

# REPORT S9/L4

## File di Log di Windows

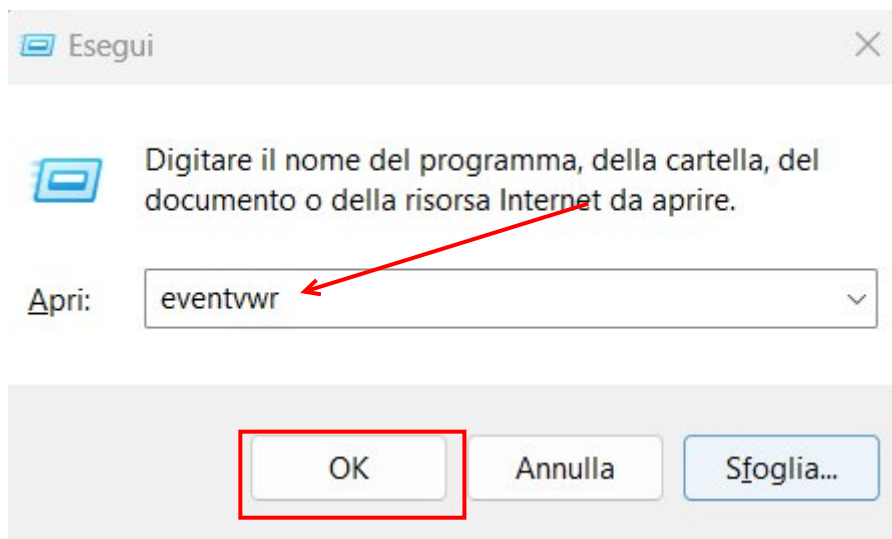
### Traccia

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

1. Accedere al Visualizzatore Eventi:
  - Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
  - Digita eventvwr e premi Invio.
2. Configurare le Proprietà del Registro di Sicurezza:
  - Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".
3. Analizzare gli eventi con Categoria Attività Logon e Special Logon

### Svolgimento

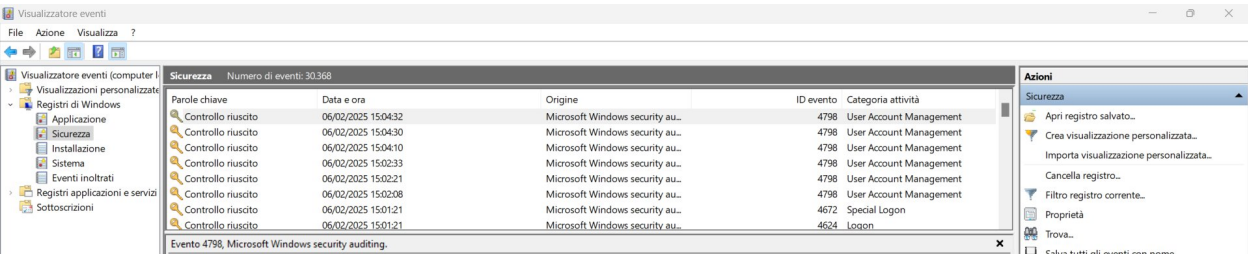
Per svolgere l'esercizio di oggi seguiamo i passaggi scritti nella consegna:



Premendo **Win + R** e digitando **eventvwr** (Event Viewer) otteniamo:



Poi spostandoci su **Registri di Windows, Sicurezza**:



A questo punto possiamo analizzare gli eventi della categoria **Logon e Special Logon**:

	Controllo riuscito	30/01/2025 12:19:05	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	30/01/2025 12:19:05	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	30/01/2025 12:54:59	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	05/02/2025 13:04:24	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	30/01/2025 12:55:00	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	30/01/2025 12:42:49	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	05/02/2025 13:04:24	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	05/02/2025 09:04:02	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	30/01/2025 12:50:49	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	30/01/2025 12:54:58	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	06/02/2025 11:39:28	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	03/02/2025 09:00:02	Microsoft Windows security au...	4624	Logon
	Controllo riuscito	03/02/2025 17:29:06	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	06/02/2025 10:07:24	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	29/01/2025 10:27:28	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	28/01/2025 10:42:28	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	29/01/2025 10:27:29	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	03/02/2025 13:30:31	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	03/02/2025 09:09:04	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	06/02/2025 10:06:34	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	03/02/2025 09:06:05	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	06/02/2025 13:14:50	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	03/02/2025 17:03:52	Microsoft Windows security au...	4672	Special Logon
	Controllo riuscito	06/02/2025 10:07:14	Microsoft Windows security au...	4672	Special Logon

