Sicurezza del carico di lavoro

Data Infrastructure Insights

NetApp
January 17, 2025

Sommario

Sicurezza del carico di lavoro

Informazioni su Storage workload Security

Data Infrastructure Insights Storage workload Security (in precedenza Cloud Secure) aiuta a proteggere i dati con informazioni pratiche su minacce interne. Offre visibilità e controllo centralizzati di tutti gli accessi ai dati aziendali negli ambienti di cloud ibrido per garantire il rispetto degli obiettivi di sicurezza e conformità.

Visibilità

Ottieni visibilità e controllo centralizzati dell'accesso degli utenti ai tuoi dati aziendali critici memorizzati on-premise o nel cloud.

Sostituire strumenti e processi manuali che non forniscono una visibilità puntuale e precisa dell'accesso e del controllo dei dati. Workload Security funziona in modo esclusivo sia sul cloud che sui sistemi storage on-premise per fornire avvisi in tempo reale di comportamenti dannosi degli utenti.

Protezione

Proteggi i dati dell'organizzazione da un utilizzo improprio da parte di utenti malintenzionati o compromessi attraverso l'apprendimento automatico avanzato e il rilevamento delle anomalie.

Avvisa l'utente in caso di accesso anomalo ai dati attraverso l'apprendimento automatico avanzato e il rilevamento delle anomalie del comportamento dell'utente.

Conformità

Garantire la conformità aziendale verificando l'accesso dei dati degli utenti ai dati aziendali critici memorizzati on-premise o nel cloud.

Per iniziare

Introduzione alla sicurezza del carico di lavoro

È necessario completare alcune attività di configurazione prima di poter iniziare a utilizzare workload Security per monitorare l'attività dell'utente.

Il sistema workload Security utilizza un agente per raccogliere i dati di accesso dai sistemi storage e le informazioni utente dai server Directory Services.

Prima di iniziare la raccolta dei dati, è necessario configurare quanto segue:

Attività	Informazioni correlate

Configurare un agente	"Requisiti dell'agente" "Aggiungi agente" "**Video**: Implementazione dell'agente"
Configurare un connettore di directory utente	"Aggiungi connettore directory utente" "**Video**: Connessione Active Directory"
Configurare i data colleziones	Fare clic su **sicurezza del carico di lavoro > Collectors** fare clic sul data collector che si desidera configurare. Vedere la sezione riferimento fornitore Data Collector della documentazione. "**Video**: Connessione SVM ONTAP"
Creare account utente	"Gestire gli account utente"
Risoluzione dei problemi	"**Video**: Risoluzione dei problemi"

Workload Security può integrarsi anche con altri strumenti. Ad esempio, "consultare questa guida" sull'integrazione con Splunk.

Requisiti dell'agente per la sicurezza del carico di lavoro

È necessario "Installare un Agent"per acquisire informazioni dai propri data collector. Prima di installare l'Agent, assicurarsi che l'ambiente soddisfi i requisiti di sistema operativo, CPU, memoria e spazio su disco.

Componente	Requisiti Linux
Sistema operativo	Un computer che esegue una versione con licenza di una delle seguenti versioni: * CentOS 8 11 9,4 Stream (64 64 bit), CentOS 9 9,3 Stream, SELinux * openSUSE Leap da 64 a 64 (64 bit) * Oracle Linux da 64 a 20,04, 15 SP5 a 64 (15 SP3 bit) * Red Hat Enterprise Linux da 9,4 a 8,8, da 9,2 a 9,4 (9,4 bit), SELinux * 9,1-8,6 bit e Linux * 9,1-8,6 bit (Linux) * 64-8,8-22,04-15,3-15,5-64-10-24,04 e Linux. Si consiglia di utilizzare un server dedicato.
Comandi	per l'installazione è necessario decomprimere. Inoltre, il comando 'sudo su –' è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
CPU	4 core CPU
Memoria	16 GB DI RAM

Componente	Requisiti Linux
Spazio su disco disponibile	Lo spazio su disco dovrebbe essere allocato in questo modo: /Opt/NetApp 36 GB (minimo 35 GB di spazio libero dopo la creazione del filesystem) Nota: Si consiglia di allocare un po' di spazio su disco extra per consentire la creazione del filesystem. Assicurarsi che ci siano almeno 35 GB di spazio libero nel filesystem. Se /opt è una cartella montata da un dispositivo di archiviazione NAS, assicurarsi che gli utenti locali abbiano accesso a questa cartella. L'installazione di Agent o Data Collector potrebbe non riuscire se gli utenti locali non dispongono dell'autorizzazione per questa cartella. Per ulteriori informazioni, vedere la sezione."risoluzione dei problemi"
Rete	Connessione Ethernet da 100 Mbps a 1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi e porta richiesta per l'istanza di workload Security (80 o 443).

Nota: L'agente di sicurezza del carico di lavoro può essere installato sullo stesso computer di un'unità di acquisizione e/o di un agente di Data Infrastructure Insights. Tuttavia, è consigliabile installarli in computer separati. Nel caso in cui siano installati sullo stesso computer, allocare lo spazio su disco come mostrato di seguito:

Spazio su disco disponibile	50-55 GB per Linux, lo spazio su disco deve essere allocato in questo modo: /Opt/netapp 25-30 GB /var/log/netapp 25 GB

Consigli aggiuntivi

- Si consiglia vivamente di sincronizzare l'ora sul sistema ONTAP e sul computer dell'agente utilizzando **protocollo NTP (Network Time Protocol)** o **SNTP (Simple Network Time Protocol)**.

Regole di accesso alla rete cloud

Per ambienti di workload Security * basati su * Stati Uniti:

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	Accesso a Data Infrastructure Insights
TCP	443	Agente di sicurezza del carico di lavoro	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Per ambienti di sicurezza dei workload **basati sull'Europa**:

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	Accesso a Data Infrastructure Insights
TCP	443	Agente di sicurezza del carico di lavoro	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Per ambienti di sicurezza dei workload * basati su APAC*:

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	Accesso a Data Infrastructure Insights
TCP	443	Agente di sicurezza del carico di lavoro	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Regole in-network

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAPS / start-tls)	Agente di sicurezza del carico di lavoro	URL del server LDAP	Connettersi a LDAP

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	Cluster o SVM Management IP Address (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP
TCP	35000 - 55000	Indirizzi IP LIF dati SVM	Agente di sicurezza del carico di lavoro	Comunicazione da ONTAP all'agente di sicurezza del carico di lavoro per gli eventi Fpolicy. Affinché ONTAP possa inviarvi eventi, compresi eventuali firewall presenti nell'agente di protezione del carico di lavoro stesso (se presente), è necessario aprire queste porte verso l'agente di protezione del carico di lavoro. SI NOTI che non è necessario riservare **tutte** di queste porte, ma le porte che si riservano per questo devono rientrare in questo intervallo. Si consiglia di iniziare riservando ~100 porte e aumentando, se necessario.
TCP	7	Agente di sicurezza del carico di lavoro	Indirizzi IP LIF dati SVM	Eco dai Agent ai LIF dati SVM
SSH	22	Agente di sicurezza del carico di lavoro	Gestione del cluster	Necessario per il blocco degli utenti CIFS/SMB.

Dimensionamento del sistema

Consultare la "Controllo della velocità degli eventi" documentazione per informazioni sul dimensionamento.

Installazione di workload Security Agent

Workload Security (in precedenza Cloud Secure) raccoglie i dati delle attività degli utenti utilizzando uno o più agenti. Gli agenti si connettono ai dispositivi del tenant e raccolgono i dati che vengono inviati al livello SaaS di sicurezza dei workload per l'analisi. Vedere

"Requisiti dell'agente" per configurare una VM agente.

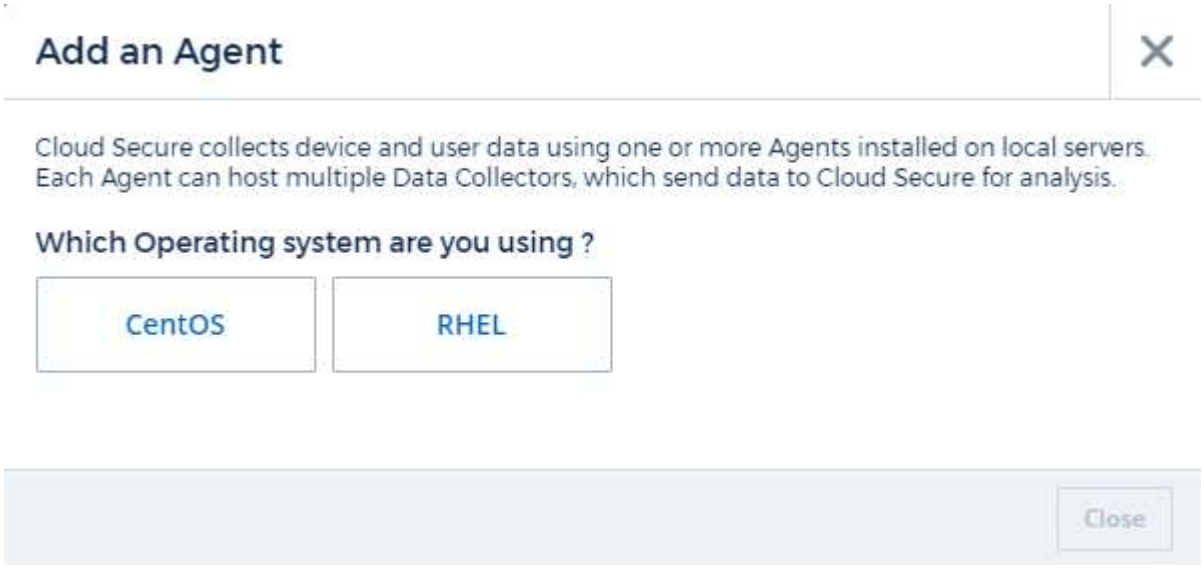
Prima di iniziare

- Il privilegio sudo è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
- Durante l'installazione dell'agente, sul computer vengono creati un utente locale *cssys* e un gruppo locale *cssys*. Se le impostazioni di autorizzazione non consentono la creazione di un utente locale e richiedono invece Active Directory, nel server Active Directory deve essere creato un utente con il nome utente *cssys*.
- È possibile leggere informazioni sulla sicurezza di Data Infrastructure Insights "qui".

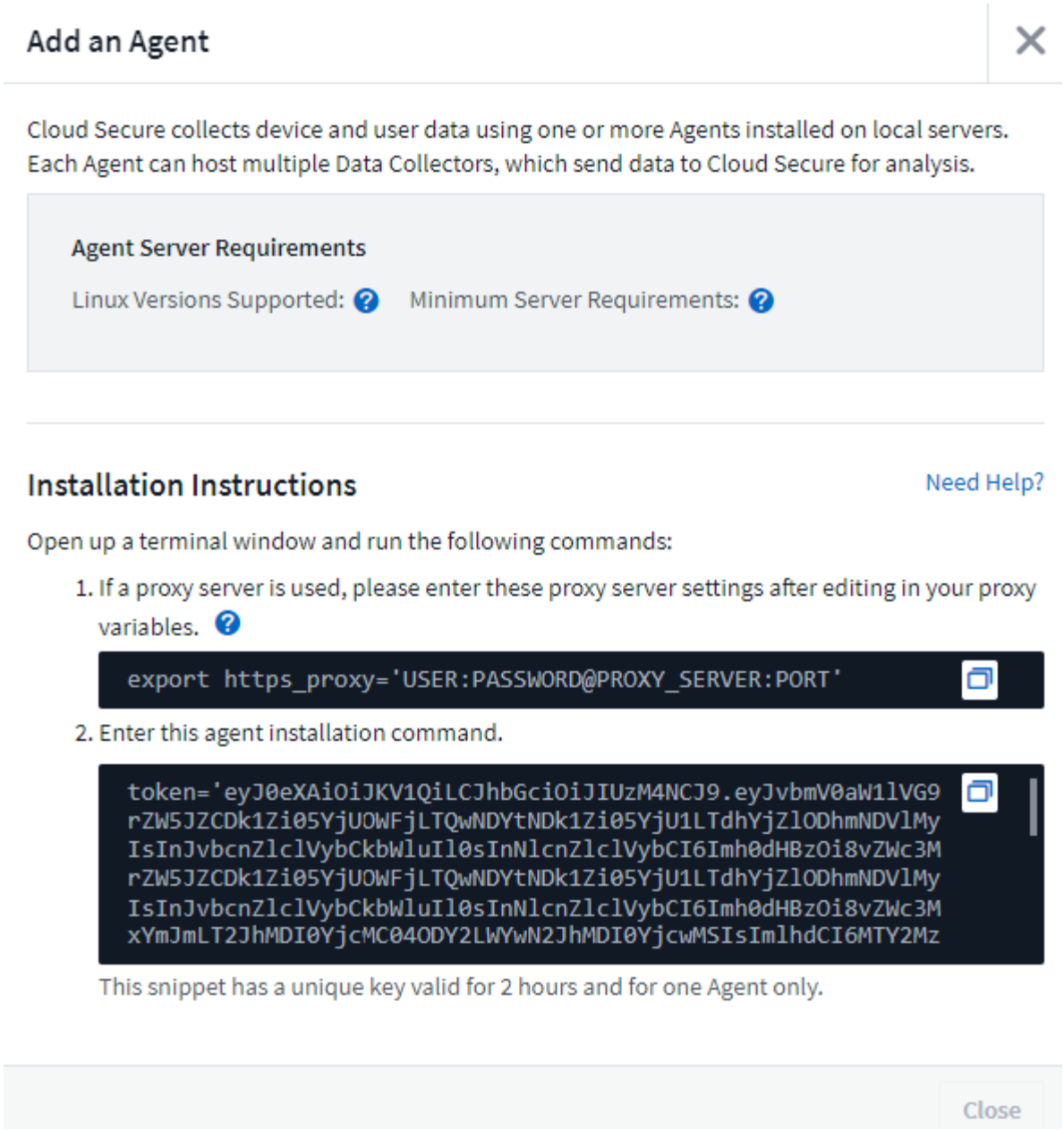
Procedura per l'installazione dell'agente

1. Accedere come Amministratore o Proprietario dell'account all'ambiente workload Security.
2. Selezionare **Collector > Agents > +Agent**

   Viene visualizzata la pagina Add an Agent (Aggiungi un agente):



3. Verificare che il server degli agenti soddisfi i requisiti minimi di sistema.
4. Per verificare che sul server degli agenti sia in esecuzione una versione supportata di Linux, fare clic su *versioni supportate (i)*.
5. Se la rete utilizza un server proxy, impostare i dettagli del server proxy seguendo le istruzioni nella sezione Proxy.



6. Fare clic sull'icona Copia negli Appunti per copiare il comando di installazione.
7. Eseguire il comando di installazione in una finestra del terminale.
8. Al termine dell'installazione, il sistema visualizza il seguente messaggio:

Una volta terminato

1. È necessario configurare un "User Directory Collector".
2. È necessario configurare uno o più Data Collector.

Configurazione di rete

Eseguire i seguenti comandi sul sistema locale per aprire le porte che verranno utilizzate da workload Security. In caso di problemi di sicurezza relativi all'intervallo di porte, è possibile utilizzare un intervallo di porte inferiore, ad esempio *35000:35100*. Ogni SVM utilizza due porte.

Fasi

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Segui i passaggi successivi in base alla piattaforma:

CentOS 7.x/RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Output di esempio:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x/RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000` (Per CentOS 8)

Output di esempio:

```
35000-55000/tcp
```

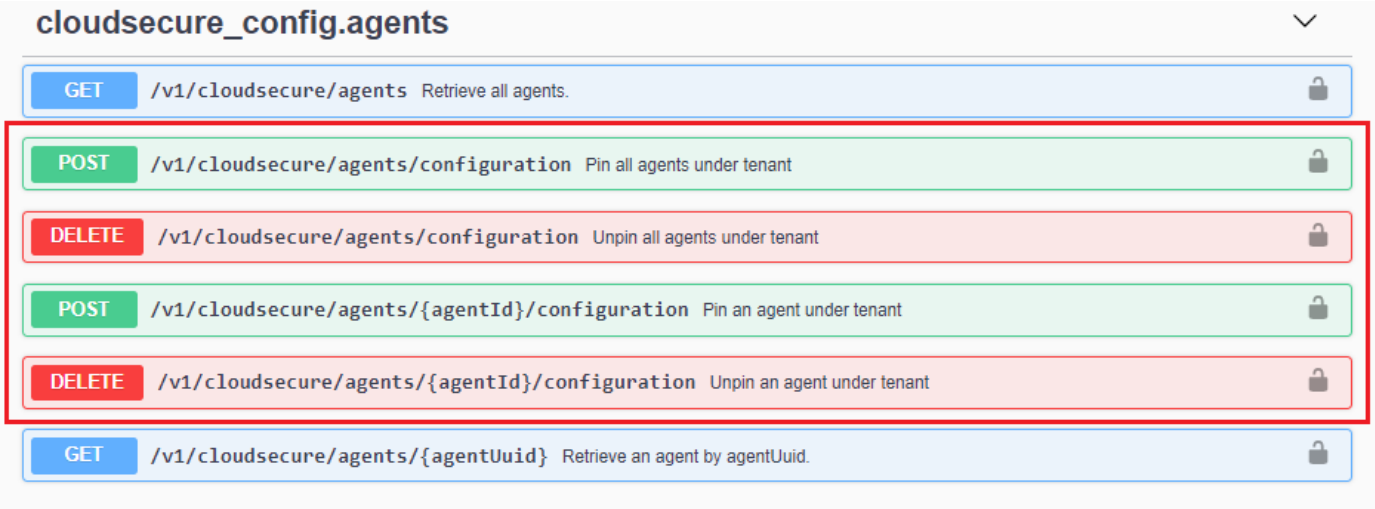
"Inserimento" di un agente nella versione corrente

Per impostazione predefinita, Data Infrastructure Insights workload Security aggiorna automaticamente gli agenti. Alcuni clienti potrebbero voler sospendere l'aggiornamento automatico, lasciando un Agent nella versione corrente fino a quando non si verifica una delle seguenti situazioni:

- Il cliente riprende gli aggiornamenti automatici dell'agente.
- sono passati 30 giorni. Tenere presente che i 30 giorni iniziano il giorno dell'ultimo aggiornamento dell'Agente, non il giorno in cui l'Agente viene messo in pausa.

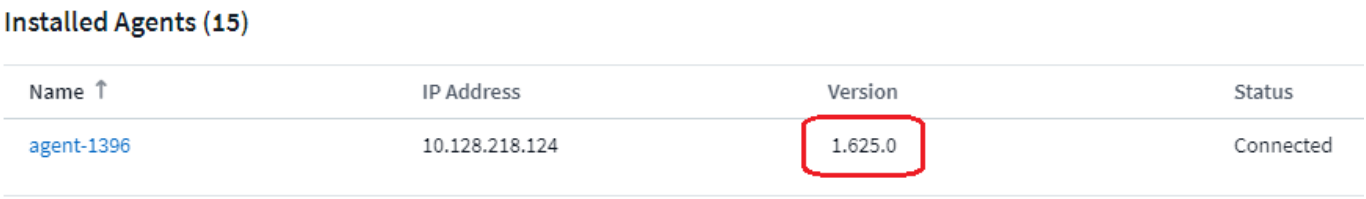
In ciascuno di questi casi, l'agente verrà aggiornato al prossimo aggiornamento di sicurezza del carico di lavoro.

Per sospendere o riprendere gli aggiornamenti automatici dell'agente, utilizzare le API *cloudSecure_config.agents*:



Nota: Potrebbero essere necessari fino a cinque minuti affinché l'azione di pausa o ripresa diventi effettiva.

È possibile visualizzare le versioni correnti di Agent nella pagina **sicurezza del carico di lavoro > Collectors**, nella scheda **Agenti**.



