S9L4

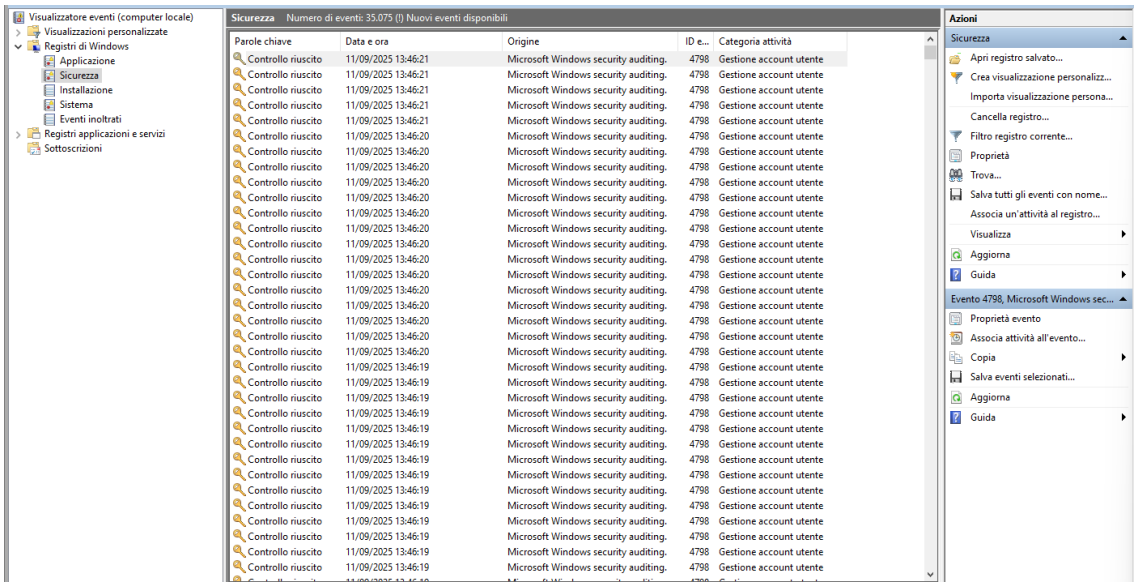
Esercizio di oggi: Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

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

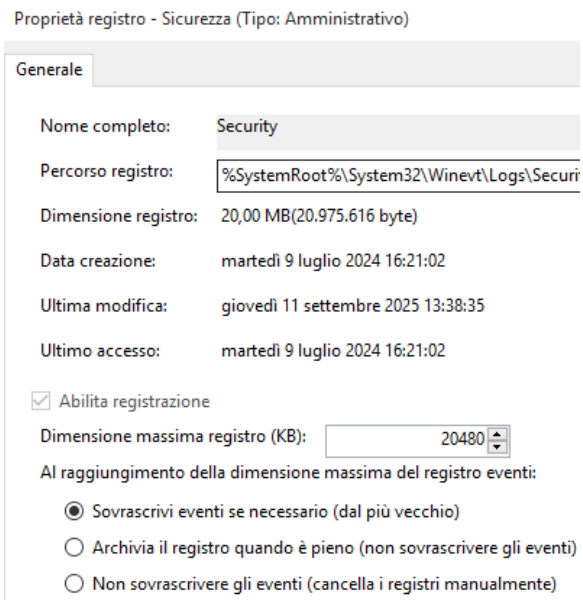
Istruzioni:

1) Accedere al Visualizzatore Eventi:
   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

Seguendo le indicazioni dell'esercizio, ci ritroviamo in questa schermata



Analizzando le proprietà del registro mi accorgo di una regola che non mi ha convinto molto, ovvero; ***Sovrascrivi eventi se necessario (dal più vecchio).***



Questo tipo di impostazione è molto comune in macchine ad uso privato (utente medio), ma in ambiti dove la sicurezza è importante, come grandi aziende, è sconsigliato. Elencherò i pro e i contro di questa impostazione:

Pro

Continuità del logging → il registro non smette mai di scrivere: anche se è pieno, i nuovi eventi sostituiscono i vecchi, evitando di perdere log recenti.

