

File di Log di Windows

profilo studente

data: 04/02/2026

studente: Gabriel Giustinelli

Epicode Classe: CS0525

Cyber Sercurity Specialist

Obiettivo

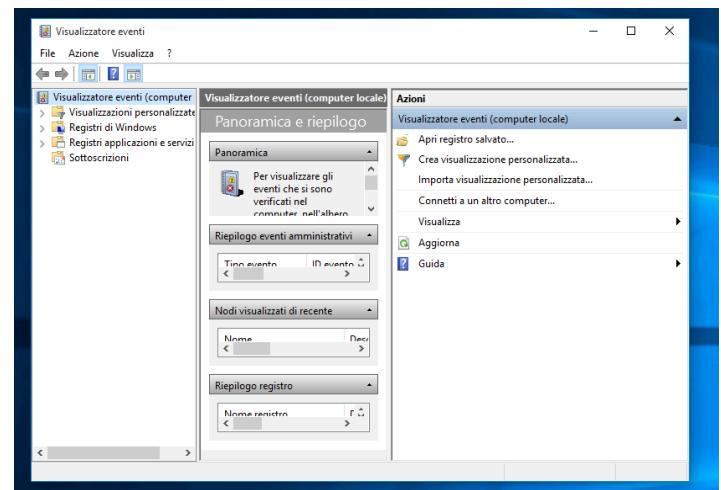
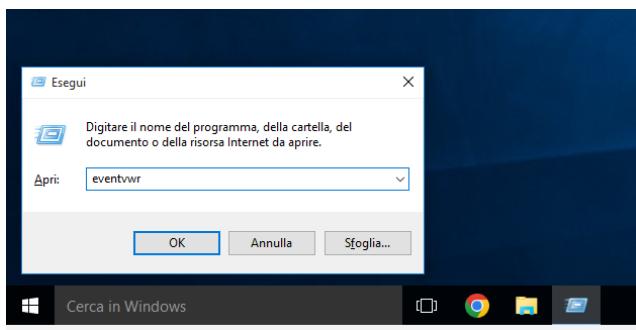
Creazione e Gestione delle Regole per i File di Log della Sicurezza, utilizzando il Visualizzatore eventi in Windows.

Andando a impostare il log dei **login/logout** così da visualizarli nello strumento di visualizzazione eventi di windows.

1. Accesso al Visualizzatore Eventi

Queste sono istruzioni rapide per aprire lo strumento:

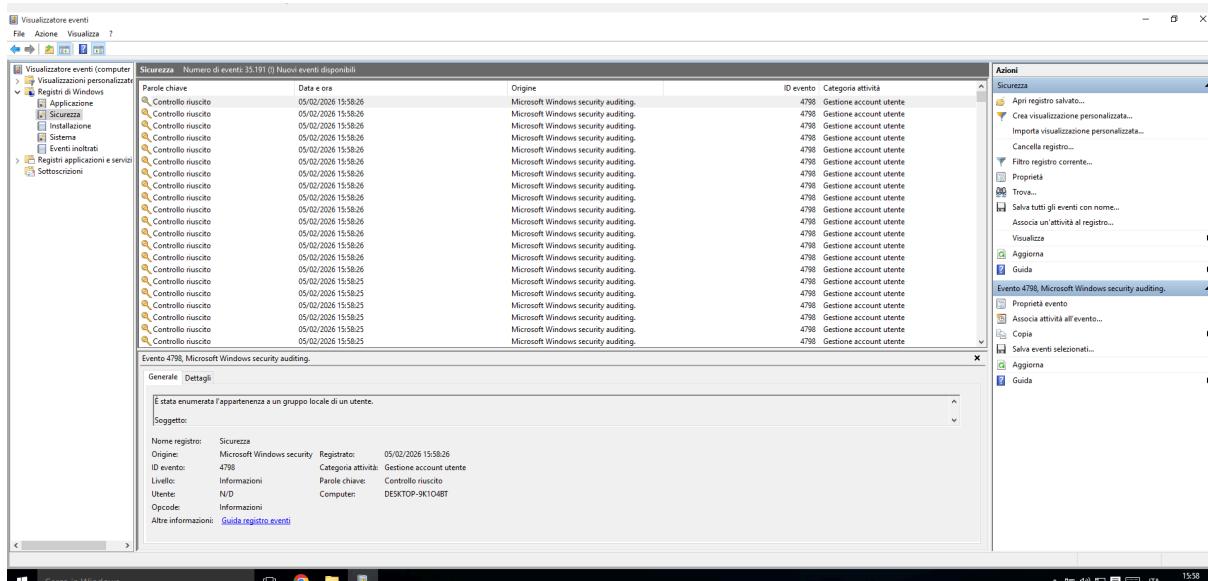
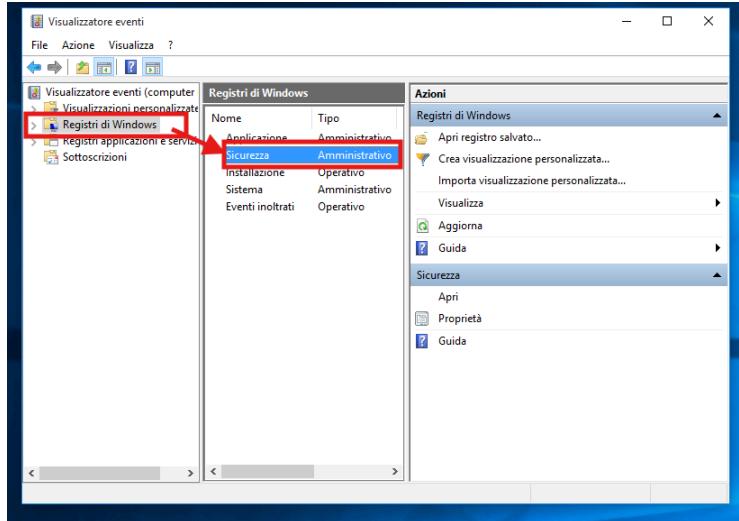
- si premono contemporaneamente i tasti di **win +R** sulla tastiera
- nella finestra “esegui” che apparirà si inserisce **eventvwr**
- una volta mandato si aprirà il visualizzatore di eventi



