S9L4

U3

Marco Falchi

Consegna

Esercizio di oggi: Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

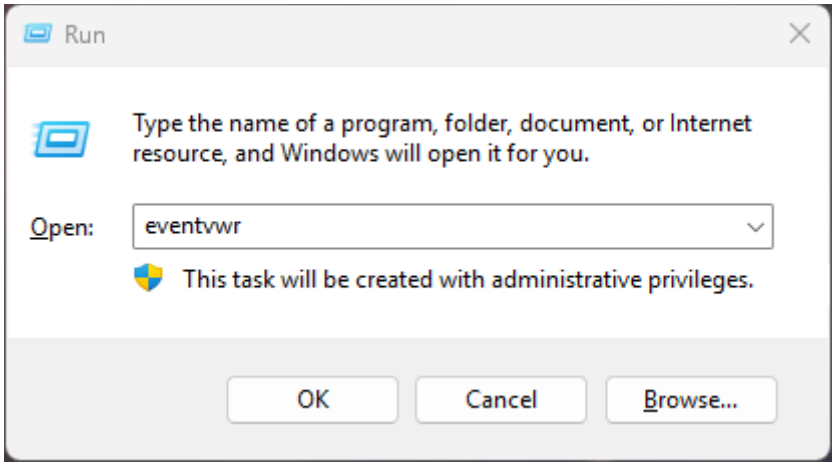
Obiettivo: Configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows.

Istruzioni:

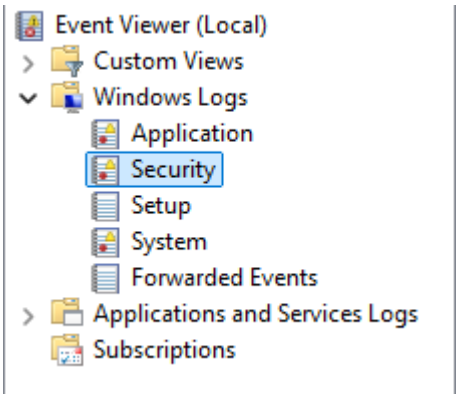
1) Accedere al Visualizzatore Eventi:
   a) Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
   b) Digita eventvwr e premi Invio.
2) Configurare le Proprietà del Registro di Sicurezza:
   a) Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".
3) Provate a impostare il log dei Login/Logoff

