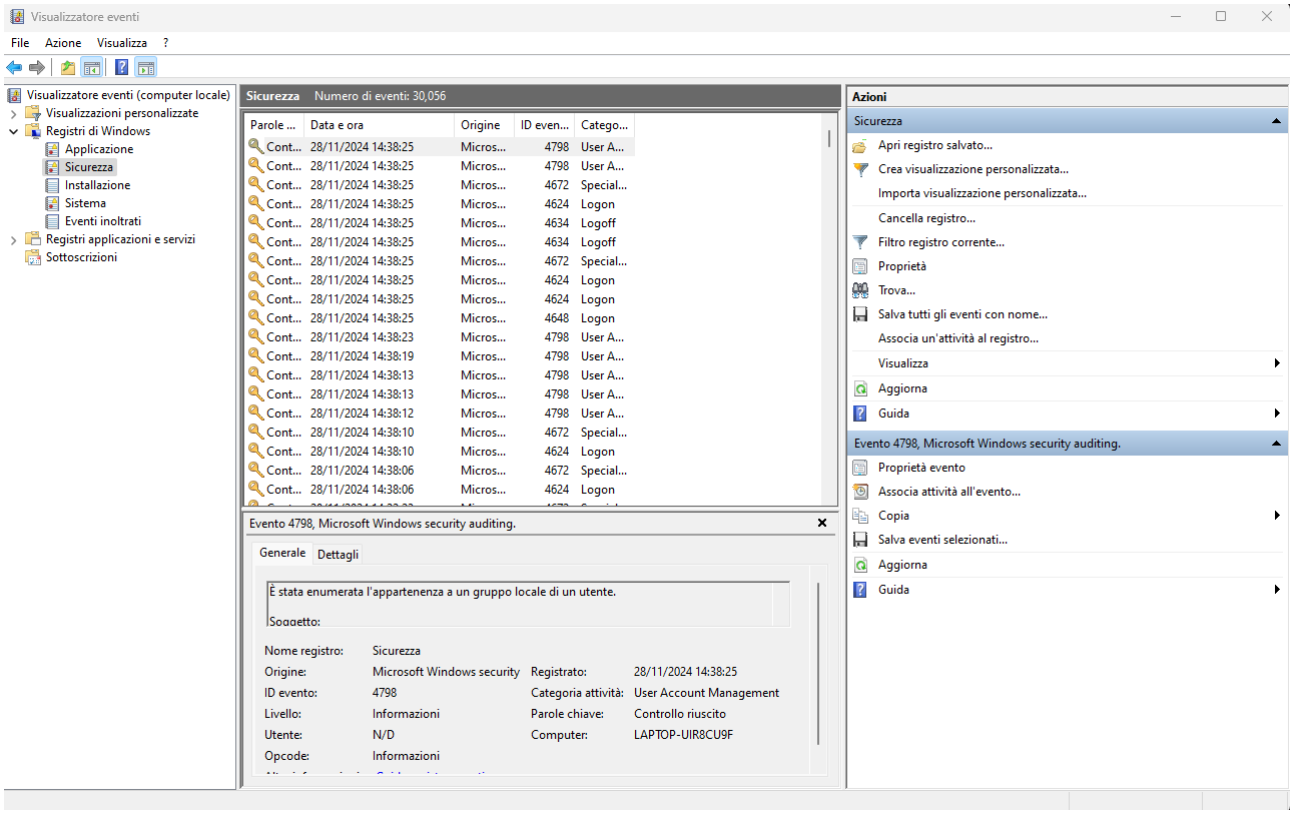
File Log Windows

Nell'esercitazione odierna siamo stati introdotti **all'event viewer** di **Windows**, mediante il quale è possibile configurare e gestire i file di log del sistema.

Nello specifico, mediante il comando **Win + R** è stata aperta la finestra esegui, nella quale mediante il comando **eventvwr** è stato possibile accedere ai file log.

In modo particolare siamo andati nella sezione sicurezza e da li possiamo controllare gli eventi relativi ai log della stessa.



I **file di log** sono file di testo che registrano eventi, attività o messaggi generati da un sistema, un software o un'applicazione. Servono come una sorta di **cronologia** delle operazioni, utile per monitorare, analizzare e diagnosticare il funzionamento del sistema. Essi forniscono informazioni come:

- **Informazioni su eventi** (es. accessi, errori, avvii, arresti).
- **Timestamp** per indicare quando è avvenuto un evento.
- ***Dettagli come IP, utenti, messaggi di errore***.

Mediante essi inoltre si può effettuare:

- **Monitoraggio**: Analizzare il funzionamento del sistema o dell'applicazione.
- **Debugging**: Trovare e correggere errori.
- **Sicurezza**: Rilevare accessi sospetti o comportamenti anomali.
- **Auditing**: Tracciare modifiche o attività per motivi legali o normativi.