Zero interruzioni → non rischi che un processo o un servizio non riesca a scrivere eventi a causa di un log pieno.

Meno manutenzione manuale → non serve svuotare o archiviare il registro frequentemente, il sistema "si autogestisce".

Contro

Perdita di dati storici → i log più vecchi vengono eliminati senza avviso: se servono per analisi forense o audit, rischi di non averli più.

Maggiore esposizione a tecniche di anti-forensics → un attaccante che genera molti eventi può "spingere fuori" quelli rilevanti dal registro (log flooding).

Non ideale per ambienti regolamentati → in contesti come ISO 27001, GDPR o SOX, la perdita di log può costituire una non conformità.

Analisi retrospettiva limitata → se devi investigare incidenti avvenuti settimane/mesi prima, potresti non avere i dati necessari.

Per quanto riguarda i contesti aziendali, sarebbe più opportuno utilizzare l'opzione **Archivia il registro quando è pieno (non sovrascrivere gli eventi)**

Pro

Tutti gli eventi sono conservati finché non vengono archiviati.

Maggiore affidabilità in analisi forense e auditing.

Conforme a requisiti di sicurezza e normative (ISO, GDPR, SOX ecc.).

Contro

Se il log è pieno, **gli eventi nuovi non vengono registrati** → rischio di perdere informazioni cruciali in tempo reale.

Richiede monitoraggio costante e procedure di archiviazione automatica/manuale.

Può saturare rapidamente lo storage se non gestito bene.

In sintesi possiamo riassumere queste due impostazioni così:

Sovrascrivi eventi se necessario = praticità, ma rischi di perdere prove. (user medio)

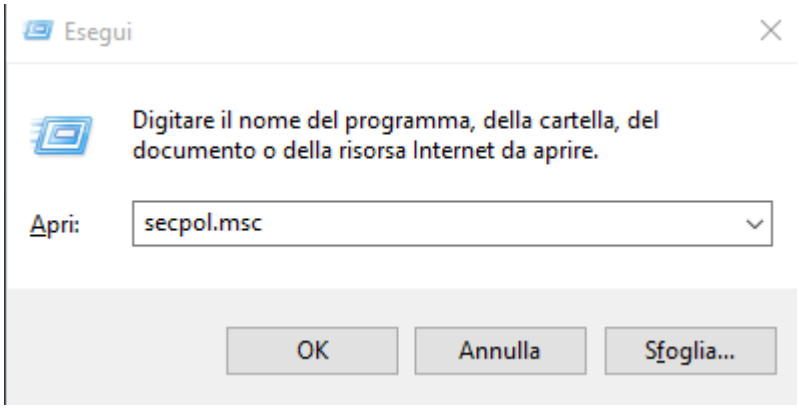
Non sovrascrivere eventi = sicurezza e tracciabilità, ma richiede disciplina e automazione per non bloccare la registrazione. (aziende)