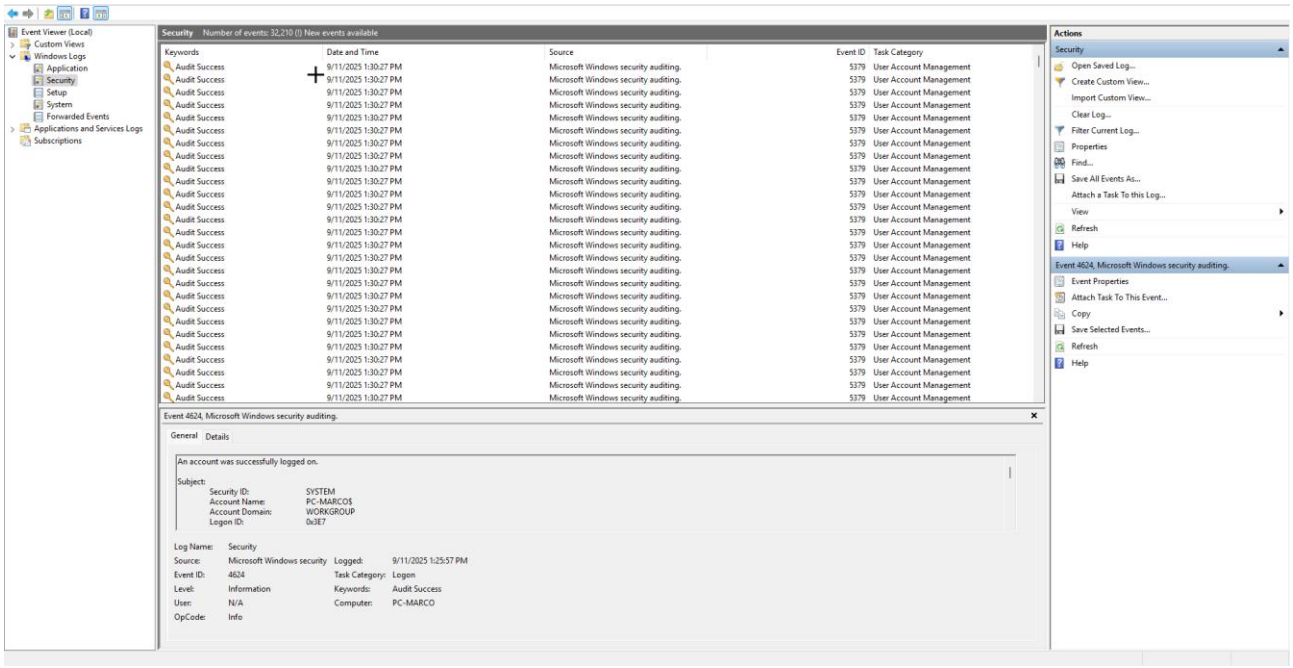
Esecuzione della consegna

1)

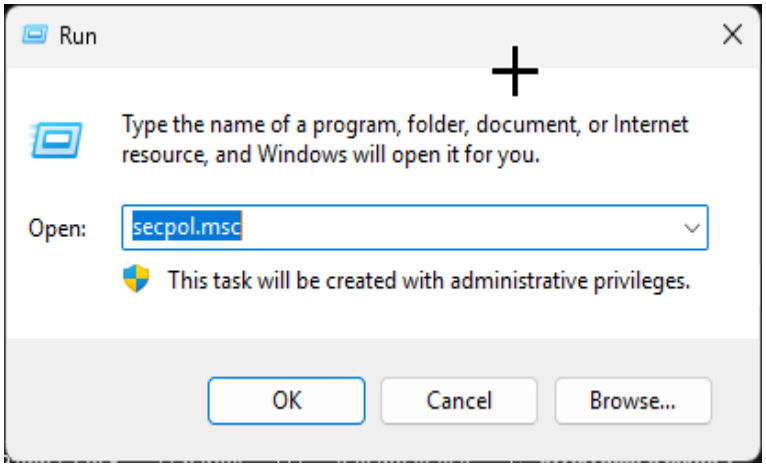


2)

