

Report Esercizio 06/02/2025

Analisi Visualizzatore Eventi Windows Leonardo Catalano

“La traccia di oggi ci chiede di effettuare un’analisi con il Visualizzatore eventi di Windows .”

-Istruzioni:

Nello specifico nel Visualizzatore Eventi dovremmo andare nella sezione “Registri di Windows” e categoria “Sicurezza”.

Gli eventi da analizzare saranno quelli con “Categoria attività” Special Logon e Logon.

-Visualizzatore eventi:

Evento Special Logon:

The screenshot displays the Windows Event Viewer interface. The left pane shows the tree structure with 'Registri di Windows' expanded and 'Sicurezza' selected. The main pane shows a list of security events. The event list has columns for 'Parole chiave', 'Data e ora', 'Origine', 'ID evento', and 'Categoria attività'. Event 4672 is highlighted, with the category 'Special Logon'. The right pane shows the 'Azioni' menu with options like 'Apri registro salvato...', 'Crea visualizzazione personalizzata...', 'Importa visualizzazione personalizzata...', 'Cancella registro...', 'Filtro registro corrente...', 'Proprietà', 'Trova...', 'Salva tutti gli eventi con nome...', 'Associa un'attività al registro...', 'Visualizza', 'Aggiorna', and 'Guida'. Below the event list, the details for event 4672 are shown. The 'Generale' tab is active, displaying the following information:

Evento 4672, Microsoft Windows security auditing.

Generale **Dettagli**

Privilegi speciali assegnati a nuovo accesso.

Soggetto:

- ID sicurezza: SYSTEM
- Nome account: SYSTEM
- Dominio account: NT AUTHORITY
- ID accesso: 0x3E7

Privilegi:

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

Nome registro: Sicurezza

Origine: Microsoft Windows security **Registrato:** 06/02/2025 14:31:38

ID evento: 4672 **Categoria attività:** Special Logon

Livello: Informazioni **Parole chiave:** Controllo riuscito

Utente: N/D **Computer:** LAPTOP-...

Opcode: Informazioni

Come da screen è riportato il 1° Special Logon in ordine cronologico con ID evento n. 4672, questo ID sta a significare un particolare evento:

“Evento 4672: Accesso speciale per un utente con privilegi elevati (d’amministratore)”.

Sono riportate altre informazioni :

Origine dell'evento: Microsoft Windows security

Il Livello : Informazioni

Il Soggetto:

ID SICUREZZA: SYSTEM

Nome account: SYSTEM

Dominio account NT AUTHORITY

ID accesso: 0x3E7

L'id di Sicurezza SYSTEM, e l'account SYSTEM sono legati e associati al sistema operativo Windows e rappresentano l'utente di sistema. L'evento ci indica che l'accesso è del sistema non dell'utente umano, e che questo processo di sistema ha ottenuto privilegi elevati.

Privilegi assegnati all'utente:

- 1) SeAssignPrimaryTokenPrivilege: Permessso di assegnare un token di accesso primario ad un altro processo.
- 2)SeTcbPrivilege: Privilegio che consente di agire come sistema di controllo di sicurezza (Trust Computer Base).
- 3)SeTakeOwnershipPrivilege: Permessso di prendere possesso di un file o di una risorsa.
- 4)SeLoadDriverPrivilege: Permessso di caricare un driver di dispositivo.
- 5)SeBackupPrivilege: Permessso di eseguire il backup di file e cartelle, ignorando le restrizioni di sicurezza.
- 6)SeRestorePrivilege: Permessso di ripristinare file e cartelle.
- 7)SeDebugPrivilege: Privilegio di debug dei processi.
- 8)seAuditPrivilege: Privilegio di modificare le impostazioni di auditing del sistema.
- 9)seSystemEnvironmentPrivilege: Permessso di modificare variabili di ambiente di sistema.
- 10)seImpersonatePrivilege: Permessso di impersonare un altro utente.

11)seDelegateSessionUserImpersonatePrivilege: Permetto di impersonare un altro utente in sessioni di delega.

Evento Logon:

Visualizzatore eventi

File Azione Visualizza ?

