PRATICA S9L4

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.

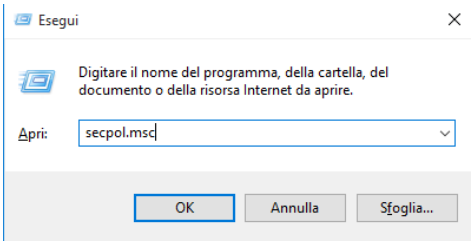
Istruzioni:

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

2. Configurare le Proprietà del Registro di Sicurezza:
   - Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".

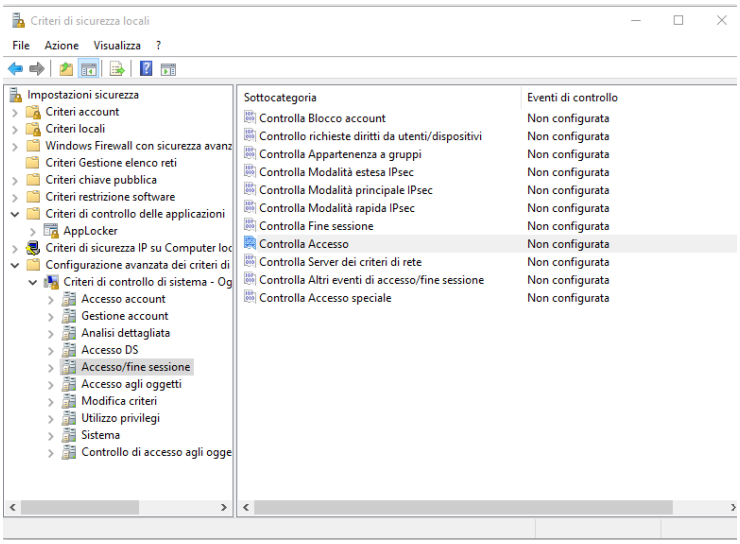
Modifica dei criteri di sicurezza locali

Ho aperto il prompt "Esegui" su Windows e ho digitato il comando `secpol.msc`. Questo mi ha permesso di accedere direttamente al pannello delle **Impostazioni di sicurezza locali**, dove posso gestire criteri di sicurezza avanzati per il sistema. È uno strumento utile quando voglio modificare policy come l'accesso utente, le regole di auditing o le impostazioni di sicurezza per la rete.



Successivamente, mi sono addentrato nella sezione **Configurazione avanzata dei criteri di controllo**, in particolare sotto **Criteri di controllo di sistema - Oggetti**. Qui ho trovato una serie di voci relative al monitoraggio degli accessi e delle connessioni, come:

- *Controlla Accesso*
- *Controlla Accesso speciale*

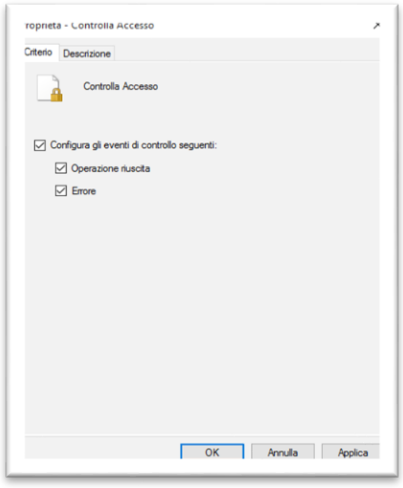


Tutte queste voci risultavano **non configurate**, quindi ho deciso di intervenire manualmente.

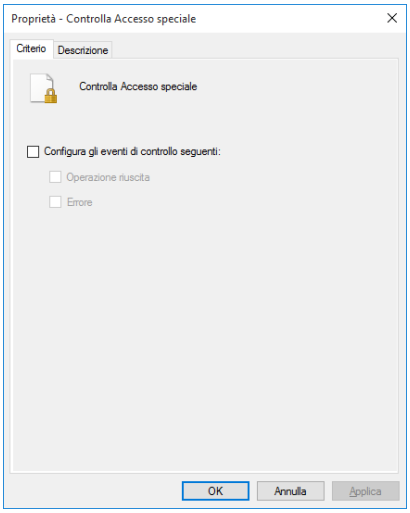
Ho aperto le proprietà di **Controlla Accesso** e ho attivato entrambe le opzioni di auditing:

- *Operazione riuscita*
- *Errore*

In questo modo, il sistema registrerà sia gli accessi riusciti che quelli falliti, migliorando la tracciabilità e la sicurezza.