Risoluzione dei problemi relativi agli errori dell'agente

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

Problema:	Risoluzione:
L'installazione dell'agente non riesce a creare la cartella /opt/netapp/cloudsecsicuro/Agent/logs/agent.log e il file install.log non fornisce informazioni rilevanti.	Questo errore si verifica durante il bootstrap dell'agente. L'errore non viene registrato nei file di log perché si verifica prima dell'inizializzazione del logger. L'errore viene reindirizzato all'output standard ed è visibile nel log di servizio utilizzando il `journalctl -u cloudsecure-agent.service` comando. Questo comando può essere utilizzato per risolvere ulteriormente il problema. est
L'installazione dell'agente non riesce 'questa distribuzione linux non è supportata. Uscire dall'installazione'.	Questo errore viene visualizzato quando si tenta di installare l'agente su un sistema non supportato. Vedere "Requisiti dell'agente".
Installazione dell'agente non riuscita con l'errore: "-bash: Unzip: Command not found"	Installare unzip ed eseguire nuovamente il comando di installazione. Se Yum è installato sul computer, provare a "yum install unzip" per installare il software unzip. Quindi, copiare nuovamente il comando dall'interfaccia utente di installazione dell'agente e incollarlo nell'interfaccia utente per eseguire nuovamente l'installazione.

Problema:	Risoluzione:
L’agente è stato installato ed era in esecuzione. Tuttavia, l’agente si è arrestato improvvisamente.	SSH al computer dell’agente. Controllare lo stato del servizio agente tramite `sudo systemctl status cloudsecure-agent.service`. 1. Controllare se nei registri viene visualizzato il messaggio "Impossibile avviare il servizio del daemon di sicurezza del carico di lavoro" . 2. Verificare se l’utente cssys è presente o meno nel computer dell’agente. Eseguire i seguenti comandi uno alla volta con l’autorizzazione root e controllare se l’utente e il gruppo cssys esistono. `sudo id cssys` `sudo groups cssys` 3. Se non esiste alcun criterio di monitoraggio centralizzato, l’utente cssys potrebbe essere stato eliminato da un criterio di monitoraggio centralizzato. 4. Creare manualmente l’utente e il gruppo csys eseguendo i seguenti comandi. `sudo useradd cssys` `sudo groupadd cssys` 5. Riavviare il servizio dell’agente eseguendo il comando seguente: `sudo systemctl restart cloudsecure-agent.service` 6. Se ancora non è in esecuzione, controllare le altre opzioni di risoluzione dei problemi.
Impossibile aggiungere più di 50 Data colleziones a un Agente.	È possibile aggiungere solo 50 Data colleziones a un Agente. Questa può essere una combinazione di tutti i tipi di collector, ad esempio Active Directory, SVM e altri tipi di raccolta.
L’interfaccia utente mostra che l’agente è in stato NOT_CONNECTED.	Procedura per riavviare l’agente. 1. SSH al computer dell’agente. 2. Riavviare il servizio dell’agente eseguendo il comando seguente: `sudo systemctl restart cloudsecure-agent.service` 3. Controllare lo stato del servizio agente tramite `sudo systemctl status cloudsecure-agent.service`. 4. L’agente deve passare allo stato CONNESSO.
La macchina virtuale dell’agente è dietro il proxy Zscaler e l’installazione dell’agente non riesce. A causa dell’ispezione SSL del proxy Zscaler, i certificati di workload Security vengono presentati in quanto firmati da Zscaler CA, in modo che l’agente non stia fidando della comunicazione.	Disattivare l’ispezione SSL nel proxy Zscaler per l’URL *.cloudinsights.netapp.com. Se Zscaler esegue l’ispezione SSL e sostituisce i certificati, la sicurezza del carico di lavoro non funzionerà.

Problema:	Risoluzione:
Durante l’installazione dell’agente, l’installazione si blocca dopo la decompressione.	Il comando "chmod 755 -RF" non funziona correttamente. Il comando non riesce quando il comando di installazione dell’agente viene eseguito da un utente sudo non root che ha file nella directory di lavoro, appartenenti a un altro utente, e le autorizzazioni di tali file non possono essere modificate. A causa del comando chmod non funzionante, il resto dell’installazione non viene eseguito. 1. Creare una nuova directory denominata "cloudSecure". 2. Accedere a tale directory. 3. Copiare e incollare il comando di installazione completo “token=… … ./cloudSecure-Agent-install.sh" e premere invio. 4. L’installazione dovrebbe essere in grado di procedere.
Se l’Agente non riesce ancora a connettersi a Saas, aprire un caso con il supporto NetApp. Fornire il numero di serie di Data Infrastructure Insights per aprire un caso e allegare registri al caso come indicato.	Per allegare i registri al caso: 1. Eseguire il seguente script con l’autorizzazione root e condividere il file di output (cloudSecure-Agent-symptoms.zip). a. /opt/NetApp/cloudSecure/Agent/bin/cloudsecure-agent-symptom-collector.sh 2. Eseguire i seguenti comandi uno ad uno con l’autorizzazione root e condividere l’output. a. id cssys b. raggruppa cssys c. Cat /etc/os-release
Lo script cloudsecure-agent-symptom-collector.sh non riesce e viene visualizzato il seguente errore. [Root@machine tmp] n. /opt/netapp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh raccolta log del servizio raccolta log dell’applicazione raccolta di configurazioni dell’agente acquisizione di snapshot dello stato del servizio acquisizione di snapshot della struttura della directory dell’agente …… . …… . /Opt/netapp/cloudsecura/Agent/bin/cloudsecura-Agent-Symptom-collector.sh: Riga 52: zip: Errore comando non trovato: Impossibile creare /tmp/cloudsecure-agent-symptoms.zip	Lo strumento ZIP non è installato. Installare lo strumento zip eseguendo il comando "yum install zip". Quindi eseguire di nuovo il file cloudsecure-agent-symptom-collector.sh.
L’installazione dell’agente non riesce con useradd: Impossibile creare la directory /home/cssys	Questo errore può verificarsi se la directory di login dell’utente non può essere creata in /home, a causa della mancanza di permessi. La soluzione consiste nel creare un utente cssys e aggiungerne manualmente la directory di accesso utilizzando il seguente comando: *Sudo useradd user_name -m -d HOME_DIR* -m :creare la home directory dell’utente se non esiste. -D : il nuovo utente viene creato utilizzando HOME_DIR come valore per la directory di accesso dell’utente. Ad esempio, *sudo useradd cssys -m -d /cssys*, aggiunge un utente *cssys* e crea la directory di login sotto root.

Problema:	Risoluzione:
L'agente non è in esecuzione dopo l'installazione. *Systemctl status cloudsecure-agent.service* 2s NetApp 25889 12:26 126 1 mostra quanto segue: [Root@demo ~]# systemctl status cloudsecure-agent.service agent.service 25889 126 1 03 21 cloudsecure-agent.service – workload Security Agent Daemon Service caricato: Caricato (/usr/lib/systemd/system/cloudsecure-agent.service; 126 03 21 cloudsecure-agent.service: 12:26 abilitato; vendor preset: Disabilitato) attivo: Attivazione (auto-restart) (risultato: Exit-code) da mar 2021-08-03 21:12:26 Agosto 03 21:12:26 sistema dimostrativo[1]: cloudsecure-agent.service non riuscito.	Questo potrebbe non riuscire perché l'utente *cssys* potrebbe non disporre dell'autorizzazione per l'installazione. Se /opt/netapp è un mount NFS e l'utente *cssys* non ha accesso a questa cartella, l'installazione avrà esito negativo. *Cssys* è un utente locale creato dal programma di installazione di workload Security che potrebbe non disporre dell'autorizzazione per accedere alla condivisione montata. Per verificarlo, tentare di accedere a /opt/netapp/cloudsecrect/Agent/bin/cloudsecrect-Agent utilizzando *cssys* user. Se restituisce "autorizzazione negata", l'autorizzazione all'installazione non è presente. Invece di una cartella montata, installarla in una directory locale del computer.
L'agente era inizialmente connesso tramite un server proxy e il proxy era impostato durante l'installazione dell'agente. Ora il server proxy è cambiato. Come si può modificare la configurazione del proxy dell'Agente?	È possibile modificare agent.properties per aggiungere i dettagli del proxy. Attenersi alla seguente procedura: 1. Passare alla cartella contenente il file di proprietà: cd /opt/netapp/cloudsecsicuro/conf 2. Utilizzando l'editor di testo preferito, aprire il file *agent.properties* per la modifica. 3. Aggiungere o modificare le seguenti righe: AGENT_PROXY_HOST=scspa1950329001.vm.NetApp.com AGENT_PROXY_PORT=80 AGENT_PROXY_user=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Salvare il file. 5. Riavviare l'agente: Sudo systemctl riavviare cloudsecure-agent.service

Eliminazione di un agente di sicurezza del carico di lavoro

Quando si elimina un agente di sicurezza del carico di lavoro, è necessario eliminare prima tutti i dati di raccolta associati all'agente.

Eliminazione di un agente

L'eliminazione di un agente comporta l'eliminazione di tutti i Data Collector associati all'agente. Se si prevede di configurare i data collector con un agente diverso, è necessario creare un backup delle configurazioni di Data Collector prima di eliminare l'agente.

Prima di iniziare

1. Assicurarsi che tutti i data raccoglitori associati all'agente siano eliminati dal portale workload Security.

   Nota: Ignorare questo passaggio se tutti i collettori associati sono in stato DI ARRESTO.

Procedura per l'eliminazione di un agente:

1. SSH nella macchina virtuale dell'agente ed eseguire il seguente comando. Quando richiesto, immettere "y" per continuare.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Fare clic su **sicurezza del carico di lavoro > Collector > Agenti**

   Viene visualizzato l'elenco degli agenti configurati.

3. Fare clic sul menu delle opzioni dell'agente che si desidera eliminare.
4. Fare clic su **Delete** (Elimina).

   Viene visualizzata la pagina **Delete Agent** (Elimina agente).

5. Fare clic su **Delete** (Elimina) per confermare l'eliminazione.

Configurazione di un servizio di raccolta directory utente Active Directory (ad)

Workload Security può essere configurato per raccogliere gli attributi utente dai server Active Directory.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore di Data Infrastructure Insights o un proprietario dell'account.
- È necessario disporre dell'indirizzo IP del server che ospita il server Active Directory.
- Prima di configurare un connettore di directory utente, è necessario configurare un agente.

Procedura per la configurazione di un servizio di raccolta directory utente

1. Nel menu protezione del carico di lavoro, fare clic su: **Collector > User Directory Collector > + User Directory Collector** e selezionare **Active Directory**

   Viene visualizzata la schermata Add User Directory (Aggiungi directory utente).

Configurare User Directory Collector inserendo i dati richiesti nelle seguenti tabelle:

Nome	Descrizione
Nome	Nome univoco della directory utente. Ad esempio *GlobalADCollector*
Agente	Selezionare un agente configurato dall'elenco
IP del server/Nome dominio	Indirizzo IP o FQDN (Fully-qualified Domain Name) del server che ospita la directory attiva

Nome foresta	Livello di foresta della struttura di directory. Il nome della foresta consente di utilizzare entrambi i seguenti formati: *X. y.y.z* ⇒ nome di dominio diretto così come lo si dispone sulla SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ nomi distinti relativi [esempio: DC=hq,DC= nomeazienda,DC=com] oppure è possibile specificare quanto segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [per filtrare in base all'ingegneria specifica dell'unità organizzativa] *CN=nome utente,OU=engineering,DC=companyname, DC=netapp, DC=com* [per ottenere solo un utente specifico con <username> da OU <engineering>] *CN=utenti Acrobat,CN=utenti,DC=hq,DC=companyname,DC=co mpanyname,DC=companyname,o=tutti gli utenti attendibili all'interno di quest'organizzazione sono supportati da Acrobat_S=i domini che sono supportati da Microsoft,S=i domini Microsoft,S=IT*.
DN di binding	Utente autorizzato a cercare nella directory. Ad esempio: *username@companyname.com* o *username@domainname.com* inoltre, è richiesta l'autorizzazione di sola lettura del dominio. L'utente deve essere membro del gruppo di protezione *Controller di dominio di sola lettura*.
ASSOCIARE la password	Password del server di directory (ad es. Password per il nome utente utilizzato in Bind DN)
Protocollo	ldap, ldaps, ldap-start-tls
Porte	Selezionare la porta

Se i nomi degli attributi predefiniti sono stati modificati in Active Directory, immettere i seguenti attributi richiesti per il server di directory. Nella maggior parte dei casi, questi nomi di attributi vengono *non* modificati in Active Directory, nel qual caso è possibile semplicemente procedere con il nome dell'attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome visualizzato	nome
SID	objectsid
Nome utente	SAMAccountName

Fare clic su Includi attributi facoltativi per aggiungere uno dei seguenti attributi:

Attributi	Nome attributo in Directory Server
Indirizzo e-mail	mail
Numero di telefono	numero di telefono
Ruolo	titolo

Paese	co
Stato	stato
Reparto	reparto
Foto	thumbnailphoto
ManagerDN	manager
Gruppi	MemberOf

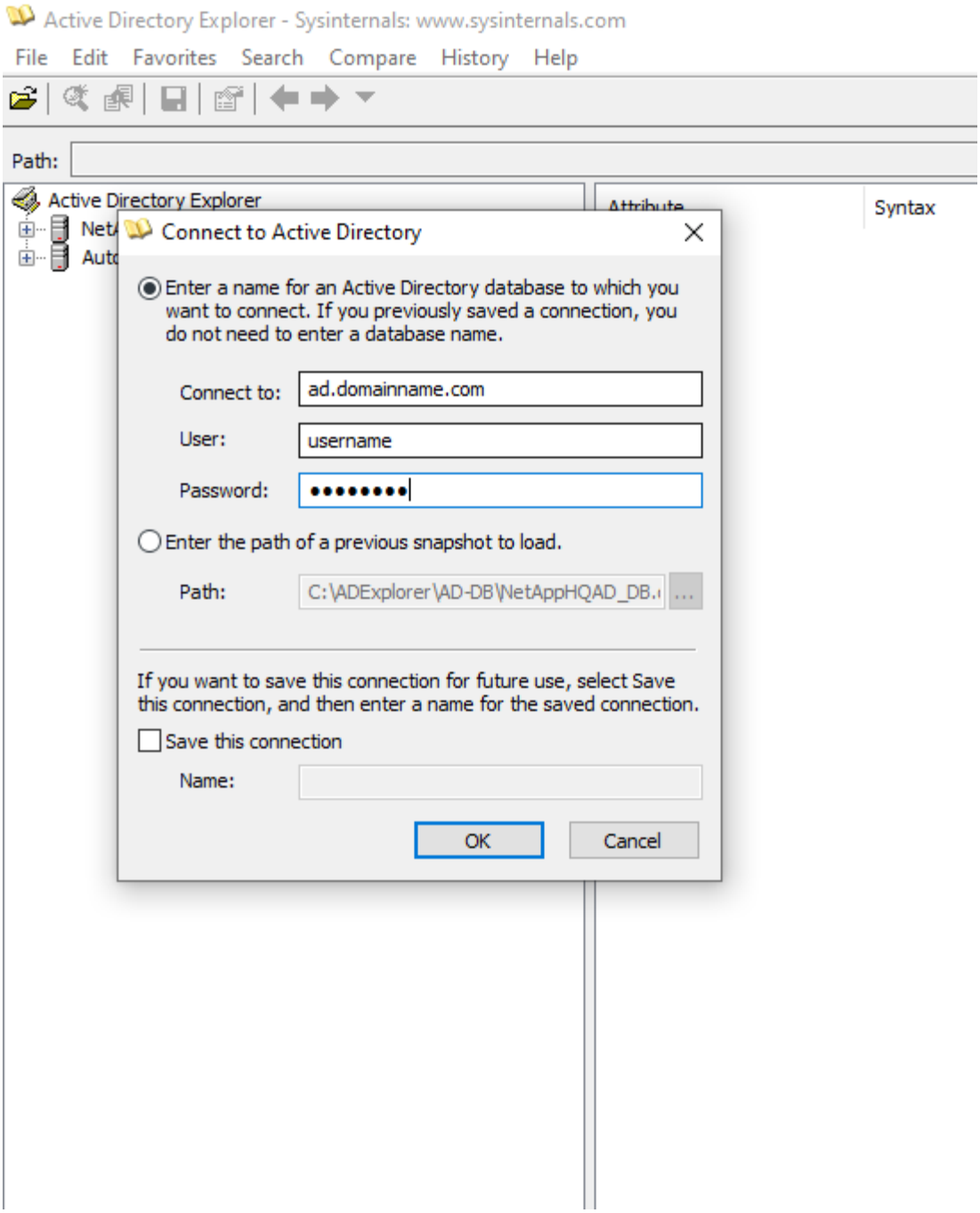
Verifica della configurazione di User Directory Collector

È possibile convalidare le autorizzazioni utente LDAP e le definizioni degli attributi utilizzando le seguenti procedure:

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP per la sicurezza del carico di lavoro:

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Utilizzare ad Explorer per navigare in un database ad, visualizzare le proprietà e gli attributi degli oggetti, visualizzare le autorizzazioni, visualizzare lo schema di un oggetto, eseguire ricerche sofisticate che è possibile salvare ed eseguire nuovamente.
  - Installare "AD Explorer" su qualsiasi computer Windows in grado di connettersi al server ad.
  - Connettersi al server ad utilizzando il nome utente/la password del server di directory ad.



Risoluzione degli errori di configurazione di User Directory Collector

La seguente tabella descrive i problemi noti e le risoluzioni che possono verificarsi durante la configurazione di Collector:

Problema:	Risoluzione:
L'aggiunta di un connettore directory utente determina lo stato 'Error'. Viene visualizzato il messaggio di errore "credenziali non valide fornite per il server LDAP".	Nome utente o password forniti non corretti. Modificare e fornire il nome utente e la password corretti.

Problema:	Risoluzione:
L’aggiunta di un connettore directory utente determina lo stato ‘Error’. L’errore dice: "Impossibile ottenere l’oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome della foresta".	Nome di foresta specificato errato. Modificare e fornire il nome corretto della foresta.
Gli attributi facoltativi dell’utente di dominio non vengono visualizzati nella pagina Profilo utente sicurezza workload.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. Modificare e fornire i nomi degli attributi facoltativi corretti.
Data collector in stato di errore con "Impossibile recuperare utenti LDAP. Motivo dell’errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore facendo clic sul pulsante *Restart*.
L’aggiunta di un connettore directory utente determina lo stato ‘Error’.	Assicurarsi di aver fornito valori validi per i campi obbligatori (Server, nome-foresta, BIND-DN, BIND-Password). Assicurarsi che l’input bind-DN sia sempre fornito come ‘Amministratore@<domain_forest_name>’ o come account utente con privilegi di amministratore di dominio.
L’aggiunta di un connettore directory utente determina lo stato ‘RETENTATIVO'. Mostra l’errore "Impossibile definire lo stato del raccoglitore, motivo comando TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] non riuscito a causa di java.net.ConnectionException:Connection rifiutato."	IP o FQDN non corretti forniti per il server ad. Modificare e fornire l’indirizzo IP o l’FQDN corretto.
L’aggiunta di un connettore directory utente determina lo stato ‘Error’. Viene visualizzato il messaggio di errore "Impossibile stabilire la connessione LDAP".	IP o FQDN non corretti forniti per il server ad. Modificare e fornire l’indirizzo IP o l’FQDN corretto.
L’aggiunta di un connettore directory utente determina lo stato ‘Error’. L’errore indica che non è stato possibile caricare le impostazioni. Motivo: Si è verificato un errore nella configurazione dell’origine dati. Motivo specifico: /Connector/conf/application.conf: 70: ldap.ldap-port ha una STRINGA di tipo piuttosto che UN NUMERO"	Valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server ad.
Ho iniziato con gli attributi obbligatori e ho funzionato. Dopo aver aggiunto i dati facoltativi, i dati degli attributi facoltativi non vengono recuperati da ad.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi opzionali aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. Modificare e fornire il nome dell’attributo obbligatorio o facoltativo corretto.
Dopo aver riavviato il collector, quando avverrà la sincronizzazione ad?	La sincronizzazione AD viene eseguita immediatamente dopo il riavvio del collector. Il recupero dei dati utente di circa 300.000 utenti richiede circa 15 minuti e viene aggiornato automaticamente ogni 12 ore.