Visualizzatore eventi (computer)

Visualizzazioni personalizzate

Registri di Windows

Applicazione

Sicurezza

Installazione

Sistema

Eventi inoltrati

Registri applicazioni e servizi

Sottoscrizioni

Sicurezza

Numero di eventi: 32.092 (1) Nuovi eventi disponibili

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4798	User Account Ma...
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4798	User Account Ma...
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4798	User Account Ma...
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4798	User Account Ma...
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4798	User Account Ma...
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4798	User Account Ma...
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4672	Special Logon
Controllo rius...	06/02/2025 14:31:38	Microsoft Windo...	4624	Logon
Controllo rius...	06/02/2025 14:27:43	Microsoft Windo...	5059	Other System Eve...
Controllo rius...	06/02/2025 14:27:43	Microsoft Windo...	5061	System Integrity
Controllo rius...	06/02/2025 14:27:43	Microsoft Windo...	5058	Other System Eve...
Controllo rius...	06/02/2025 14:27:20	Microsoft Windo...	5059	Other System Eve...
Controllo rius...	06/02/2025 14:27:20	Microsoft Windo...	5061	System Integrity
Controllo rius...	06/02/2025 14:27:20	Microsoft Windo...	5058	Other System Eve...
Controllo rius...	06/02/2025 14:27:00	Microsoft Windo...	5059	Other System Eve...
Controllo rius...	06/02/2025 14:27:00	Microsoft Windo...	5061	System Integrity
Controllo rius...	06/02/2025 14:27:00	Microsoft Windo...	5058	Other System Eve...
Controllo rius...	06/02/2025 14:27:00	Microsoft Windo...	4798	User Account Ma...

Azioni

Sicurezza

Apri registro salvato...

Crea visualizzazione personalizzata...

Importa visualizzazione personalizzata...

Cancella registro...

Filtro registro corrente...

Proprietà

Trova...

Salva tutti gli eventi con nome...

Associa un'attività al registro...

Visualizza

Aggiorna

Guida

Evento 4624, Microsoft Windows security auditing.

Proprietà evento

Associa attività all'evento...

Salva eventi selezionati...

Copia

Aggiorna

Guida

Evento 4624, Microsoft Windows security auditing.

Generale Dettagli

Accesso di un account riuscito.

Soggetto:

ID sicurezza: SYSTEM

Nome account: LAPTOP- [redacted]

Dominio account: WORKGROUP

ID accesso: 0x3E7

Informazioni di accesso:

Tipo di accesso: 5

Modalità amministrativa limitata: -

Credential Guard remoto: -

Account virtuale: No

Token elevato: Sì

Livello rappresentazione:

Rappresentazione

Nuovo accesso:

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 06/02/2025 14:31:38

ID evento: 4624 Categoria attività: Logon

Livello: Informazioni Parole chiave: Controllo riuscito

Utente: N/D Computer: LAPTOP- [redacted]

Opcode: Informazioni

Sicurezza Numero di eventi: 32.092 (1) Nuovi eventi disponibili

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riusc...	06/02/2025 14:31:38	Microsoft Windo...	4672	Special Logon
Controllo riusc...	06/02/2025 14:31:38	Microsoft Windo...	4624	Logon
Controllo riusc...	06/02/2025 14:27:43	Microsoft Windo...	5059	Other System Eve...
Controllo riusc...	06/02/2025 14:27:43	Microsoft Windo...	5061	System Integrity
Controllo riusc...	06/02/2025 14:27:43	Microsoft Windo...	5058	Other System Eve...
Controllo riusc...	06/02/2025 14:27:20	Microsoft Windo...	5059	Other System Eve...
Controllo riusc...	06/02/2025 14:27:20	Microsoft Windo...	5061	System Integrity
Controllo riusc...	06/02/2025 14:27:20	Microsoft Windo...	5058	Other System Eve...
Controllo riusc...	06/02/2025 14:27:00	Microsoft Windo...	5059	Other System Eve...

Evento 4624, Microsoft Windows security auditing.

