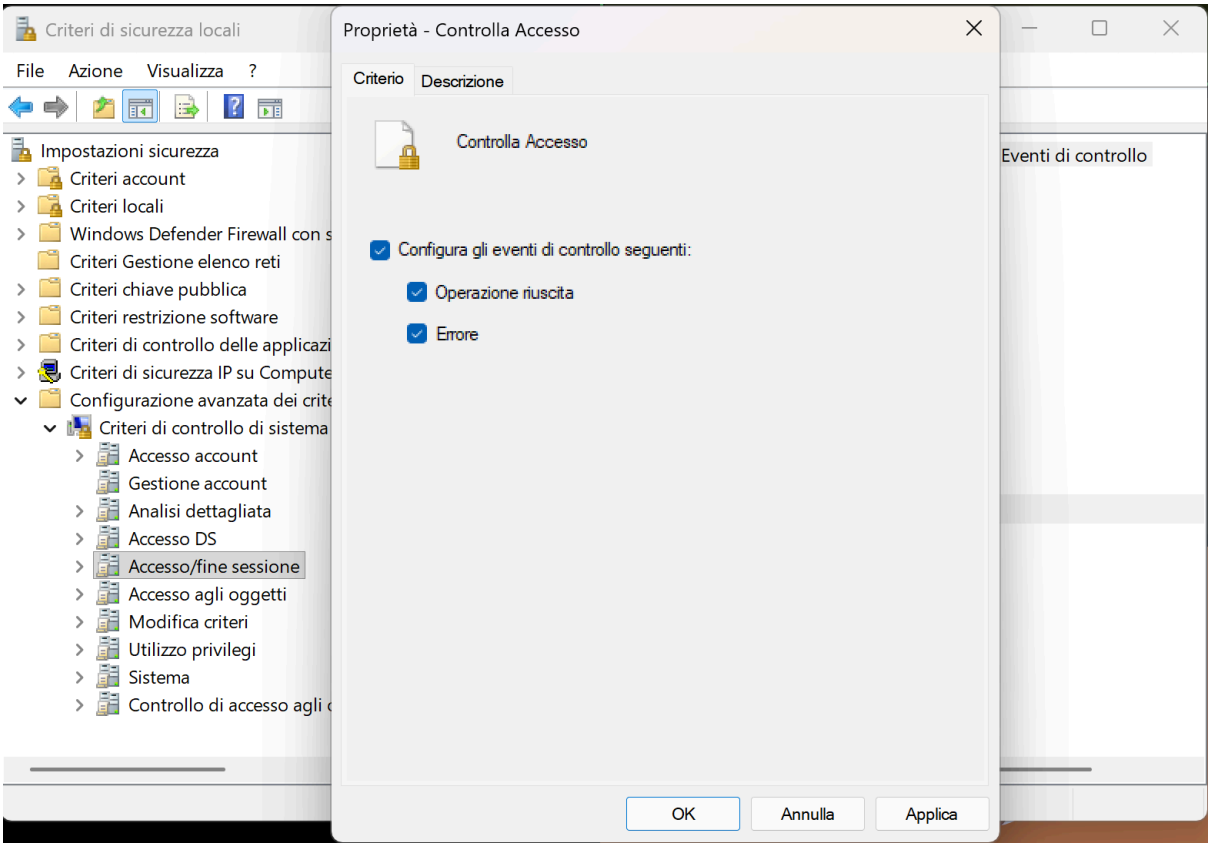
1. Nella finestra dei **Criteri di sicurezza locali**, andare in: **Criteri di controllo di sistema → Controlla Accesso/Fine sessione**