Problema:	Risoluzione:
I dati dell'utente vengono sincronizzati da ad a CloudSecure. Quando verranno cancellati i dati?	I dati dell'utente vengono conservati per 13 mesi in caso di mancato aggiornamento. Se il tenant viene cancellato, i dati verranno cancellati.
User Directory Connector si trova nello stato 'Error'. "Connettore in stato di errore. Nome del servizio: UsersLdap. Motivo dell'errore: Impossibile recuperare gli utenti LDAP. Motivo del guasto: 80090308: LdapErr: DSID-0C090453, commento: AcceptSecurityContext error, data 52e, v3839"	Nome di foresta specificato errato. Vedere sopra per informazioni su come fornire il nome corretto della foresta.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Ciò è probabilmente dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare il collettore di Active Directory specifico che sta recuperando le informazioni dell'utente da Active Directory. 2. Si noti che, in base agli attributi facoltativi, è presente un nome di campo "numero telefonico" mappato all'attributo di Active Directory "numero telefonico". 4. Utilizzare lo strumento Active Directory Explorer come descritto in precedenza per sfogliare Active Directory e visualizzare il nome dell'attributo corretto. 3. Assicurarsi che in Active Directory sia presente un attributo denominato 'numero telefonico' che abbia effettivamente il numero di telefono dell'utente. 5. Diciamo che in Active Directory è stato modificato in "numero di telefono". 6. Quindi, modificare il raccoglitore di elenchi di utenti CloudSecure. Nella sezione opzionale degli attributi, sostituire 'Telephonenumber' con 'phonenumber'. 7. Salvare il collettore di Active Directory, il collettore si riavvierà e riceverà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è attivato sul server Active Directory (ad), il servizio di raccolta directory utente di workload Security non può connettersi al server ad.	Disattivare la crittografia ad Server prima di configurare un User Directory Collector. Una volta recuperato il dettaglio dell'utente, questo sarà disponibile per 13 mesi. Se il server ad si disconnette dopo aver recuperato i dettagli dell'utente, i nuovi utenti aggiunti in ad non verranno recuperati. Per recuperare di nuovo, è necessario connettere ad ad il raccoglitore di directory dell'utente.
I dati di Active Directory sono presenti in CloudInsights Security. Eliminare tutte le informazioni utente da CloudInsights.	Non è possibile eliminare SOLO le informazioni utente di Active Directory da CloudInsights Security. Per eliminare l'utente, è necessario eliminare l'intero tenant.

Configurazione di un servizio di raccolta LDAP Directory Server

È possibile configurare la sicurezza del carico di lavoro per raccogliere gli attributi utente dai server di directory LDAP.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore di Data Infrastructure Insights o un proprietario dell'account.
- È necessario disporre dell'indirizzo IP del server che ospita il server di directory LDAP.
- Prima di configurare un connettore di directory LDAP, è necessario configurare un agente.

Procedura per la configurazione di un servizio di raccolta directory utente

1. Nel menu protezione del carico di lavoro, fare clic su: **Collector > User Directory Collector > + User Directory Collector** e selezionare **LDAP Directory Server**

   Viene visualizzata la schermata Add User Directory (Aggiungi directory utente).

Configurare User Directory Collector inserendo i dati richiesti nelle seguenti tabelle:

Nome	Descrizione
Nome	Nome univoco della directory utente. Ad esempio *GlobalLDAPCollector*
Agente	Selezionare un agente configurato dall'elenco
IP del server/Nome dominio	Indirizzo IP o FQDN (Fully-qualified Domain Name) del server che ospita il server di directory LDAP
Base di ricerca	Search base (base di ricerca) del server LDAP Search base (base di ricerca) consente di utilizzare entrambi i seguenti formati: *X. y.y.z* ⇒ nome di dominio diretto, così come lo si dispone sulla SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ nomi distinti relativi [esempio: DC=hq,DC= nomeazienda,DC=com] oppure è possibile specificare quanto segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [to filtering by specific ou engineering] *CN=Username,OU=engineering,DC=companyname, DC=netapp, DC=com* [to get only specific user with <username> from OU <engineering>] _CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com panyname,DC=com,o=companyname of the U.S.
DN di binding	Utente autorizzato a cercare nella directory. Ad esempio: uid=ldapuser,cn=users,cn=accounts,DC=domain,DC= companyname,DC=com uid=john,cn=users,cn=accounts,DC=dorp,DC=Compa ny,DC=com per un utente john@dorp.company.com. dorp.company.com
--account	--utenti
--giovanni	--anna
ASSOCIARE la password	Password del server di directory (ad es. Password per il nome utente utilizzato in Bind DN)
Protocollo	ldap, ldaps, ldap-start-tls

Porte	Selezionare la porta

Se i nomi degli attributi predefiniti sono stati modificati in LDAP Directory Server, immettere i seguenti attributi richiesti per Directory Server. Nella maggior parte dei casi, questi nomi di attributi vengono *non* modificati in LDAP Directory Server, nel qual caso è possibile semplicemente procedere con il nome di attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome visualizzato	nome
UNIXID	uidnumber
Nome utente	uid

Fare clic su Includi attributi facoltativi per aggiungere uno dei seguenti attributi:

Attributi	Nome attributo in Directory Server
Indirizzo e-mail	mail
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato
Reparto	numero di parte
Foto	foto
ManagerDN	manager
Gruppi	MemberOf

Verifica della configurazione di User Directory Collector

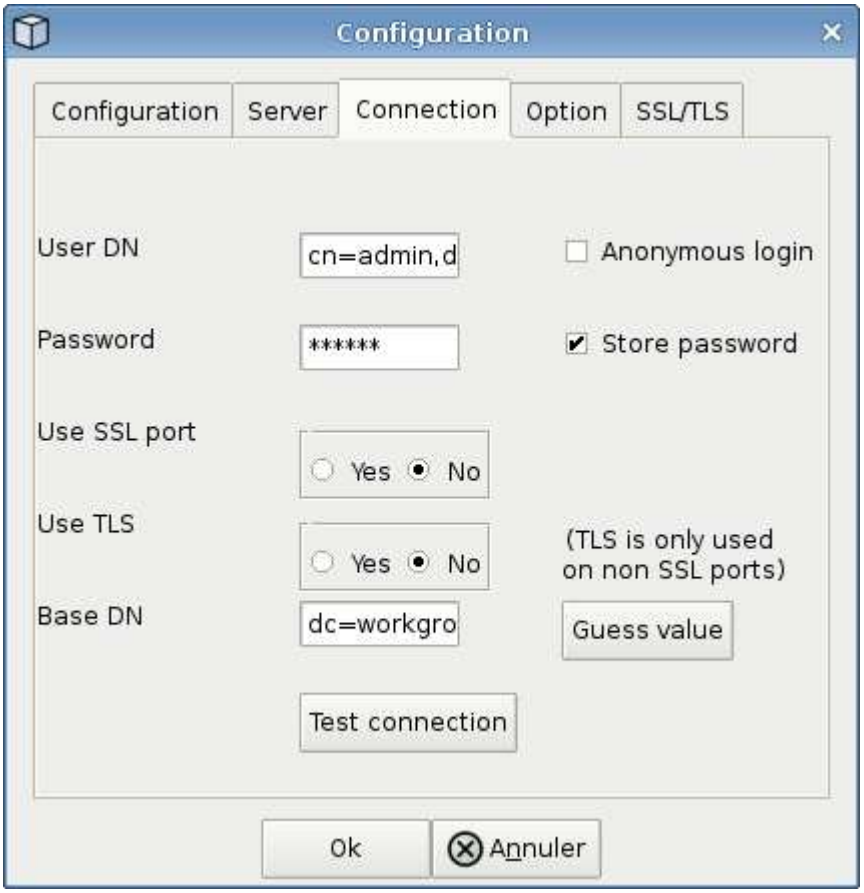
È possibile convalidare le autorizzazioni utente LDAP e le definizioni degli attributi utilizzando le seguenti procedure:

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP per la sicurezza del carico di lavoro:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilizzare LDAP Explorer per navigare in un database LDAP,
visualizzare le proprietà e gli attributi degli oggetti, visualizzare le
autorizzazioni, visualizzare lo schema di un oggetto, eseguire ricerche
sofisticate che è possibile salvare ed eseguire nuovamente.
```

  - Installare LDAP Explorer (http://ldaptool.sourceforge.net/) o Java LDAP Explorer) (http://jxplorer.org/su qualsiasi computer Windows in grado di connettersi al server LDAP.

- Connettersi al server LDAP utilizzando il nome utente/la password del server di directory LDAP.



Risoluzione degli errori di configurazione di LDAP Directory Collector

La seguente tabella descrive i problemi noti e le risoluzioni che possono verificarsi durante la configurazione di Collector:

Problema:	Risoluzione:
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. Viene visualizzato il messaggio di errore "credenziali non valide fornite per il server LDAP".	DN di binding o password di binding o base di ricerca forniti non corretti. Modificare e fornire le informazioni corrette.
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. L'errore dice: "Impossibile ottenere l'oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome della foresta".	Base di ricerca fornita errata. Modificare e fornire il nome corretto della foresta.
Gli attributi facoltativi dell'utente di dominio non vengono visualizzati nella pagina Profilo utente sicurezza workload.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. I campi distinguono tra maiuscole e minuscole. Modificare e fornire i nomi degli attributi facoltativi corretti.

Problema:	Risoluzione:
Data collector in stato di errore con "Impossibile recuperare utenti LDAP. Motivo dell'errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore facendo clic sul pulsante *Restart*.
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'.	Assicurarsi di aver fornito valori validi per i campi obbligatori (Server, nome-foresta, BIND-DN, BIND-Password). Assicurarsi che l'input bind-DN sia sempre fornito come uid=ldapuser,cn=users,cn=accounts,DC=domain,DC=companyname,DC=com.
L'aggiunta di un connettore di directory LDAP determina lo stato 'RETENTATIVO'. Mostra l'errore "Impossibile determinare lo stato del raccoglitore e riprovare"	Assicurarsi che siano forniti l'IP del server e la base di ricerca corretti ////
Durante l'aggiunta della directory LDAP viene visualizzato il seguente messaggio di errore: "Impossibile determinare lo stato del raccoglitore entro 2 tentativi, riavviare nuovamente il raccoglitore (codice errore: AGENT008)"	Verificare che siano forniti l'indirizzo IP del server e la base di ricerca corretti
L'aggiunta di un connettore di directory LDAP determina lo stato 'RETENTATIVO'. Mostra l'errore "Impossibile definire lo stato del raccoglitore, motivo comando TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] non riuscito a causa di java.net.ConnectionException:Connection rifiutato."	IP o FQDN non corretti forniti per il server ad. Modificare e fornire l'indirizzo IP o l'FQDN corretto. ////
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. Viene visualizzato il messaggio di errore "Impossibile stabilire la connessione LDAP".	Indirizzo IP o FQDN errato fornito per il server LDAP. Modificare e fornire l'indirizzo IP o l'FQDN corretto. O valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server LDAP.
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. L'errore indica che non è stato possibile caricare le impostazioni. Motivo: Si è verificato un errore nella configurazione dell'origine dati. Motivo specifico: /Connector/conf/application.conf: 70: ldap.ldap-port ha una STRINGA di tipo piuttosto che UN NUMERO"	Valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server ad.
Ho iniziato con gli attributi obbligatori e ho funzionato. Dopo aver aggiunto i dati facoltativi, i dati degli attributi facoltativi non vengono recuperati da ad.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi opzionali aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. Modificare e fornire il nome dell'attributo obbligatorio o facoltativo corretto.

Problema:	Risoluzione:
Dopo aver riavviato il collector, quando avverrà la sincronizzazione LDAP?	La sincronizzazione LDAP viene eseguita immediatamente dopo il riavvio del collector. Il recupero dei dati utente di circa 300.000 utenti richiede circa 15 minuti e viene aggiornato automaticamente ogni 12 ore.
I dati dell'utente vengono sincronizzati da LDAP a CloudSecure. Quando verranno cancellati i dati?	I dati dell'utente vengono conservati per 13 mesi in caso di mancato aggiornamento. Se il tenant viene cancellato, i dati verranno cancellati.
LDAP Directory Connector si trova nello stato 'Error'. "Connettore in stato di errore. Nome del servizio: UsersLdap. Motivo dell'errore: Impossibile recuperare gli utenti LDAP. Motivo del guasto: 80090308: LdapErr: DSID-0C090453, commento: AcceptSecurityContext error, data 52e, v3839"	Nome di foresta specificato errato. Vedere sopra per informazioni su come fornire il nome corretto della foresta.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Ciò è probabilmente dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare il collettore di Active Directory specifico che sta recuperando le informazioni dell'utente da Active Directory. 2. Si noti che, in base agli attributi facoltativi, è presente un nome di campo "numero telefonico" mappato all'attributo di Active Directory "numero telefonico". 4. Utilizzare lo strumento Active Directory Explorer come descritto in precedenza per cercare il server LDAP Directory e visualizzare il nome dell'attributo corretto. 3. Assicurarsi che nella rubrica LDAP sia presente un attributo denominato 'numero telefonico' che abbia effettivamente il numero di telefono dell'utente. 5. Diciamo che in LDAP Directory è stato modificato in 'numero telefonico'. 6. Quindi, modificare il raccoglitore di elenchi di utenti CloudSecure. Nella sezione opzionale degli attributi, sostituire 'Telephonenumber' con 'phonenumber'. 7. Salvare il collettore di Active Directory, il collettore si riavvierà e riceverà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è attivato sul server Active Directory (ad), il servizio di raccolta directory utente di workload Security non può connettersi al server ad.	Disattivare la crittografia ad Server prima di configurare un User Directory Collector. Una volta recuperato il dettaglio dell'utente, questo sarà disponibile per 13 mesi. Se il server ad si disconnette dopo aver recuperato i dettagli dell'utente, i nuovi utenti aggiunti in ad non verranno recuperati. Per recuperare di nuovo, è necessario connettere ad ad ad il raccoglitore di directory dell'utente.

Configurazione del Data Collector SVM di ONTAP

Workload Security utilizza i data colleator per raccogliere i dati di accesso ai file e agli utenti dai dispositivi.

Prima di iniziare

- Questo data collector è supportato con i seguenti elementi:
  - Data ONTAP 9.2 e versioni successive. Per prestazioni ottimali, utilizzare una versione Data ONTAP superiore a 9.13.1.
  - Protocollo SMB versione 3.1 e precedenti.
  - Versioni di NFS fino a NFS 4,1 con ONTAP 9.15.1 o versioni successive comprese.
  - FlexGroup è supportato da ONTAP 9.4 e versioni successive
  - ONTAP Select è supportato
- Sono supportati solo i tipi di dati SVM. Le SVM con volumi infiniti non sono supportate.
- SVM ha diversi sottotipi. Di questi, sono supportati solo *default*, *Sync_source* e *Sync_destination*.
- Un agente "deve essere configurato" prima di poter configurare i data collector.
- Assicurarsi di disporre di un connettore User Directory configurato correttamente, altrimenti gli eventi mostreranno i nomi utente codificati e non il nome effettivo dell'utente (come memorizzato in Active Directory) nella pagina "Activity Forensics" (analisi delle attività).
- • ONTAP Persistent Store è supportato da 9.14.1.
- Per ottenere prestazioni ottimali, è necessario configurare il server FPolicy in modo che si trova sulla stessa subnet del sistema di storage.
- È necessario aggiungere una SVM utilizzando uno dei due metodi seguenti:
  - Utilizzando l'IP del cluster, il nome SVM e il nome utente e la password di gestione del cluster. ***questo è il metodo consigliato.***
    - Il nome SVM deve essere identico a quello mostrato in ONTAP ed è sensibile al maiuscolo/minuscolo.
  - Utilizzando SVM Vserver Management IP, Username e Password
  - Se non si è in grado o non si è disposti a utilizzare l'intero nome utente e la password di gestione del cluster/SVM dell'amministratore, è possibile creare un utente personalizzato con Privileges di minore entità, come indicato nella "Nota sulle autorizzazioni"sezione seguente. Questo utente personalizzato può essere creato per l'accesso a SVM o Cluster.
    - o è anche possibile utilizzare un utente ad con un ruolo che disponga almeno delle autorizzazioni di csrole, come indicato nella sezione "A note about permissions" (Nota sulle autorizzazioni) riportata di seguito. Fare riferimento anche alla "Documentazione ONTAP".
- Assicurarsi che siano impostate le applicazioni corrette per SVM eseguendo il seguente comando:

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

Output di esempio:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------  ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Assicurati che l'SVM disponga di un server CIFS configurato: Clustershell:> `vserver cifs show`

  Il sistema restituisce il nome del server Vserver, il nome del server CIFS e i campi aggiuntivi.

- Impostare una password per l'utente vsadmin di SVM. Se si utilizza un utente personalizzato o un utente amministratore del cluster, ignorare questo passaggio. Clustershell:> `security login password -username vsadmin -vserver svmname`
- Sbloccare l'utente vsadmin di SVM per l'accesso esterno. Se si utilizza un utente personalizzato o un utente amministratore del cluster, ignorare questo passaggio. Clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Assicurarsi che la policy firewall della LIF dati sia impostata su 'mgmt' (non su 'dATA'). Saltare questo passaggio se si utilizza un lif di gestione dedicato per aggiungere la SVM. Clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Quando un firewall è attivato, è necessario definire un'eccezione per consentire il traffico TCP per la porta che utilizza il servizio di raccolta dati Data ONTAP.

  Vedere "Requisiti dell'agente" per informazioni sulla configurazione. Ciò vale per gli agenti e gli agenti on-premise installati nel cloud.

- Quando un agente viene installato in un'istanza di AWS EC2 per monitorare una SVM Cloud ONTAP, l'agente e lo storage devono trovarsi nello stesso VPC. Se si trovano in VPC separati, deve esserci un percorso valido tra i VPC.

Prerequisiti per il blocco dell'accesso utente

Tenere presente quanto segue per "Blocco degli accessi degli utenti":

Per il funzionamento di questa funzionalità sono necessarie credenziali a livello di cluster.

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni a workload Security per bloccare l'utente.

Per gli utenti csuser con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Nota sulle autorizzazioni

Autorizzazioni per l'aggiunta tramite Cluster Management IP:

Se non è possibile utilizzare l'utente amministratore della gestione del cluster per consentire a workload Security di accedere al data collector SVM di ONTAP, è possibile creare un nuovo utente denominato "csuser" con i ruoli indicati nei comandi seguenti. Utilizzare il nome utente "csuser" e la password per "csuser" quando si configura il data collector di workload Security per l'utilizzo di Cluster Management IP.

Per creare il nuovo utente, accedere a ONTAP con il nome utente/password dell'amministratore della gestione del cluster ed eseguire i seguenti comandi sul server ONTAP:

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Autorizzazioni per l'aggiunta tramite Vserver Management IP:

Se non è possibile utilizzare l'utente amministratore della gestione del cluster per consentire a workload Security di accedere al data collector SVM di ONTAP, è possibile creare un nuovo utente denominato "csuser" con i ruoli indicati nei comandi seguenti. Utilizzare il nome utente "csuser" e la password per "csuser" quando si configura il data collector di workload Security per utilizzare Vserver Management IP.

Per creare il nuovo utente, accedere a ONTAP con il nome utente/password dell'amministratore della gestione del cluster ed eseguire i seguenti comandi sul server ONTAP. Per semplicità, copiare questi comandi in un editor di testo e sostituire <vservername> con il nome del server virtuale prima di eseguire questi comandi su ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole -vserver <vservername>
```

Modalità Protobuf

Workload Security configurerà il motore FPolicy in modalità protobuf quando questa opzione è attivata nelle impostazioni *Advanced Configuration* del Collector. La modalità Protobuf è supportata in ONTAP versione 9,15 e successive.

Ulteriori dettagli su questa funzione sono disponibili nella "Documentazione ONTAP".

Sono necessarie autorizzazioni specifiche per il protobuf (alcune o tutte queste possono già esistere):

Modalità cluster:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Modalità Vserver:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Autorizzazioni per la protezione autonoma da ransomware ONTAP e accesso ONTAP negato

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni alla sicurezza del carico di lavoro per raccogliere informazioni relative all'ARP da ONTAP.

