Configurazione e Gestione dei Log di Sicurezza in Windows

S9L4

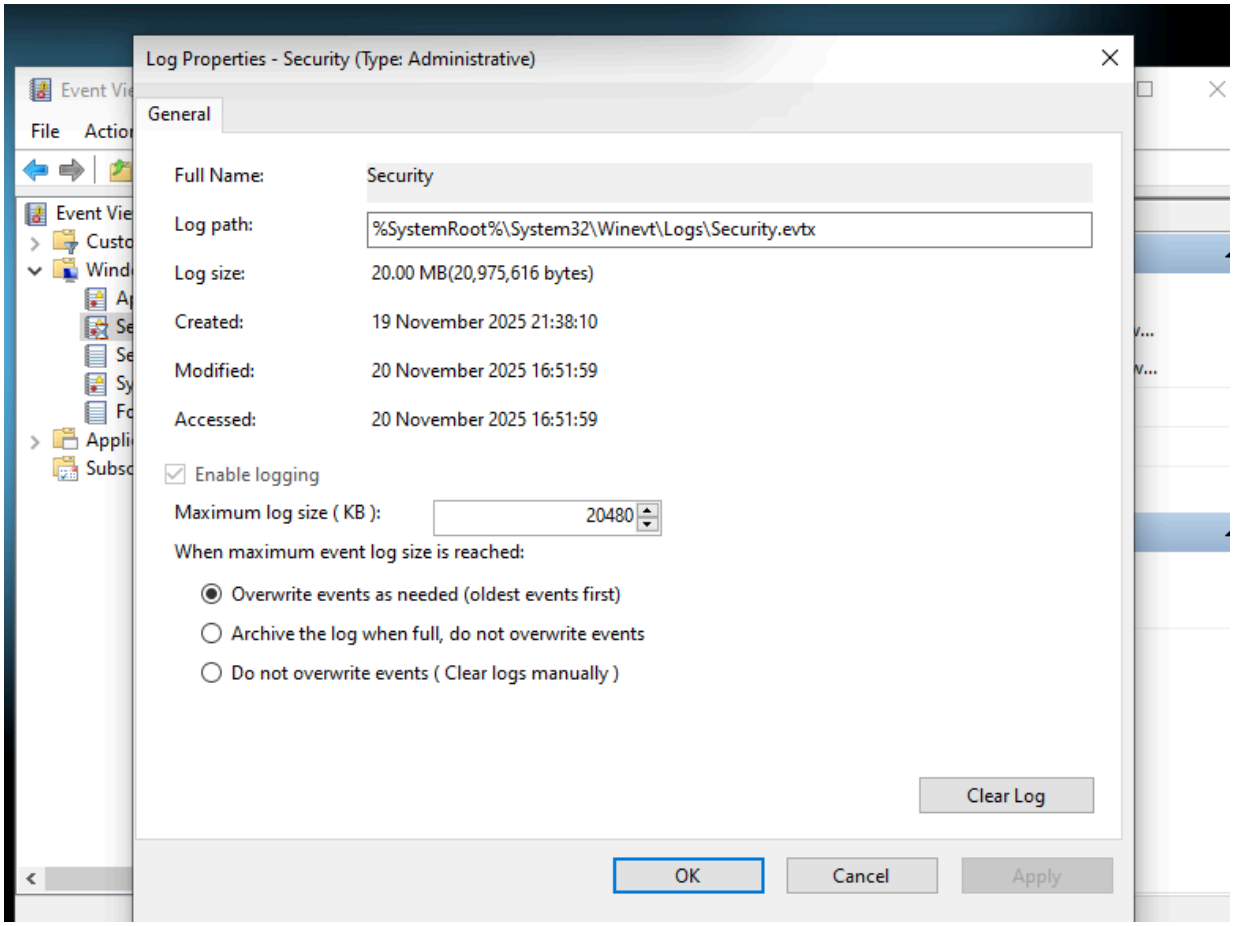
Obiettivo:

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

Fase 1: configurazione delle proprietà del registro

Per garantire che il sistema continui a registrare eventi senza bloccarsi una volta riempito lo spazio allocato, è necessario configurare la politica di rotazione dei log.

