

CREAZIONE E GESTIONE DELLE REGOLE PER I FILE DI LOG DELLA SICUREZZA IN WINDOWS



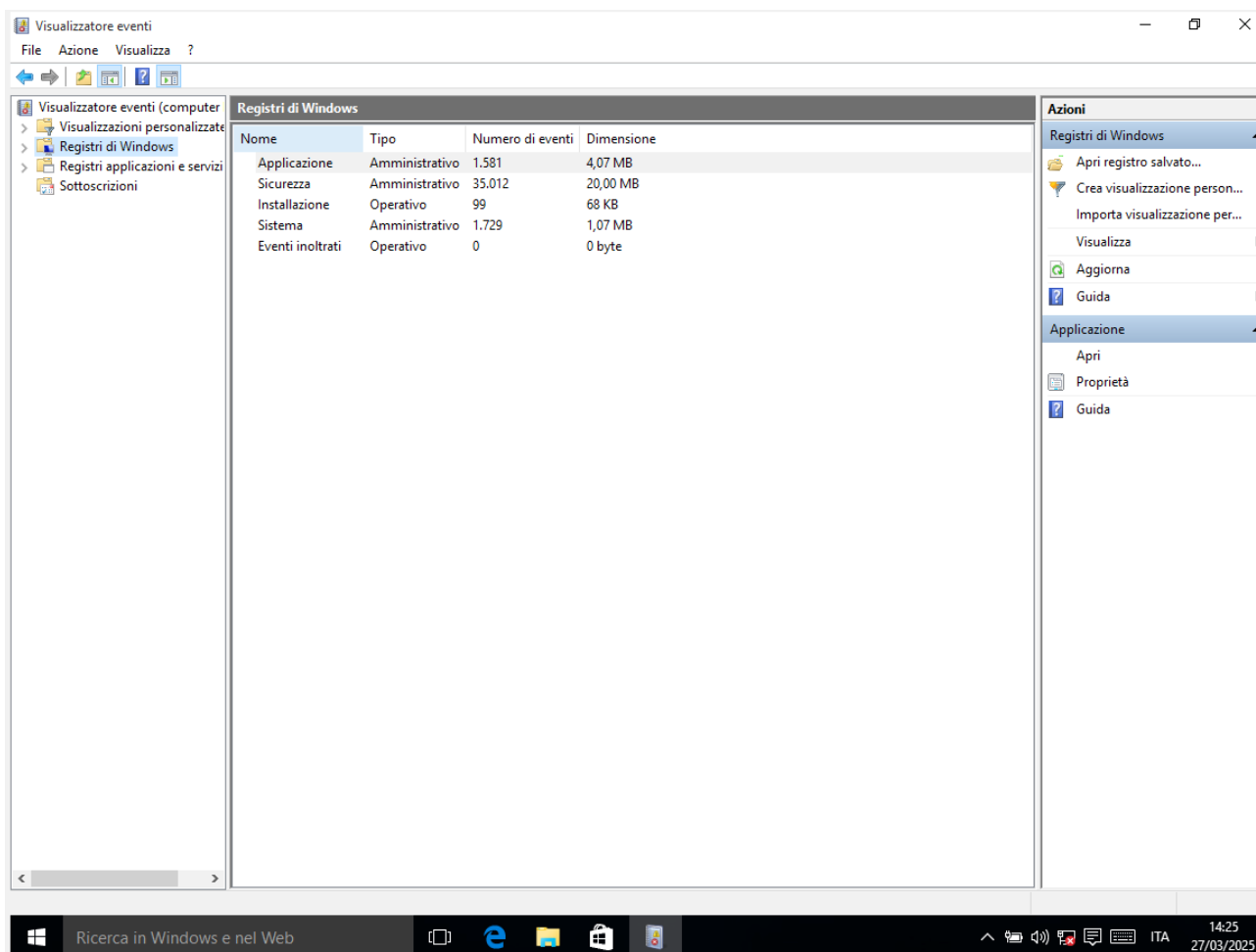
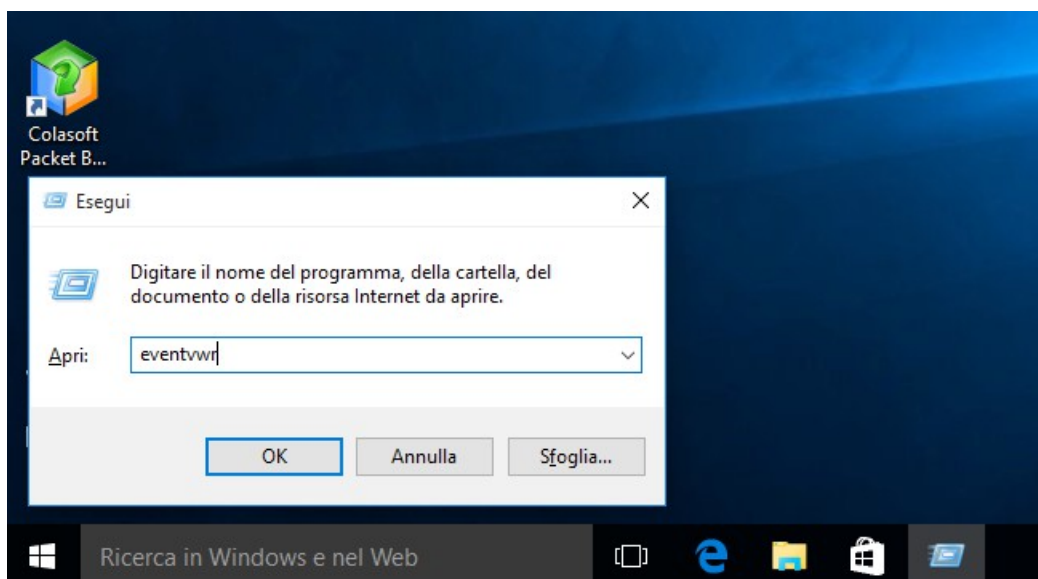
Configurare e gestire i file di log della sicurezza utilizzando il **Visualizzatore eventi di Windows**.