Per ulteriori informazioni, consultare la sezione "Integrazione con accesso ONTAP negato"

1. "Integrazione con la protezione ransomware autonoma di ONTAP"

Configurare il data collector

Procedura per la configurazione

1. Accedere come Amministratore o Proprietario dell'account al proprio ambiente Data Infrastructure Insights.
2. Fare clic su **sicurezza del carico di lavoro > Collector > +Data Collector**

   Il sistema visualizza i Data Collector disponibili.

3. Passare il mouse sul riquadro **NetApp SVM e fare clic su *+Monitor**.

   Viene visualizzata la pagina di configurazione SVM di ONTAP. Inserire i dati richiesti per ciascun campo.

Campo	Descrizione

Nome	Nome univoco del Data Collector
Agente	Selezionare un agente configurato dall'elenco.
Connessione tramite IP di gestione per:	Selezionare Cluster IP (IP cluster) o SVM Management IP (IP gestione SVM)
Cluster / SVM Management IP Address (Indirizzo IP gestione cluster/SVM)	L'indirizzo IP del cluster o della SVM, a seconda della selezione effettuata in precedenza.
Nome SVM	Il nome della SVM (questo campo è obbligatorio quando ci si connette tramite l'IP del cluster)
Nome utente	Nome utente per accedere a SVM/Cluster quando si aggiunge tramite l'IP del cluster, le opzioni sono: 1. Cluster-admin 2. 'csuser' 3. AD-user che ha un ruolo simile a csuser. Quando si aggiunge tramite IP SVM, le opzioni sono: 4. Vsadmin 5. 'csuser' 6. NOME utente AD con ruolo simile a csuser.
Password	Password per il nome utente sopra indicato
Filtra condivisioni/volumi	Scegliere se includere o escludere condivisioni/volumi dalla raccolta eventi
Inserire i nomi di condivisione completi da escludere/includere	Elenco di condivisioni separate da virgole da escludere o includere (a seconda dei casi) dalla raccolta di eventi
Inserire i nomi completi dei volumi da escludere/includere	Elenco separato da virgole di volumi da escludere o includere (a seconda dei casi) dalla raccolta di eventi
Monitorare l'accesso alle cartelle	Se selezionata, questa opzione attiva gli eventi per il monitoraggio dell'accesso alle cartelle. Tenere presente che la creazione/ridenominazione e l'eliminazione delle cartelle verranno monitorate anche senza selezionare questa opzione. L'attivazione di questa opzione aumenta il numero di eventi monitorati.
Impostare la dimensione del buffer di invio ONTAP	Imposta la dimensione del buffer di invio ONTAP Fpolicy. Se si utilizza una versione di ONTAP precedente a 9.8p7 e si verifica un problema di prestazioni, è possibile modificare le dimensioni del buffer di invio ONTAP per migliorare le prestazioni di ONTAP. Contatta il supporto NetApp se non vedi questa opzione e desideri esplorarla.

Al termine

- Nella pagina dei Data Collector installati, utilizzare il menu delle opzioni a destra di ciascun collector per modificare il data collector. È possibile riavviare il data collector o modificare gli attributi di configurazione del data collector.

Configurazione consigliata per MetroCluster

Per MetroCluster si consiglia quanto segue:

1. Collegare due data collettori, uno alla SVM di origine e l'altro alla SVM di destinazione.

2. I data collezioner devono essere collegati da *Cluster IP*.
3. In qualsiasi momento, un data collector dovrebbe essere in esecuzione, un altro potrebbe essere in errore.

   L'attuale data collector SVM 'in esecuzione' viene visualizzato come *in esecuzione*. L'attuale data collector SVM 'sin cima' viene visualizzato come *Error*.

4. Ogni volta che si verifica uno switchover, lo stato del data collector passa da 'in esecuzione' a 'errore' e viceversa.
5. Il data collector richiede fino a due minuti per passare dallo stato di errore allo stato di esecuzione.

Policy di servizio

Se si utilizza la politica di servizio con ONTAP **versione 9.9.1 o successiva**, per connettersi al Data Source Collector, è necessario il servizio *data-fpolicy-client* insieme al servizio dati *data-nfs* e/o *data-cifs*.

Esempio:

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

Nelle versioni di ONTAP precedenti alla 9.9 non è necessario impostare *data-fpolicy-client*.

Riproduci-Pausa Data Collector

2 nuove operazioni sono ora visualizzate sul menu kebab del raccoglitore (PAUSA e RIPRESA).

Se Data Collector è in stato *running*, è possibile sospendere la raccolta. Aprire il menu "tre punti" per il raccoglitore e selezionare PAUSA. Mentre il raccoglitore è in pausa, non vengono raccolti dati da ONTAP e non vengono inviati dati dal raccoglitore a ONTAP. Ciò significa che non verranno trasmessi eventi Fpolicy da ONTAP al data collector e da lì a Data Infrastructure Insights.

Tenere presente che se in ONTAP vengono creati nuovi volumi e così via mentre il collector è in pausa, workload Security non raccoglierà i dati e quei volumi, ecc. non verranno riflessi in dashboard o tabelle.

Tenere presente quanto segue:

- L'eliminazione degli snapshot non avviene in base alle impostazioni configurate su un raccoglitore in pausa.
- Gli eventi EMS (come ONTAP ARP) non verranno elaborati su un raccoglitore in pausa. Ciò significa che se ONTAP identifica un attacco ransomware, la sicurezza dei workload di Data Infrastructure Insights non sarà in grado di acquisire quell'evento.
- Le e-mail di notifica dello stato NON verranno inviate per un raccoglitore in pausa.
- Le azioni manuali o automatiche (come Snapshot o blocco utente) non sono supportate in un raccoglitore in pausa.
- In caso di aggiornamenti dell'agente o del raccoglitore, di riavvio/riavvio della VM dell'agente o di riavvio del servizio dell'agente, un raccoglitore in pausa rimarrà nello stato *Paused*.
- Se il data collector si trova nello stato *Error*, il collector non può essere modificato nello stato *Paused*. Il

pulsante Pausa viene attivato solo se lo stato del raccoglitore è *in esecuzione*.

- Se l'agente è disconnesso, non è possibile modificare lo stato del collettore in *Paused*. Il raccoglitore passerà allo stato *Stopped* e il pulsante Pausa verrà disattivato.

Memorizzazione persistente

L'archivio persistente è supportato con ONTAP 9.14.1 e versioni successive. Le istruzioni relative al nome del volume variano da ONTAP 9,14 a 9,15.

È possibile attivare Archivio persistente selezionando la casella di controllo nella pagina di modifica/aggiunta del raccoglitore. Dopo aver selezionato la casella di controllo, viene visualizzato un campo di testo per accettare il nome del volume. Il nome del volume è un campo obbligatorio per l'abilitazione dell'archivio permanente.

- Per ONTAP 9.14.1, è necessario creare il volume prima di attivare la funzione e specificare lo stesso nome nel campo *Nome volume*. La dimensione del volume consigliata è 16GB.
- Per ONTAP 9.15.1, il volume viene creato automaticamente con dimensioni 16GB dal raccoglitore, utilizzando il nome fornito nel campo *Nome volume*.

Sono necessarie autorizzazioni specifiche per l'archivio permanente (alcune o tutte queste possono già esistere):

Modalità cluster:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

Modalità Vserver:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

Risoluzione dei problemi

Vedere la "Risoluzione dei problemi di SVM Collector" pagina per suggerimenti sulla risoluzione dei problemi.

Configurazione di Cloud Volumes ONTAP e Amazon FSX per NetApp ONTAP Collector

Workload Security utilizza i data colleator per raccogliere i dati di accesso ai file e agli utenti dai dispositivi.

Configurazione dello storage Cloud Volumes ONTAP

Consulta la documentazione di OnCommand Cloud Volumes ONTAP per configurare un'istanza AWS con nodo singolo/ha per l'hosting dell'agente di sicurezza dei workload: https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

Una volta completata la configurazione, segui la procedura per configurare la tua SVM: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html

Piattaforme supportate

- Cloud Volumes ONTAP, supportato in tutti i provider di servizi cloud disponibili, ovunque sia disponibile. Ad esempio: Amazon, Azure, Google Cloud.
- ONTAP, Amazon FSX

Configurazione del computer dell'agente

Il computer dell'agente deve essere configurato nelle rispettive subnet dei provider di servizi cloud. Per ulteriori informazioni sull'accesso alla rete, consultare [requisiti dell'agente].

Di seguito sono riportati i passaggi per l'installazione dell'agente in AWS. Per l'installazione, è possibile seguire procedure equivalenti, applicabili al provider di servizi cloud, in Azure o Google Cloud.

In AWS, attenersi alla seguente procedura per configurare il computer in modo che venga utilizzato come agente di sicurezza del carico di lavoro:

Per configurare il computer in modo che venga utilizzato come agente di sicurezza del carico di lavoro, procedere come segue:

Fasi

1. Accedere alla console AWS, accedere alla pagina EC2-Instances e selezionare *Launch instance*.
2. Selezionare un RHEL o CentOS AMI con la versione appropriata, come indicato in questa pagina: https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html
3. Selezionare il VPC e la subnet in cui risiede l'istanza di Cloud ONTAP.
4. Selezionare *t2.xlarge* (4 vcpus e 16 GB di RAM) come risorse allocate.
    a. Creare l'istanza EC2.
5. Installare i pacchetti Linux richiesti utilizzando il gestore dei pacchetti YUM:
    a. Installare *wget* e *unzip* pacchetti Linux nativi.

Installare Workload Security Agent

1. Accedere come Amministratore o Proprietario dell'account al proprio ambiente Data Infrastructure Insights.
2. Accedere a sicurezza del carico di lavoro **Collectors** e fare clic sulla scheda **Agenti**.
3. Fare clic su **+Agent** e specificare RHEL come piattaforma di destinazione.
4. Copiare il comando Installazione agente.
5. Incollare il comando Installazione agente nell'istanza RHEL EC2 a cui si è connessi. In questo modo viene installato l'agente workload Security, a condizione che vengano soddisfatti tutti i "Prerequisiti dell'agente"criteri.

Per la procedura dettagliata, fare riferimento a questo collegamento: https://docs.NetApp.com/us-en/

cloudinsights/task_cs_add_Agent.html#steps-to-install-Agent

Risoluzione dei problemi

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

Problema	Risoluzione
"Sicurezza del carico di lavoro: Impossibile determinare il tipo di ONTAP per il data collector Amazon FxSN" viene visualizzato dal Data Collector." Il cliente non riesce ad aggiungere il nuovo data collector Amazon FSxN in workload Security. La connessione al cluster FSxN sulla porta 443 dell'agente è in timeout. I gruppi di protezione firewall e AWS dispongono delle regole necessarie per consentire la comunicazione. Un agente è già implementato e si trova nello stesso account AWS. Lo stesso agente viene utilizzato per connettere e monitorare i dispositivi NetApp rimanenti (e tutti funzionano).	Risolvere questo problema aggiungendo il segmento di rete LIF fsxadmin alla regola di sicurezza dell'agente. Permesso a tutte le porte se non si è sicuri delle porte.

Gestione utenti

Gli account utente di sicurezza del carico di lavoro vengono gestiti tramite Data Infrastructure Insights.

Data Infrastructure Insights fornisce quattro livelli di account utente: Proprietario dell'account, amministratore, utente e ospite. A ciascun account vengono assegnati livelli di autorizzazione specifici. Un account utente con privilegi di amministratore può creare o modificare gli utenti e assegnare a ciascun utente uno dei seguenti ruoli di workload Security:

Ruolo	Accesso alla sicurezza del carico di lavoro
Amministratore	È in grado di eseguire tutte le funzioni di workload Security, incluse quelle per Avvisi, analisi, raccolta dati, policy di risposta automatizzate e API per workload Security. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di sicurezza del carico di lavoro.
Utente	Consente di visualizzare e gestire gli avvisi e visualizzare le analisi. Il ruolo dell'utente può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente e limitare l'accesso dell'utente.
Ospite	Consente di visualizzare avvisi e analisi. Il ruolo ospite non può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente o limitare l'accesso dell'utente.

Fasi

1. Accedere a workload Security

2. Nel menu, fare clic su **Admin > User Management**

   Verrai inoltrato alla pagina Gestione utenti di Data Infrastructure Insights.

3. Selezionare il ruolo desiderato per ciascun utente.

Durante l'aggiunta di un nuovo utente, è sufficiente selezionare il ruolo desiderato (di solito utente o ospite).

Ulteriori informazioni sugli account utente e sui ruoli sono disponibili nella documentazione di Data Infrastructure Insights"Ruolo dell'utente".

SVM Event Rate Checker (Guida al dimensionamento dell'agente)

La funzione di verifica del tasso di eventi viene utilizzata per controllare la velocità di eventi combinata NFS/SMB nella SVM prima di installare un data collector SVM ONTAP, per verificare il numero di macchine SVM che un agente è in grado di monitorare. Utilizza Event Rate Checker come guida al dimensionamento per pianificare il tuo ambiente di sicurezza.

Un agente può supportare fino a un massimo di 50 raccoglitori di dati.

Requisiti:

- IP cluster
- Nome utente e password dell'amministratore del cluster

> Durante l'esecuzione di questo script, non deve essere eseguito alcun Data Collector SVM ONTAP per la SVM per la quale viene determinata la frequenza degli eventi.

Fasi:

1. Installare l'Agent seguendo le istruzioni in CloudSecure.
2. Una volta installato l'agente, eseguire lo script *server_data_rate_checker.sh* come utente sudo:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Questo script richiede l'installazione di _sshpass_ nella macchina
linux. Esistono due modi per installarlo:
```

   a. Eseguire il seguente comando:

```
 linux_prompt> yum install sshpass
.. Se questo non funziona, scaricare _sshpass_ sulla macchina linux
dal web ed eseguire il seguente comando:
```

```
linux_prompt> rpm -i sshpass
```

3. Fornire i valori corretti quando richiesto. Per un esempio, vedere di seguito.
4. L'esecuzione dello script richiede circa 5 minuti.
5. Al termine dell'esecuzione, lo script stampa la frequenza degli eventi dalla SVM. È possibile controllare il tasso di eventi per SVM nell'output della console:

```
"Svm svm_rate is generating 100 events/sec".
```

Ciascun Data Collector SVM di ONTAP può essere associato a una singola SVM, il che significa che ciascun data collector potrà ricevere il numero di eventi generati da una singola SVM.

Tenere presente quanto segue:

A) utilizzare questa tabella come guida generale al dimensionamento. È possibile aumentare il numero di core e/o memoria per aumentare il numero di data collector supportati, fino a un massimo di 50 data collector:

Configurazione del computer dell'agente	Numero di Data Collector SVM	Tasso massimo di eventi che il computer dell'agente può gestire
4 core, 16 GB	10 raccolta di dati	20.000 eventi/sec
4 core, 32 GB	20 raccolta di dati	20.000 eventi/sec

B) per calcolare il totale degli eventi, aggiungere gli eventi generati per tutte le SVM per quell'agente.

C) se lo script non viene eseguito durante le ore di punta o se il traffico di picco è difficile da prevedere, mantenere un buffer del tasso di eventi del 30%.

B + C deve essere inferiore A A, altrimenti il computer dell'agente non potrà eseguire il monitoraggio.

In altre parole, il numero di raccolta dati che è possibile aggiungere a una macchina a singolo agente deve essere conforme alla formula seguente:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Consultare la
xref:{relative_path}concept_cs_agent_requirements.html["Requisiti
dell'agente"] pagina per ulteriori prerequisiti e requisiti.
```

Esempio

Diciamo che abbiamo tre SVM che generano percentuali di eventi rispettivamente di 100, 200 e 300 eventi al secondo.

Applichiamo la formula:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

L'output della console è disponibile nella macchina Agente nel nome del file *fpolicy_stat_<SVM Name>.log* nella directory di lavoro corrente.

Lo script può fornire risultati errati nei seguenti casi:

- Vengono fornite credenziali, IP o nome SVM errati.
- Un fpolicy già esistente con lo stesso nome, numero di sequenza, ecc. genera un errore.
- Lo script viene arrestato bruscamente durante l'esecuzione.

Di seguito è riportato un esempio di esecuzione di script:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

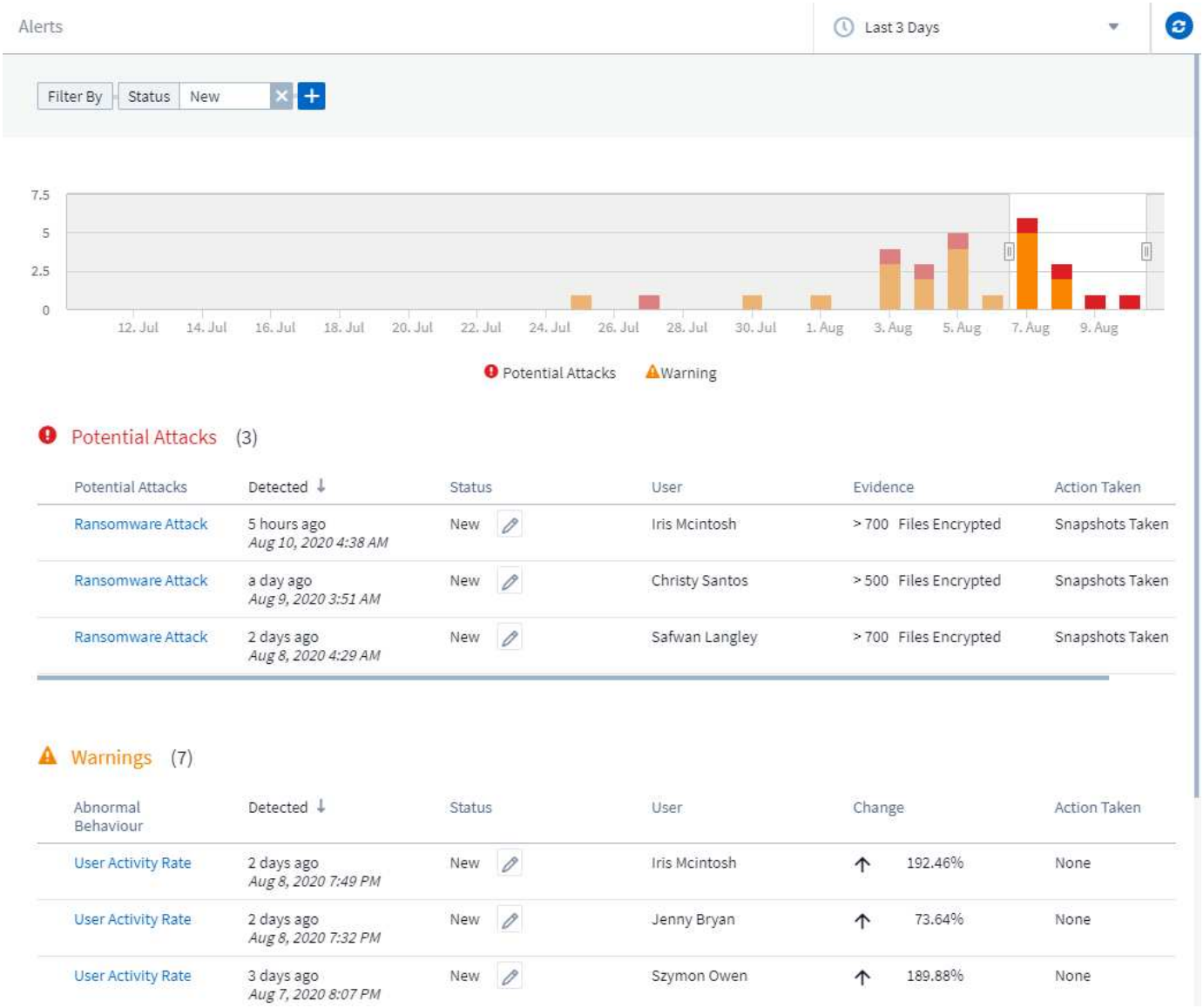
```
[root@ci-cs-data agent]#
```

Risoluzione dei problemi

Domanda	Risposta
Se si esegue questo script su una SVM già configurata per la sicurezza del carico di lavoro, viene utilizzata solo la configurazione fpolicy esistente sulla SVM oppure viene impostata una configurazione temporanea ed è possibile eseguire il processo?	La funzione Event Rate Checker può essere eseguita correttamente anche per una SVM già configurata per la sicurezza del carico di lavoro. Non dovrebbe esserci alcun impatto.
È possibile aumentare il numero di SVM su cui è possibile eseguire lo script?	Sì. È sufficiente modificare lo script e modificare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se si aumenta il numero di SVM, si aumenterà il tempo di esecuzione dello script?	No. Lo script viene eseguito per un massimo di 5 minuti, anche in caso di aumento del numero di SVM.
È possibile aumentare il numero di SVM su cui è possibile eseguire lo script?	Sì. È necessario modificare lo script e modificare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se si aumenta il numero di SVM, si aumenterà il tempo di esecuzione dello script?	No. Lo script viene eseguito per un massimo di 5mins TB, anche in caso di aumento del numero di SVM.
Cosa succede se si esegue Event Rate Checker con un agente esistente?	L'esecuzione di Event Rate Checker con un agente già esistente può causare un aumento della latenza sulla SVM. Questo aumento sarà temporaneo durante l'esecuzione di Event Rate Checker.

Avvisi

La pagina Workload Security Alerts (Avvisi di sicurezza del carico di lavoro) mostra una tempistica degli attacchi e/o degli avvisi recenti e consente di visualizzare i dettagli relativi a ciascun problema.



Avviso

L'elenco degli avvisi visualizza un grafico che mostra il numero totale di potenziali attacchi e/o avvisi che sono stati generati nell'intervallo di tempo selezionato, seguito da un elenco degli attacchi e/o avvisi che si sono verificati in quell'intervallo di tempo. È possibile modificare l'intervallo di tempo regolando i cursori ora di inizio e ora di fine nel grafico.

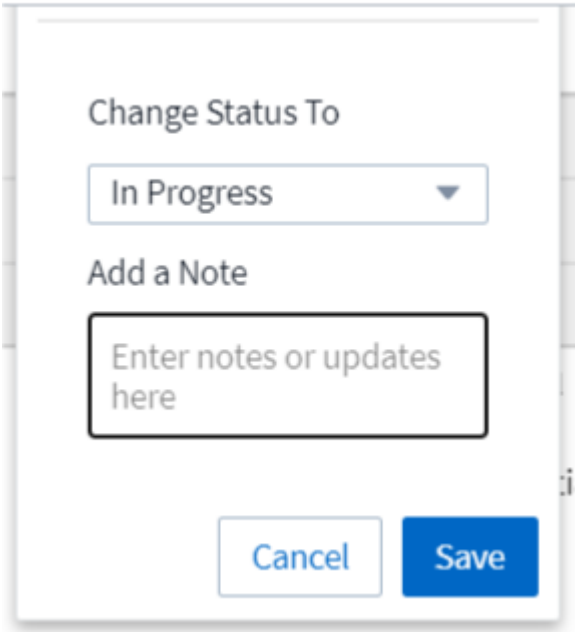
Per ogni avviso viene visualizzato quanto segue:

Potenziali attacchi:

- Il tipo di *potenziale attacco* (ad esempio ransomware o Sabotage)

- La data e l'ora in cui il potenziale attacco è stato *rilevato*
- Il *Stato* dell'avviso:
  - **Nuovo**: Impostazione predefinita per i nuovi avvisi.
  - **In corso**: L'avviso è sotto esame da uno o più membri del team.
  - **Resolved**: L'avviso è stato contrassegnato come risolto da un membro del team.
  - **Respinto**: L'avviso è stato respinto come comportamento falso positivo o previsto.

  Un amministratore può modificare lo stato dell'avviso e aggiungere una nota per agevolare l'analisi.



- L' *utente* il cui comportamento ha attivato l'avviso
- *Prova* dell'attacco (ad esempio, un gran numero di file è stato crittografato)
- L' *azione intrapresa* (ad esempio, è stata scattata una snapshot)

Avvertenze:

- Il *comportamento anomalo* che ha attivato l'avviso
- La data e l'ora in cui il comportamento è stato *rilevato*
- Il *Stato* dell'avviso (nuovo, in corso, ecc.)
- L' *utente* il cui comportamento ha attivato l'avviso
- Una descrizione di *Change* (ad esempio, un aumento anomalo dell'accesso al file)
- L' *azione intrapresa*

Opzioni filtro

È possibile filtrare gli avvisi in base a quanto segue:

- Il *Stato* dell'avviso
- Testo specifico nella *Nota*

- Il tipo di *attacchi/Avvertenze*
- L' *utente* le cui azioni hanno attivato l'avviso/avviso

La pagina Dettagli avviso

È possibile fare clic su un collegamento di avviso nella pagina dell'elenco degli avvisi per aprire una pagina dei dettagli per l'avviso. I dettagli degli avvisi possono variare in base al tipo di attacco o avviso. Ad esempio, una pagina dei dettagli di un attacco ransomware potrebbe mostrare le seguenti informazioni:

Sezione riepilogativa:

- Tipo di attacco (ransomware, Sabotage) e ID avviso (assegnato da workload Security)
- Data e ora in cui è stato rilevato l'attacco
- Azione intrapresa (ad esempio, è stata eseguita una snapshot automatica. L'ora dell'istantanea viene visualizzata immediatamente sotto la sezione riepilogativa)
- Stato (nuovo, in corso, ecc.)

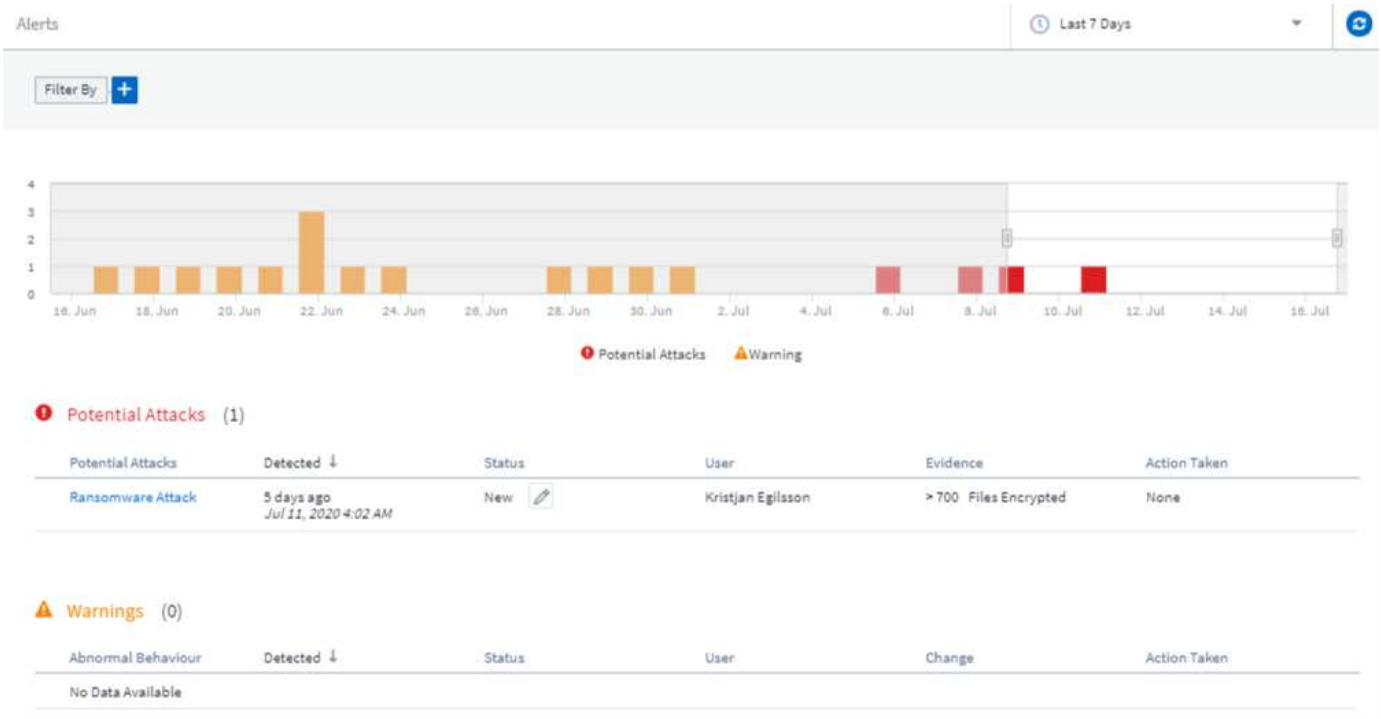
Sezione dei risultati degli attacchi:

- Numero di volumi e file interessati
- Un riepilogo del rilevamento
- Un grafico che mostra l'attività del file durante l'attacco

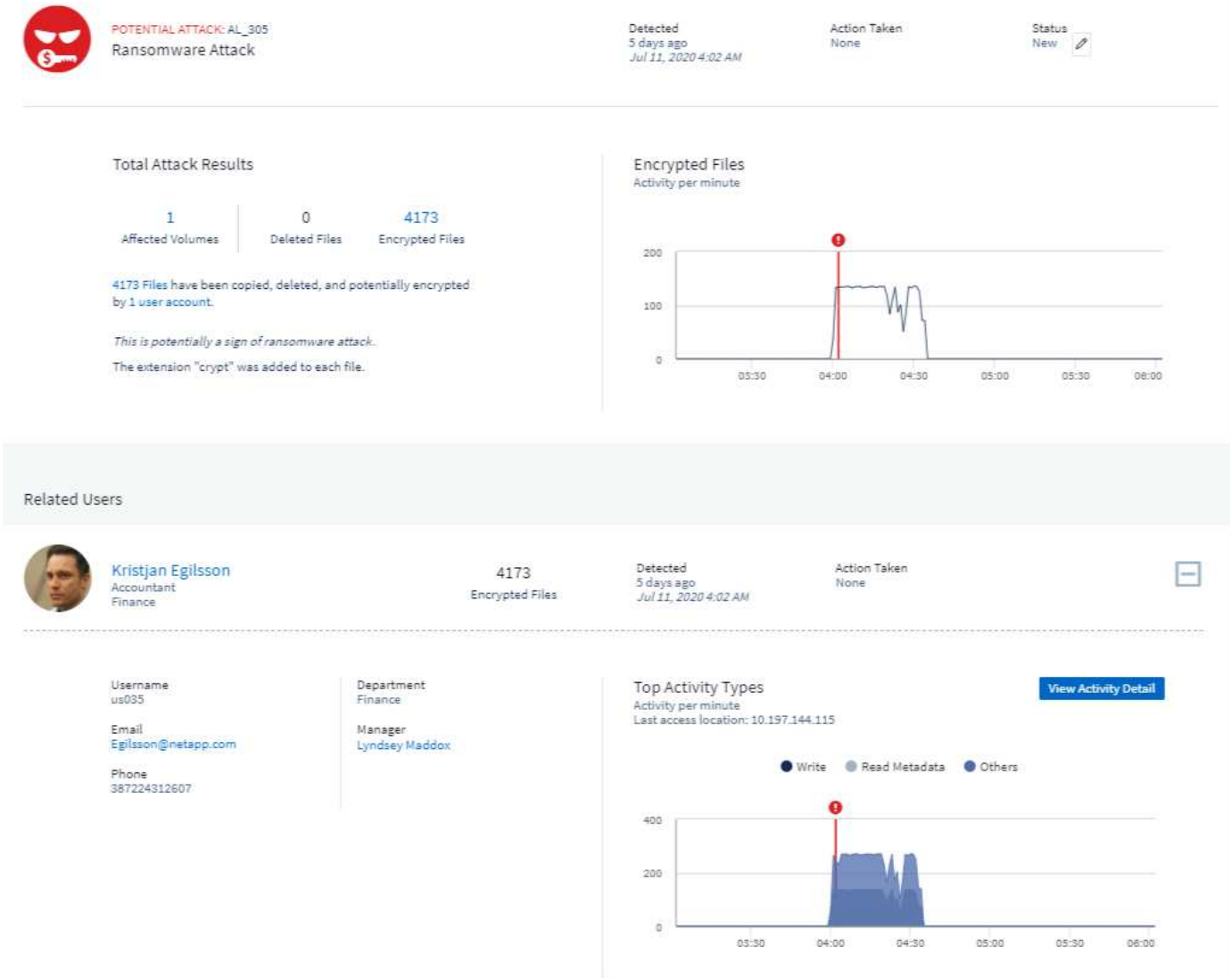
Sezione utenti correlati:

Questa sezione mostra i dettagli relativi all'utente coinvolto nel potenziale attacco, incluso un grafico delle attività principali per l'utente.

Pagina Alert (questo esempio mostra un potenziale attacco ransomware):



Pagina dei dettagli (questo esempio mostra un potenziale attacco ransomware):

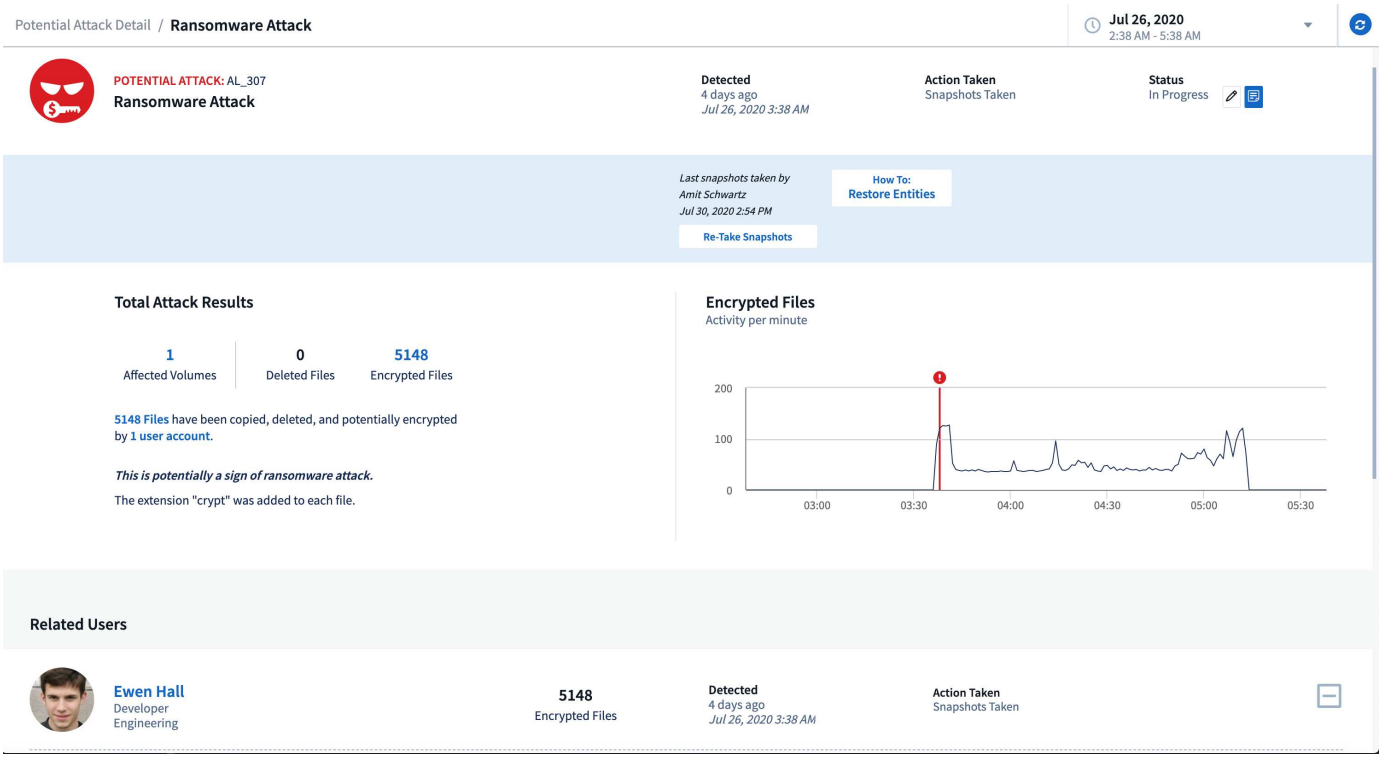


Eseguire un'azione Snapshot

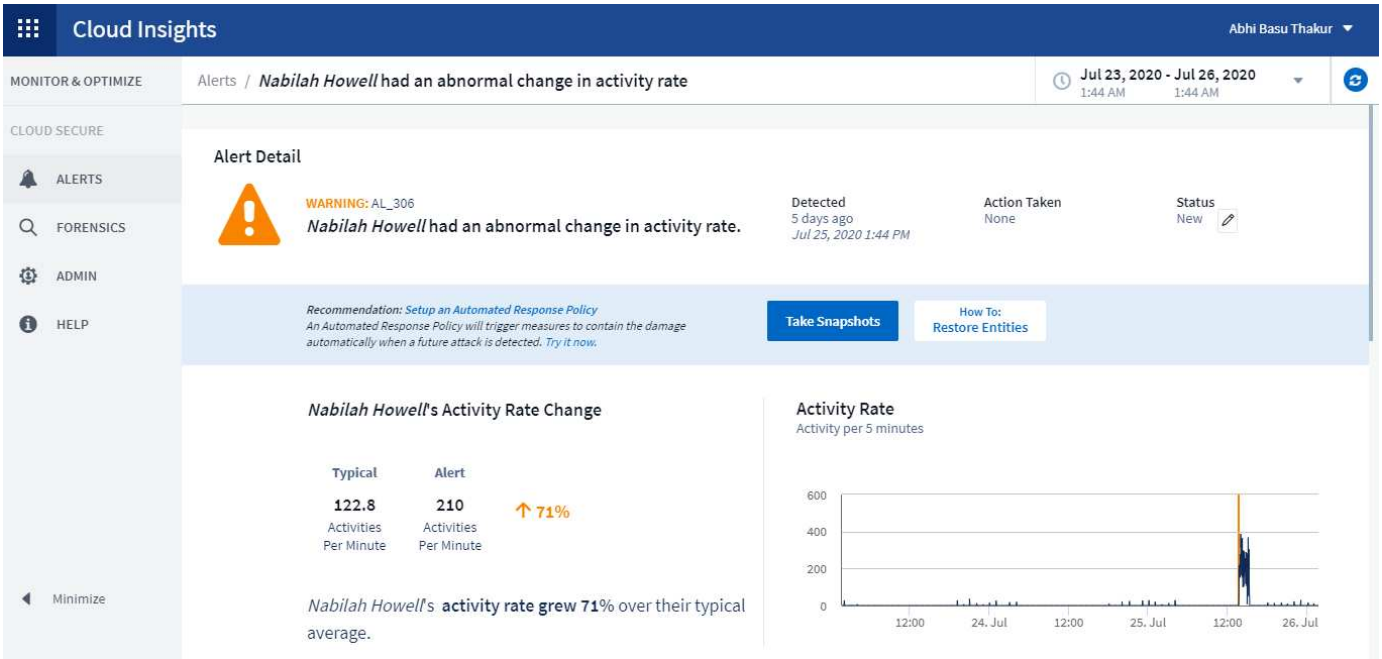
Workload Security protegge i tuoi dati eseguendo automaticamente un'istantanea quando vengono rilevate attività dannose, garantendo un backup sicuro dei tuoi dati.

Puoi definire "policy di risposta automatizzate" che acquisiscono una snapshot quando viene rilevato un attacco ransomware o un'altra attività anomala dell'utente. È anche possibile acquisire un'istantanea manualmente dalla pagina di avviso.

Snapshot automatica acquisita:



Istantanea manuale:



Notifiche di avviso

Le notifiche e-mail degli avvisi vengono inviate a un elenco di destinatari degli avvisi per ogni azione dell'avviso. Per configurare i destinatari degli avvisi, fare clic su **Admin > Notifiche** e inserire un indirizzo e-mail per ciascun destinatario.

Policy di conservazione

Gli avvisi e le avvertenze vengono conservati per 13 mesi. Gli avvisi e le avvertenze di età superiore a 13 mesi verranno eliminati. Se si elimina l'ambiente workload Security, vengono eliminati anche tutti i dati associati

all'ambiente.

Risoluzione dei problemi

Problema:	Prova:
Esiste una situazione in cui ONTAP esegue snapshot orarie al giorno. Le snapshot di workload Security (WS) ne influenzeranno? WS Snapshot prenderà lo snapshot orario? Lo snapshot orario predefinito viene arrestato?	Le snapshot di workload Security non influiscono sulle snapshot orarie. Le snapshot WS non acquisiranno lo spazio orario delle snapshot e questo dovrebbe continuare come prima. Lo snapshot orario predefinito non viene arrestato.
Cosa accade se viene raggiunto il numero massimo di snapshot in ONTAP?	Se viene raggiunto il numero massimo di snapshot, l'acquisizione successiva di Snapshot non riesce e Workload Security visualizza un messaggio di errore che indica che Snapshot è pieno. L'utente deve definire le policy di Snapshot per eliminare le snapshot meno recenti, altrimenti non verranno eseguite. In ONTAP 9.3 e versioni precedenti, un volume può contenere fino a 255 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume può contenere fino a 1023 copie Snapshot. Consultare la documentazione di ONTAP per informazioni su "Impostazione del criterio di eliminazione Snapshot".
Workload Security non è in grado di acquisire snapshot.	Assicurarsi che il ruolo utilizzato per creare gli snapshot abbia il xref:./ diritti appropriati assegnati. Assicurarsi che *csrole* sia creato con i diritti di accesso appropriati per lo snapshot: Ruolo di login di sicurezza create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Gli snapshot non riescono per gli avvisi precedenti sulle SVM che sono stati rimossi da workload Security e successivamente aggiunti di nuovo. Per i nuovi avvisi che si verificano dopo l'aggiunta di SVM, vengono create delle istantanee.	Si tratta di uno scenario raro. In caso di problemi, accedere a ONTAP e acquisire manualmente le istantanee per gli avvisi precedenti.
Nella pagina *Dettagli avviso*, sotto il pulsante *Esegui snapshot* viene visualizzato il messaggio di errore "ultimo tentativo non riuscito". Passando il mouse sull'errore viene visualizzato il messaggio "Invoke API command has timeout for the data collector with id" (il comando API Invoke è scaduto per il data collector con id).	Questo può accadere quando un data collector viene aggiunto alla sicurezza del carico di lavoro tramite l'IP di gestione SVM, se la LIF della SVM è nello stato *disabled* in ONTAP. Attivare la LIF specifica in ONTAP e attivare *Take Snapshot Manually* dalla sicurezza del carico di lavoro. L'azione Snapshot avrà esito positivo.

Analisi

Forensics - tutte le attività

La pagina All Activity (tutte le attività) consente di comprendere le azioni eseguite sulle entità nell'ambiente workload Security.

Esame di tutti i dati delle attività

Fare clic su **Forensics > Activity Forensics** (analisi > analisi delle attività) e fare clic sulla scheda **All Activity** (tutte le attività) per accedere alla pagina All Activity (tutte le attività). In questa pagina viene fornita una panoramica delle attività sul tenant, evidenziando le seguenti informazioni:

- Un grafico che mostra *Cronologia attività* (in base all'intervallo temporale globale selezionato)

  È possibile ingrandire il grafico trascinando un rettangolo nel grafico. L'intera pagina viene caricata per visualizzare l'intervallo di tempo di zoom. Quando si esegue lo zoom avanti, viene visualizzato un pulsante che consente all'utente di eseguire lo zoom indietro.

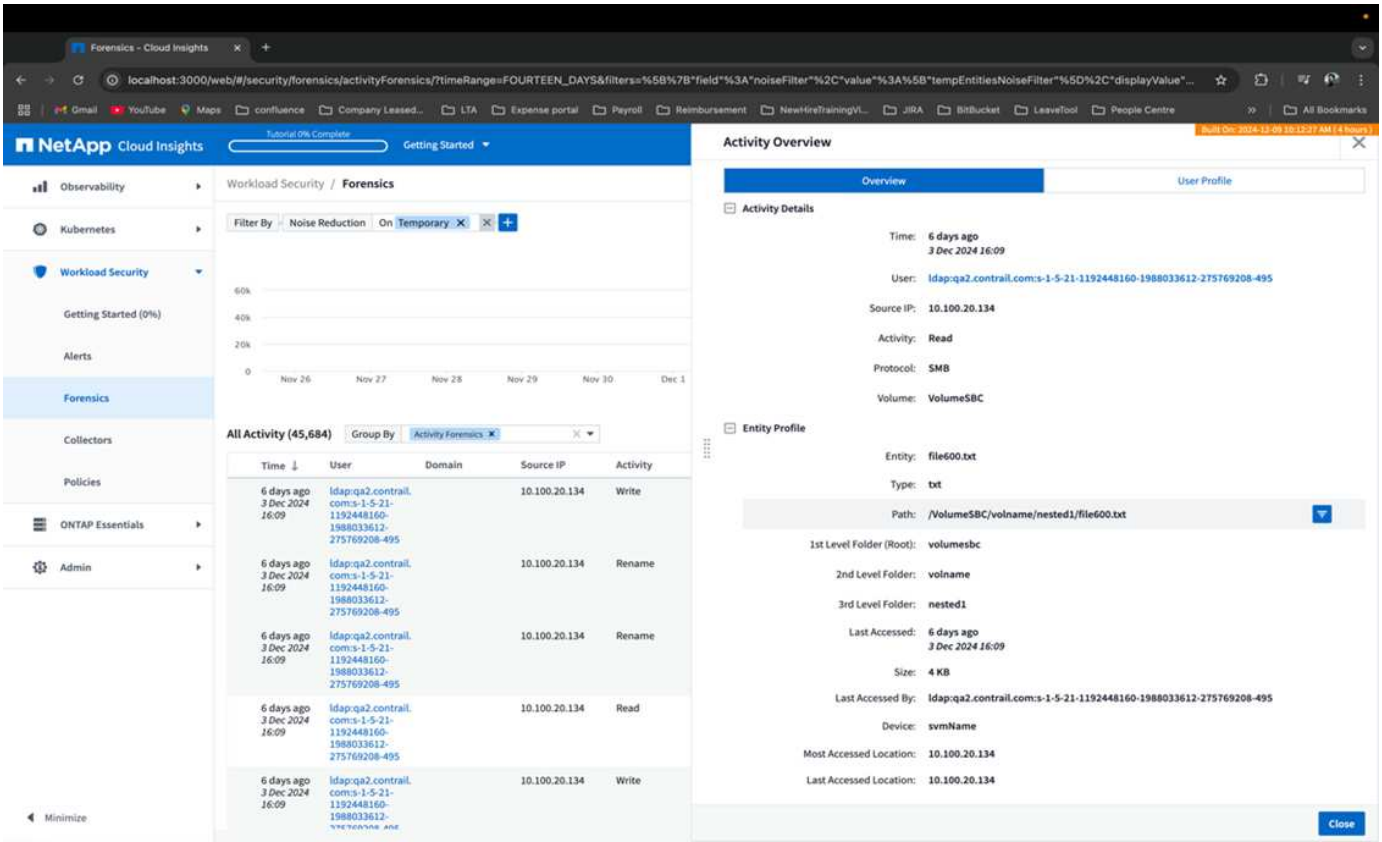
- Un elenco dei dati *tutte le attività*.
- Un elenco a discesa raggruppa per fornisce l'opzione di raggruppare l'attività per utenti, percorso, tipo di entità, ecc.
- Un pulsante di percorso comune sarà disponibile sopra la tabella con un clic del quale è possibile estrarre il pannello con i dettagli del percorso dell'entità.

La tabella **tutte le attività** mostra le seguenti informazioni. Nota: Non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare facendo clic sull'icona "marcia".

- L'ora * in cui è stato effettuato l'accesso a un'entità, inclusi l'anno, il mese, il giorno e l'ora dell'ultimo accesso.
- Il **utente** che ha effettuato l'accesso all'entità con un collegamento al "Informazioni sull'utente"come pannello scorrevole.
- L'attività * eseguita dall'utente. I tipi supportati sono:
  - **Cambia proprietà del gruppo** - la proprietà del gruppo è del file o della cartella è stata modificata. Per ulteriori informazioni sulla proprietà del gruppo, vedere "questo link."
  - **Cambia proprietario** - la proprietà del file o della cartella viene modificata in un altro utente.
  - **Cambia permesso** - l'autorizzazione per file o cartelle viene modificata.
  - **Crea** - Crea file o cartella.
  - **Delete** - Elimina file o cartella. Se una cartella viene eliminata, si ottengono gli eventi *delete* per tutti i file in quella cartella e sottocartelle.
  - **Read** - il file viene letto.
  - **Read Metadata** - solo se si attiva l'opzione di monitoraggio delle cartelle. Verrà generato all'apertura di una cartella su Windows o all'esecuzione di "ls" all'interno di una cartella in Linux.
  - **Rinomina** - Rinomina il file o la cartella.
  - **Write** - i dati vengono scritti in un file.
  - **Write Metadata** - i metadati del file vengono scritti, ad esempio, i permessi modificati.
  - **Altra modifica** - qualsiasi altro evento non descritto in precedenza. Tutti gli eventi non mappati vengono mappati al tipo di attività "Altro cambiamento". Applicabile a file e cartelle.
- Il percorso **Path** è il percorso *entity*. Questo deve essere il percorso esatto dell'entità (ad esempio, "*/home/userX/nested1/nested2/abc.txt*") O la parte di directory del percorso per la ricerca ricorsiva (ad esempio, "*/home/userX/nested1/nested2/*"). NOTA: I modelli di percorso regex (ad esempio *userX*) NON sono consentiti qui. In alternativa, è possibile specificare filtri a livello di cartella di percorso singoli, come indicato di seguito, per il filtraggio dei percorsi.

- La cartella **1st Level (Root)** è la directory principale del percorso dell'entità in minuscolo.
- La cartella **2nd Level** è la directory di secondo livello del percorso dell'entità in minuscolo.
- La cartella **3rd Level** è la directory di terzo livello del percorso dell'entità in minuscolo.
- La cartella **4th Level** è la directory di quarto livello del percorso dell'entità in minuscolo.
- L'estensione **Entity Type**, inclusa l'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 rinominare gli eventi quando il file originale è stato rinominato. Questa colonna non è visibile nella tabella per impostazione predefinita. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- Il **Volume** in cui risiedono le entità. Questa colonna non è visibile nella tabella per impostazione predefinita. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.

Selezionando una riga di tabella si apre un pannello a scorrimento con il profilo utente in una scheda e la panoramica dell'attività e dell'entità in un'altra scheda.



Il metodo *Group by* predefinito è *Activity forensics*. Se si seleziona un metodo *Raggruppa per* diverso, ad esempio tipo di entità, verrà visualizzata la tabella entità *Raggruppa per*. Se non viene effettuata alcuna selezione, viene visualizzato *Group by* **All** (Raggruppa per_ **tutto**).

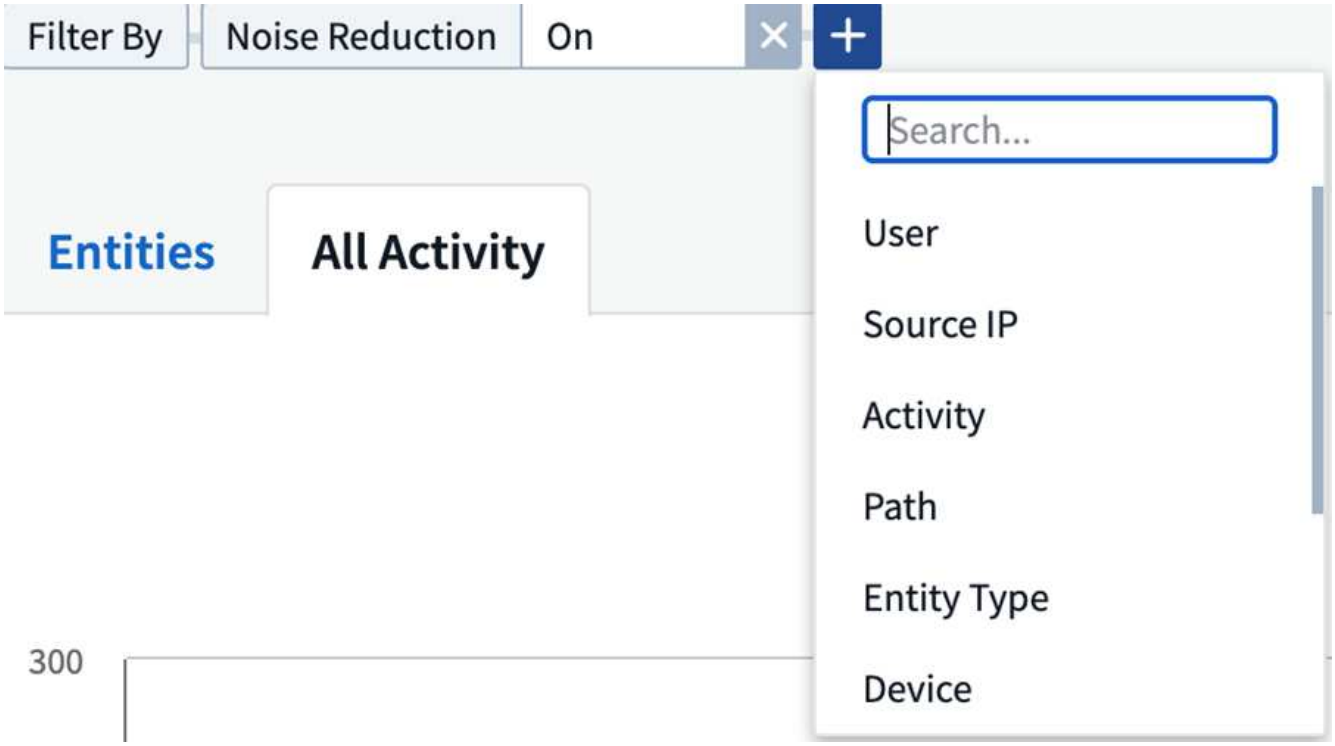
- Il conteggio delle attività viene visualizzato come collegamento ipertestuale; selezionando questa opzione si aggiunge il raggruppamento selezionato come filtro. La tabella delle attività verrà aggiornata in base a quel filtro.
- Se si modifica il filtro, si modifica l'intervallo di tempo o si aggiorna lo schermo, non sarà possibile tornare ai risultati filtrati senza dover impostare nuovamente il filtro.

Filtraggio dei dati Forensic Activity History

Per filtrare i dati è possibile utilizzare due metodi.

- Il filtro può essere aggiunto dal pannello scorrevole. Il valore viene aggiunto ai filtri appropriati nell'elenco *Filter by* principale.
- Filtrare i dati digitando il campo *Filtra per*:

  Selezionare il filtro appropriato dal widget 'Filtra per' in alto facendo clic sul pulsante **[+]**:



  Inserire il testo di ricerca

  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 **Activity**.
- **IP di origine** da cui è stato effettuato l'accesso all'entità. È necessario fornire un indirizzo IP di origine valido tra virgolette doppie, ad esempio "10.1.1.1". Gli IP incompleti come "10.1.1.**", "10.1.**.*", ecc. non funzionano.
- **Protocollo** per recuperare le attività specifiche del protocollo.
- **Nome utente** dell'utente che esegue l'attività. Specificare il nome utente esatto da filtrare. La ricerca con il nome utente parziale o con il prefisso '*' non funziona.
- **Riduzione del rumore** per filtrare i file creati nelle ultime 2 ore dall'utente. Viene inoltre utilizzato per filtrare i file temporanei (ad esempio, i file .tmp) a cui l'utente accede.
- **Dominio** dell'utente che esegue l'attività. È necessario fornire il **dominio esatto** da filtrare. La ricerca di un dominio parziale o di un dominio parziale prefisso o suffisso con carattere jolly ('*') non funzionerà. *Nessuno* può essere specificato per cercare il dominio mancante.

I seguenti campi sono soggetti a speciali regole di filtraggio:

- **Tipo di entità**, utilizzando l'estensione dell'entità (file) - è preferibile specificare il tipo di entità esatto all'interno delle virgolette. Ad esempio *"txt"*.
- **Percorso** dell'entità - questo deve essere il percorso esatto dell'entità (ad esempio, "*/home/userX/nested1/nested2/abc.txt*") O la porzione di directory del percorso per la ricerca ricorsiva (ad esempio, "*/home/userX/nested1/nested2/*"). NOTA: I modelli di percorso regex (ad esempio, **userX**) NON sono consentiti qui. Filtri percorso directory (stringa di percorso che termina con /) per risultati più rapidi si consiglia di utilizzare fino a 4 directory di profondità. Ad esempio, "*/home/userX/nested1/nested2/*". Fare riferimento alla tabella riportata di seguito per ulteriori dettagli.
- Cartella livello 1st (radice) - directory principale di percorso entità come filtri. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, allora è possibile usare home O "home".
- Cartella a 2nd livelli - directory a 2nd livelli di filtri percorso entità. Per esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, allora userX O "userX" possono essere usati.
- Cartella a 3rd livelli: Directory a 3rd livelli di filtri percorso entità.
- Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, allora si può usare nested1 O "nested1".
- Cartella a 4th livelli - Directory a 4th livelli directory dei filtri percorso entità. Ad esempio, se il percorso dell'entità è /home/userX/nested1/nested2/, allora si può usare nested2 O "nested2".
- **Utente** esecuzione dell'attività - è preferibile specificare l'utente esatto tra virgolette. Ad esempio, *"Amministratore"*.
- **Dispositivo** (SVM) in cui risiedono le entità
- **Volume** dove risiedono le entità
- Il percorso **originale** utilizzato per rinominare gli eventi quando il file originale è stato rinominato.

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

- Il valore esatto deve essere compreso tra virgolette: Esempio: "Searchtext"
- Le stringhe con caratteri jolly non devono contenere virgolette: Esempio: Searchtext, 's*searchtext*, filtrerà le stringhe contenenti il carattere 'earchtext'.
- Stringa con un prefisso, ad esempio: Searchtext* , cerca le stringhe che iniziano con 'searchtext'.

Esempi di filtro analisi attività:

Espressione filtro applicato dall'utente	Risultato previsto	Valutazione delle prestazioni	Commento
Percorso = "/home/userX/nested1/nested2/"	Ricerca ricorsiva di tutti i file e le cartelle in una determinata directory	Veloce	Le ricerche nelle directory sono rapide fino a 4 directory.
Percorso = "/home/userX/nested1/"	Ricerca ricorsiva di tutti i file e le cartelle in una determinata directory	Veloce	Le ricerche nelle directory sono rapide fino a 4 directory.
Percorso = "/home/userX/nested1/test"	Corrispondenza esatta dove il valore del percorso corrisponde a /home/userX/nested1/test	Più lento	La ricerca esatta sarà più lenta rispetto alle ricerche nella directory.

Espressione filtro applicato dall'utente	Risultato previsto	Valutazione delle prestazioni	Commento
Percorso = "/home/userX/nested1/nested2/nested3/"	Ricerca ricorsiva di tutti i file e le cartelle in una determinata directory	Più lento	Più di 4 ricerche di directory sono più lente da ricercare.
Qualsiasi altro filtro non basato su percorso. Si consiglia di inserire tra virgolette i filtri User e Entity Type, ad esempio User="Administrator" Entity Type="txt"		Veloce	

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 compreso tra *settembre 1st 10:15 e settembre 7th 10:15* mostra i conteggi delle attività tra settembre 1st 10:00 e settembre 7th 10:30.
2. Analogamente, le metriche di conteggio visualizzate 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 Forensic Activity History

È possibile ordinare i dati della cronologia delle attività in base a *ora, utente, IP di origine, attività,*, *tipo di entità*, cartella a 1st livelli (principale), cartella a 2nd livelli, cartella a 3rd livelli e cartella a 4th livelli. Per impostazione predefinita, la tabella viene ordinata in base a un ordine *time* decrescente, il che significa che i dati più recenti verranno visualizzati per primi. L'ordinamento è disattivato per i campi *Device* e *Protocol*.

Guida dell'utente per le esportazioni asincrone

Panoramica

La funzionalità di esportazione asincrona di Storage workload Security è progettata per gestire grandi esportazioni di dati.

Guida dettagliata: Esportazione dei dati con esportazioni asincrone

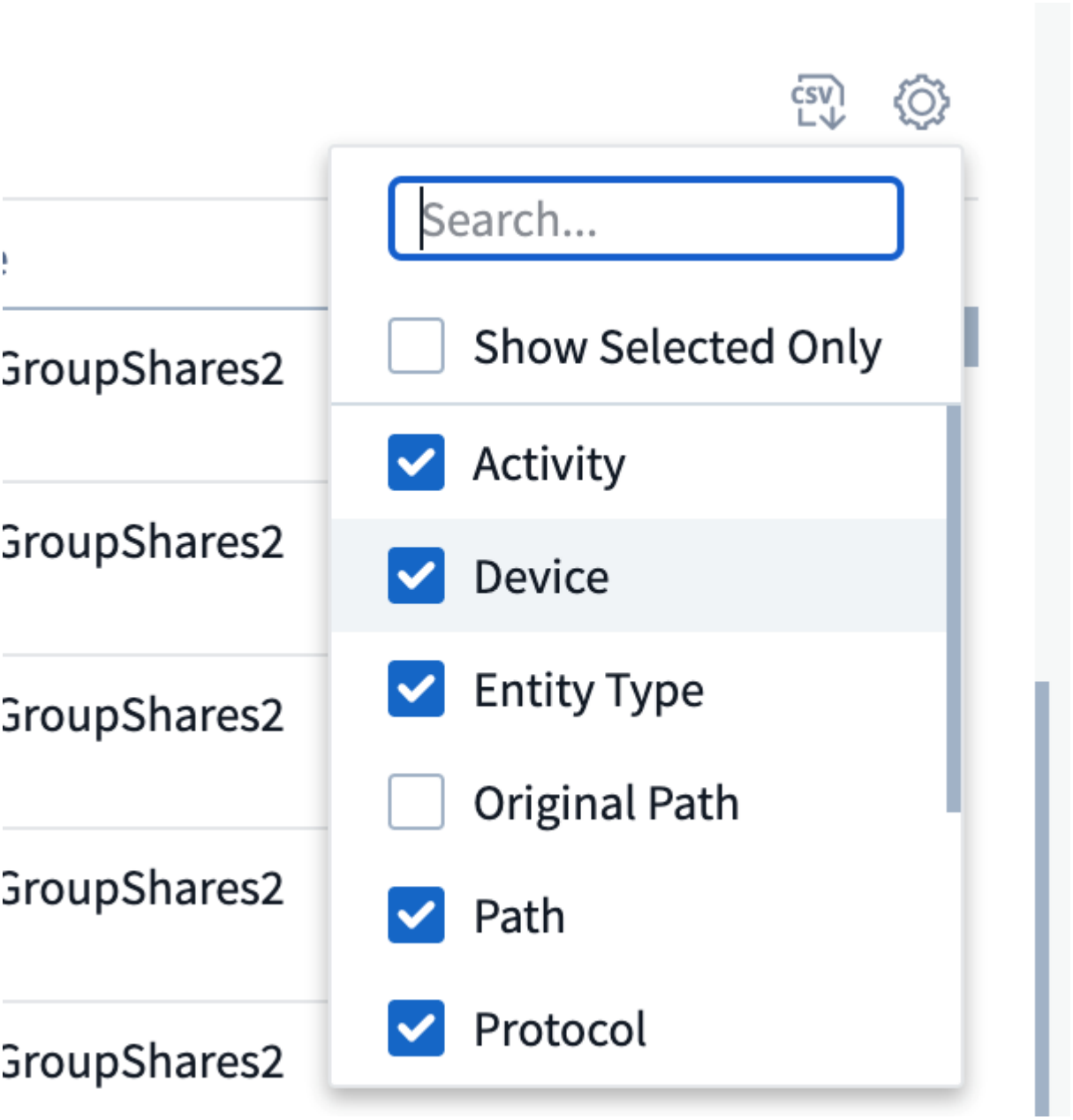
1. **Initiate Export** (inizia esportazione): Selezionare la durata desiderata e i filtri per l'esportazione, quindi fare clic sul pulsante Export (Esporta).
2. **Attendere il completamento dell'esportazione**: Il tempo di elaborazione può variare da alcuni minuti a poche ore. Potrebbe essere necessario aggiornare la pagina forense alcune volte. Una volta completato il processo di esportazione, viene attivato il pulsante "Scarica ultimo file CSV di esportazione".
3. **Download**: Fare clic sul pulsante "Scarica ultimo file di esportazione creato" per ottenere i dati esportati in formato .zip. Questi dati saranno disponibili per il download fino a quando l'utente non inizia un'altra esportazione asincrona o fino a quando non sono trascorsi 3 giorni, a seconda di quale delle due condizioni si verifica per prima. Il pulsante rimane abilitato fino a quando non viene avviata un'altra esportazione asincrona.
4. **Limitazioni**:
    - Il numero di download asincroni è attualmente limitato a 1 per utente e 3 per tenant.

- I dati esportati sono limitati a un massimo di 1 milioni di record.

Un esempio di script per estrarre dati forensi tramite API è presente all'indirizzo */opt/NetApp/cloudSecure/Agent/export-script/* dell'agente. Per ulteriori informazioni sullo script, vedere il file Leggimi in questa posizione.

Selezione colonna per tutte le attività

La tabella *All activity* mostra le colonne Select per impostazione predefinita. Per aggiungere, rimuovere o modificare le colonne, fare clic sull'icona a forma di ingranaggio a destra della tabella e selezionare dall'elenco delle colonne disponibili.



Conservazione della cronologia delle attività

La cronologia delle attività viene mantenuta per 13 mesi per gli ambienti di sicurezza dei workload attivi.

Applicabilità dei filtri nella pagina Forensics

Filtro	Che cosa fa	Esempio	Applicabile per questi filtri	Non applicabile per questi filtri	Risultato
* (Asterisco)	consente di cercare tutto	Auto*03172022 se il testo di ricerca contiene un trattino o un trattino basso, date l'espressione tra parentesi. Es. (svm*) per la ricerca in svm-123	Utente, tipo di entità, dispositivo, volume, percorso originale, cartella 1stLevel, cartella 2ndLevel, cartella 3rdLevel, cartella 4thLevel		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, periferica, Volume, cartella 1stLevel, cartella 2ndLevel, cartella 3rdLevel, cartella 4thLevel		Restituisce AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 e così via
OPPURE	consente di specificare più entità	AutoSabotageUser1_03172022 O AutoRansomUser4_03162022	Utente, dominio, tipo di entità, percorso originale		Restituisce uno qualsiasi di AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NO	consente di escludere il testo dai risultati della ricerca	NON AutoRansomUser4_03162022	Utente, dominio, tipo di entità, percorso originale, cartella 1stLevel, cartella 2ndLevel, cartella 3rdLevel, cartella 4thLevel	Dispositivo	Restituisce tutto ciò che non inizia con "AutoRansomUser4_03162022"
Nessuno	Ricerca i 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 (caso non sensibile)

"/AutoDir1/ "	Funziona; restituisce tutte le attività con directory a 1st livelli corrispondenti a AutoDir1 (caso non sensibile)
"/AutoDir1/AutoFile03242022/"	Funziona; restituisce tutte le attività con directory a 1st livelli corrispondenti a directory a AutoDir1 e 2nd livelli corrispondenti a AutoFile03242022 (caso non sensibile)
/AutoDir1/AutoFile03242022 O /AutoDir1/AutoFile03242022	Non funziona
NON /AutoDir1/AutoFile03242022	Non funziona
NON /AutoDir1	Non funziona
NON /AutoFile03242022	Non funziona
*	Non funziona

Modifiche all'attività utente della SVM principale locale

Se un utente della SVM root locale sta eseguendo un'attività, l'IP del client su cui è montata la condivisione NFS viene ora considerato nel nome utente, che verrà mostrato come root@<ip-address-of-the-client> sia nelle pagine di attività forense che in quelle di attività utente.

Ad esempio:

- Se SVM-1 viene monitorato tramite la sicurezza del carico di lavoro 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 dell'attività forense sarà *root@10.197.12.40*.
- Se la stessa SVM-1 è montata in un altro client con indirizzo IP 10.197.12.41, il nome utente mostrato nella pagina dell'attività forense sarà *root@10.197.12.41*.

*• questo è fatto per separare l'attività dell'utente root NFS dall'indirizzo IP. In precedenza, tutta l'attività veniva considerata eseguita solo da *root* utente, senza distinzione IP.

Risoluzione dei problemi

Problema	Provare

Nella tabella "tutte le attività", sotto la colonna ‘utente’, il nome utente viene visualizzato come: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” o "ldap:default:80038003"	I motivi possibili potrebbero essere: 1. Nessun User Directory Collector ancora configurato. Per aggiungerne uno, andare a **sicurezza workload > Collector > User Directory Collector** e fare clic su **+User Directory Collector**. Scegliere *Active Directory* o *LDAP Directory Server*. 2. È stato configurato un servizio di raccolta directory utente, tuttavia è stato arrestato o si trova in stato di errore. Andare a **Collector > User Directory Collectors** e controllare lo stato. Per suggerimenti sulla risoluzione dei problemi, consultare "Risoluzione dei problemi di User Directory Collector"la sezione della documentazione. Una volta eseguita la configurazione corretta, il nome verrà risolto automaticamente entro 24 ore. Se il problema persiste, verificare di aver aggiunto il Data Collector utente corretto. Assicurarsi che l’utente faccia effettivamente parte del server Active Directory/LDAP Directory aggiunto.
Alcuni eventi NFS non vengono visualizzati nell’interfaccia utente.	Controllare quanto segue: 1. È necessario eseguire un User Directory Collector per server ad con attributi POSIX impostati con l’attributo unixid attivato dall’interfaccia utente. 2. Qualsiasi utente che effettua l’accesso NFS deve essere visualizzato quando effettua una ricerca nella pagina utente dall’interfaccia utente 3. Gli eventi raw (eventi per i quali l’utente non è ancora stato scoperto) non sono supportati per NFS 4. L’accesso anonimo all’esportazione NFS non verrà monitorato. 5. Assicurati che la versione di NFS sia utilizzata in meno di NFS4,1.
Dopo aver digitato alcune lettere contenenti un carattere jolly come l’asterisco (*) nei filtri delle pagine Forensics *All Activity* o *Entities*, le pagine vengono caricate molto lentamente.	Un asterisco (**) nella stringa di ricerca cerca tutto. Tuttavia, le stringhe di caratteri jolly iniziali come **<searchTerm>** o *<*searchTerm*>** comporteranno una query lenta. Per ottenere prestazioni migliori, utilizzare le stringhe di prefisso nel formato *<searchTerm>** (in altre parole, aggiungere l’asterisco (*) *dopo* un termine di ricerca). Esempio: Utilizzare la stringa *testvolume**, invece di **testvolume* o **test*volume*. Usate una ricerca di directory per vedere ricorsivamente tutte le attività al di sotto di una data cartella (ricerca gerarchica). Per esempio, “/path1/path2/PATH3/” elencherà ricorsivamente tutte le attività al di sotto di /path1/path2/PATH3. In alternativa, utilizzare l’opzione "Aggiungi al filtro" nella scheda tutte le attività."
Si verifica un errore di richiesta non riuscita con codice di stato 500/503 quando si utilizza un filtro percorso.	Provare a utilizzare un intervallo di date più piccolo per filtrare i record.

L’interfaccia utente forense sta caricando i dati lentamente quando si utilizza il filtro *path*.	Filtri percorso directory (stringa di percorso che termina con /) per ottenere risultati più rapidi si consiglia di utilizzare fino a 4 directory profonde. Ad esempio, se il percorso della directory è /AAA/BBB/CCC/DDD, cercare “/AAA/BBB/CCC/DDD/” per caricare i dati più velocemente.

Panoramica dell’utente legale

Le informazioni per ciascun utente sono fornite nella Panoramica utente. Utilizzare queste viste per comprendere le caratteristiche dell’utente, 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 e-mail dell’utente
- Manager 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 recente
  - Ultima posizione di accesso
  - Grafico delle attività
  - Avvisi
- Operazioni per gli ultimi sette giorni
  - Numero di operazioni

Intervallo di refresh

L’elenco utenti viene aggiornato ogni 12 ore.

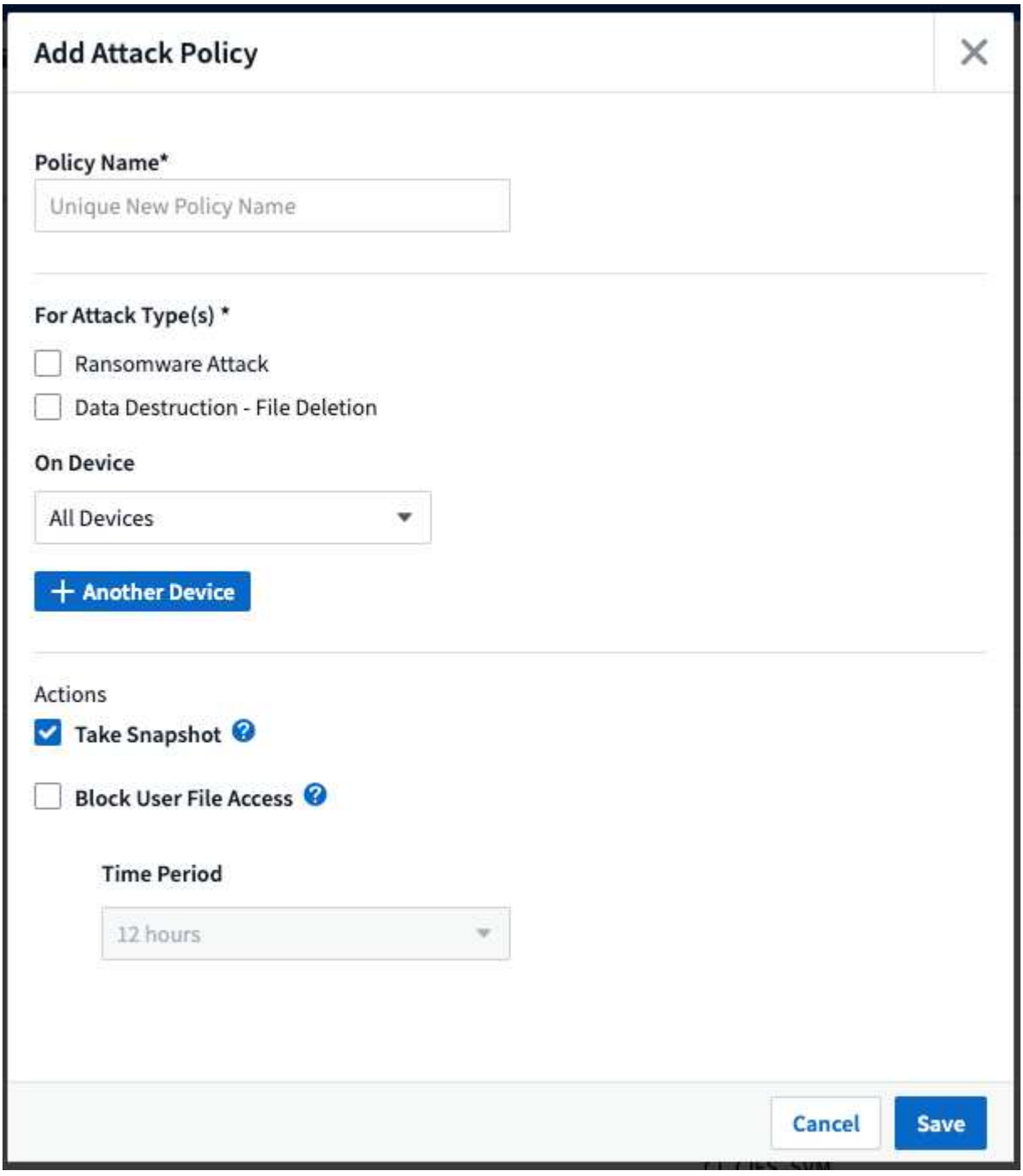
Policy di conservazione

Se non viene aggiornato nuovamente, l’elenco utenti viene conservato per 13 mesi. Dopo 13 mesi, i dati verranno cancellati. Se l’ambiente workload Security viene cancellato, tutti i dati associati all’ambiente vengono cancellati.

Policy di risposta automatizzate

Le policy di risposta attivano azioni come l'esecuzione di uno snapshot o la limitazione dell'accesso dell'utente in caso di attacco o comportamento anomalo dell'utente.

È possibile impostare criteri su dispositivi specifici o su tutti i dispositivi. Per impostare un criterio di risposta, selezionare **Admin > Automated Response Policies** (Amministrazione > Criteri di risposta automatici) e fare clic sul pulsante **+Policy** appropriato. È possibile creare policy per gli attacchi o per gli avvisi.



È necessario salvare il criterio con un nome univoco.

Per disattivare un'azione di risposta automatica (ad esempio, Take Snapshot), è sufficiente deselezionare

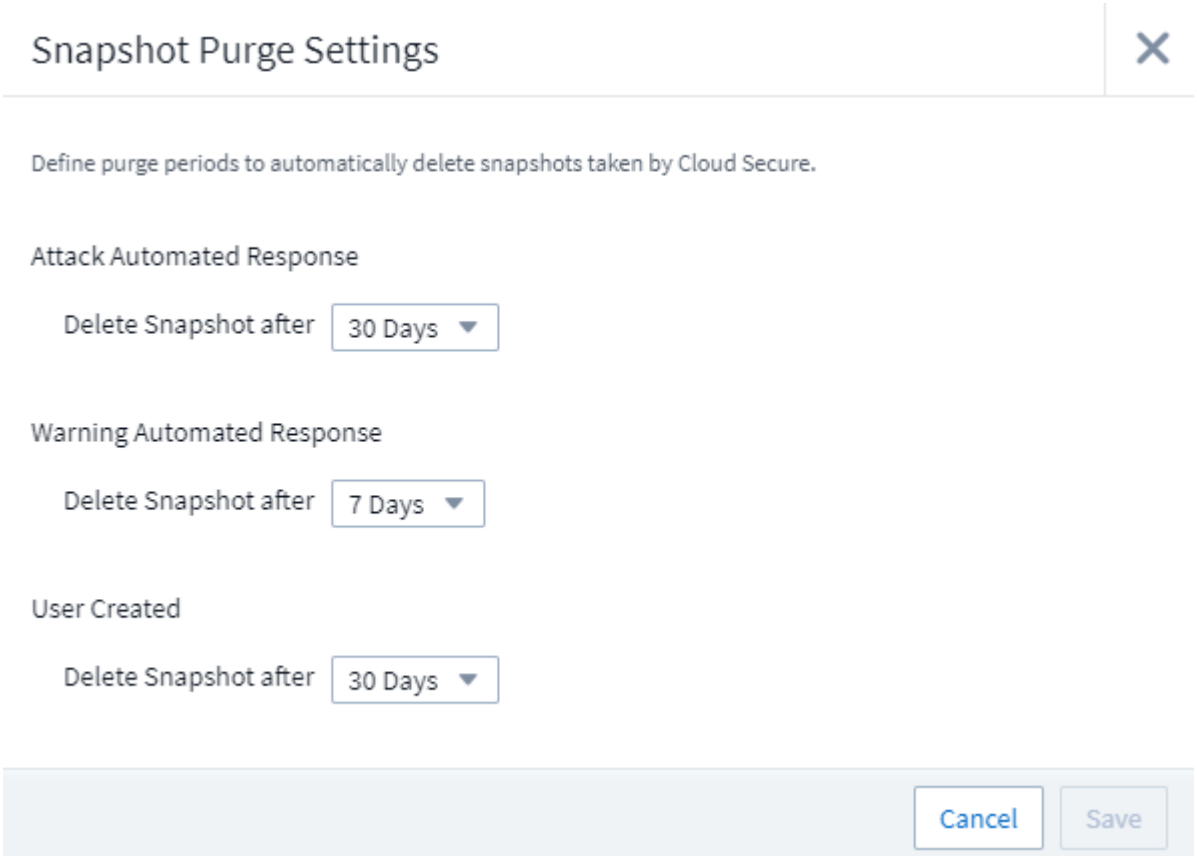
l'azione e salvare la policy.

