

File di Log di Windows

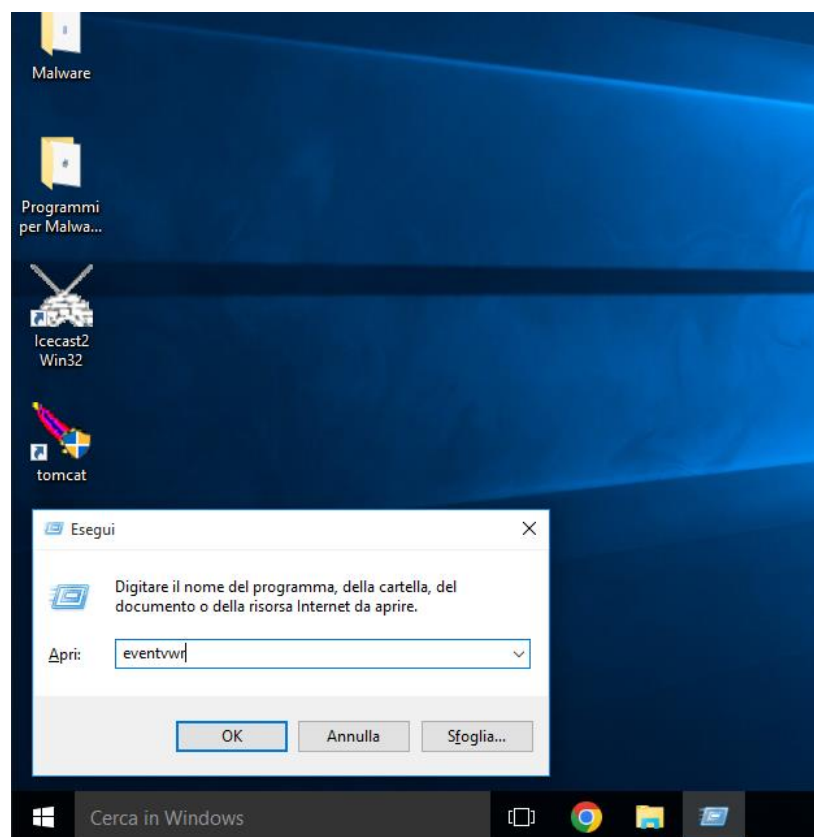
Executive Summary

Il documento presenta un'analisi condotta sui registri di sicurezza di Windows della macchina **Windows10**. L'obiettivo del report è monitorare l'attività di accesso e disconnessione. (**Login/Logoff**)