Generale Dettagli

Nuovo accesso:

ID sicurezza: SYSTEM
Nome account: SYSTEM
Dominio account: NT AUTHORITY
ID accesso: 0x3E7
ID accesso collegato: 0x0
Nome account di rete: -
Dominio account di rete: -
GUID accesso: {00000000-0000-0000-0000-000000000000}

Informazioni sul processo:

ID processo: 0x5ec
Nome processo: C:\Windows\System32\services.exe

Informazioni di rete:

Nome Workstation: -
Indirizzo rete di origine: -
Porta di origine: -

Informazioni di autenticazione dettagliate:

Processo di accesso: Advapi
Pacchetto di autenticazione: Negotiate
Servizi transitati: -
Nome pacchetto (solo NTLM): -
Lunghezza chiave: 0

Questo evento viene generato quando viene creata una sessione di accesso. Viene generato nel computer in cui è stato effettuato l'accesso.

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 06/02/2025 14:31:38
ID evento: 4624 Categoria attività: Logon
Livello: Informazioni Parole chiave: Controllo riuscito
Utente: N/D Computer: LAPTOP-
Opcode: Informazioni

Come da screen ho riportato il 1° evento Logon in ordine cronologico con ID evento n. 4624, questo ID sta a significare un particolare evento:

“Evento 4624: Logon riuscito (l’utente ha effettuato l’accesso con successo al sistema)
Evento 4625: Tentativo di Logon fallito (c’è stato un tentativo di accesso ed è fallito) ”.

Sono riportate altre informazioni:

Origine dell’evento: Microsoft Windows security

Il Livello : Informazioni

Il Soggetto:

ID SICUREZZA: SYSTEM

Nome account: LAPTOP-

Dominio account WORKGROUP

ID accesso: 0x3E7

L'evento 4624 ci segnala che c'è stato un accesso riuscito con delle determinate caratteristiche:

1)Tipo di accesso: 5 (Servizio), questo tipo di accesso si verifica quando un servizio di sistema di Windows viene avviato.

2)Account Virtuale: No (L'accesso non riguarda un account virtuale)

3)Token elevato: Si (Indica che l'accesso è avvenuto con privilegi elevati, tipicamente d'amministratore)

Sezione Nuovo Accesso:

In questa sezione troviamo lo stesso SYSTEM di prima, ossia un account di sistema windows che viene usato per le operazioni internet al sistema operativo, quindi non un account utente, ma di un account interno dell'OS.

Informazioni sul processo:

ID processo: 0x5ec

Nome processo: C:\Windows\System32\services.exe

Questo processo è critico perchè gestisce i servizi del sistema operativo Windows, vuol dire quindi che un servizio di sistema ha richiesto l'accesso a questo particolare servizio "services.exe".

-Tipi di accesso (LOGON Type):

Una cosa molto importante per gli eventi Logon sono i vari Tipi di accesso che possono esserci:

Tipo di Accesso	Descrizione
2	Interattivo: Accesso effettuato direttamente tramite dall'utente fisico sulla macchina con tastiera e mouse.
3	Rete: Accesso tramite connessione ad una cartella condivisa o altre risorse di rete da un altro computer sulla stessa rete.
4	Batch: Accesso tramite attività pianificata (eseguito da un processo pianificato, come un lavoro di cronologia).
5	Servizio: Accesso avviato da un servizio di sistema, ad esempio quando un servizio viene avviato automaticamente.
7	Unlock: Accesso effettuato quando una workstation con sreen saver, protetta da password viene sbloccata.

8	NetworkClearText: Accesso in cui le credenziali sono inviate in chiaro (ad esempio, login su IIS con “autenticazione di base”).
9	Nuove Credenziali: Accesso con credenziali alternative, come nel caso di RunAs o mappatura di un’unità di rete con credenziali diverse. Questo tipo di accesso non appare frequentemente negli eventi, ma è utile per tracciare gli accessi con credenziali diverse.
10	RemoteInteractive: Accesso remoto al sistema (tramite Terminal Services, Desktop remoto o Assistenza Remota).
11	CachedInteractive: Accesso effettuato con credenziali di dominio memorizzate nella cache, ad esempio quando un utente si connette a un laptop in modalità offline (senza connessione alla rete).