Login/Logoff

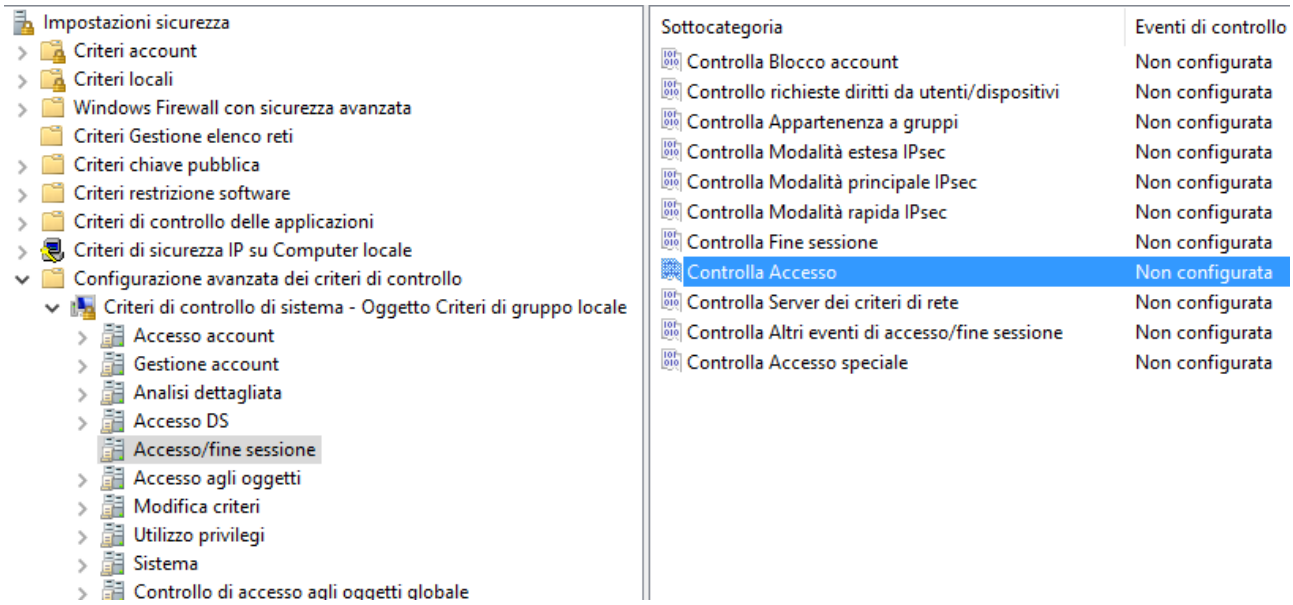
Nella finestra dei **Criteri di sicurezza locali** di Windows (Local Security Policy, “secpol.msc”) si possono trovare numerose impostazioni che regolano come il sistema gestisce aspetti critici di sicurezza, accessi(*login/logoff*), auditing, account e protezione delle risorse.

Il nostro scopo è quello di attivare la registrazione di eventi di login e di logoff, per farlo procediamo in questo modo:

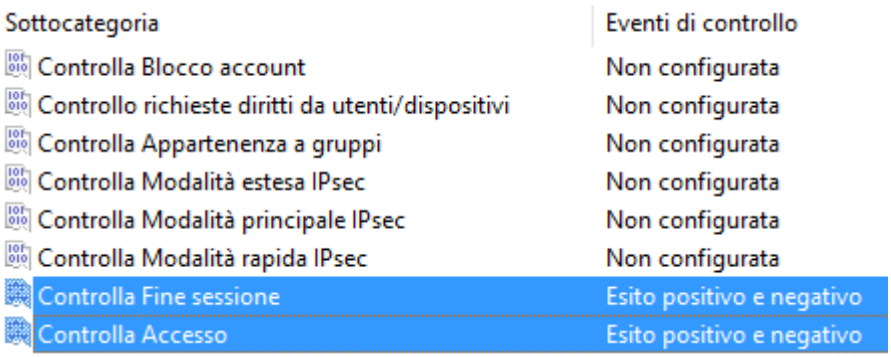
Apertura console Win+R, secpol.msc



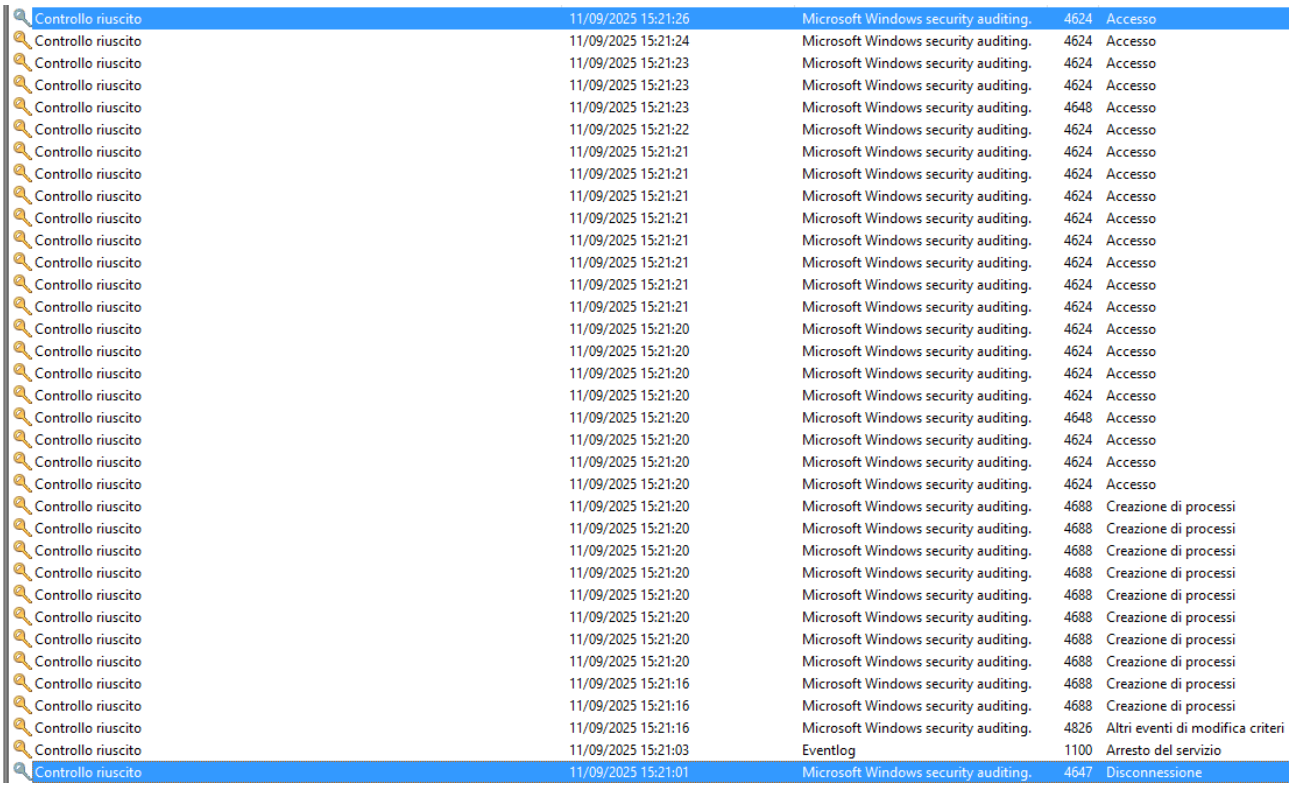
Navigazione all’interno di **Configurazione avanzata criteri di controllo**



Abilito i criteri di accesso/login e i criteri di fine sessione/logoff, sia con esito positivo che negativo



Infine, per verificare il corretto funzionamento delle regole appena implementate riavviamo la macchina e controlliamo i log. Il risultato è il seguente



```
Controllo riuscito    11/09/2025 15:21:26    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:24    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:23    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:23    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:23    Microsoft Windows security auditing.    4648    Accesso
Controllo riuscito    11/09/2025 15:21:22    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:21    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4648    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4624    Accesso
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:20    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:16    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:16    Microsoft Windows security auditing.    4688    Creazione di processi
Controllo riuscito    11/09/2025 15:21:16    Microsoft Windows security auditing.    4826    Altri eventi di modifica criteri
Controllo riuscito    11/09/2025 15:21:03    Eventlog                                1100    Arresto del servizio
Controllo riuscito    11/09/2025 15:21:01    Microsoft Windows security auditing.    4647    Disconnessione
```

Troviamo un log di disconnessione (**logoff**) con codice 4647 alle 15:21:01 (riavvio) e un log di accesso (**login**) alle 15:21:26 (avvio dopo il riavvio)

Con questo documento illustriamo in modo dettagliato alcune procedure di configurazione del registro sicurezza di windows. Questo report evidenzia l'importanza del monitoraggio degli eventi di sistema per garantire maggiore sicurezza. La corretta implementazione di regole come ad esempio la regola impostata per il login/logoff, ci permette di registrare in modo automatico informazioni cruciali come l'orario di login, l'utente che ha effettuato l'accesso e l'esito dell'operazione fornendo traccia di ogni passo per identificare attività sospette.

In sintesi dimostriamo come una configurazione mirata del registro di sistema sia uno strumento essenziale per la gestione della sicurezza informatica e la conformità delle normative interne.

-Simone Starvaggi