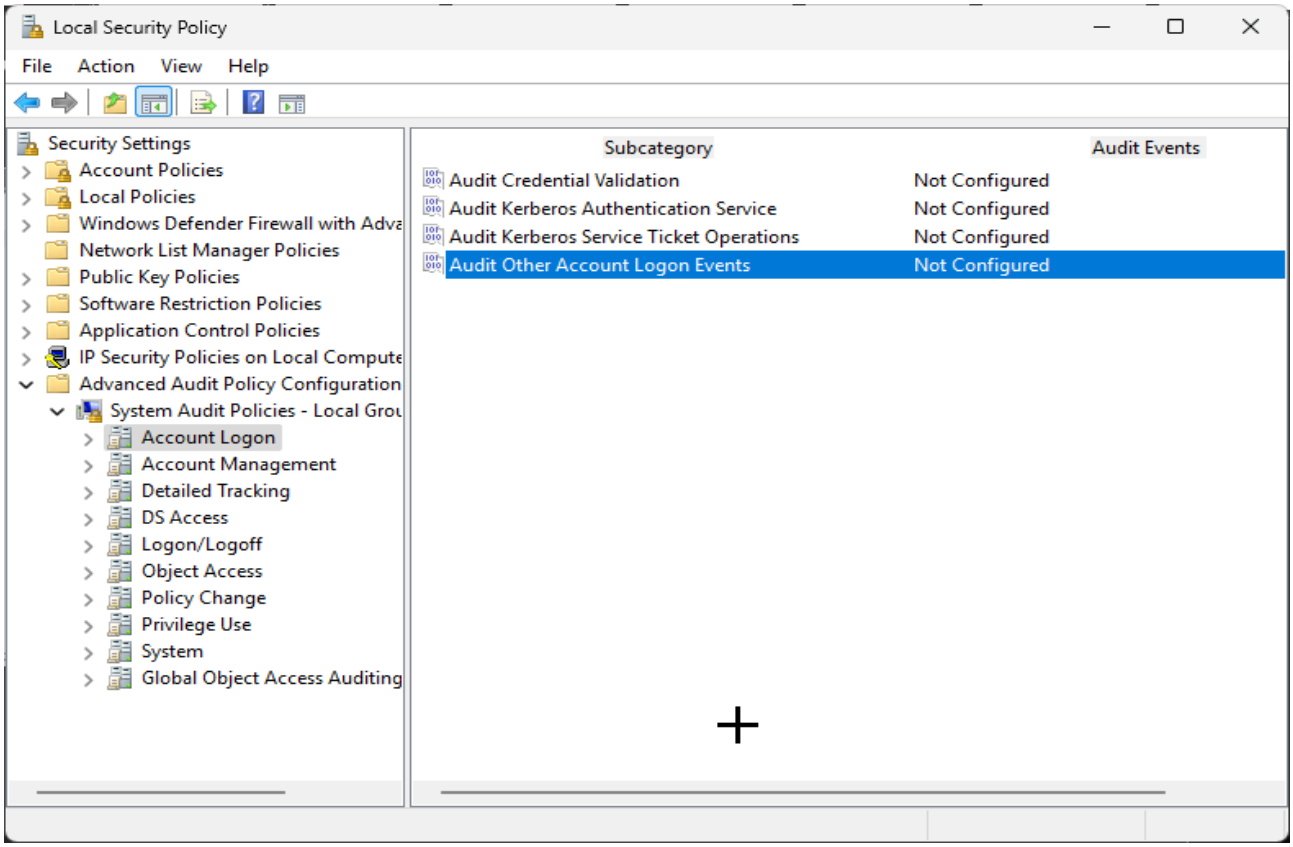

Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Logs
Subscriptions


Security Number of events: 32,210 (!) New events available
Keywords Date and Time Source Event ID Task Category
Audit Success 9/11/2025 1:30:27 PM Microsoft Windows security auditing. 5379 User Account Management
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4624, Microsoft Windows security auditing.
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
General Details
An account was successfully logged on.
Subject:
Security ID: SYSTEM
Account Name: PC-MARCO$
Account Domain: WORKGROUP
Logon ID: 0x3E7
Log Name: Security
Source: Microsoft Windows security
Logged: 9/11/2025 1:25:57 PM
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: PC-MARCO
OpCode: Info

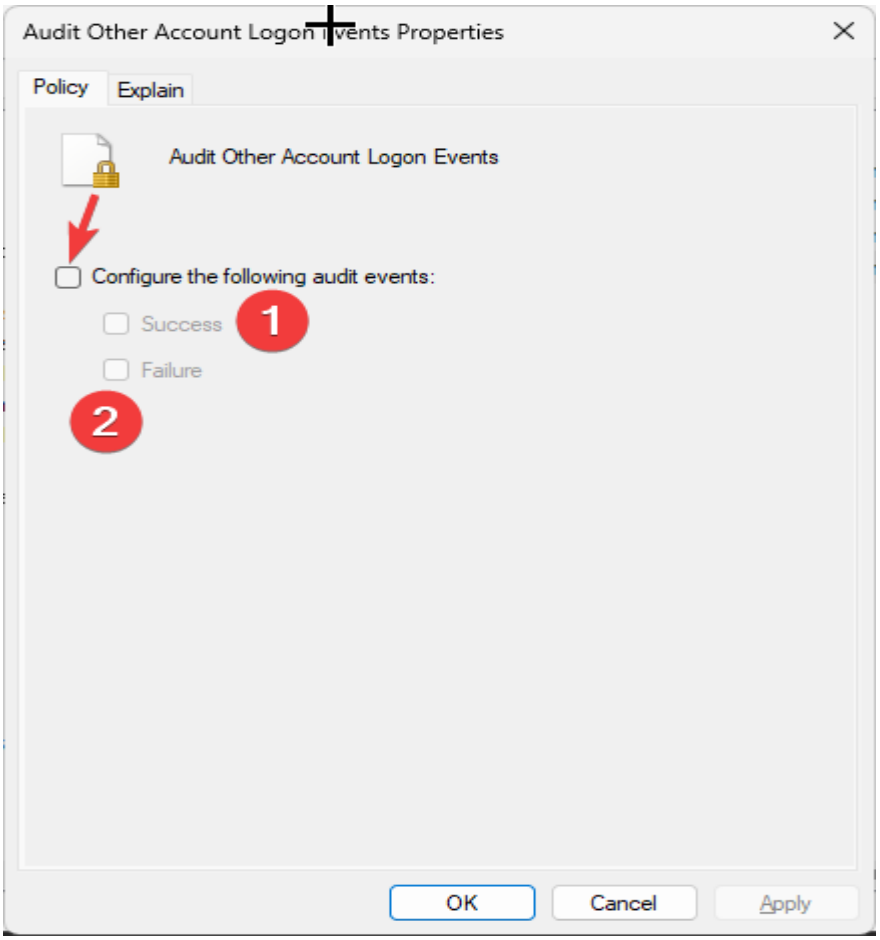
2) Per impostare i log dei login/logoff ho iniziato cercando il comando secpol.msc su Windows+R



