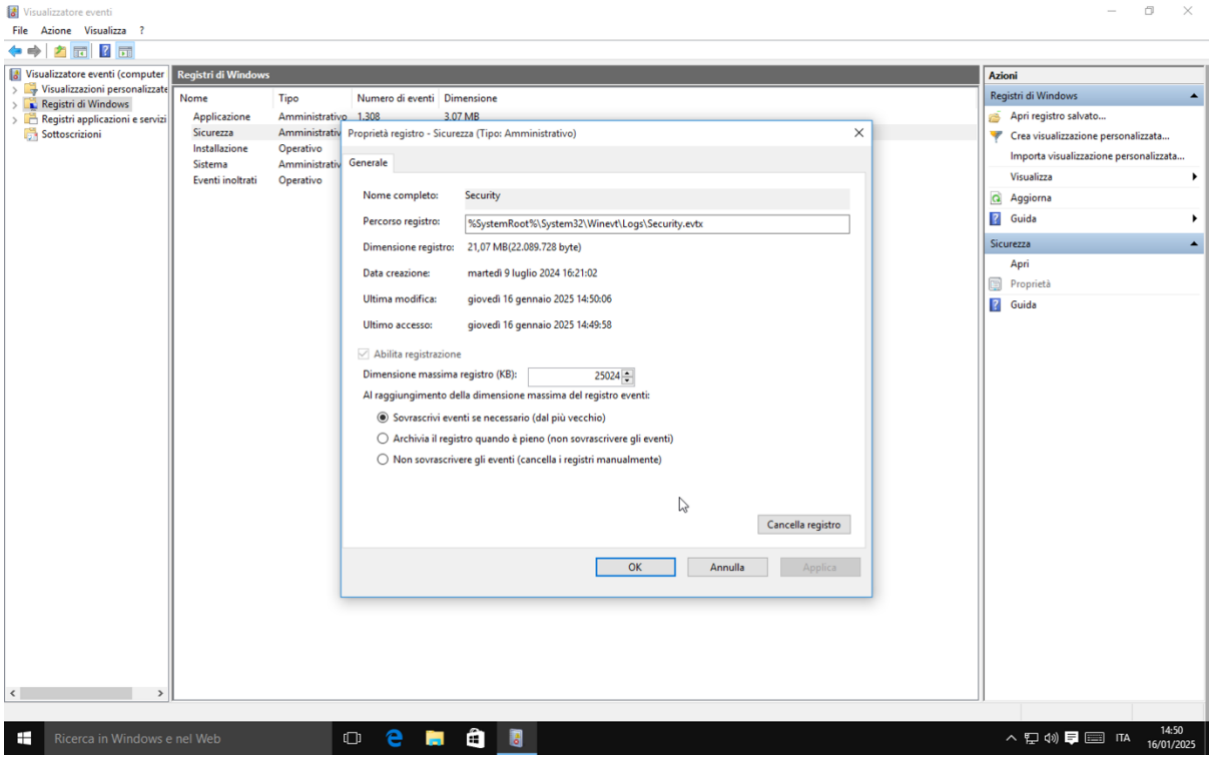
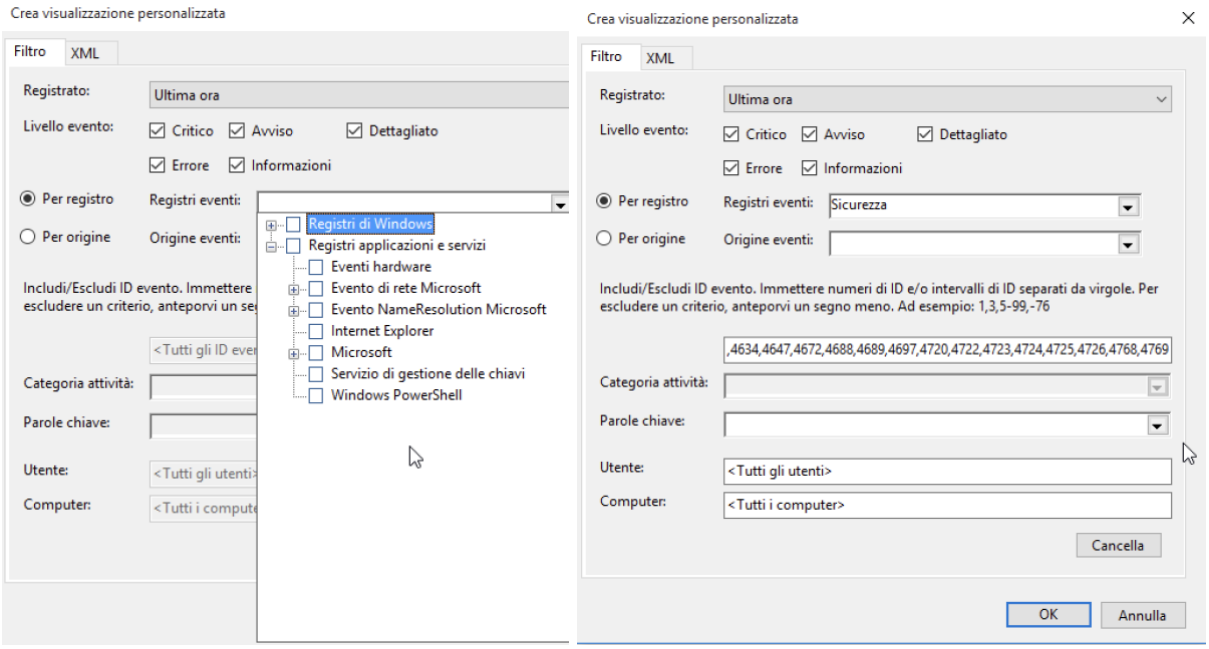
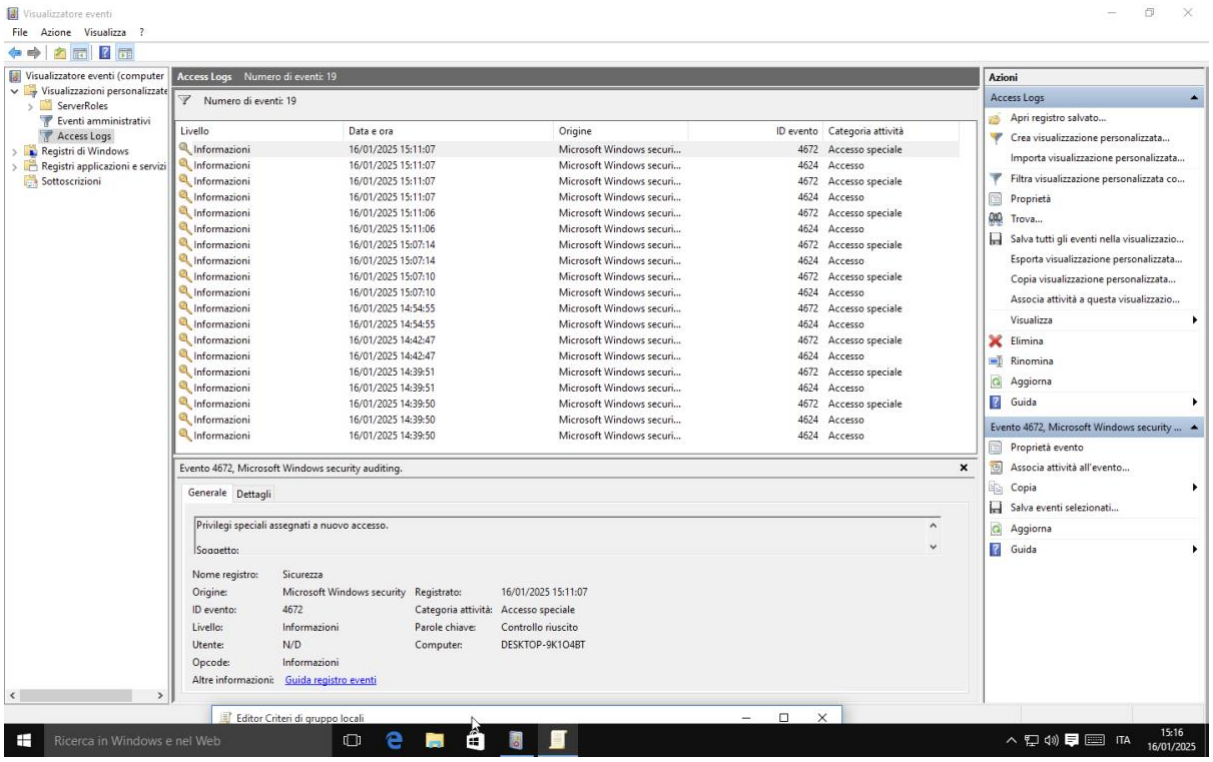
Rapporto

Per prima cosa ho impostato le proprietà del registro su Windows, poi ho scelto la sicurezza dai registri di Windows e ho configurato altre parti:

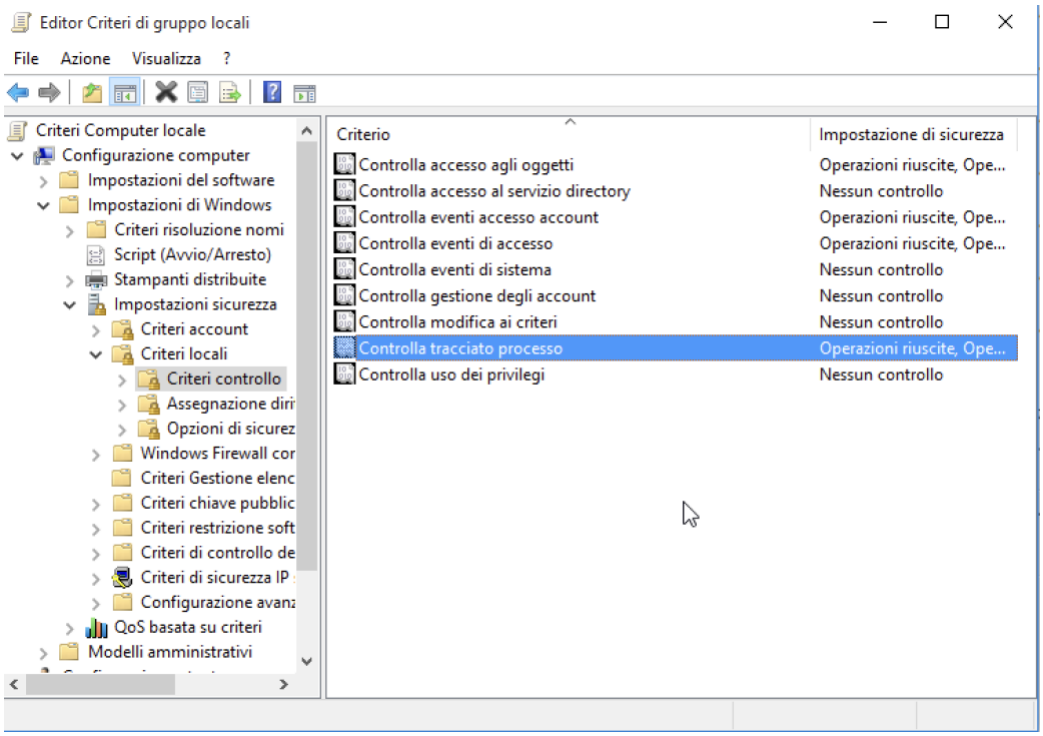




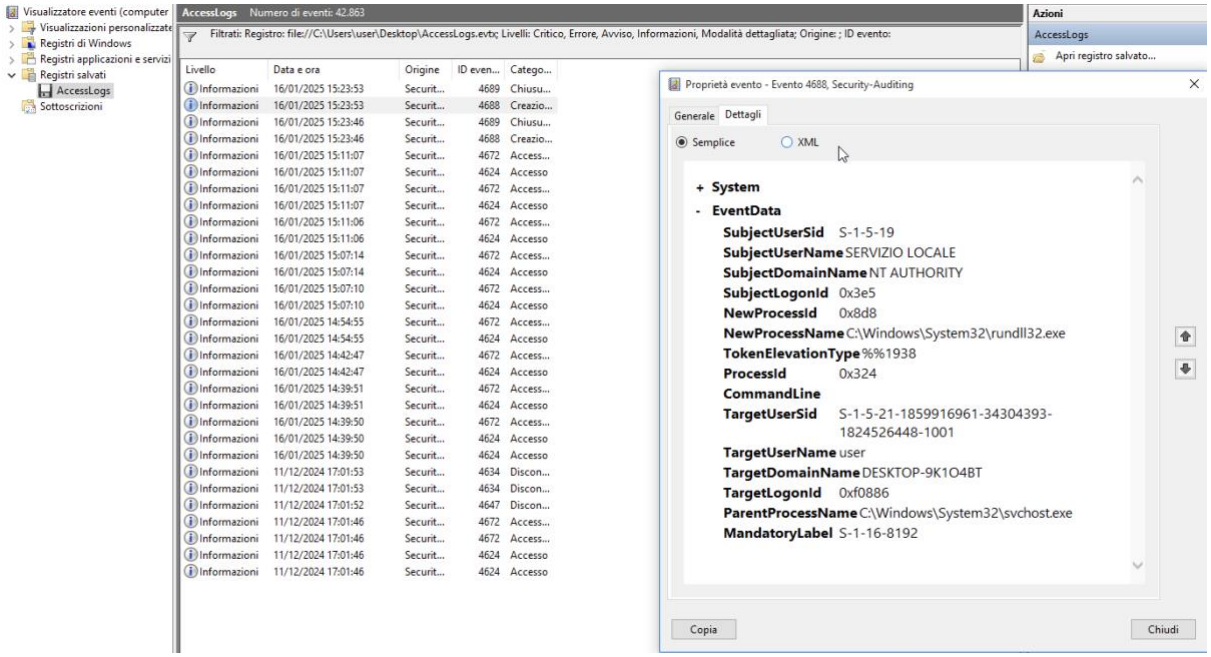