Ricordiamo che la differenza tra "logon" e "special logon" si riferisce al tipo di sessione di accesso in un sistema operativo di Windows. Un logon standard è l'accesso normale a un sistema, mentre un "special logon" è un tipo di logon che ha privilegi di amministratore equivalente e può essere utilizzato per elevare un processo a un livello superiore. **Un logon speciale può essere utile per monitorare eventuali attività sospette, come tentativi di accesso con privilegi elevati o movimenti laterali di un attaccante all'interno di un sistema.**

Per analizzare più precisamente gli eventi basterà cliccare su un evento, premere il tasto destro e cliccare su “proprietà evento” per avere maggiori dettagli:

Controllo riuscito	30/01/2025 20:28:22		Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	03/02/2025 14:46:35	Proprietà evento	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	31/01/2025 10:27:28	Associa attività all'evento...	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	03/02/2025 10:27:28	Copia	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	29/01/2025 10:27:28	Salva eventi selezionati...	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	30/01/2025 10:27:28	Aggiorna	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	03/02/2025 10:27:28	?	Microsoft Windows security au...	4672	Special Logon
Controllo riuscito	05/02/2025 14:46:35		Microsoft Windows security au...	4672	Special Logon

La schermata che ci appare sarà di questo tipo:

Proprietà evento - Evento 4672, Microsoft Windows security auditing.

Generale

Dettagli

Privilegi speciali assegnati a nuovo accesso.

Soqgetto:

ID sicurezza:SYSTEM

Nome account:SYSTEM

Dominio account:NT AUTHORITY

ID accesso:0x3E7

Privilegi:

SeAssignPrimaryTokenPrivilege

SeTcbPrivilege

SeSecurityPrivilege

SeTakeOwnershipPrivilege

SeLoadDriverPrivilege

SeBackupPrivilege

SeRestorePrivilege

SeDebugPrivilege

SeAuditPrivilege

SeSystemEnvironmentPrivilege

SeImpersonatePrivilege

SeDelegateSessionUserImpersonatePrivilege

Nome registro: Sicurezza

Origine: Microsoft Windows security auditing

ID evento: 4672

Livello: Informazioni

Utente: N/D

Opcode: Informazioni

Altre informazioni: [Guida registro eventi](#)