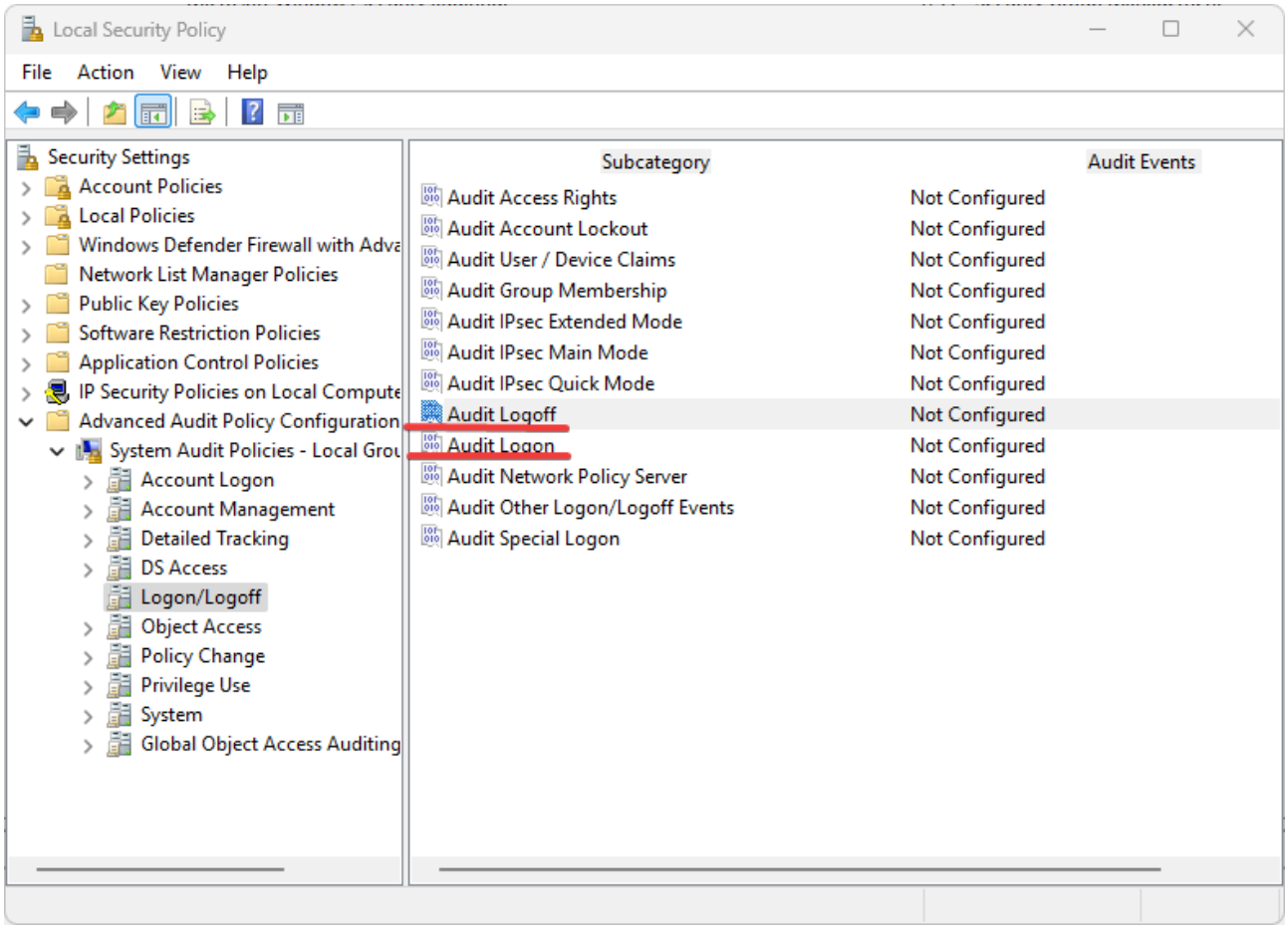
Successivamente ho aperto la sezione **"Advanced Audit Policy Configuration"**, successivamente **Account Logon** e ho poi aperto **"Audit Other Account Logon Events"**