Quindi ho salvato la configurazione come "Access Logs":

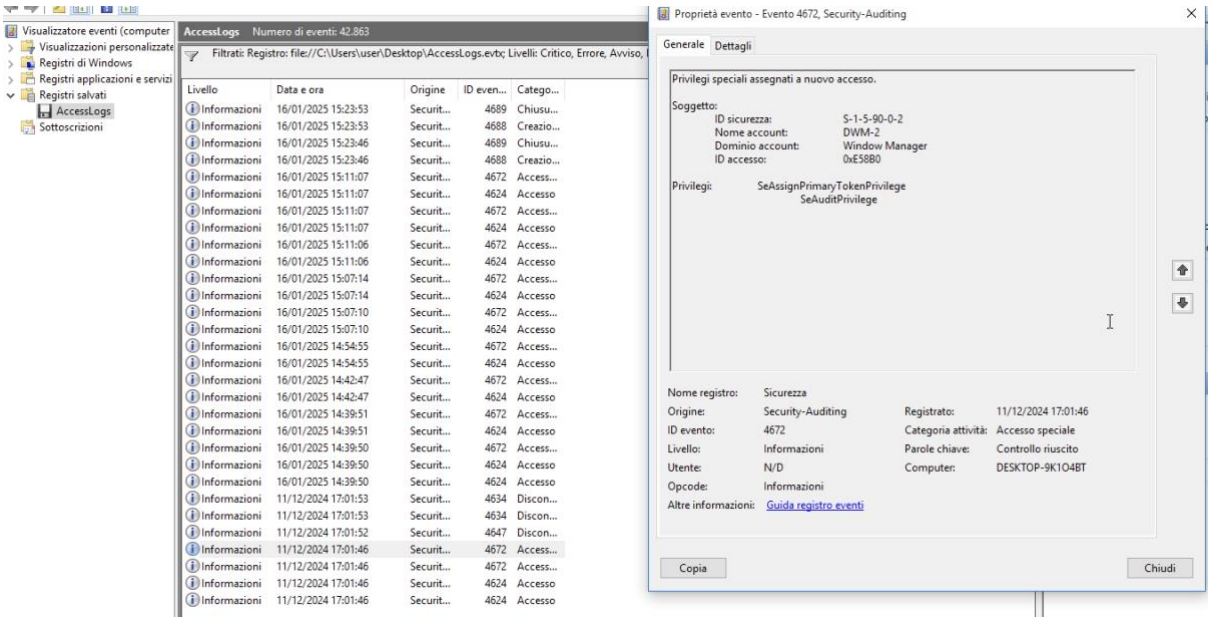


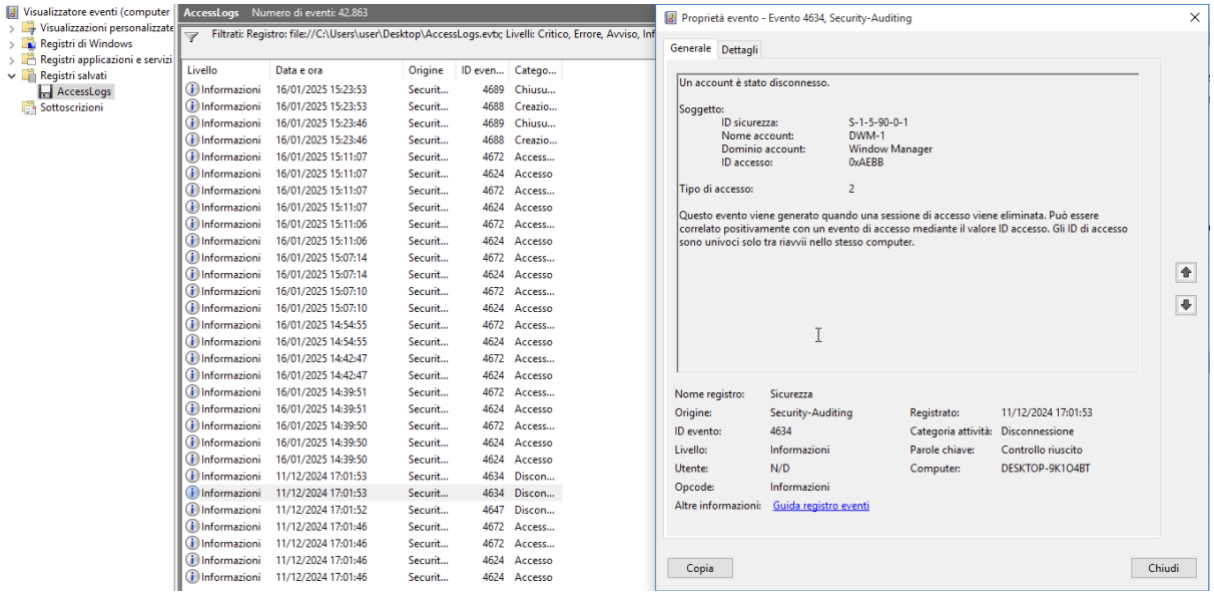
L'abilitazione delle policy di auditing è un passaggio essenziale per garantire che gli eventi correlati alla sicurezza vengano registrati correttamente sul sistema. Pertanto ne ho abilitate alcune:



Tutti i log sono ora visualizzati correttamente. Li ho esportati come file output.evtx:


Visualizzatore eventi (computer
Visualizzazioni personalizzate
Registri di Windows
Registri applicazioni e servizi
Registri salvati
AccessLogs
Sottoscrizioni
AccessLogs Numero di eventi: 42.863
Filtrati: Registro: file://C:\Users\user\Desktop\AccessLogs.evtx; Livelli: Critico, Errore, Avviso, Informazioni, Modalità dettagliata; Origine: ; ID evento:
Livello Data e ora Origine ID even... Catego...
Informazioni 16/01/2025 15:23:53 Securit... 4689 Chiusu...
Informazioni 16/01/2025 15:23:53 Securit... 4688 Creazio...
Informazioni 16/01/2025 15:23:46 Securit... 4689 Chiusu...
Informazioni 16/01/2025 15:23:46 Securit... 4688 Creazio...
Informazioni 16/01/2025 15:11:07 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:07 Securit... 4624 Accesso
Informazioni 16/01/2025 15:11:07 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:07 Securit... 4624 Accesso
Informazioni 16/01/2025 15:11:06 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:06 Securit... 4624 Accesso
Informazioni 16/01/2025 15:07:14 Securit... 4672 Access...
Informazioni 16/01/2025 15:07:14 Securit... 4624 Accesso
Informazioni 16/01/2025 15:07:10 Securit... 4672 Access...