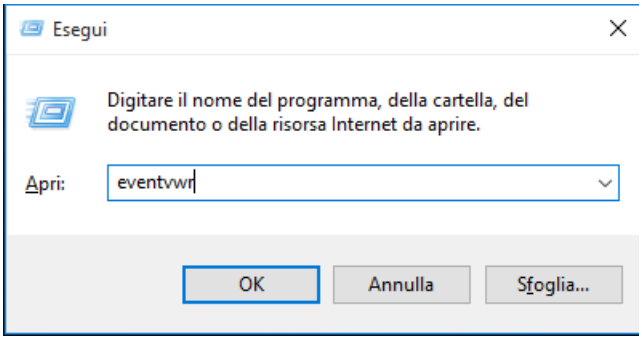
Poi ho fatto lo stesso per **Controlla Accesso speciale**, abilitando anche lì il controllo per operazioni riuscite ed errori. Questo mi permette di monitorare eventi più specifici e sensibili, come accessi a risorse protette o tentativi non autorizzati.



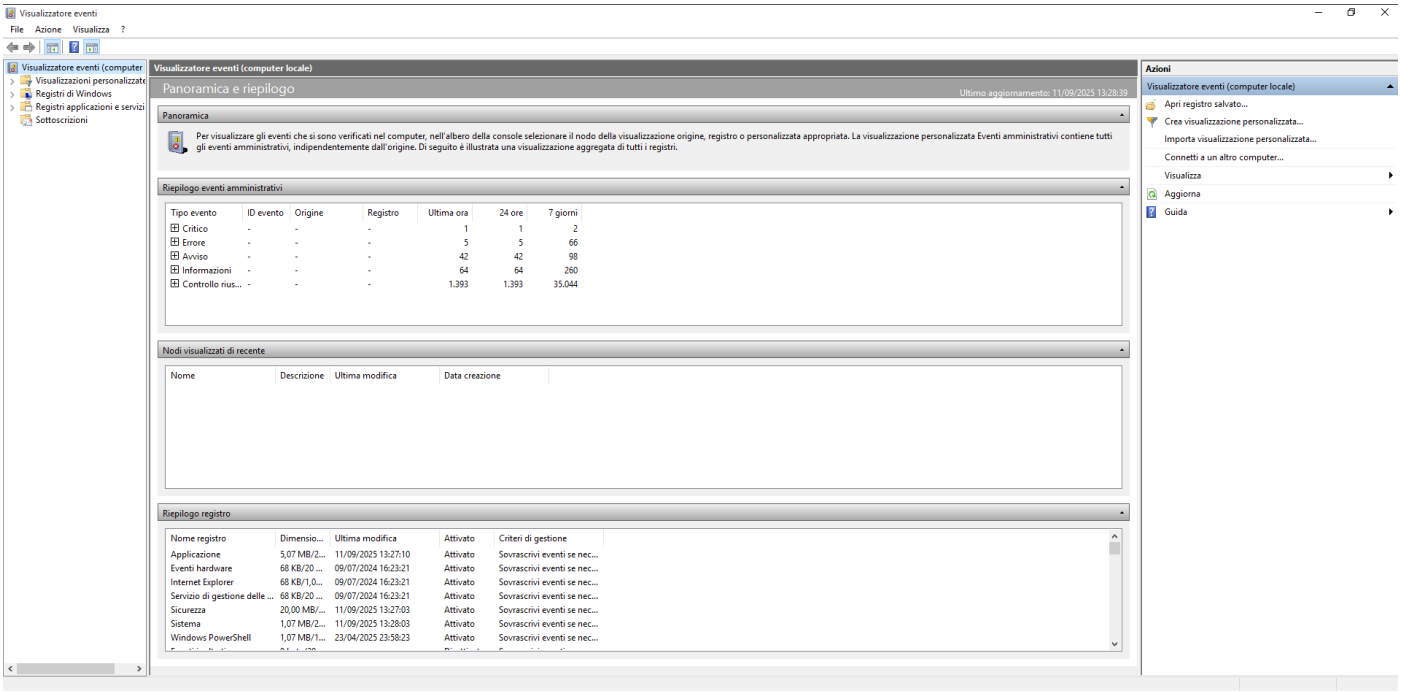
Accedere al Visualizzatore Eventi (sicurezza)

Dopo aver configurato i criteri di auditing per l'accesso e l'accesso speciale, ho voluto verificare che tutto fosse correttamente attivo e funzionante. Per farlo, ho aperto nuovamente il prompt **Esegui** e ho digitato `eventvwr`, il comando che apre il **Visualizzatore eventi** di Windows.

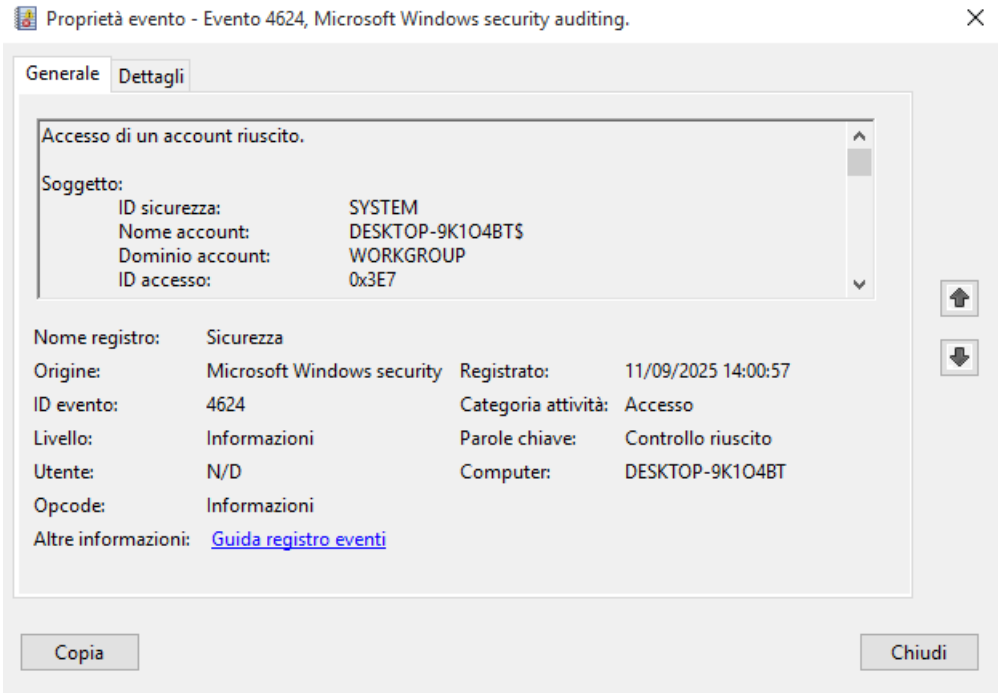
Questo strumento mi permette di monitorare in tempo reale tutti gli eventi registrati dal sistema, inclusi quelli relativi agli accessi riusciti e falliti, come da configurazione appena impostata. È una risorsa fondamentale per tenere traccia delle attività degli utenti e per individuare eventuali anomalie o tentativi di accesso non autorizzati.