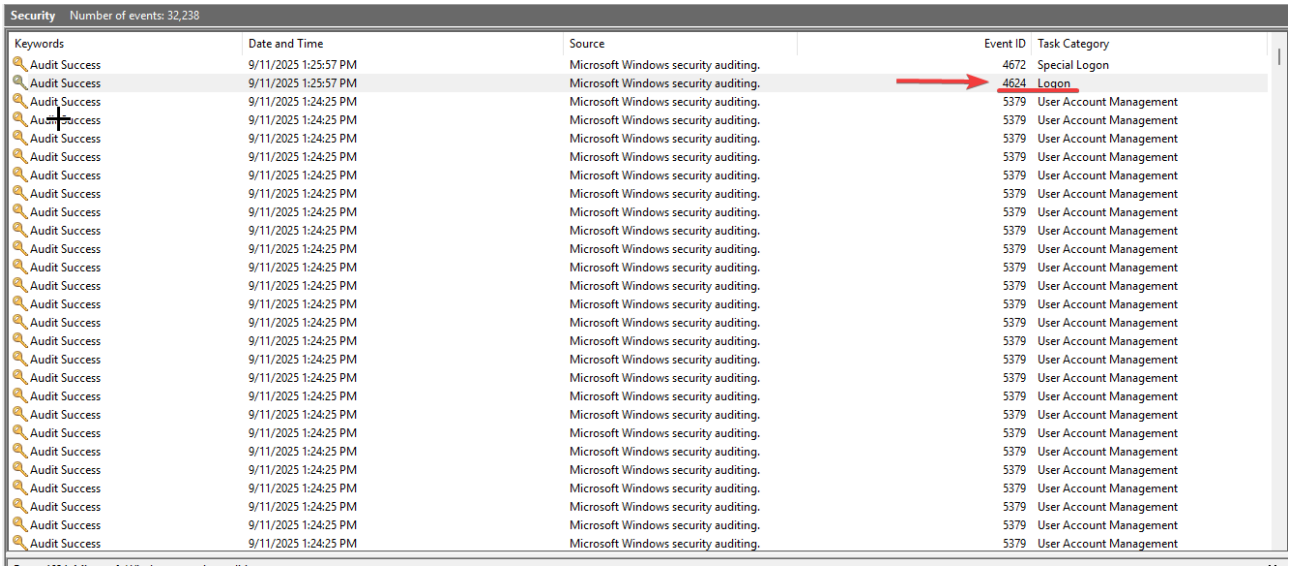
Possiamo successivamente attivare i log come si vede qua sotto


Audit Other Account Logon Events Properties
Policy
Explain
Audit Other Account Logon Events
Configure the following audit events:
Success
Failure
1
2
OK
Cancel
Apply

Possiamo anche attivarli singolarmente andando nella sezione Logon/Logoff e modificando i parametri sottolineati come prima



Vediamo successivamente come possiamo visualizzare i logon e logoff seguendo il passaggio 1 e 2



General | Details

An account was successfully logged on.

Subject:
- Security ID: SYSTEM
- Account Name: PC-MARCO$
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Information:
- Logon Type: 5
- Restricted Admin Mode: -
- Remote Credential Guard: -
- Virtual Account: No
- Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
- Security ID: SYSTEM
- Account Name: SYSTEM
- Account Domain: NT AUTHORITY
- Logon ID: 0x3E7
- Linked Logon ID: 0x0
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
- Process ID: 0x5fc
- Process Name: C:\Windows\System32\services.exe

Network Information:
- Workstation Name: -
- Source Network Address: -
- Source Port: -

