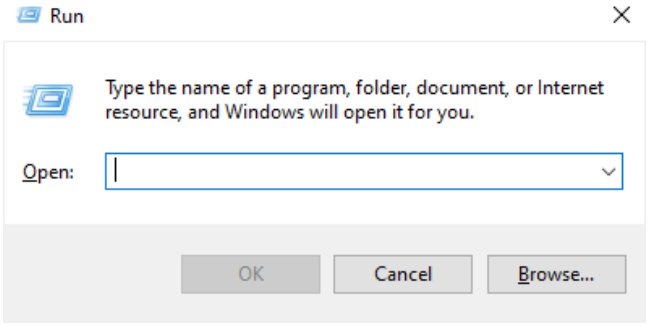
Consegna S9/L4

Obiettivo

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

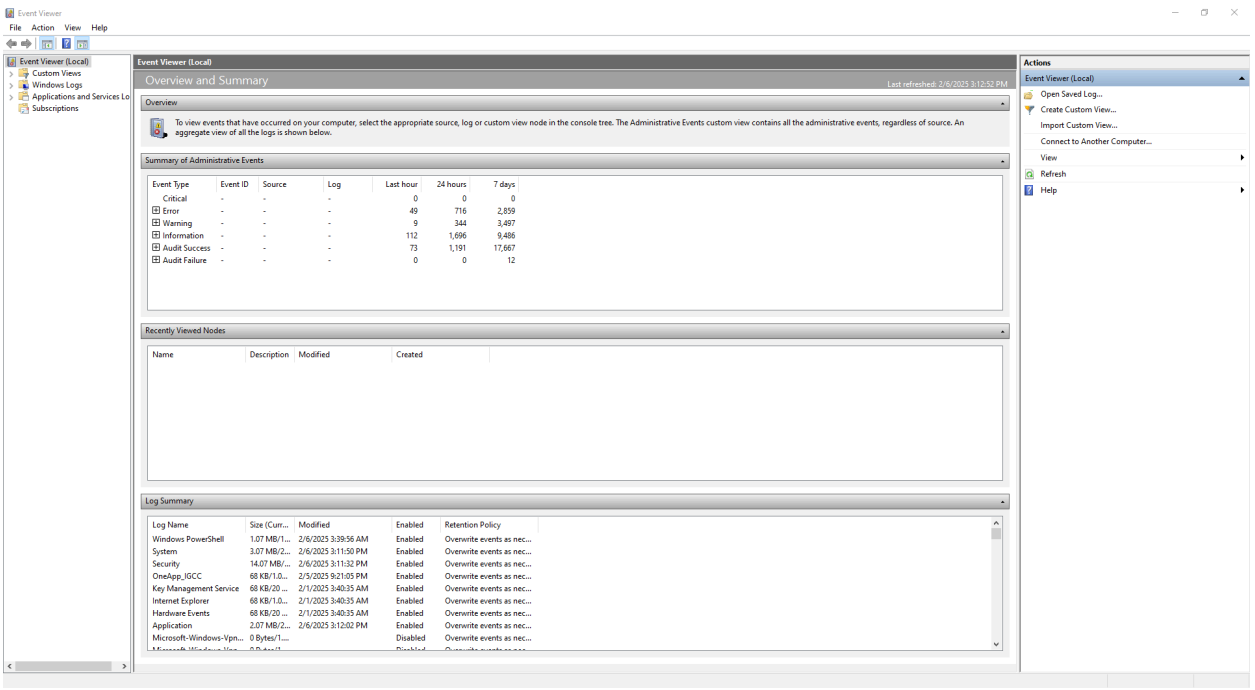
Accedo al Visualizzatore Eventi

Per prima cosa, apro la finestra Esegui premendo **Win + R** sulla tastiera.



Digitare **eventvwr** e premo Invio. Questo mi apre il Visualizzatore eventi di Windows

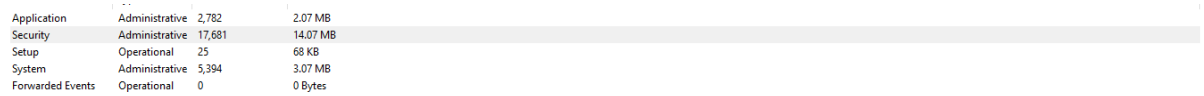
.