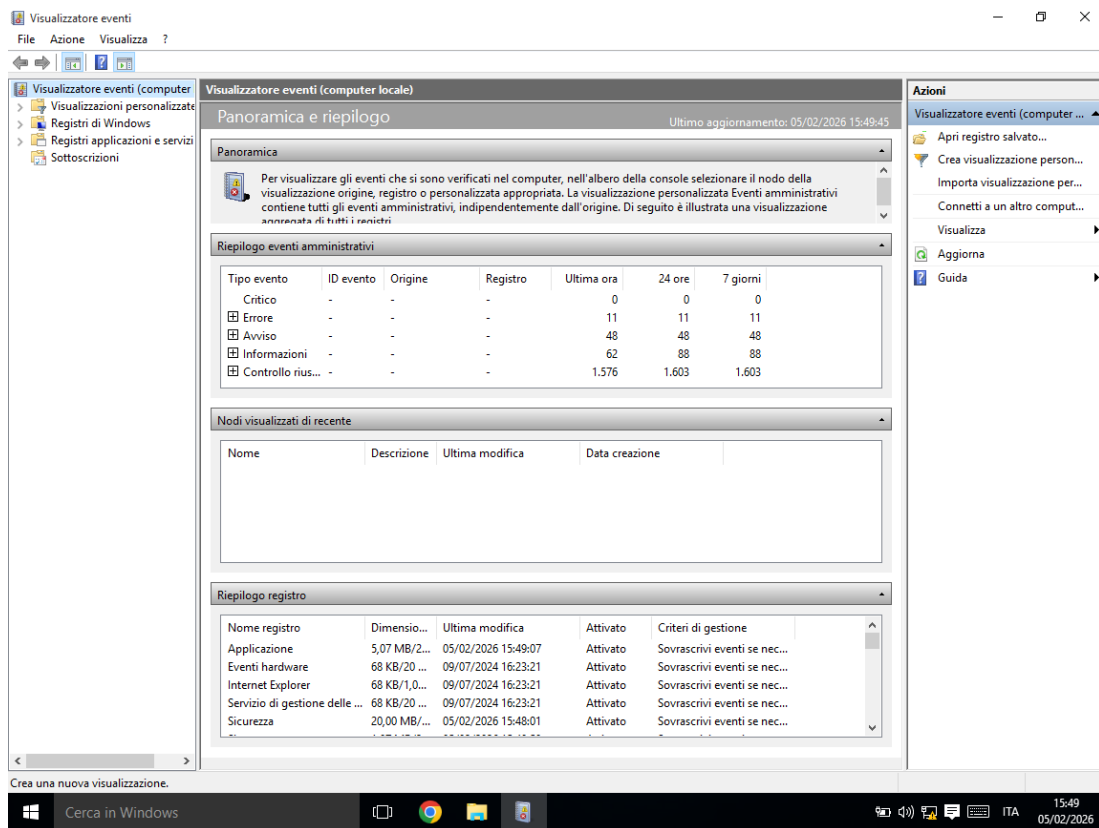
Strumenti Laboratorio

- **Windows10:** macchina host
 - **Event viewer:** gestione log
-

Fase1 – Accesso Event Viewer



**Fig.1 Accesso al registro*

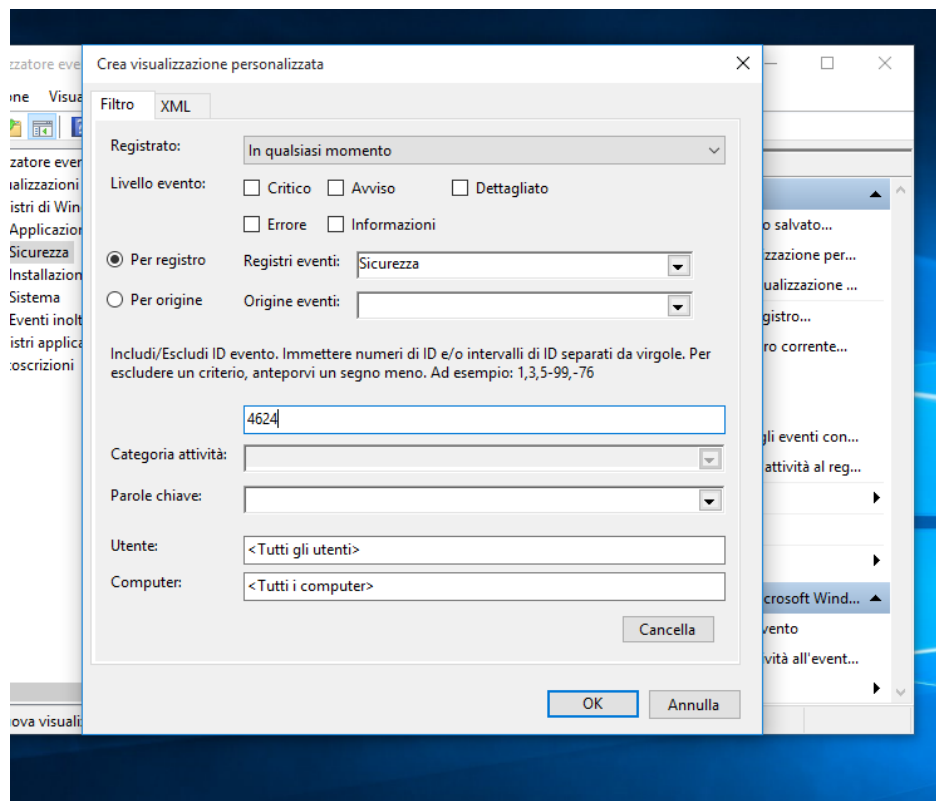


**Fig.2 Schermata principale Visualizzatore Eventi*

L'accesso al registro è stato eseguito tramite la combinazione di tasti **Win + R**, digitando il comando **eventvwr** che permette l'accesso alla schermata principale dei log di sistema.

Fase2 – Gestione dei Log

1) Log Login



*Fig.4 Filtraggio log accessi

Numero di eventi: 103

Livello	Data e ora	Origine	ID evento	Categoria attività
Informazioni	05/02/2026 17:12:58	Microsoft Windo...	4624	Accesso
Informazioni	05/02/2026 17:12:55	Microsoft Windo...	4624	Accesso
Informazioni	05/02/2026 17:12:54	Microsoft Windo...	4624	Accesso
Informazioni	05/02/2026 17:12:52	Microsoft Windo...	4624	Accesso
Informazioni	05/02/2026 17:12:52	Microsoft Windo...	4624	Accesso
Informazioni	05/02/2026 17:12:52	Microsoft Windo...	4624	Accesso

Evento 4624, Microsoft Windows security auditing.