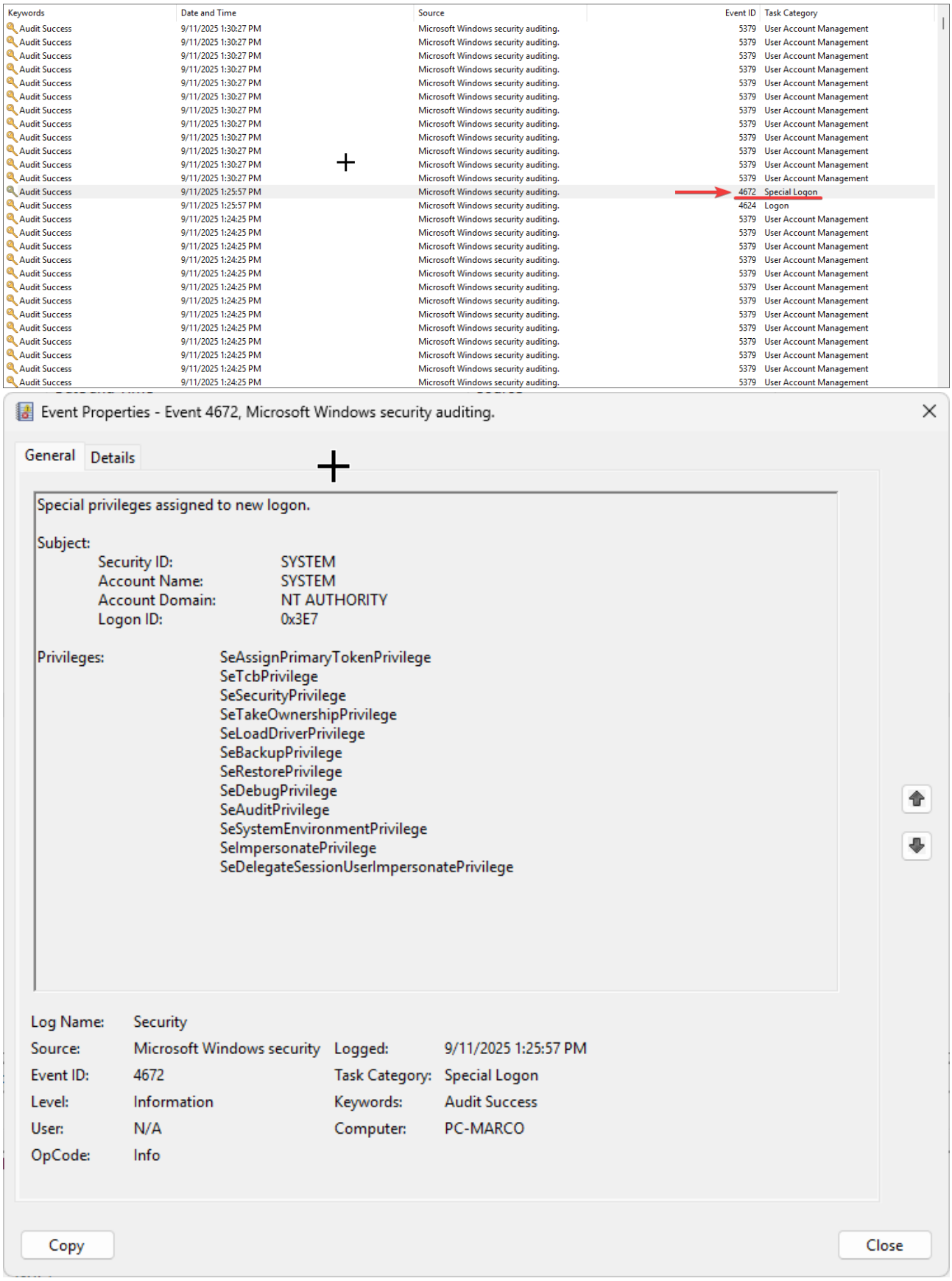
Detailed Authentication Information:
- Logon Process: Advapi
- Authentication Package: Negotiate
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/11/2025 1:25:57 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	PC-MARCO
OpCode:	Info		



Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:30:27 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:25:57 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	9/11/2025 1:25:57 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management
Audit Success	9/11/2025 1:24:25 PM	Microsoft Windows security auditing.	5379	User Account Management

```
Special privileges assigned to new logon.

Subject:
        Security ID:            SYSTEM
        Account Name:           SYSTEM
        Account Domain:         NT AUTHORITY
        Logon ID:               0x3E7

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeTcbPrivilege
                        SeSecurityPrivilege
                        SeTakeOwnershipPrivilege
                        SeLoadDriverPrivilege
                        SeBackupPrivilege
                        SeRestorePrivilege
                        SeDebugPrivilege
                        SeAuditPrivilege
                        SeSystemEnvironmentPrivilege
                        SeImpersonatePrivilege
                        SeDelegateSessionUserImpersonatePrivilege
```

Log Name: Security
Source: Microsoft Windows security
Logged: 9/11/2025 1:25:57 PM
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: PC-MARCO
OpCode: Info