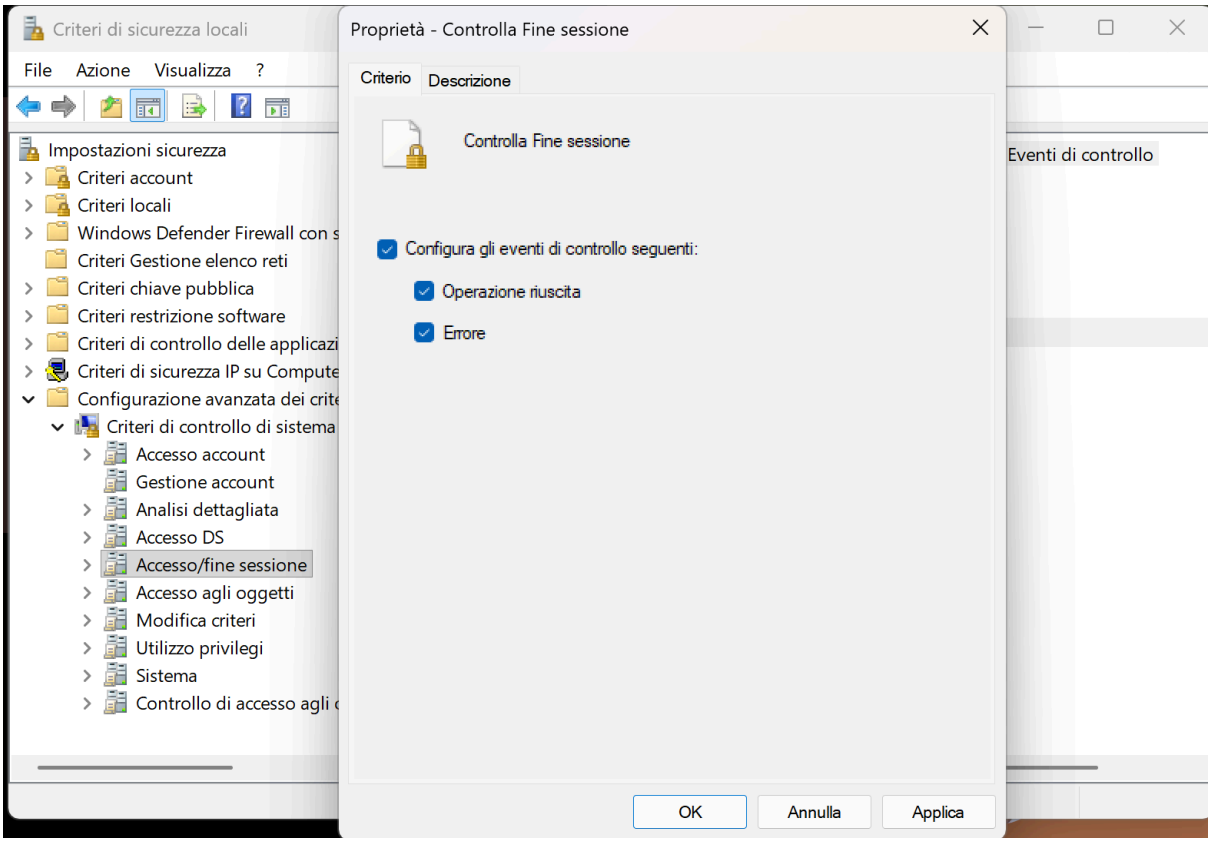
2. Abilitare le opzioni:

    - **Operazione riuscita**

    - **Errore**

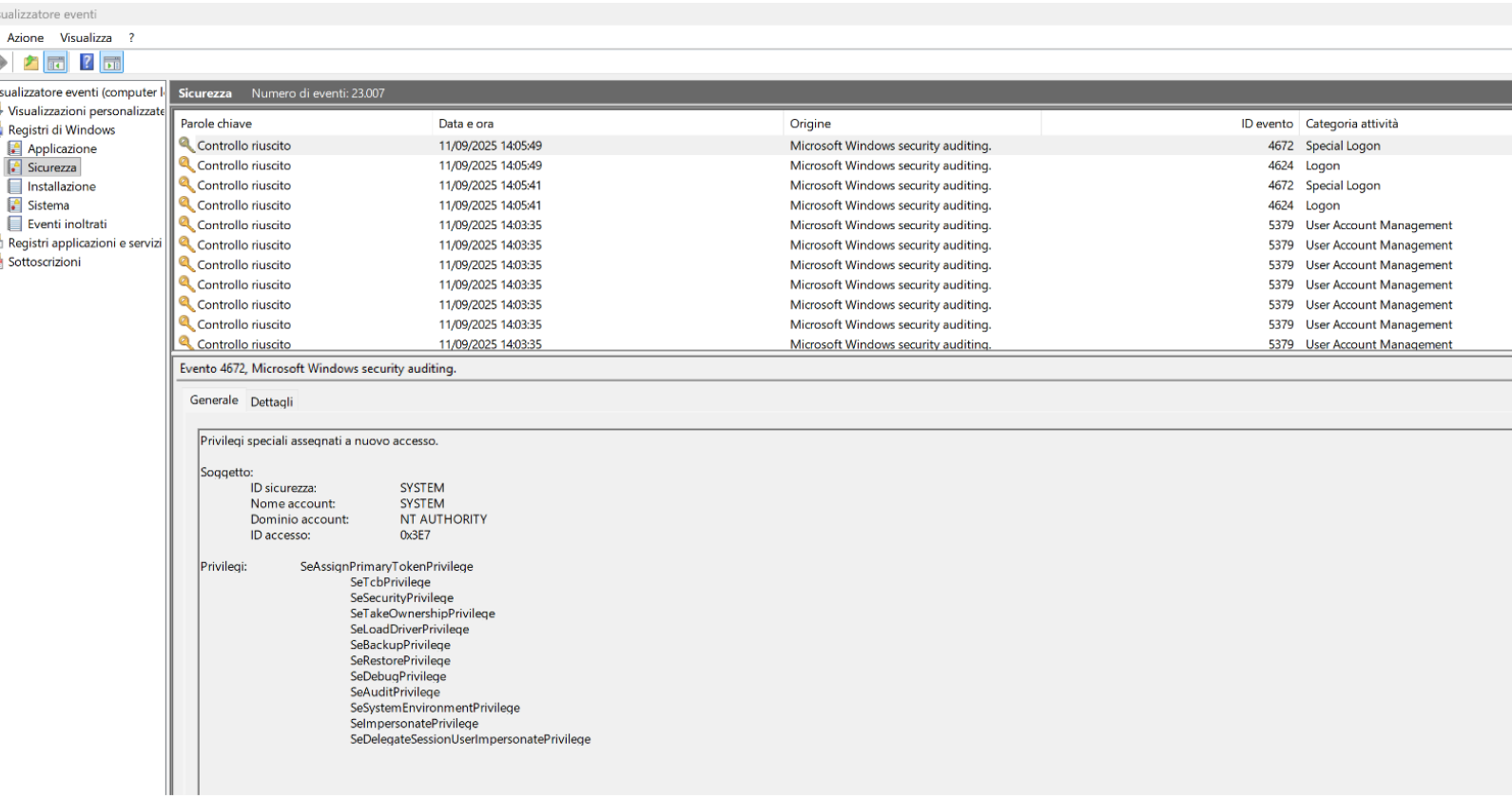
3. Confermare con **Applica** e poi **OK**.





3.4 Verifica dei Log di Sicurezza

1. Tornare nel Visualizzatore Eventi.
2. Accedere a Registri di Windows → Sicurezza.
3. Controllare che vengano registrati correttamente gli eventi relativi a:
    - Accessi
    - Fine sessione
    - Modifiche ai privilegi
    - Errori di autenticazione



Sicurezza Numero di eventi: 23.007

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	11/09/2025 14:05:49	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	11/09/2025 14:05:49	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	11/09/2025 14:05:41	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	11/09/2025 14:05:41	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	11/09/2025 14:03:35	Microsoft Windows security auditing.	5379	User Account Management

Evento 4672, Microsoft Windows security auditing.

```
Privilegi speciali assegnati a nuovo accesso.

Soggetto:
          ID sicurezza:             SYSTEM
          Nome account:             SYSTEM
          Dominio account:          NT AUTHORITY
          ID accesso:               0x3E7

Privilegi:          SeAssignPrimaryTokenPrivilege
                              SeTcbPrivilege
                              SeSecurityPrivilege
                              SeTakeOwnershipPrivilege
                              SeLoadDriverPrivilege
                              SeBackupPrivilege
                              SeRestorePrivilege
                              SeDebugPrivilege
                              SeAuditPrivilege
                              SeSystemEnvironmentPrivilege
                              SeImpersonatePrivilege
                              SeDelegateSessionUserImpersonatePrivilege
```

4. Risultati Ottenuti

- Le regole di controllo per Accesso e Fine sessione sono state configurate con successo.

- Il Visualizzatore Eventi mostra ora tutti i log relativi:
    - Eventi di login e logoff.
    - Operazioni riuscite e fallite.
    - Eventuali errori di sicurezza.

5. Conclusione

Grazie alla configurazione dei criteri di sicurezza locali e alla gestione dei log di sicurezza, il sistema ora registra e monitora in modo dettagliato tutte le attività di accesso.
Questa procedura è fondamentale per:

- Migliorare la sicurezza del sistema.
- Identificare tentativi di accesso non autorizzato.
- Fornire tracciabilità completa delle operazioni effettuate.