Il **Visualizzatore eventi di Windows** è uno strumento per monitorare e analizzare l'attività del sistema operativo. In termini semplici, registra eventi che si verificano nel computer, fornendo informazioni preziose per la diagnosi e la risoluzione di problemi.

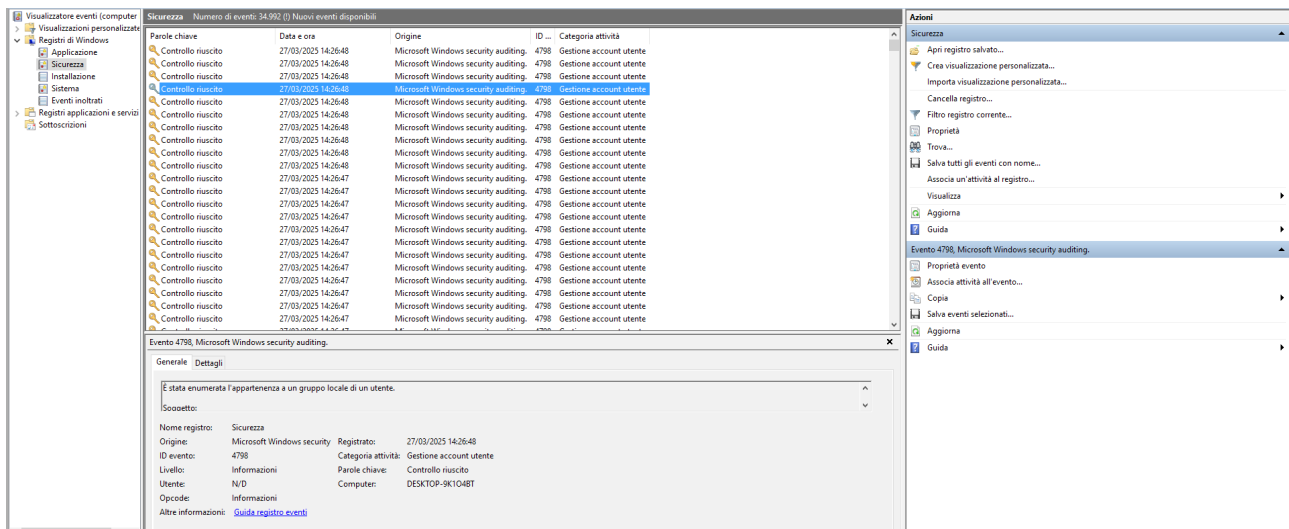
In particolare per il lato Sicurezza è possibile:

- Creare regole per rilevare tentativi di accesso non autorizzati, modifiche ai privilegi o attività sospette.
- Configurare notifiche immediate per gli amministratori di sistema in caso di eventi di sicurezza critici.

Per accedere al Visualizzatore Eventi bisogna premere la combinazione di tasti **Win + R** per aprire la finestra "**Esegui**" e digitare "**eventvwr**" e premere Invio.

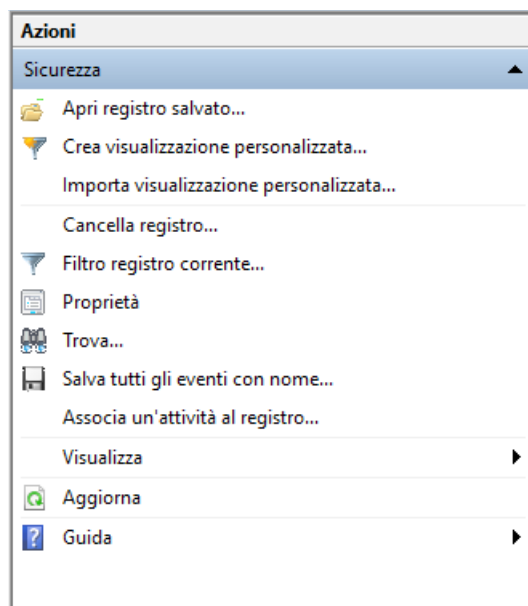


Per configurare le Proprietà del Registro di Sicurezza nel pannello di sinistra bisogna espandere **"Registri di Windows"** e seleziona **"Sicurezza"**.



Verrà restituita la schermata con elencati tutti gli eventi registrati inerenti la Sicurezza della macchina

Tramite il menù **Azioni** che si trova a destra, è possibile effettuare operazioni sul Registro, come per esempio applicare filtri sull'elenco, salvare il registro per una successiva consultazione, personalizzare le colonne di dettaglio visibili.



Andando a selezionare un singolo evento verrà aperta la schermata di dettaglio dello stesso.

[illegible]