1. Configurare le Proprietà del Registro di Sicurezza

Espandiamo "Registri di Windows".

Seleziono "Sicurezza".

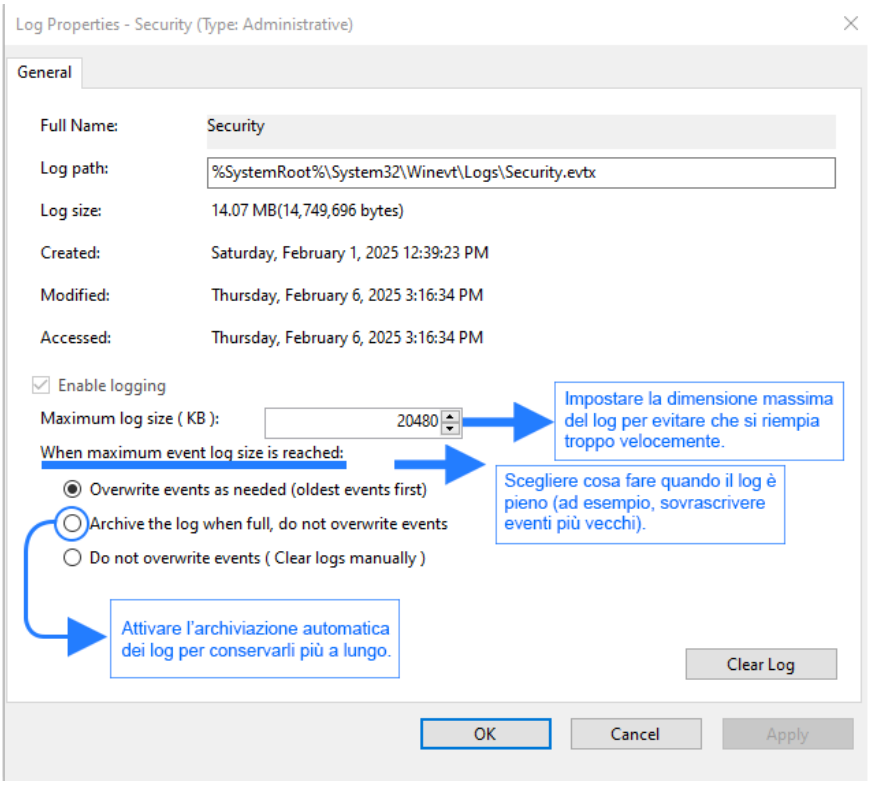


Application	Administrative	2,782	2.07 MB
Security	Administrative	17,681	14.07 MB
Setup	Operational	25	68 KB
System	Administrative	5,394	3.07 MB
Forwarded Events	Operational	0	0 Bytes

Clicco con il tasto destro su "Sicurezza" e scelgo "Proprietà".

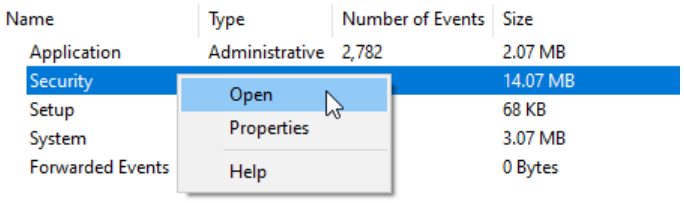
Qui posso:

- Impostare la dimensione massima del log per evitare che si riempia troppo velocemente.
- Scegliere cosa fare quando il log è pieno (ad esempio, sovrascrivere eventi più vecchi).
- Attivare l'archiviazione automatica dei log per conservarli più a lungo.



3. Analizzo gli Eventi di Accesso (Logon e Special Logon)

Ora voglio controllare gli eventi di accesso, quindi clicco su sicurezza con il tasto destro e clicco apri



3. Analizzo gli Eventi di Accesso (Logon e Special Logon)

Ora devo controllare gli eventi di accesso, quindi:

Filtro gli eventi per la categoria Logon:

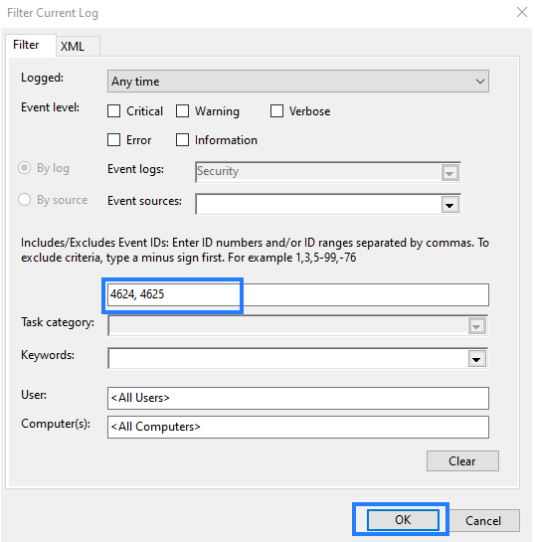
Clicco su **"Filtra registro corrente"** nel pannello di destra.

Nella finestra che si apre, inserisco questi ID evento:

4624 → Accesso riuscito.

4625 → Tentativo di accesso non riuscito.

Confermo con **OK** per applicare il filtro.



4624 Accesso riuscito.

Filtered: Log: Security; Source: ; Event ID: 4624, 4625. Number of events: 2,534

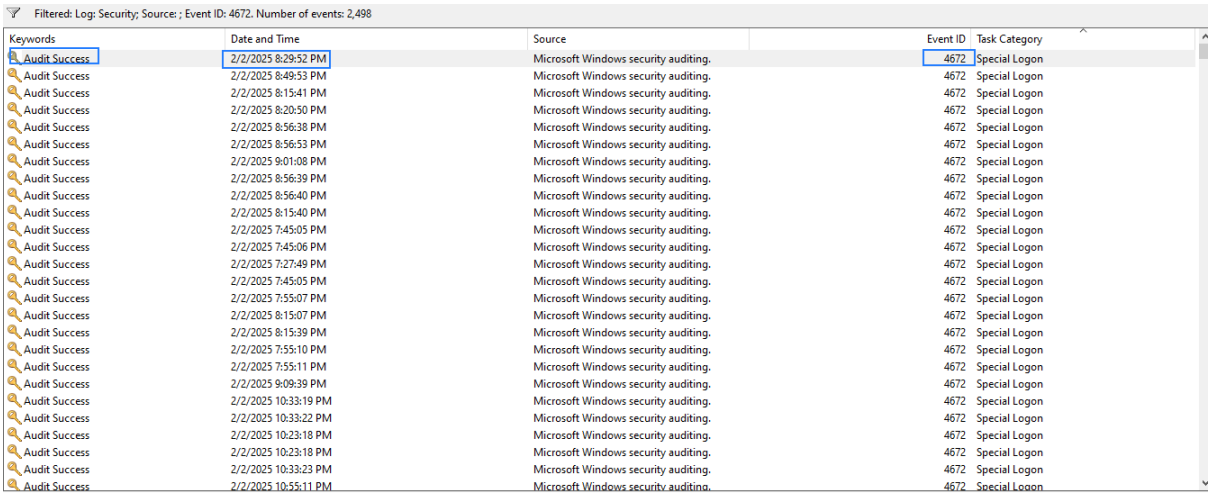
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/2/2025 7:45:05 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/2/2025 7:45:05 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/2/2025 7:27:48 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/2/2025 7:27:49 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/2/2025 7:45:06 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/2/2025 7:55:11 PM	Microsoft Windows security auditing.	4624	Logon

4625 Tentativo di accesso non riuscito.

Audit Failure	2/1/2025 4:00:01 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	2/1/2025 4:53:04 AM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	2/1/2025 3:44:26 AM	Microsoft Windows security auditing.	4625	Logon

Controllo anche gli eventi Special Logon, che indicano accessi con privilegi elevati:

Cerco eventi con ID **4672**



Filtered: Log: Security; Source: ; Event ID: 4672. Number of events: 2,498

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/2/2025 8:29:52 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:49:53 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:15:41 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:20:50 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:56:38 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:56:53 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 9:01:08 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:56:39 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:56:40 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:15:40 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:45:05 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:45:06 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:27:49 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:45:05 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:55:07 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:15:07 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 8:15:39 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:55:10 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 7:55:11 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 9:09:39 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 10:33:19 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 10:33:22 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 10:23:18 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 10:23:18 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 10:33:23 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2/2/2025 10:55:11 PM	Microsoft Windows security auditing.	4672	Special Logon