

Relazione File di Log di Windows

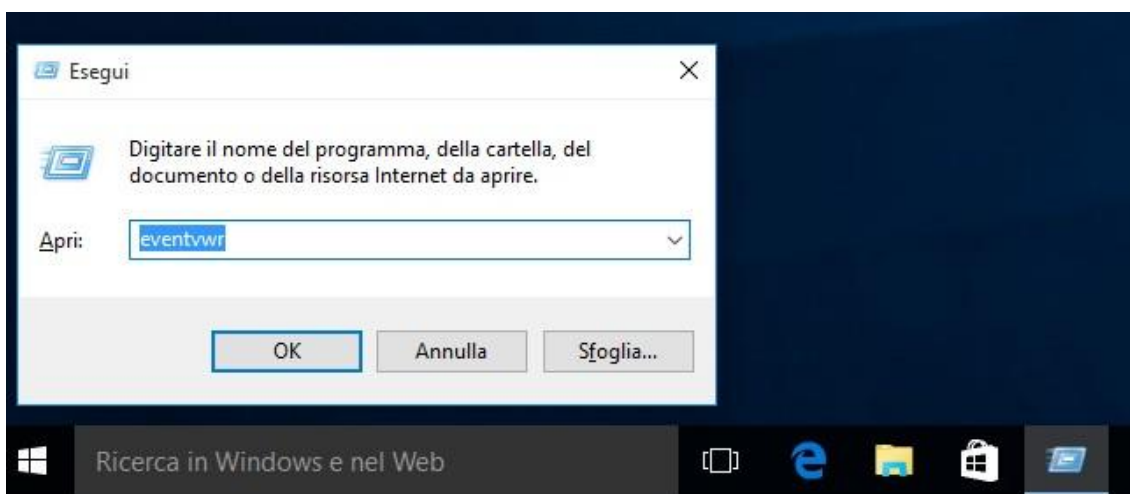
Come richiesto dalla traccia dobbiamo configurare e gestire i file di log della sicurezza, utilizzando il **Visualizzatore degli eventi** della macchina Windows.

Nella seguente immagine, illustro come accedere al Visualizzatore degli eventi di Windows con la combinazione di tasti, come da immagine seguente:



Una volta effettuata la combinazione dei tasti, come da immagine precedente, si apre una finestra dove dobbiamo inserire il comando specifico, che ci servirà per accedere al Visualizzatore degli eventi di Windows, digitando il comando:

- **digito il comando Eventvwr**
- **clicko sul pulsante OK**



The screenshot shows the Windows Event Viewer application. The left sidebar contains a tree view with the following items:

- Visualizzatore eventi (computer locale)
 - Visualizzazioni personalizzate
 - Registri di Windows
 - Registri applicazioni e servizi
 - Sottoscrizioni

The main pane is titled "Visualizzatore eventi (computer locale)" and "Panoramica e riepilogo". It shows the last update as "10/10/2024...". Below this, there is a section for "Panoramica" with a brief description of how to use the tool. The "Riepilogo eventi amministrativi" section displays a table of administrative events:

Tipo evento	ID evento	Origine	Registro	Ultima
Critico	-	-	-	-
Errore	-	-	-	-
Avviso	-	-	-	-
Informazioni	-	-	-	-

Below the table, there is a section for "Nodi visualizzati di recente" showing a list of nodes:

Nome	Descrizione	Ultima modifica	Data c
Registri di Windows\Sicu...	N/D	10/10/2024 11:58:36	09/07/...

The bottom section, "Riepilogo registro", shows a table of registry entries:

Nome registro	Dimensio...	Ultima modifica	Att
Applicazione	5,07 MB/20...	10/10/2024 11:58:43	Att
Eventi hardware	68 KB/20 ...	09/07/2024 16:23:21	Att
Internet Explorer	68 KB/1,0...	09/07/2024 16:23:21	Att
Servizi di gestione della...	68 KB/20...	09/07/2024 16:23:21	Att

The right pane, titled "Azioni", contains the following actions:

- Visualizzatore eventi (computer locale)
- Apri registro salvato...
- Crea visualizzazione personalizzata...
- Importa visualizzazione personalizzata...
- Connetti a un altro computer...
- Visualizza
- Aggiorna
- Guida

Visualizzatore eventi

File

Azione

Visualizza ?