Registrato: 29/01/2025 10:27:28

Categoria attività: Special Logon

Parole chiave: Controllo riuscito

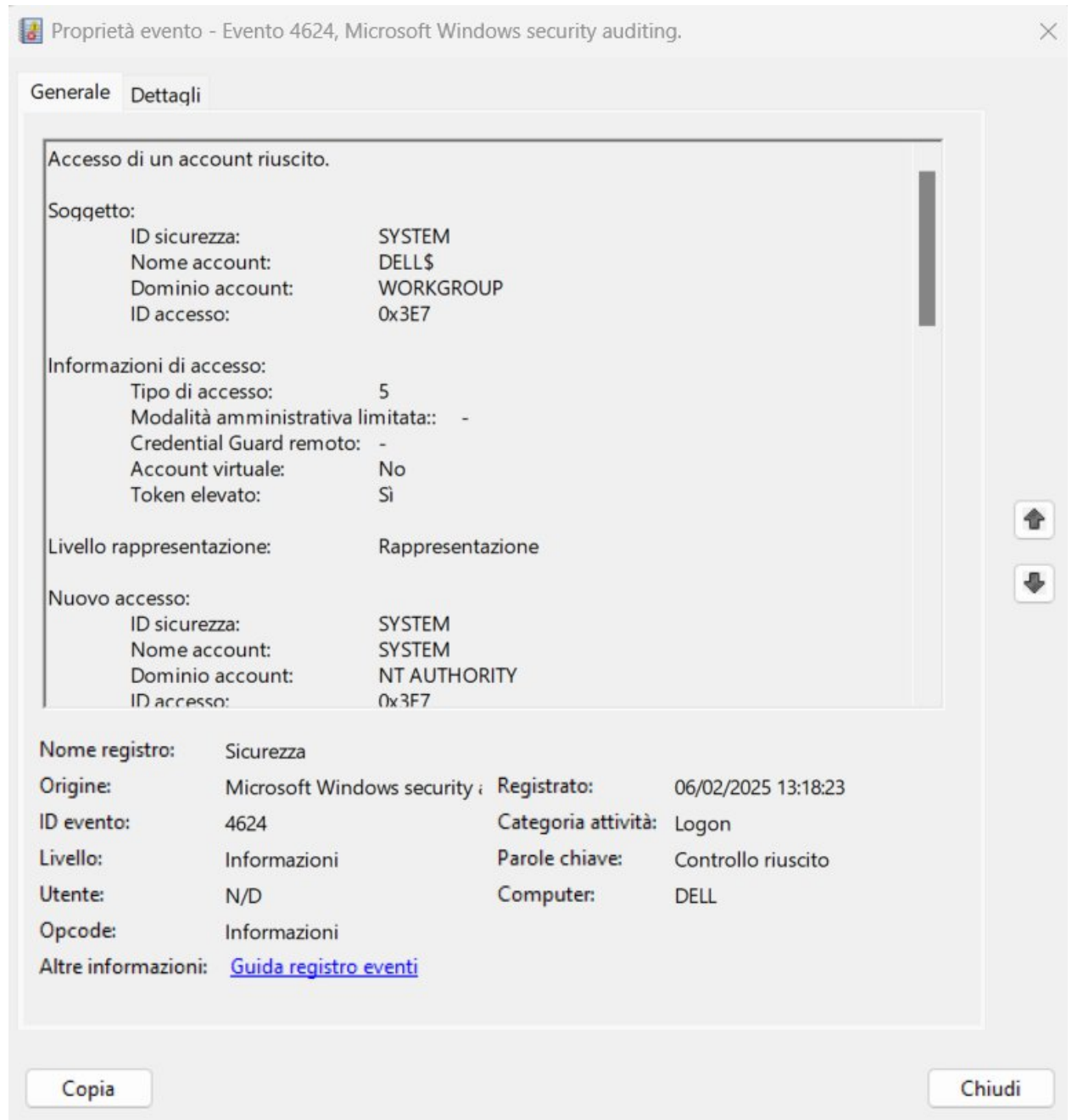
Computer: DELL

Copia

Chiudi

L'ID dell'evento ci dice quale evento si è verificato e dalla finestra dei dettagli capiamo cosa analizzare e perchè. Ad esempio:

#### Eventi di Accesso (ID 4624)



Questo evento viene generato quando viene creata una sessione di accesso.

Il campo **Soggetto** indica l'account nel sistema locale che ha richiesto l'accesso. Generalmente si tratta di un servizio, quale il servizio Server, o di un processo locale, ad esempio Winlogon.exe o Services.exe.

Il campo **Tipo di accesso** indica il tipo di accesso che è stato effettuato. I tipi più comuni sono 2 (interattivo) e 3 (rete).



Il campo **Nuovo accesso** indica l'account per il quale è stato creato il nuovo accesso, vale a dire l'account che ha effettuato l'accesso.

I campi **Informazioni di rete** indicano l'origine della richiesta di accesso remoto. Il nome della workstation non è sempre disponibile e può essere vuoto in alcuni casi.

Il campo **Livello rappresentazione** indica la portata della rappresentazione consentita a un processo nella sessione di accesso.

Il campo **Informazioni di autenticazione** fornisce informazioni dettagliate sulla specifica richiesta di accesso.

- GUID è un identificatore univoco che può essere utilizzato per correlare questo evento a un evento KDC (key distribution center è parte di un crittosistema il cui scopo è ridurre i rischi dovuti allo scambio delle chiavi).
- Servizi transitati indica quali servizi intermedi hanno partecipato alla richiesta di accesso.
- Nome pacchetto indica quale sotto-protocollo dei protocolli NTLM (NT LAN Manager è una suite di protocolli di autenticazione sviluppati da Microsoft che fornisce autenticazione, integrità e confidenzialità agli utenti nelle reti Windows) è stato utilizzato.
- Lunghezza chiave indica la lunghezza della chiave di sessione generata. Se non è stata richiesta alcuna chiave di sessione, la lunghezza sarà 0.

Vediamo ora un breve elenco degli ID più comuni.

**EventID 528:** Un utente si è connesso al computer. Questo evento può essere di tipo interattivo, rete, batch, servizio, sblocco, testo non crittografato in rete, nuove credenziali, remote interactive o cached interactive.

**EventID 529:** Errore di accesso. È stato effettuato un tentativo di accesso con un nome utente sconosciuto o con un nome utente noto ma password errata.

**EventID 530:** Errore di accesso. È stato effettuato un tentativo di accesso con un account utente oltre il tempo consentito.

**EventID 531:** Errore di accesso. È stato effettuato un tentativo di accesso con un account disattivato.

**EventID 532:** Errore di accesso. È stato effettuato un tentativo di accesso con un account scaduto.

**EventID 534:** Errore di accesso. L'utente ha tentato di connettersi con un tipo di accesso non consentito.

**EventID 4624:** Logon riuscito. L'utente si autentica con successo sul sistema. Contiene informazioni sul tipo di logon (interattivo, remoto, ecc.), sull'utente e sul dominio.

**EventID 4625:** An account failed to log on, fa parte della categoria "Logon/Logoff" e può essere utile per individuare e monitorare tutti i tentativi di logon falliti.

**EventID 4672:** Special privileges assigned to new logon, fa parte della categoria "Logon/Logoff" e viene registrato a seguito di un evento 4624 (An account was successfully logged on).

**EventID 4740:** Account bloccato. Registrato quando un account utente viene bloccato, solitamente a causa di troppi tentativi di accesso falliti.