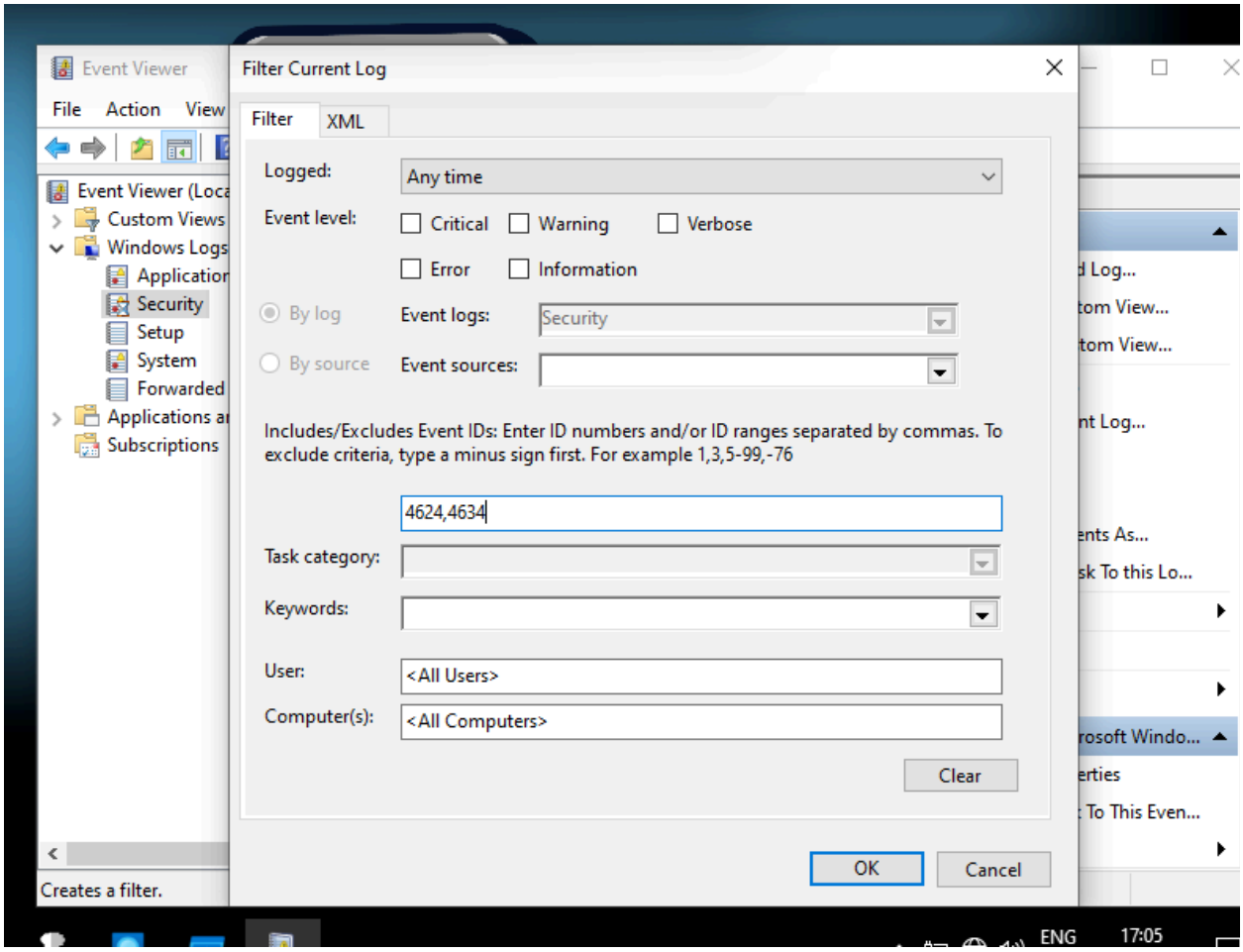
- **Azione:** Accesso alle proprietà del registro "Security" tramite `eventvwr`.
- **Configurazione:** È stata impostata la modalità **"Sovrascrivi eventi se necessario"** (Overwrite events as needed).
- **Motivazione tecnica:** Questa impostazione previene la perdita di operatività del sistema o il blocco della registrazione (Denial of Service sui log) quando il file raggiunge la dimensione massima.



Fase 2: impostazione del filtro per login/logoff

Il registro di sicurezza contiene migliaia di eventi. Per analizzare gli accessi, è stato applicato un filtro basato sugli ID Evento standard di Windows.