Generale Dettagli

Accesso di un account riuscito.

Soggetto:

- ID sicurezza: SYSTEM
- Nome account: DESKTOP-9K1O4BT\$
- Dominio account: WORKGROUP
- ID accesso: 0x3E7

Informazioni di accesso:

- Tipo di accesso: 5
- Modalità amministrativa limitata: -
- Account virtuale: No
- Token elevato: Sì

Livello rappresentazione: Rappresentazione

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 05/02/2026 17:12:58

ID evento: 4624 Categoria attività: Accesso

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: DESKTOP-9K1O4BT

Opcode: Informazioni

Altre informazioni: [Guida registro eventi](#)

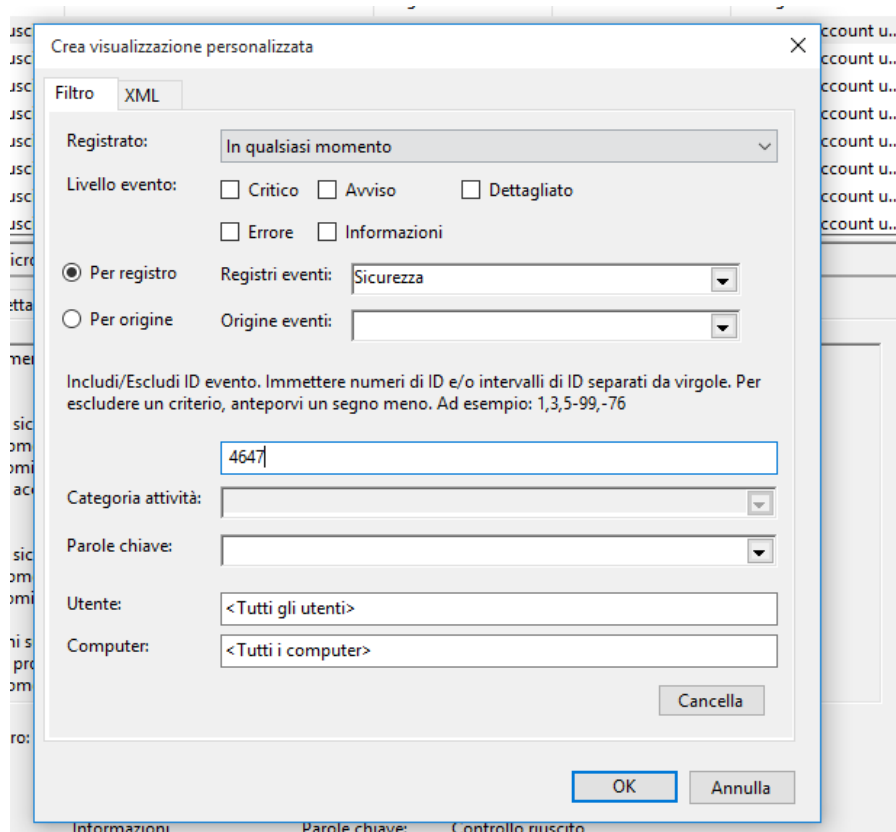
*Fig.5 Filtro login attivo

Per analizzare correttamente le sessioni di accesso, è stata creata una regola di filtraggio impostando il parametro **ID evento: 4624**. Questa configurazione permette di isolare esclusivamente i log relativi agli **accessi riusciti**, facilitando il monitoraggio delle attività degli utenti e del sistema.