2. Configurazione del Registro di Sicurezza

Dal visualizzatore di eventi andiamo a individuare i log che ci interessano

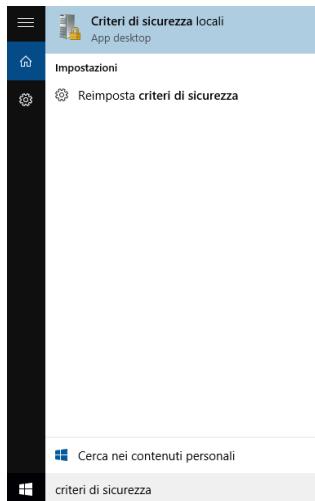
- per espandere la categoria andiamo su **registri di windows** nel pannello di sinistra
 - Selezionando la voce **sicurezza**, vedremo l'elenco di tutti gli eventi di sicurezza registrati dal sistema windows.



3. Impostare il log dei Login/Logoff

Per visualizzare i **login/logout** nel visualizzatore eventi, Windows deve avere quei criteri di controllo attivi.

- Dalla barra di ricerca di windows si scrive **Criteri di sicurezza**



- da lì andiamo su **Criteri locali** e nella sezione di **Criteri controllo**
- una volta dentro cerchiamo la voce **Controlla eventi di accesso**
- Con un doppio clic facciamo l'accesso e andiamo a spuntare le caselle di **Operazioni riuscite** e **Operazioni non riuscite**

The image consists of three screenshots of the Windows Local Security Policy snap-in:

- Screenshot 1:** Shows the left navigation pane with "Criteri di sicurezza locali" expanded, and "Criteri locali" selected. A red arrow points to "Criteri locali". The main pane displays a table with two rows: "Criteri controllo" and "Criteri account".
- Screenshot 2:** Shows the "Criteri controllo" table with "Criteri controllo" selected. A red arrow points to "Criteri controllo". The right pane shows the "Criteri" section with "Controlla eventi di accesso" selected. A red box highlights this item, and another red box highlights the "Operazioni riuscite, Ope..." entry in the "Impostazione di sicurezza" column.
- Screenshot 3:** A detailed view of the "Controlla eventi di accesso" properties. It shows the "Controlla i seguenti tentativi:" section with both "Operazioni riuscite" and "Operazioni non riuscite" checked. A warning message at the bottom states: "È possibile che questa impostazione non venga utilizzata se un altro criterio è configurato per sostituire il criterio di controllo a livello di categoria. Per ulteriori informazioni, vedere [Controlla eventi di accesso](#). (Q921468)".

Log in/off

Da questo momento ogni volta che qualcuno entra o esce dal pc, il Visualizzatore Eventi creerà un nuovo record nel registro sicurezza che abbiamo aperto.

Controllo riuscito	05/02/2026 16:40:19	Microsoft Windows security auditing.	4634 Disconnessione
Controllo riuscito	05/02/2026 16:40:19	Microsoft Windows security auditing.	4634 Disconnessione
Controllo riuscito	05/02/2026 16:40:19	Microsoft Windows security auditing.	4798 Gestione account utente
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4672 Accesso speciale
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4672 Accesso speciale
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4627 Appartenenza a gruppi
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4624 Accesso
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4627 Appartenenza a gruppi
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4624 Accesso
Controllo riuscito	05/02/2026 16:40:18	Microsoft Windows security auditing.	4648 Accesso

- **ID 4624 (Accesso):** Indica che l'utente è entrato nel sistema con successo.
- **ID 4634 (Disconnessione):** Indica la chiusura della sessione.
- **ID 4672 (Accesso speciale):** Indica che l'account che ha effettuato l'accesso ha privilegi da amministratore.

La presenza degli ID mostrati, dimostra che i criteri di controllo sono attivi e monitorano correttamente i privilegi e gli accessi degli utenti