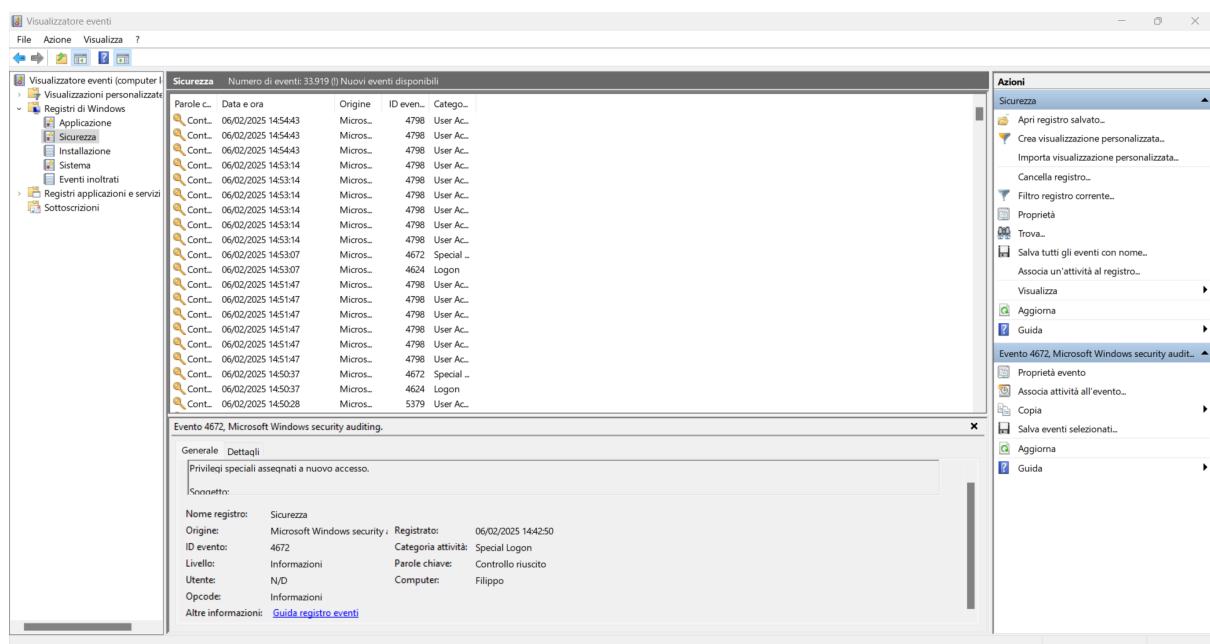


# REPORT S9/L4

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

## SVOLGIMENTO

Ho aperto il Visualizzatore Eventi col comando *eventvwr*, dopo di che sono andato nella sezione Registri di Windows e ho selezionato la voce Sicurezza.



Tra i vari eventi presenti ho analizzato quelli di **Logon** e **Special Logon**.

Per trovare gli eventi in questione ho filtrato i veri eventi.

Filtro registro corrente

Filtro XML

Registrato: In qualsiasi momento

Livello evento: ☐ Critico ☐ Avviso ☐ Dettagliato  
☐ Errore ☐ Informazioni

☒ Per registro Registri eventi: Sicurezza

☐ Per origine Origine eventi:

Includi/Escludi ID evento. Immettere numeri di ID e/o intervalli di ID separati da virgole. Per escludere un criterio, anteporvi un segno meno. Ad esempio: 1,3,5-99,-76

4626,4625,4672

Categoria attività:

Parole chiave:

Utente: <Tutti gli utenti>

Computer: <Tutti i computer>

Cancella

OK Annulla

Filtrati: Registro: Security; Origine: ; ID evento: 4626,4625,4672. Numero di eventi: 958

Parole c...	Data e ora	Origine	ID even...	Catego...
Cont...	06/02/2025 17:40:22	Micros...	4672	Special ...
Cont...	06/02/2025 17:39:42	Micros...	4672	Special ...
Cont...	06/02/2025 17:39:39	Micros...	4672	Special ...
Cont...	06/02/2025 17:39:38	Micros...	4672	Special ...
Cont...	06/02/2025 17:32:44	Micros...	4672	Special ...
Cont...	06/02/2025 17:29:14	Micros...	4672	Special ...

Evento 4672, Microsoft Windows security auditing.

Generale Dettagli

Privilegi speciali assegnati a nuovo accesso.

Soggetto:

ID sicurezza: SYSTEM

Nome account: [REDACTED]

Dominio account: NT AUTHORITY

ID accesso: 0x3E7

Privilegi:

- SeAssignPrimaryTokenPrivilege
- SeTcbPrivilege
- SeSecurityPrivilege
- SeTakeOwnershipPrivilege
- SeLoadDriverPrivilege
- SeBackupPrivilege
- SeRestorePrivilege
- SeDebugPrivilege

Nome registro: Sicurezza

Origine: Microsoft Windows security ; Registrato: 06/02/2025 17:40:22

ID evento: 4672 Categoria attività: Special Logon

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: [REDACTED]

Opcode: Informazioni

Altre informazioni: [Guida registro eventi](#)

Risultato della ricerca di uno **Special Logon**.

Vengono fornite informazioni dettagliate, tra cui data, ora e ID utente, per analizzare il comportamento del sistema in relazione alla sicurezza e agli accessi.