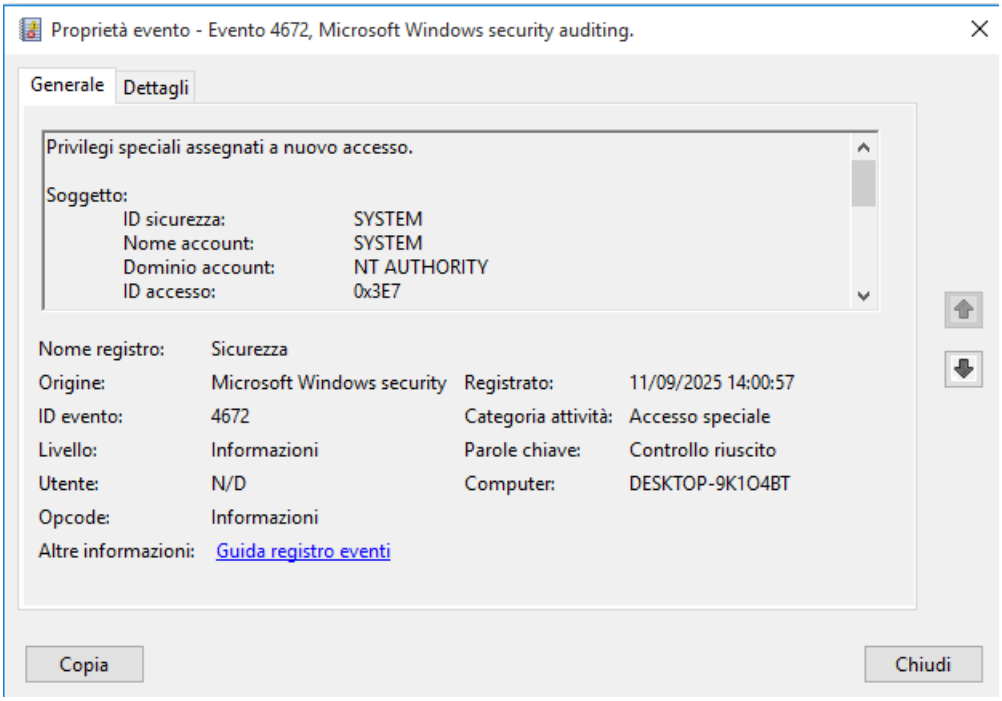
Una volta aperto il **Visualizzatore eventi**, Questo mi ha dato un primo quadro generale delle criticità presenti.



Poi mi sono spostato nel registro **Sicurezza**, dove ho trovato una serie di eventi con ID **4624**, che indicano **accessi riusciti** al sistema. Ogni voce include dettagli come il nome dell'account, il tipo di accesso, il processo coinvolto e il pacchetto di autenticazione utilizzato (*Negotiate*). Questi dati sono fondamentali per verificare chi ha effettuato l'accesso e in che modalità.



Un evento particolarmente interessante è stato l'ID **4672**, che segnala l'assegnazione di **privilegi speciali** a una nuova sessione di accesso. Questo tipo di evento è cruciale per monitorare attività con potenziali rischi elevati, come l'uso di credenziali di sistema o l'esecuzione di operazioni amministrative.



Conclusione

Attraverso questo esercizio ho configurato e verificato il sistema di auditing locale su Windows, con l'obiettivo di monitorare in modo efficace gli accessi e le attività sensibili.

1. **Configurazione dei criteri di controllo** Ho abilitato il tracciamento degli eventi per *Accesso* e *Accesso speciale*, selezionando sia le operazioni riuscite che gli errori. Questo garantisce una visibilità completa su chi accede al sistema e su eventuali tentativi falliti o sospetti.

2. **Verifica tramite Visualizzatore eventi** Ho consultato il registro **Sicurezza** nel Visualizzatore eventi, dove ho potuto confermare la registrazione degli eventi con ID **4624** (accesso riuscito) e **4672** (assegnazione di privilegi speciali). Questi log dimostrano che le policy di auditing sono attive e funzionanti.
3. **Analisi degli eventi amministrativi** Ho esaminato anche gli eventi di sistema e applicazione, rilevando errori e avvisi legati a componenti come *DistributedCOM* e *Perflib*. Questo mi ha permesso di avere una panoramica più ampia sullo stato di salute del sistema.