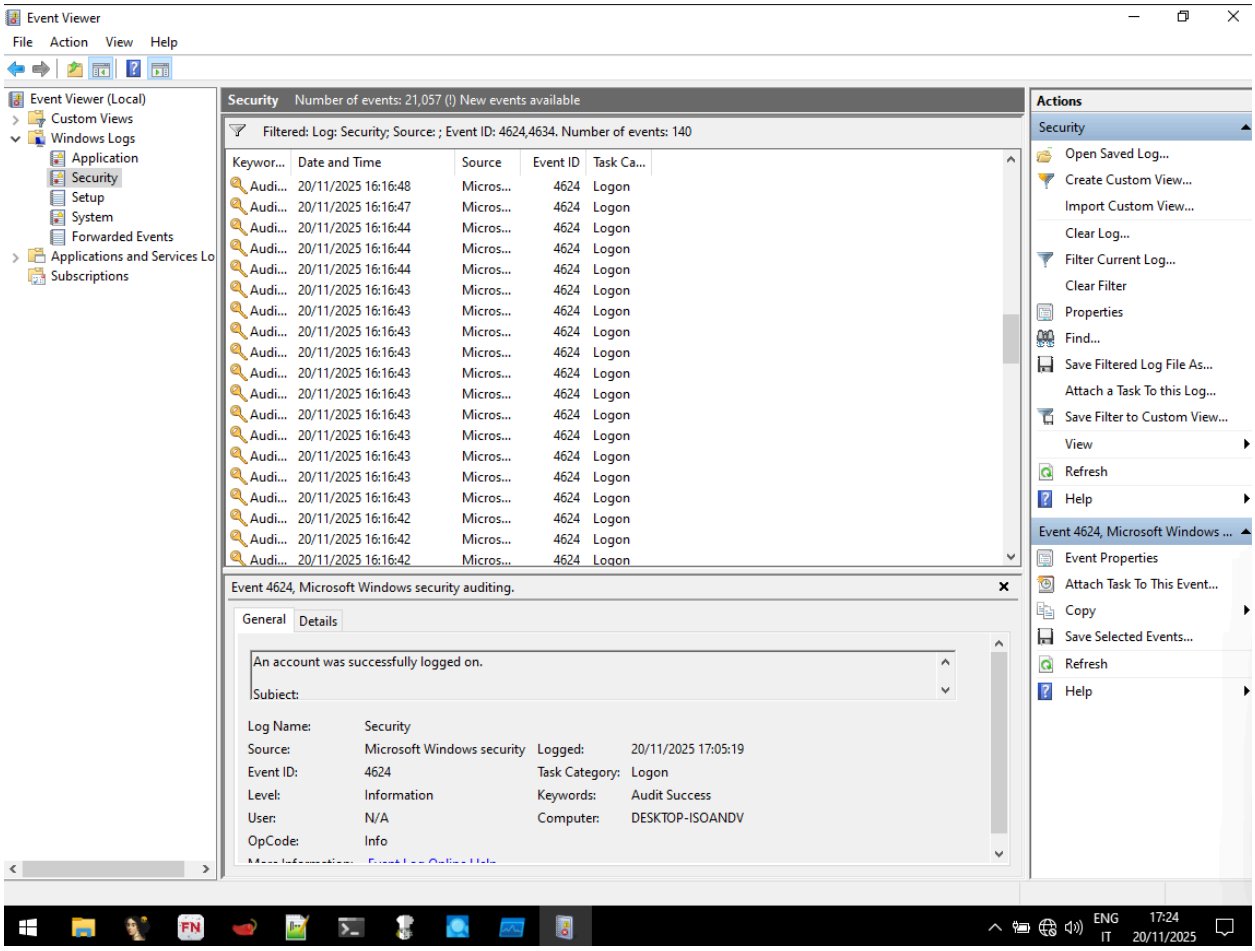
- **Azione:** Utilizzo della funzione "Filtro registro corrente" (Filter Current Log).
- **Parametri inseriti:**
  - **ID 4624:** Accesso riuscito (Logon).
  - **ID 4634:** Disconnessione (Logoff).



Fase 3: analisi e verifica dei risultati

Dopo l'applicazione del filtro, il Visualizzatore Eventi ha escluso tutto il traffico non pertinente, mostrando una timeline chiara delle attività di accesso utente.

- **Risultato:** La dashboard mostra ora esclusivamente gli eventi richiesti.
- **Verifica:** Selezionando un evento 4624, i dettagli confermano "An account was successfully logged on", permettendo di identificare chi ha effettuato l'accesso e quando.



Security Number of events: 21,057 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4624,4634. Number of events: 140

Keywor...	Date and Time	Source	Event ID	Task Ca...
Audi...	20/11/2025 16:16:48	Micros...	4624	Logon
Audi...	20/11/2025 16:16:47	Micros...	4624	Logon
Audi...	20/11/2025 16:16:44	Micros...	4624	Logon
Audi...	20/11/2025 16:16:44	Micros...	4624	Logon
Audi...	20/11/2025 16:16:44	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:43	Micros...	4624	Logon
Audi...	20/11/2025 16:16:42	Micros...	4624	Logon
Audi...	20/11/2025 16:16:42	Micros...	4624	Logon
Audi...	20/11/2025 16:16:42	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	20/11/2025 17:05:19
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-ISOANDV
OpCode:	Info		

Conclusioni:

L'esercitazione ha dimostrato come trasformare il Visualizzatore Eventi da un semplice contenitore di dati grezzi a uno strumento di analisi efficace. La corretta gestione della dimensione dei log e la capacità di filtrare per ID specifici (4624/4634) sono competenze essenziali per identificare accessi non autorizzati o anomalie nel comportamento degli utenti.