Visualizzatore eventi (computer locale)

Visualizzazioni personalizzate

Registri di Windows

Applicazione

Sicurezza

Installazione

Sistema

Eventi inoltrati

Registri applicazioni e servizi

Sottoscrizioni

Sicurezza

Numero di eventi: 35.066 (1) Nuovi eventi disponibili

Parole c...	Data e ora	Origine	ID evento	Categori...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:27	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:26	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:26	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:26	Microsof...	4798	Gestione ...
Contr...	10/10/2024 12:07:26	Microsof...	4798	Gestione ...

Evento 4798, Microsoft Windows security auditing.

Generale

Dettagli

È stata enumerata l'appartenenza a un gruppo locale di un utente.

Soggetto:

Nome registro: Sicurezza

Origine: Microsoft Windows security Registrato: 10/10/

ID evento: 4798 Categoria attività: Gestio

Livello: Informazioni Parole chiave: Contr

Utente: N/D Computer: DESK1

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 4798, Microsoft Windows security auditing.

Proprietà evento

Associa attività all'evento...

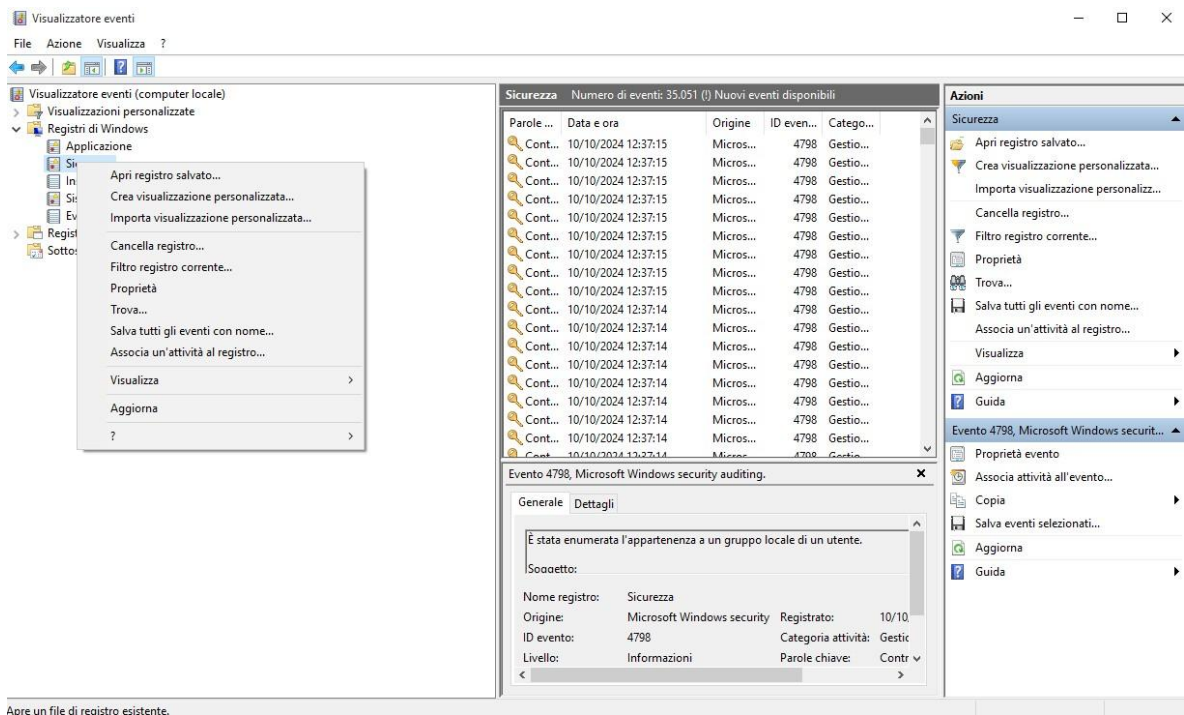
Copia

Salva eventi selezionati...

Aggiorna

Guida

Dopo aver cliccato sulla scheda “Sicurezza”, sempre sulla scheda “Sicurezza”, con il tasto destro del mouse, apro il menù dove trovo la voce “**Proprietà**” da dove posso cambiare la configurazione e gestire i file di Log della Sicurezza:



Nella scheda “Proprietà”, come accennato in precedenza, posso configurare a gestire i file di Log della Sicurezza