Informazioni 16/01/2025 15:07:10 Securit... 4624 Accesso
Informazioni 16/01/2025 14:54:55 Securit... 4672 Access...
Informazioni 16/01/2025 14:54:55 Securit... 4624 Accesso
Informazioni 16/01/2025 14:42:47 Securit... 4672 Access...
Informazioni 16/01/2025 14:42:47 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:51 Securit... 4672 Access...
Informazioni 16/01/2025 14:39:51 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:50 Securit... 4672 Access...
Informazioni 16/01/2025 14:39:50 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:50 Securit... 4624 Accesso
Informazioni 11/12/2024 17:01:53 Securit... 4634 Discon...
Informazioni 11/12/2024 17:01:53 Securit... 4634 Discon...
Informazioni 11/12/2024 17:01:52 Securit... 4647 Discon...
Informazioni 11/12/2024 17:01:46 Securit... 4672 Access...
Informazioni 11/12/2024 17:01:46 Securit... 4672 Access...
Informazioni 11/12/2024 17:01:46 Securit... 4624 Accesso
Informazioni 11/12/2024 17:01:46 Securit... 4624 Accesso
Azioni
AccessLogs
Apri registro salvato...
Proprietà evento - Evento 4688, Security-Auditing
Generale Dettagli
Semplice XML
+ System
- EventData
SubjectUserSid S-1-5-19
SubjectUserName SERVIZIO LOCALE
SubjectDomainName NT AUTHORITY
SubjectLogonId 0x3e5
NewProcessId 0x8d8
NewProcessName C:\Windows\System32\rundll32.exe
TokenElevationType %%1938
ProcessId 0x324
CommandLine
TargetUserSid S-1-5-21-1859916961-34304393-1824526448-1001
TargetUserName user
TargetDomainName DESKTOP-9K1O4BT
TargetLogonId 0xf0886
ParentProcessName C:\Windows\System32\svchost.exe
MandatoryLabel S-1-16-8192
Copia
Chiudi


Visualizzatore eventi (computer
Visualizzazioni personalizzate
Registri di Windows
Registri applicazioni e servizi
Registri salvati
AccessLogs
Sottoscrizioni
AccessLogs Numero di eventi: 42.863
Livello Data e ora Origine ID even... Catego...
Informazioni 16/01/2025 15:23:53 Securit... 4689 Chiusu...
Informazioni 16/01/2025 15:23:53 Securit... 4688 Creazio...
Informazioni 16/01/2025 15:23:46 Securit... 4689 Chiusu...
Informazioni 16/01/2025 15:23:46 Securit... 4688 Creazio...
Informazioni 16/01/2025 15:11:07 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:07 Securit... 4624 Accesso
Informazioni 16/01/2025 15:11:07 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:07 Securit... 4624 Accesso
Informazioni 16/01/2025 15:11:06 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:06 Securit... 4624 Accesso
Informazioni 16/01/2025 15:07:14 Securit... 4672 Access...
Informazioni 16/01/2025 15:07:14 Securit... 4624 Accesso
Informazioni 16/01/2025 15:07:10 Securit... 4672 Access...
Informazioni 16/01/2025 15:07:10 Securit... 4624 Accesso
Informazioni 16/01/2025 14:54:55 Securit... 4672 Access...
Informazioni 16/01/2025 14:54:55 Securit... 4624 Accesso
Informazioni 16/01/2025 14:42:47 Securit... 4672 Access...
Informazioni 16/01/2025 14:42:47 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:51 Securit... 4672 Access...
Informazioni 16/01/2025 14:39:51 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:50 Securit... 4672 Access...
Informazioni 16/01/2025 14:39:50 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:50 Securit... 4624 Accesso
Informazioni 11/12/2024 17:01:53 Securit... 4634 Discon...
Informazioni 11/12/2024 17:01:53 Securit... 4634 Discon...
Informazioni 11/12/2024 17:01:52 Securit... 4647 Discon...
Informazioni 11/12/2024 17:01:46 Securit... 4672 Access...
Informazioni 11/12/2024 17:01:46 Securit... 4672 Access...
Informazioni 11/12/2024 17:01:46 Securit... 4624 Accesso
Informazioni 11/12/2024 17:01:46 Securit... 4624 Accesso
Proprietà evento - Evento 4672, Security-Auditing
Generale Dettagli
Privilegi speciali assegnati a nuovo accesso.
