# Modifiche Apportate e Motivazioni

I file di log della sicurezza rappresentano una componente cruciale per garantire il monitoraggio delle attività di sistema e per rilevare eventuali anomalie o incidenti. Una corretta configurazione dei log consente di mantenere un equilibrio tra sicurezza, tracciabilità e gestione dello spazio di archiviazione. Questo documento illustra alcune modifiche chiave per ottimizzare la configurazione dei log di sicurezza in Windows, con particolare attenzione a tre aspetti fondamentali: dimensioni e sovrascrittura, registrazione degli eventi critici e protezione del registro di sicurezza.

Modifiche Apportate e Motivazioni

I file di log della sicurezza rappresentano una componente cruciale per garantire il monitoraggio delle attività di sistema e per rilevare eventuali anomalie o incidenti. Una corretta configurazione dei log consente di mantenere un equilibrio tra sicurezza, tracciabilità e gestione dello spazio di archiviazione. Questo documento illustra alcune modifiche chiave per ottimizzare la configurazione dei log di sicurezza in Windows, con particolare attenzione a tre aspetti fondamentali: dimensioni e sovrascrittura, registrazione degli eventi critici e protezione del registro di sicurezza.

Modifiche Apportate e Motivazioni

Questo documento descrive le modifiche apportate nella configurazione dei file di log della sicurezza in Windows, concentrandosi sui punti 1, 2 e 6. Sono inclusi i motivi per cui queste modifiche sono state implementate, con l'obiettivo di migliorare la sicurezza e la gestione dei log.

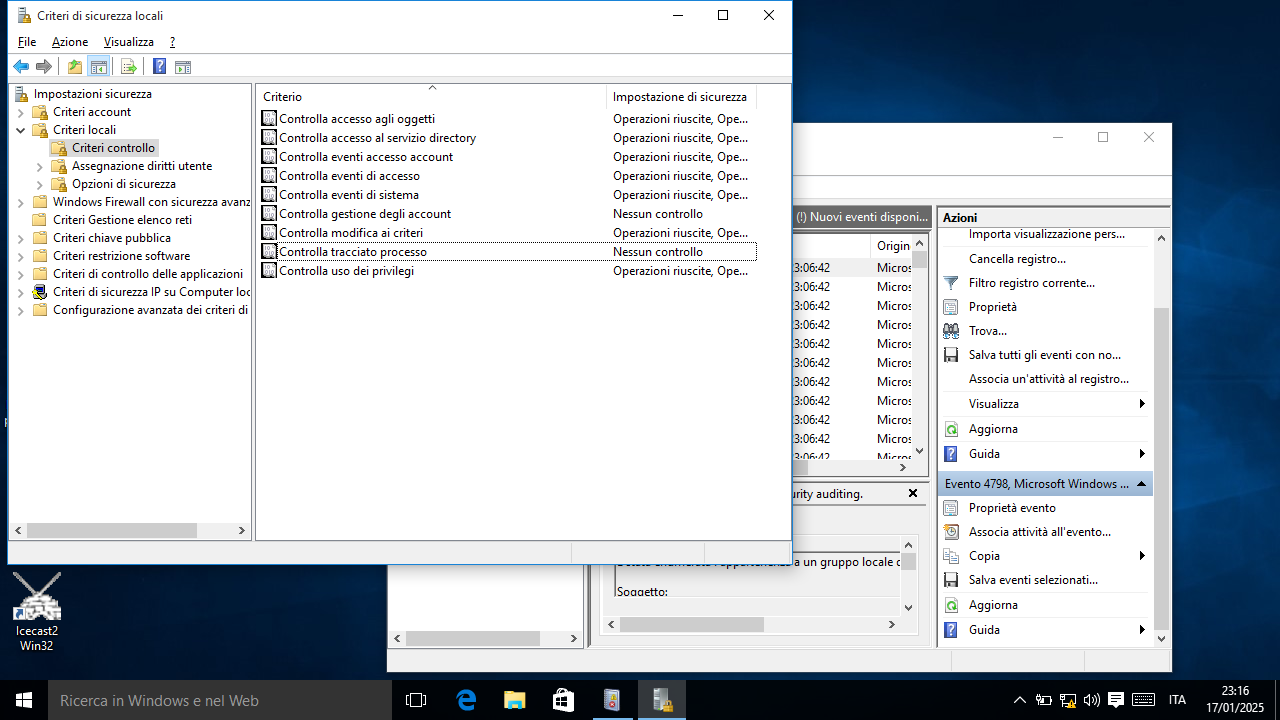
## 1. Configura Dimensioni e Sovrascrittura del Registro

Per garantire che i registri di sicurezza non vadano persi, è stata configurata una dimensione adeguata per il registro di sicurezza (es. 20 MB) e un comportamento di sovrascrittura specifico. Questo consente di mantenere un equilibrio tra l'archiviazione di dati storici importanti e lo spazio disponibile sul sistema.

Motivazione: La configurazione della dimensione massima evita la perdita di eventi critici a causa di uno spazio insufficiente. La scelta di sovrascrivere solo eventi più vecchi di un determinato numero di giorni consente di mantenere i dati recenti accessibili.

## 2. Attiva la Registrazione degli Eventi Critici

Screenshot relativo alla configurazione delle dimensioni del registro:



Sono stati abilitati i criteri di controllo per registrare eventi critici, come tentativi di accesso (riusciti e falliti), modifiche ai criteri di sicurezza e utilizzo di privilegi speciali. Queste configurazioni garantiscono una maggiore visibilità sulle attività di sistema.

Motivazione: La registrazione di eventi critici è fondamentale per rilevare attività sospette, investigare incidenti di sicurezza e assicurare la conformità alle normative aziendali o legali.

## 3. Proteggi il Registro di Sicurezza

Sono state configurate autorizzazioni specifiche per il registro di sicurezza, limitando l'accesso ai soli utenti con privilegi amministrativi. Questa modifica impedisce modifiche non autorizzate ai log, garantendo l'integrità dei dati.

Motivazione: Proteggere il registro di sicurezza è essenziale per evitare manipolazioni che potrebbero compromettere l'affidabilità dei dati e ostacolare le indagini su eventi di sicurezza.

Screenshot relativo alla configurazione delle dimensioni del registro:

Screenshot relativo alla protezione del registro di sicurezza:

