



## **Medicina legale**

### **Data Infrastructure Insights**

NetApp

February 11, 2026

This PDF was generated from [https://docs.netapp.com/it-it/data-infrastructure-insights/forensic\\_activity\\_history.html](https://docs.netapp.com/it-it/data-infrastructure-insights/forensic_activity_history.html) on February 11, 2026. Always check docs.netapp.com for the latest.

# Sommario

- Medicina legale ..... 1
  - Analisi forense - Tutte le attività ..... 1
    - Esame di tutti i dati di attività ..... 1
    - Filtraggio dei dati della cronologia delle attività forensi ..... 3
    - Esempi di filtri forensi per l'attività: ..... 5
    - Ordinamento dei dati della cronologia delle attività forensi ..... 6
    - Guida utente per le esportazioni asincrone ..... 6
    - Selezione della colonna per tutte le attività ..... 7
    - Conservazione della cronologia delle attività ..... 7
    - Applicabilità dei filtri nella pagina forense ..... 7
    - Ricerca percorso ..... 9
    - Modifiche all'attività dell'utente SVM radice locale ..... 9
    - Risoluzione dei problemi ..... 9
  - Panoramica utente forense ..... 11
    - Profilo utente ..... 11
    - Comportamento dell'utente ..... 11
    - Intervallo di aggiornamento ..... 11
    - Politica di conservazione ..... 12

# Medicina legale

## Analisi forense - Tutte le attività

La pagina Tutte le attività consente di comprendere le azioni eseguite sulle entità nell'ambiente Workload Security.

### Esame di tutti i dati di attività

Fare clic su **Forensics > Activity Forensics** e quindi sulla scheda **Tutte le attività** per accedere alla pagina Tutte le attività. Questa pagina fornisce una panoramica delle attività svolte sul tuo inquilino, evidenziando le seguenti informazioni:

- Un grafico che mostra la *cronologia delle attività* (in base all'intervallo di tempo globale selezionato)

È possibile ingrandire il grafico trascinando un rettangolo al suo interno. Verrà caricata l'intera pagina per visualizzare l'intervallo di tempo ingrandito. Quando si esegue lo zoom avanti, viene visualizzato un pulsante che consente all'utente di rimpicciolire.

- Un elenco dei dati di *Tutte le attività*.
- Un menu a discesa "Raggruppa per" fornirà l'opzione di raggruppare l'attività in base a utenti, cartelle, tipo di entità, ecc.
- Un pulsante di percorso comune sarà disponibile sopra la tabella, cliccando sul quale potremo ottenere un pannello scorrevole con i dettagli del percorso dell'entità.

La tabella **Tutte le attività** mostra le seguenti informazioni. Si noti che non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare cliccando sull'icona "ingranaggio".

- **Ora** in cui è stato effettuato l'accesso a un'entità, inclusi anno, mese, giorno e ora dell'ultimo accesso.
- L'**utente** che ha avuto accesso all'entità con un collegamento a "[Informazioni utente](#)" come pannello scorrevole.
- L'**attività** svolta dall'utente. I tipi supportati sono:
  - **Modifica proprietà del gruppo** - La proprietà del gruppo del file o della cartella è stata modificata. Per maggiori dettagli sulla proprietà del gruppo, vedere "[questo collegamento](#)."
  - **Cambia proprietario** - La proprietà del file o della cartella è stata cambiata a un altro utente.
  - **Modifica autorizzazione** - L'autorizzazione del file o della cartella è stata modificata.
  - **Crea** - Crea file o cartella.
  - **Elimina** - Elimina file o cartella. Se una cartella viene eliminata, vengono ottenuti eventi *delete* per tutti i file presenti in quella cartella e nelle sottocartelle.
  - **Lettura** - Il file è stato letto.
  - **Leggi metadati** - Solo se si abilita l'opzione di monitoraggio delle cartelle. Verrà generato all'apertura di una cartella su Windows o eseguendo "ls" all'interno di una cartella su Linux.
  - **Rinomina** - Rinomina file o cartella.
  - **Scrittura** - I dati vengono scritti in un file.
  - **Scrivi metadati** - I metadati del file vengono scritti, ad esempio, se è stata modificata l'autorizzazione.

- **Altro cambiamento** - Qualsiasi altro evento non descritto sopra. Tutti gli eventi non mappati vengono mappati al tipo di attività "Altra modifica". Applicabile a file e cartelle.
- Il **Percorso** è il percorso dell'entità. Dovrebbe essere il percorso esatto dell'entità (ad esempio, `/home/userX/nested1/nested2/abc.txt`) OPPURE la parte di directory del percorso per la ricerca ricorsiva (ad esempio, `/home/userX/nested1/nested2/`). NOTA: i modelli di percorso regex (ad esempio, `*nested*`) NON sono consentiti qui. In alternativa, è possibile specificare anche filtri individuali a livello di cartella del percorso, come indicato di seguito, per il filtraggio del percorso.
- La **Cartella di 1° livello (Radice)** è la directory radice del percorso dell'entità in minuscolo.
- La **Cartella di secondo livello** è la directory di secondo livello del percorso dell'entità in minuscolo.
- La **Cartella di terzo livello** è la directory di terzo livello del percorso dell'entità in minuscolo.
- La **Cartella di 4° livello** è la directory di quarto livello del percorso dell'entità in minuscolo.
- **Tipo di entità**, inclusa l'estensione dell'entità (ad esempio file) (.doc, .docx, .tmp, ecc.).
- Il **Dispositivo** in cui risiedono le entità.
- Il **Protocollo** utilizzato per recuperare gli eventi.
- Il **Percorso originale** utilizzato per gli eventi di ridenominazione quando il file originale è stato rinominato. Per impostazione predefinita, questa colonna non è visibile nella tabella. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- Il **Volume** in cui risiedono le entità. Per impostazione predefinita, questa colonna non è visibile nella tabella. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- **Nome entità** è l'ultimo componente del percorso dell'entità; per il tipo di entità come file, è il nome del file.

Selezionando una riga della tabella si apre un pannello scorrevole con il profilo utente in una scheda e la panoramica delle attività e delle entità in un'altra scheda.

The screenshot shows the NetApp Cloud Insights interface. The main panel displays a table of activity logs under the 'Forensics' section. The table has columns for Time, User, Domain, Source IP, and Activity. The right-hand panel, titled 'Activity Overview', shows details for a selected activity, including User, Source IP, Activity, Protocol, Volume, Entity Profile, and Path.

Time	User	Domain	Source IP	Activity
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Write
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Rename
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Rename
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Read
6 days ago 3 Dec 2024 16:09	ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495		10.100.20.134	Write

**Activity Overview**

**Activity Details**

- Time: 6 days ago  
3 Dec 2024 16:09
- User: ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495
- Source IP: 10.100.20.134
- Activity: Read
- Protocol: SMB
- Volume: VolumeSBC

**Entity Profile**

- Entity: file600.txt
- Type: txt
- Path: /VolumeSBC/volume/nested1/file600.txt
- 1st Level Folder (Root): volumesbc
- 2nd Level Folder: volume
- 3rd Level Folder: nested1
- Last Accessed: 6 days ago  
3 Dec 2024 16:09
- Size: 4 KB
- Last Accessed By: ldap:qa2.contrail.coms-1-5-21-1192448160-1988033612-275769208-495
- Device: svmName
- Most Accessed Location: 10.100.20.134
- Last Accessed Location: 10.100.20.134

Il metodo *Raggruppa per* predefinito è *Attività forense*. Se si seleziona un metodo *Raggruppa per* diverso, ad esempio Tipo di entità, verrà visualizzata la tabella *Raggruppa per* dell'entità. Se non viene effettuata alcuna selezione, viene visualizzato *Raggruppa per tutto*.

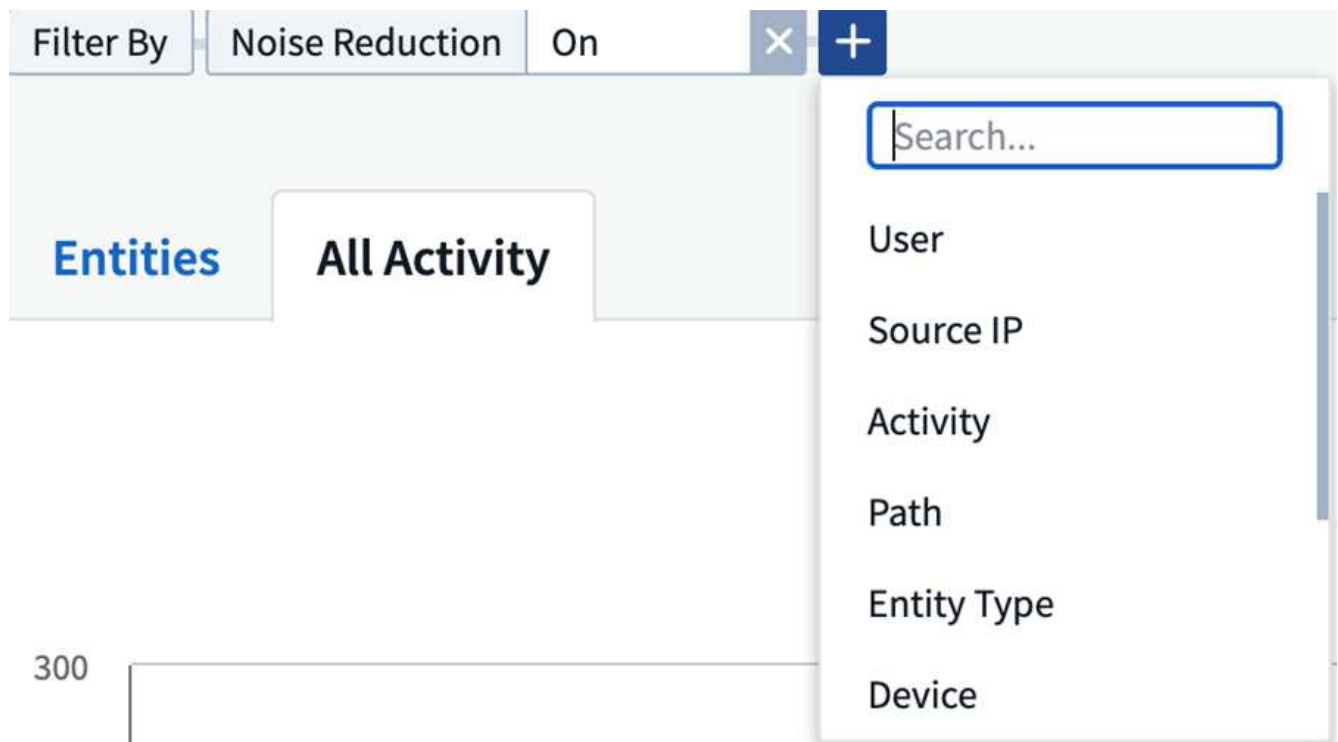
- Il conteggio delle attività viene visualizzato come collegamento ipertestuale; selezionando questa opzione, il raggruppamento selezionato verrà aggiunto come filtro. La tabella delle attività verrà aggiornata in base a quel filtro.
- Tieni presente che se modifichi il filtro, modifichi l'intervallo di tempo o aggiorni la schermata, non potrai tornare ai risultati filtrati senza impostare nuovamente il filtro.
- Si noti che quando si seleziona Nome entità come filtro, il menu a discesa *Raggruppa per* sarà disabilitato; inoltre, quando l'utente si trova già nella schermata *Raggruppa per*, il filtro Nome entità sarà disabilitato.

## Filtraggio dei dati della cronologia delle attività forensi

Esistono due metodi per filtrare i dati.

- Il filtro può essere aggiunto dal pannello scorrevole. Il valore viene aggiunto ai filtri appropriati nell'elenco *Filtra per* in alto.
- Filtra i dati digitando nel campo *Filtra per*:

Seleziona il filtro appropriato dal widget in alto "Filtra per" cliccando sul pulsante [+]:



Inserisci il testo da cercare

Premere Invio o fare clic all'esterno della casella del filtro per applicare il filtro.

È possibile filtrare i dati delle attività forensi in base ai seguenti campi:

- Il tipo **Attività**.
- **Protocollo** per recuperare attività specifiche del protocollo.

- **Nome utente** dell'utente che esegue l'attività. Per filtrare è necessario fornire il nome utente esatto. La ricerca con nome utente parziale o con nome utente parziale preceduto o suffisso '\*' non funzionerà.
- **Riduzione rumore** per filtrare i file creati nelle ultime 2 ore dall'utente. Viene utilizzato anche per filtrare i file temporanei (ad esempio, i file .tmp) a cui accede l'utente.
- **Dominio** dell'utente che esegue l'attività. Per filtrare è necessario fornire il **dominio esatto**. La ricerca di domini parziali o di domini parziali con prefisso o suffisso con carattere jolly (\*) non funzionerà. È possibile specificare *None* per cercare il dominio mancante.

I seguenti campi sono soggetti a regole di filtraggio speciali:

- **Tipo di entità**, utilizzando l'estensione dell'entità (file): è preferibile specificare il tipo di entità esatto tra virgolette. Ad esempio "txt".
- **Percorso** dell'entità: deve essere il percorso esatto dell'entità (ad esempio, "/home/userX/nested1/nested2/abc.txt") OPPURE la parte di directory del percorso per la ricerca ricorsiva (ad esempio, "/home/userX/nested1/nested2/"). NOTA: i modelli di percorso regex (ad esempio, \*nested\*) NON sono consentiti qui. Per risultati più rapidi, si consiglia di utilizzare filtri del percorso della directory (stringa del percorso che termina con /) fino a 4 directory di profondità. Ad esempio, "/home/userX/nested1/nested2/". Per maggiori dettagli, consultare la tabella sottostante.
- Cartella di 1° livello (radice): directory radice dell'entità Percorso come filtri. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare home OPPURE "home".
- Cartella di 2° livello: directory di 2° livello dei filtri del percorso dell'entità. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare userX OPPURE "userX".
- Cartella di 3° livello: directory di 3° livello dei filtri del percorso dell'entità.
- Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare nested1 OPPURE "nested1".
- Cartella di 4° livello - Directory Directory di 4° livello dei filtri del percorso dell'entità. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, è possibile utilizzare nested2 OPPURE "nested2".
- **Utente** che esegue l'attività: è preferibile specificare l'utente esatto tra virgolette. Ad esempio, "Amministratore".
- **Dispositivo** (SVM) in cui risiedono le entità
- **Volume** in cui risiedono le entità
- Il **Percorso originale** utilizzato per gli eventi di ridenominazione quando il file originale è stato rinominato.
- **IP di origine** da cui è stato effettuato l'accesso all'entità.
  - È possibile utilizzare i caratteri jolly \* e ?. Ad esempio: 10.0.0., **10.0?.0.10**, **10.10**
  - Se è richiesta una corrispondenza esatta, è necessario fornire un indirizzo IP sorgente valido tra virgolette doppie, ad esempio "10.1.1.1.". Gli IP incompleti con virgolette doppie come "10.1.1.", "10.1..\*", ecc. non funzioneranno.
- **Nome entità**: il nome del file del percorso dell'entità come filtro. Ad esempio, se il percorso dell'entità è /home/userX/nested1/testfile.txt, il nome dell'entità sarà testfile.txt. Si prega di notare che si consiglia di specificare il nome esatto del file tra virgolette; cercare di evitare le ricerche con caratteri jolly. Ad esempio, "testfile.txt". Si noti inoltre che questo filtro per nome entità è consigliato per intervalli di tempo più brevi (fino a 3 giorni).

I campi precedenti sono soggetti a quanto segue durante il filtraggio:

- Il valore esatto deve essere racchiuso tra virgolette: Esempio: "searchtext"

- Le stringhe jolly non devono contenere virgolette: Esempio: searchtext, \*searchtext\*, filtrerà tutte le stringhe contenenti 'searchtext'.
- Stringa con un prefisso, ad esempio: searchtext\* , cercherà tutte le stringhe che iniziano con 'searchtext'.

Si prega di notare che tutti i campi filtro sono di ricerca senza distinzione tra maiuscole e minuscole. Ad esempio: se il filtro applicato è Tipo di entità con valore come 'searchtext', restituirà risultati con Tipo di entità come 'searchtext', 'SearchText', 'SEARCHTEXT'

## Esempi di filtri forensi per l'attività:

Espressione del filtro applicata dall'utente	Risultato atteso	Valutazione delle prestazioni	Commento
Percorso = "/home/utenteX/nested1/nested2/"	Ricerca ricorsiva di tutti i file e le cartelle nella directory specificata	Veloce	Le ricerche nelle directory fino a 4 directory saranno rapide.
Percorso = "/home/utenteX/nested1/"	Ricerca ricorsiva di tutti i file e le cartelle nella directory specificata	Veloce	Le ricerche nelle directory fino a 4 directory saranno rapide.
Percorso = "/home/userX/nested1/test"	Corrispondenza esatta in cui il valore del percorso corrisponde a /home/userX/nested1/test	Più lentamente	La ricerca esatta sarà più lenta rispetto alle ricerche nella directory.
Percorso = "/home/utenteX/nested1/nested2/nested3/"	Ricerca ricorsiva di tutti i file e le cartelle nella directory specificata	Più lentamente	Le ricerche su più di 4 directory risultano più lente.
Qualsiasi altro filtro non basato sul percorso. Si consiglia di racchiudere i filtri di tipo utente ed entità tra virgolette, ad esempio Utente="Amministratore" Tipo di entità="txt"		Veloce	
Nome entità = "test.log"	Corrispondenza esatta in cui il nome del file è test.log	Veloce	Poiché è una corrispondenza esatta
Nome entità = *test.log	Nomi di file che terminano con test.log	Lento	A causa della wild card, può essere lento.
Nome entità = test*.log	I nomi dei file iniziano con test e terminano con .log	Lento	A causa della wild card, può essere lento.
Nome entità = test.lo	Nomi di file che iniziano con test.lo Ad esempio: corrisponderà a test.log, test.log.1, test.log1	Più lentamente	A causa della wild card alla fine, il gioco può risultare lento.

Espressione del filtro applicata dall'utente	Risultato atteso	Valutazione delle prestazioni	Commento
Nome entità = test	Nomi di file che iniziano con test	Il più lento	A causa della presenza di un carattere jolly alla fine e del valore più generico utilizzato, può risultare più lento.

NOTA:

1. Il conteggio delle attività visualizzato accanto all'icona Tutte le attività viene arrotondato a 30 minuti quando l'intervallo di tempo selezionato si estende per più di 3 giorni. Ad esempio, un intervallo di tempo dal 1° settembre alle 10:15 al 7 settembre alle 10:15 mostrerà i conteggi delle attività dal 1° settembre alle 10:00 al 7 settembre alle 10:30.
2. Allo stesso modo, le metriche di conteggio mostrate nel grafico Cronologia attività vengono arrotondate a 30 minuti quando l'intervallo di tempo selezionato si estende per più di 3 giorni.

## Ordinamento dei dati della cronologia delle attività forensi

È possibile ordinare i dati della cronologia delle attività in base a *Ora*, *Utente*, *IP sorgente*, *Attività*, *Tipo di entità*, Cartella di 1° livello (radice), Cartella di 2° livello, Cartella di 3° livello e Cartella di 4° livello. Per impostazione predefinita, la tabella è ordinata in base all'ordine decrescente *Time*, ovvero i dati più recenti verranno visualizzati per primi. L'ordinamento è disabilitato per i campi *Dispositivo* e *Protocollo*.

## Guida utente per le esportazioni asincrone

### Panoramica

La funzionalità Esportazioni asincrone di Storage Workload Security è progettata per gestire esportazioni di dati di grandi dimensioni.

### Guida passo passo: esportazione di dati con esportazioni asincrone

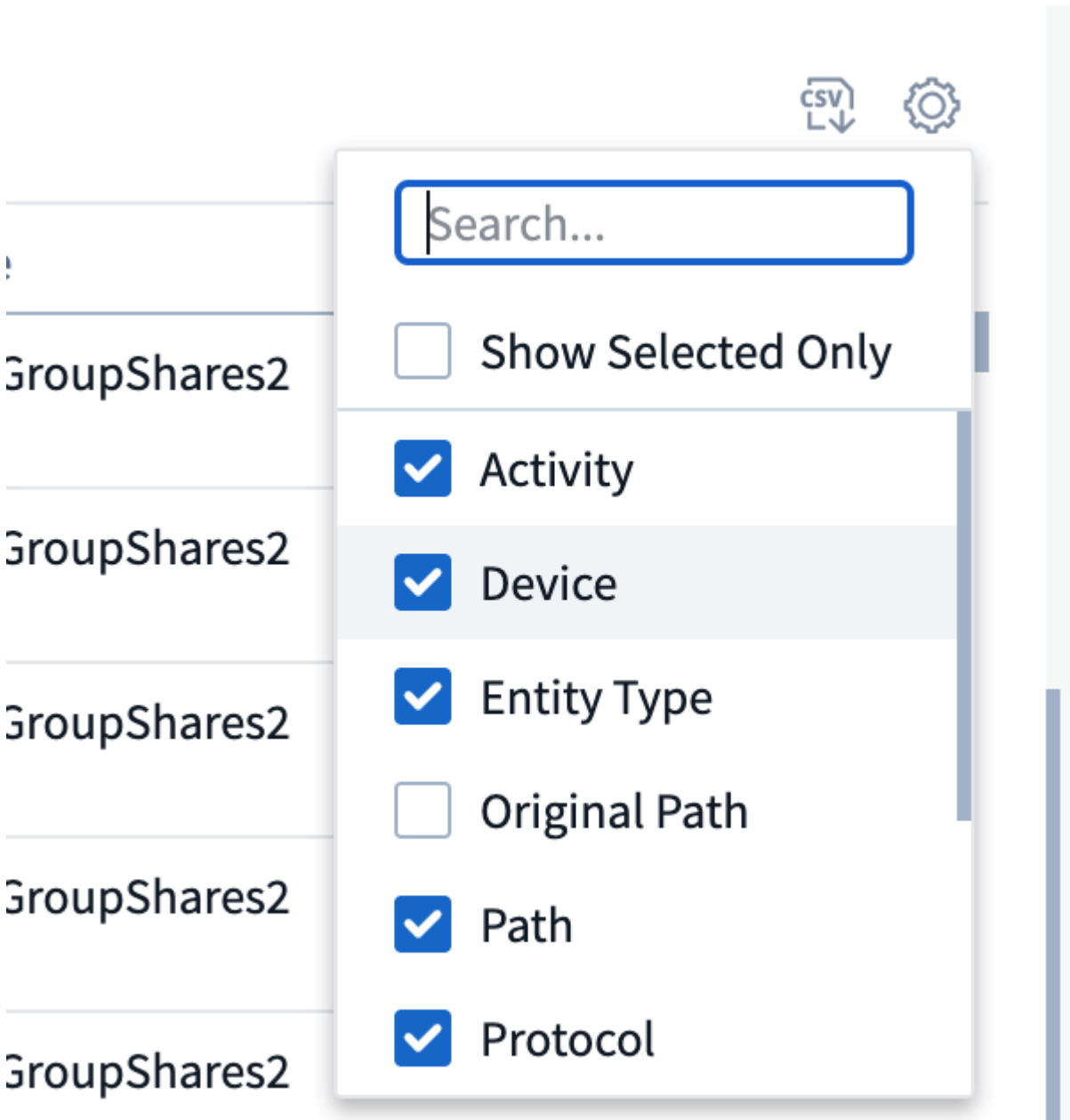
1. **Avvia esportazione:** seleziona la durata e i filtri desiderati per l'esportazione e fai clic sul pulsante Esporta.
2. **Attendi il completamento dell'esportazione:** il tempo di elaborazione può variare da pochi minuti ad alcune ore. Potrebbe essere necessario aggiornare la pagina forense più volte. Una volta completato il processo di esportazione, verrà abilitato il pulsante "Scarica l'ultimo file CSV esportato".
3. **Download:** Fare clic sul pulsante "Scarica l'ultimo file di esportazione creato" per ottenere i dati esportati in formato .zip. Questi dati saranno disponibili per il download finché l'utente non avvierà un'altra esportazione asincrona o finché non saranno trascorsi 3 giorni, a seconda di quale evento si verifichi per primo. Il pulsante rimarrà abilitato finché non verrà avviata un'altra esportazione asincrona.
4. **Limitazioni:**
  - Il numero di download asincroni è attualmente limitato a 1 per utente per ogni tabella Attività e Analisi Attività e a 3 per tenant.
  - I dati esportati sono limitati a un massimo di 1 milione di record per la tabella Attività; mentre per Raggruppa per, il limite è di mezzo milione di record.

Uno script di esempio per estrarre dati forensi tramite API è presente in `/opt/netapp/cloudsecure/agent/export-script/` sull'agente. Per maggiori dettagli sullo script, consultare il file readme in questa posizione.



## Selezione della colonna per tutte le attività

Per impostazione predefinita, la tabella *Tutte le attività* mostra colonne selezionate. Per aggiungere, rimuovere o modificare le colonne, fare clic sull'icona dell'ingranaggio a destra della tabella e selezionare dall'elenco delle colonne disponibili.



## Conservazione della cronologia delle attività

La cronologia delle attività viene conservata per 13 mesi per gli ambienti Workload Security attivi.

## Applicabilità dei filtri nella pagina forense

Filtro	Cosa fa	Esempio	Applicabile per questi filtri	Non applicabile per questi filtri	Risultato
* (Asterisco)	ti permette di cercare tutto	Auto*03172022 Se il testo di ricerca contiene un trattino o un carattere di sottolineatura, fornire l'espressione tra parentesi. Ad esempio, (svm*) per la ricerca di svm-123	Utente, Tipo di entità, Dispositivo, Volume, Percorso originale, Cartella di 1° livello, Cartella di 2° livello, Cartella di 3° livello, Cartella di 4° livello, Nome entità, IP sorgente		Restituisce tutte le risorse che iniziano con "Auto" e terminano con "03172022"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	AutoSabotageUser1_03172022?	Utente, Tipo di entità, Dispositivo, Volume, Cartella di 1° livello, Cartella di 2° livello, Cartella di 3° livello, Cartella di 4° livello, Nome entità, IP sorgente		restituisce AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 e così via
O	consente di specificare più entità	AutoSabotageUser1_03172022 O AutoRansomUser4_03162022	Utente, Dominio, Tipo di entità, Percorso originale, Nome entità, IP sorgente		restituisce uno qualsiasi tra AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NON	consente di escludere il testo dai risultati della ricerca	NOT AutoRansomUser4_03162022	Utente, dominio, tipo di entità, percorso originale, cartella di 1° livello, cartella di 2° livello, cartella di 3° livello, cartella di 4° livello, nome dell'entità, IP di origine	Dispositivo	restituisce tutto ciò che non inizia con "AutoRansomUser4_03162022"
Nessuno	cerca valori NULL in tutti i campi	Nessuno	Dominio		restituisce risultati in cui il campo di destinazione è vuoto

## Ricerca percorso

I risultati della ricerca con e senza / saranno diversi

"/AutoDir1/AutoFile03242022"	Funziona solo la ricerca esatta; restituisce tutte le attività con percorso esatto come /AutoDir1/AutoFile03242022 (senza distinzione tra maiuscole e minuscole)
"/AutoDir1/ "	Funziona; restituisce tutte le attività con directory di primo livello corrispondente ad AutoDir1 (senza distinzione tra maiuscole e minuscole)
"/AutoDir1/AutoFile03242022/"	Funziona; restituisce tutte le attività con la directory di 1° livello corrispondente ad AutoDir1 e la directory di 2° livello corrispondente ad AutoFile03242022 (senza distinzione tra maiuscole e minuscole)
/AutoDir1/AutoFile03242022 OPPURE /AutoDir1/AutoFile03242022	Non funziona
NON /AutoDir1/AutoFile03242022	Non funziona
NON /AutoDir1	Non funziona
NON /AutoFile03242022	Non funziona
*	Non funziona

## Modifiche all'attività dell'utente SVM radice locale

Se un utente root SVM locale sta eseguendo un'attività, l'IP del client su cui è montata la condivisione NFS viene ora considerato nel nome utente, che verrà visualizzato come `root@<indirizzo-ip-del-client>` sia nelle pagine delle attività forensi che in quelle delle attività utente.

Per esempio:

- Se SVM-1 è monitorato da Workload Security e l'utente root di tale SVM monta la condivisione su un client con indirizzo IP 10.197.12.40, il nome utente mostrato nella pagina delle attività forensi sarà `root@10.197.12.40`.
- Se lo stesso SVM-1 viene montato su un altro client con indirizzo IP 10.197.12.41, il nome utente mostrato nella pagina delle attività forensi sarà `root@10.197.12.41`.

\*• Ciò viene fatto per separare l'attività dell'utente root NFS in base all'indirizzo IP. In precedenza, tutte le attività erano considerate eseguite solo dall'utente `root`, senza distinzione di IP.

## Risoluzione dei problemi

Problema	Prova questo
----------	--------------

<p>Nella tabella "Tutte le attività", nella colonna "Utente", il nome utente è visualizzato come:  "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817" o  "ldap:default:80038003"</p>	<p>Le possibili ragioni potrebbero essere: 1. Non è stato ancora configurato alcun raccoglitore di directory utente. Per aggiungerne uno, vai su <b>Sicurezza del carico di lavoro &gt; Collettori &gt; Collettori directory utente</b> e fai clic su <b>+Collettore directory utente</b>. Scegliere <i>Active Directory</i> o <i>LDAP Directory Server</i>. 2. È stato configurato un User Directory Collector, ma si è arrestato o è in stato di errore. Vai su <b>Collezionisti &gt; Collezionisti directory utenti</b> e controlla lo stato. Fare riferimento al "<a href="#">Risoluzione dei problemi di User Directory Collector</a>" sezione della documentazione per suggerimenti sulla risoluzione dei problemi. Dopo aver effettuato la configurazione corretta, il nome verrà risolto automaticamente entro 24 ore. Se il problema persiste, controlla di aver aggiunto il corretto User Data Collector. Assicurarsi che l'utente faccia effettivamente parte del server Active Directory/LDAP Directory aggiunto.</p>
<p>Alcuni eventi NFS non vengono visualizzati nell'interfaccia utente.</p>	<p>Controllare quanto segue: 1. Un raccoglitore di directory utente per il server AD con attributi POSIX impostati dovrebbe essere in esecuzione con l'attributo unixid abilitato dall'interfaccia utente. 2. Tutti gli utenti che effettuano l'accesso NFS dovrebbero essere visibili quando si effettua una ricerca nella pagina utente dall'interfaccia utente 3. Gli eventi non elaborati (eventi per i quali l'utente non è ancora stato individuato) non sono supportati per NFS 4. L'accesso anonimo all'esportazione NFS non verrà monitorato. 5. Assicurarsi che la versione NFS utilizzata sia la 4.1 o una versione precedente. (Si noti che NFS 4.1 è supportato con ONTAP 9.15 o versioni successive.)</p>
<p>Dopo aver digitato alcune lettere contenenti un carattere jolly come l'asterisco (*) nei filtri delle pagine Forensics <i>All Activity</i> o <i>Entities</i>, le pagine si caricano molto lentamente.</p>	<p>Un asterisco (*) nella stringa di ricerca cerca tutto. Tuttavia, l'uso di stringhe jolly iniziali come <i>*&lt;searchTerm&gt;</i> o <i>*&lt;searchTerm&gt;*</i> causerà una query lenta. Per ottenere prestazioni migliori, utilizzare invece stringhe di prefisso nel formato <i>&lt;searchTerm&gt;*</i> (in altre parole, aggiungere l'asterisco (*) <i>dopo</i> un termine di ricerca). Esempio: utilizzare la stringa <i>testvolume*</i>, anziché <i>*testvolume</i> o <i>*test*volume</i>. Utilizzare una ricerca di directory per visualizzare ricorsivamente tutte le attività presenti in una determinata cartella (ricerca gerarchica). Ad esempio, <i>/path1/path2/path3/</i> elencherà ricorsivamente tutte le attività presenti in <i>/path1/path2/path3</i>. In alternativa, utilizzare l'opzione "Aggiungi al filtro" nella scheda Tutte le attività.</p>
<p>Quando utilizzo un filtro Percorso, ricevo l'errore "Richiesta non riuscita con codice di stato 500/503".</p>	<p>Prova a utilizzare un intervallo di date più piccolo per filtrare i record.</p>

L'interfaccia utente forense carica i dati lentamente quando si utilizza il filtro <i>path</i> .	Per risultati più rapidi, si consiglia di utilizzare filtri del percorso della directory (stringa del percorso che termina con /) fino a 4 directory di profondità. Ad esempio, se il percorso della directory è /Aaa/Bbb/Ccc/Ddd, provare a cercare "/Aaa/Bbb/Ccc/Ddd/" per caricare i dati più velocemente.
L'interfaccia utente di Forensics carica i dati lentamente e riscontra errori quando si utilizza il filtro del nome dell'entità.	Prova con intervalli di tempo più piccoli e con la ricerca del valore esatto con virgolette doppie. Ad esempio, se entityPath è "/home/userX/nested1/nested2/nested3/testfile.txt", prova con "testfile.txt" come filtro del nome dell'entità.

## Panoramica utente forense

Le informazioni per ciascun utente sono fornite nella Panoramica utente. Utilizzare queste visualizzazioni per comprendere le caratteristiche degli utenti, le entità associate e le attività recenti.

### Profilo utente

Le informazioni del profilo utente includono le informazioni di contatto e la posizione dell'utente. Il profilo fornisce le seguenti informazioni:

- Nome dell'utente
- Indirizzo email dell'utente
- Responsabile dell'utente
- Contatto telefonico per l'utente
- Posizione dell'utente

### Comportamento dell'utente

Le informazioni sul comportamento dell'utente identificano le attività e le operazioni recenti eseguite dall'utente. Queste informazioni includono:

- Attività recenti
  - Ultimo luogo di accesso
  - Grafico delle attività
  - Avvisi
- Operazioni degli ultimi sette giorni
  - Numero di operazioni

### Intervallo di aggiornamento

L'elenco degli utenti viene aggiornato ogni 12 ore.

## **Politica di conservazione**

Se non viene aggiornato nuovamente, l'elenco degli utenti viene conservato per 13 mesi. Dopo 13 mesi i dati verranno cancellati. Se l'ambiente Workload Security viene eliminato, tutti i dati associati all'ambiente vengono eliminati.

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.