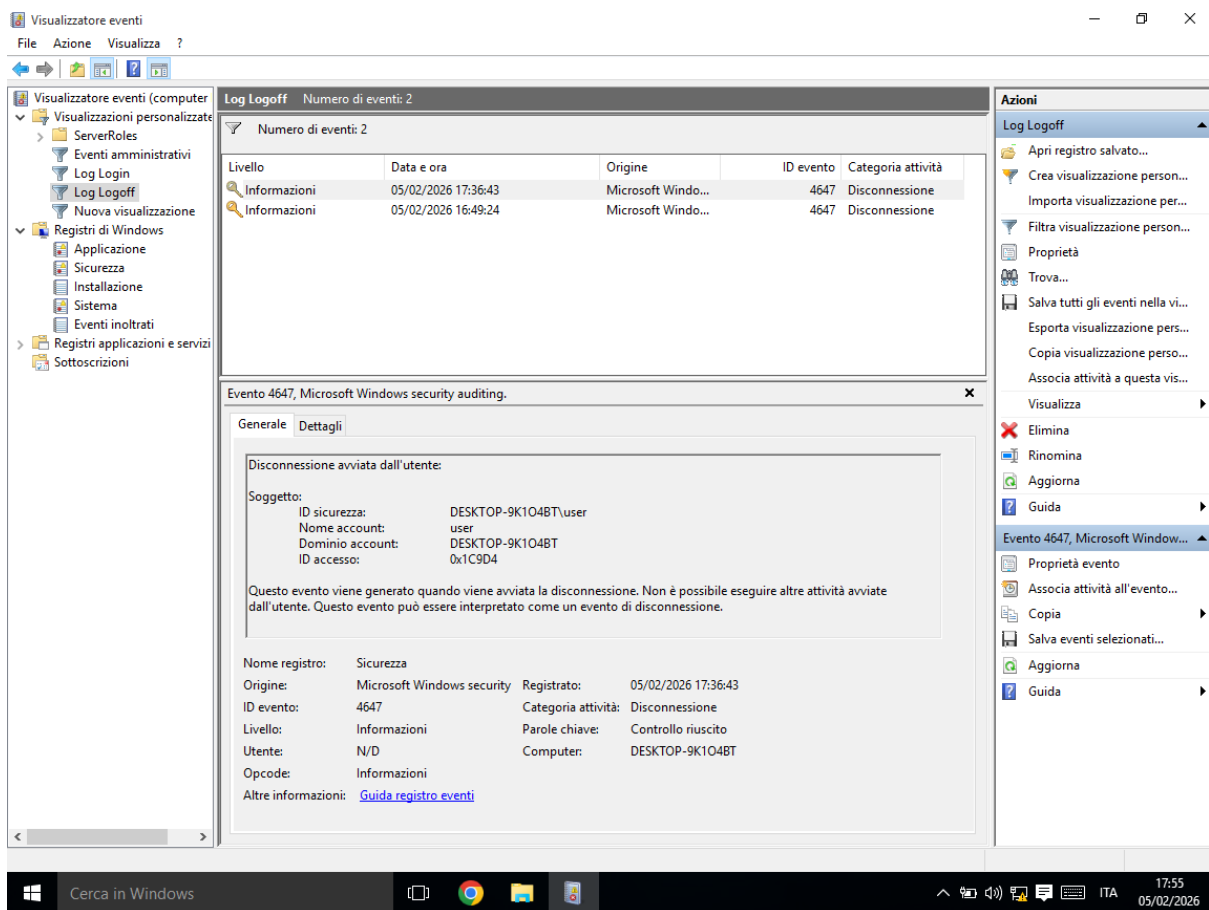
È stata verificata l'efficacia del filtro applicato isolando l'**Event ID 4624**, che conferma un **accesso riuscito** sul computer **DESKTOP-9K1O4BT** in data **05/02/2026 alle 17:12:58**.

I dettagli indicano un **accesso di servizio (Logon Type 5)** eseguito dall'account **NT AUTHORITY\SYSTEM** che rappresenta l'attivazione di un processo o servizio di sistema sul computer **DESKTOP-9K1O4BT**.

2) Log Logoff



**Fig.6 Filtraggio log disconnessioni*



**Fig. 7 Filtro logoff attivo*

Per analizzare i log di logoff, si è proceduto alla creazione di un filtro, inserendo il valore **4647** nel campo degli **ID evento**, questo ci permette di vedere il momento esatto in cui un utente avvia la procedura di **logoff**.

Una volta creato il filtro del logoff, viene evidenziato che l'utente **user** ha terminato manualmente la propria sessione sul computer **DESKTOP-9K1O4BT** in data **05/02/2026** alle **17:36:43**.

Conclusione

L'analisi condotta dimostra come i filtri nel Visualizzatore Eventi sia uno strumento attraverso il quale è stato possibile distinguere con precisione tra dei servizi e le sessioni degli utenti, eliminando il rumore di fondo che spesso nasconde tentativi di intrusione.

Per un **analista SOC**, riuscire a distinguere istantaneamente tra un normale accesso di sistema e un'attività anomala di un utente rappresenta la prima linea di difesa contro le intrusioni.