Soggetto:
ID sicurezza: S-1-5-90-0-2
Nome account: DWM-2
Dominio account: Window Manager
ID accesso: 0xE58B0
Privilegi: SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
Nome registro: Sicurezza
Origine: Security-Auditing
Registrato: 11/12/2024 17:01:46
ID evento: 4672
Categoria attività: Accesso speciale
Livello: Informazioni
Parole chiave: Controllo riuscito
Utente: N/D
Computer: DESKTOP-9K1O4BT
Opcode: Informazioni
Altre informazioni: Guida registro eventi
Copia
Chiudi


Visualizzatore eventi (computer
Visualizzazioni personalizzate
Registri di Windows
Registri applicazioni e servizi
Registri salvati
AccessLogs
Sottoscrizioni
AccessLogs Numero di eventi: 42.863
Filtrati: Registro: file://C:\Users\user\Desktop\AccessLogs.evtx; Livelli: Critico, Errore, Avviso, Inf
Livello Data e ora Origine ID even... Catego...
Informazioni 16/01/2025 15:23:53 Securit... 4689 Chiusu...
Informazioni 16/01/2025 15:23:53 Securit... 4688 Creazio...
Informazioni 16/01/2025 15:23:46 Securit... 4689 Chiusu...
Informazioni 16/01/2025 15:23:46 Securit... 4688 Creazio...
Informazioni 16/01/2025 15:11:07 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:07 Securit... 4624 Accesso
Informazioni 16/01/2025 15:11:07 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:07 Securit... 4624 Accesso
Informazioni 16/01/2025 15:11:06 Securit... 4672 Access...
Informazioni 16/01/2025 15:11:06 Securit... 4624 Accesso
Informazioni 16/01/2025 15:07:14 Securit... 4672 Access...
Informazioni 16/01/2025 15:07:14 Securit... 4624 Accesso
Informazioni 16/01/2025 15:07:10 Securit... 4672 Access...
Informazioni 16/01/2025 15:07:10 Securit... 4624 Accesso
Informazioni 16/01/2025 14:54:55 Securit... 4672 Access...
Informazioni 16/01/2025 14:54:55 Securit... 4624 Accesso
Informazioni 16/01/2025 14:42:47 Securit... 4672 Access...
Informazioni 16/01/2025 14:42:47 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:51 Securit... 4672 Access...
Informazioni 16/01/2025 14:39:51 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:50 Securit... 4672 Access...
Informazioni 16/01/2025 14:39:50 Securit... 4624 Accesso
Informazioni 16/01/2025 14:39:50 Securit... 4624 Accesso
Informazioni 11/12/2024 17:01:53 Securit... 4634 Discon...
Informazioni 11/12/2024 17:01:53 Securit... 4634 Discon...
Informazioni 11/12/2024 17:01:52 Securit... 4647 Discon...
Informazioni 11/12/2024 17:01:46 Securit... 4672 Access...
Informazioni 11/12/2024 17:01:46 Securit... 4672 Access...
Informazioni 11/12/2024 17:01:46 Securit... 4624 Accesso
Informazioni 11/12/2024 17:01:46 Securit... 4624 Accesso
Proprietà evento - Evento 4634, Security-Auditing
Generale Dettagli
Un account è stato disconnesso.
Soggetto:
ID sicurezza: S-1-5-90-0-1
Nome account: DWM-1
Dominio account: Window Manager
ID accesso: 0xAEBB
Tipo di accesso: 2
Questo evento viene generato quando una sessione di accesso viene eliminata. Può essere correlato positivamente con un evento di accesso mediante il valore ID accesso. Gli ID di accesso sono univoci solo tra riavvii nello stesso computer.
Nome registro: Sicurezza
Origine: Security-Auditing
Registrato: 11/12/2024 17:01:53
ID evento: 4634
Categoria attività: Disconnessione
Livello: Informazioni
Parole chiave: Controllo riuscito
Utente: N/D
Computer: DESKTOP-9K1O4BT
Opcode: Informazioni
Altre informazioni: Guida registro eventi
Copia
Chiudi