Quando viene attivato un avviso relativo ai dispositivi specificati (o a tutti i dispositivi, se selezionati), la policy di risposta automatica esegue un'istantanea dei dati. È possibile visualizzare lo stato dell'istantanea sul "Pagina dei dettagli degli avvisi".

Vedere la "Limitare l'accesso dell'utente" pagina per ulteriori dettagli su come limitare l'accesso degli utenti tramite IP.

È possibile modificare o sospendere una policy di risposta automatica scegliendo l'opzione nel menu a discesa della policy.

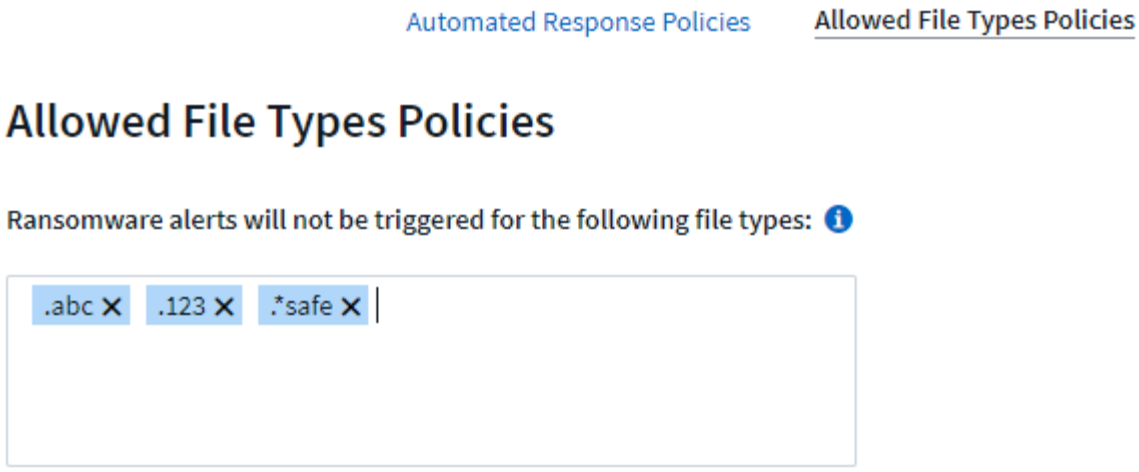
Workload Security elimina automaticamente le snapshot una volta al giorno in base alle impostazioni di Snapshot Purge.



Criteri tipi di file consentiti

Se viene rilevato un attacco ransomware per un'estensione di file nota e vengono generati degli avvisi nella schermata Alerts, è possibile aggiungere tale estensione a un elenco dei tipi di file *consentiti* per evitare avvisi non necessari.

Accedere a **sicurezza del carico di lavoro > Criteri** e andare alla scheda *Criteri del tipo di file consentiti*.



Una volta aggiunto all'elenco *allowed file types*, non verrà generato alcun avviso di attacco ransomware per quel tipo di file consentito. Si noti che la policy *tipi di file consentiti* è applicabile solo per il rilevamento del ransomware.

Ad esempio, se un file denominato *test.txt* viene rinominato *test.txt.abc* e workload Security rileva un attacco ransomware a causa dell'estensione *.abc*, l'estensione *.abc* può essere aggiunta all'elenco *allowed file types*. Dopo essere stati aggiunti all'elenco, gli attacchi ransomware non verranno più generati sui file con estensione *.abc*.

I tipi di file consentiti possono essere corrispondenze esatte (ad esempio, ".abc") o espressioni (ad esempio, "**.type", ".type**" o "**type**"). Le espressioni di tipo ".a*c", ".p*f" non sono supportate.

Integrazione con la protezione ransomware autonoma di ONTAP

La funzionalità ARP (Autonomous ransomware Protection) di ONTAP utilizza l'analisi dei carichi di lavoro in ambienti NAS (NFS e SMB) per rilevare e avvisare in modo proattivo circa attività anomale nel file che potrebbero indicare un attacco ransomware.

Ulteriori dettagli e requisiti di licenza su ARP sono disponibili "qui".

La sicurezza del carico di lavoro si integra con ONTAP per ricevere eventi ARP e fornire un ulteriore livello di analisi e risposte automatiche.

Workload Security riceve gli eventi ARP da ONTAP e intraprende le seguenti azioni:

1. Correla gli eventi di crittografia dei volumi con l'attività dell'utente per identificare chi sta causando il danno.
2. Implementa policy di risposta automatica (se definite)
3. Offre funzionalità di analisi legale:
    - Consentire ai clienti di condurre indagini sulle violazioni dei dati.
    - Identificare i file interessati, contribuendo a ripristinarli più rapidamente e a condurre indagini sulle violazioni dei dati.

Prerequisiti

1. Versione ONTAP minima: 9.11.1
2. Volumi abilitati ARP. È possibile trovare ulteriori informazioni sull'abilitazione di ARP "qui". ARP deve essere abilitato tramite Gestore di sistema di OnCommand. La sicurezza del carico di lavoro non può abilitare ARP.
3. Workload Security Collector deve essere aggiunto tramite l'IP del cluster.
4. Per il funzionamento di questa funzionalità sono necessarie credenziali a livello di cluster. In altre parole, è necessario utilizzare le credenziali a livello di cluster quando si aggiunge la SVM.

Autorizzazioni utente richieste

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni alla sicurezza del carico di lavoro per raccogliere informazioni relative all'ARP da ONTAP.

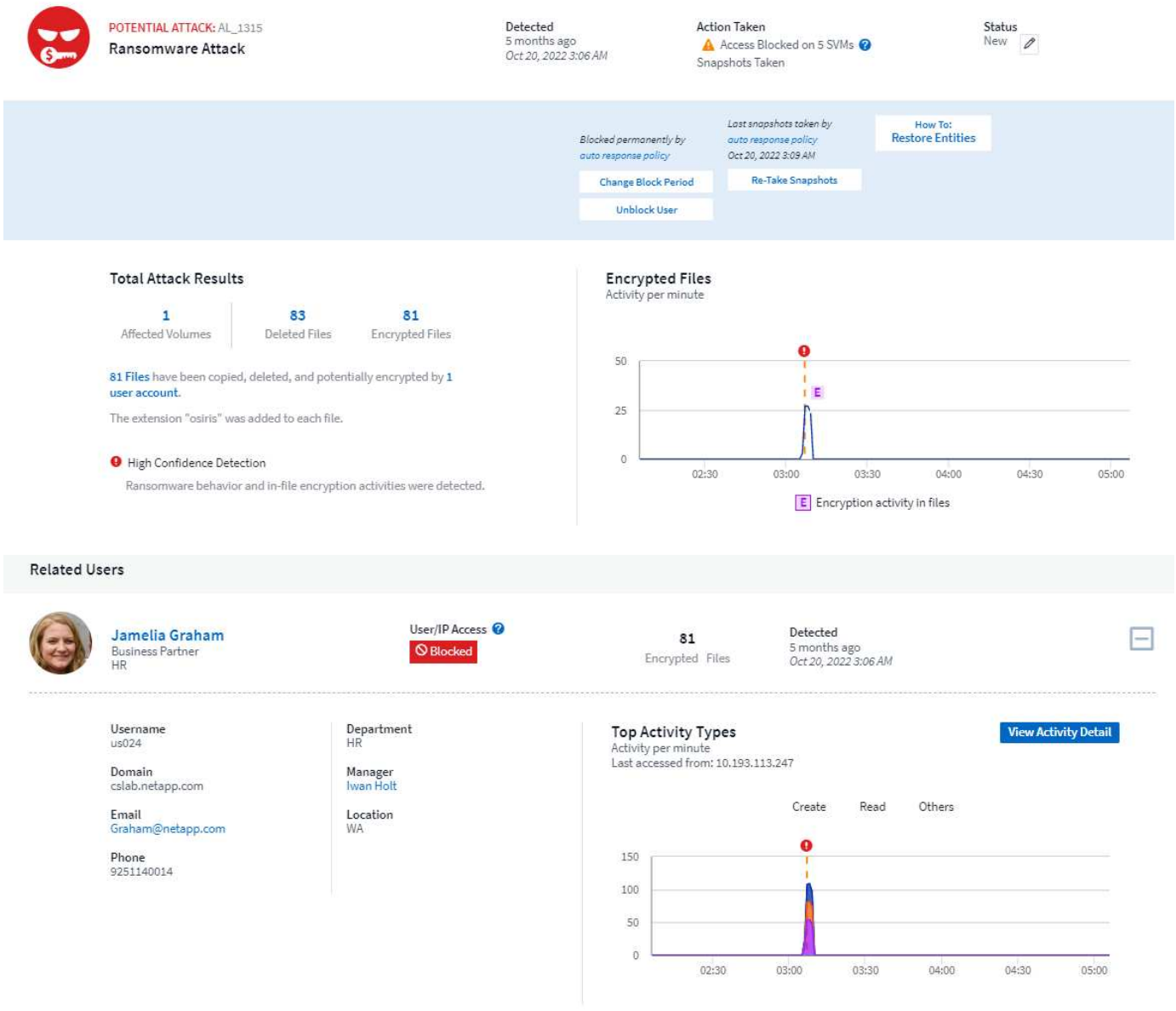
Per *csuser* con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Ulteriori informazioni sulla configurazione di Altro "Permessi ONTAP".

Avviso di esempio

Di seguito è riportato un esempio di avviso generato a causa di un evento ARP:



Un banner di alta fiducia indica che l'attacco ha mostrato un comportamento ransomware insieme alle attività di crittografia dei file. Il grafico dei file crittografati indica la data e l'ora in cui l'attività di crittografia del volume è stata rilevata dalla soluzione ARP.

Limitazioni

Nel caso in cui una SVM non venga monitorata dalla sicurezza del carico di lavoro, ma vi siano eventi ARP generati da ONTAP, gli eventi verranno comunque ricevuti e visualizzati dalla sicurezza del carico di lavoro. Tuttavia, le informazioni Forensic relative all'avviso, così come la mappatura dell'utente, non verranno acquisite o visualizzate.

Risoluzione dei problemi

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

Problema:	Risoluzione:
Gli avvisi e-mail vengono ricevuti 24 ore dopo il rilevamento di un attacco. Nell'interfaccia utente, gli avvisi vengono visualizzati 24 ore prima della ricezione delle e-mail da parte di Data Infrastructure Insights workload Security.	Quando ONTAP invia l'evento *ransomware rilevato* alla sicurezza del carico di lavoro di Data Infrastructure Insights (ad es. Sicurezza del carico di lavoro), l'email viene inviata. L'evento contiene un elenco di attacchi e i relativi indicatori di data e ora. L'interfaccia utente di workload Security visualizza la data e l'ora di avviso del primo file attaccato. ONTAP invia l'evento *ransomware Detected* a informazioni sull'infrastruttura dati quando viene codificato un determinato numero di file. Pertanto, potrebbe esserci una differenza tra l'ora in cui l'avviso viene visualizzato nell'interfaccia utente e l'ora in cui l'e-mail viene inviata.

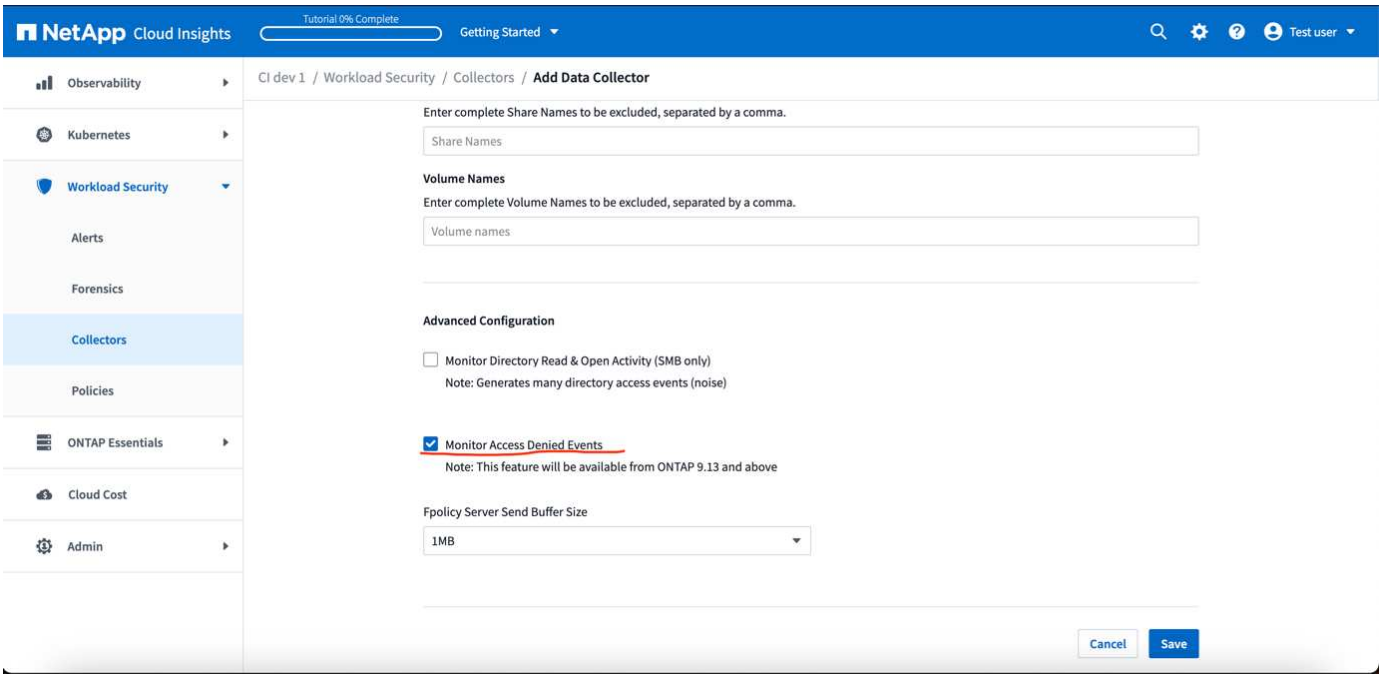
Integrazione con accesso ONTAP negato

La funzionalità accesso negato di ONTAP utilizza l'analisi dei carichi di lavoro negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e informare l'utente in caso di operazioni sui file non riuscite (ad esempio, un utente che tenta di eseguire un'operazione per cui non dispone dell'autorizzazione). Queste notifiche delle operazioni sui file non riuscite, specialmente in caso di errori relativi alla sicurezza, aiuteranno ulteriormente a bloccare gli attacchi interni nelle prime fasi.

Data Infrastructure Insights workload Security si integra con ONTAP per ricevere eventi di accesso negato e fornire un livello di risposta automatico e analitico aggiuntivo.

Prerequisiti

- Versione ONTAP minima: 9.13.0.
- Un amministratore della protezione del carico di lavoro deve attivare la funzione accesso negato durante l'aggiunta di un nuovo agente di raccolta o la modifica di un agente di raccolta esistente, selezionando la casella di controllo *Monitor Access Denied Events* in Configurazione avanzata.



Autorizzazioni utente richieste

Se Data Collector viene aggiunto utilizzando le credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se il servizio di raccolta viene aggiunto utilizzando un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, attenersi alla procedura riportata di seguito per assegnare a sicurezza del carico di lavoro l'autorizzazione necessaria per registrare gli eventi di accesso negato con ONTAP.

Per csuser con credenziali *cluster*, eseguire i seguenti comandi dalla riga di comando di ONTAP. Si noti che *csrestrole* è un ruolo personalizzato e *csuser* è un utente personalizzato di ONTAP.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Per csuser con credenziali *SVM*, eseguire i seguenti comandi dalla riga di comando di ONTAP:

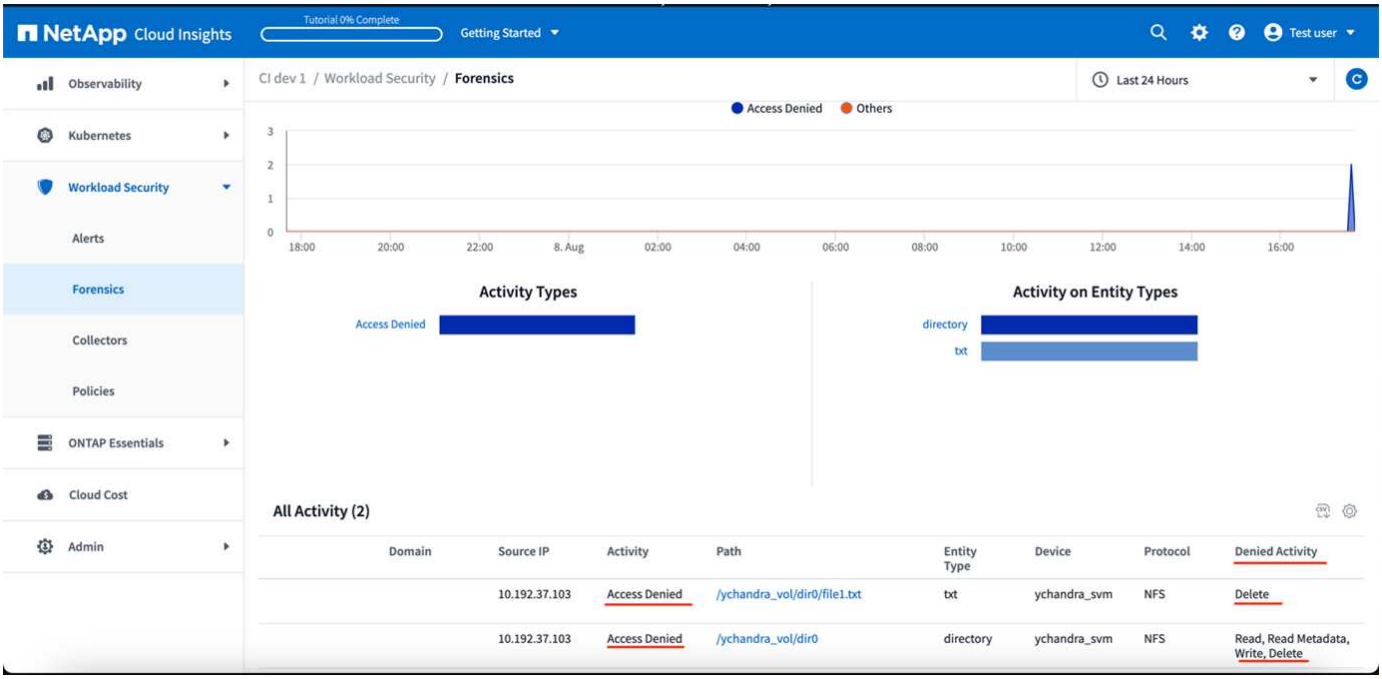
```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Ulteriori informazioni sulla configurazione di Altro "Permessi ONTAP".

Eventi di accesso negato

Una volta acquisiti gli eventi dal sistema ONTAP, la pagina analisi della sicurezza del workload mostra gli

eventi di accesso negato. Oltre alle informazioni visualizzate, è possibile visualizzare i permessi utente mancanti per una particolare operazione aggiungendo la colonna *attività desiderata* alla tabella dall'icona a forma di ingranaggio.



Blocco dell'accesso utente

Una volta rilevato un attacco, Workload Security può arrestare l'attacco bloccando l'accesso dell'utente al file system. L'accesso può essere bloccato automaticamente, utilizzando le policy di risposta automatica o manualmente dalle pagine degli avvisi o dei dettagli dell'utente.

Quando si blocca l'accesso dell'utente, è necessario definire un periodo di tempo di blocco. Al termine del periodo di tempo selezionato, l'accesso dell'utente viene ripristinato automaticamente. Il blocco degli accessi è supportato per i protocolli SMB e NFS.

L'utente è direttamente bloccato per SMB e l'indirizzo IP dei computer host che causano l'attacco sarà bloccato per NFS. Gli indirizzi IP di tali macchine non potranno accedere alle macchine virtuali di storage (SVM) monitorate da workload Security.

Ad esempio, supponiamo che Workload Security gestisca 10 SVM e che la policy di risposta automatica sia configurata per quattro di queste SVM. Se l'attacco ha origine in una delle quattro SVM, l'accesso dell'utente viene bloccato in tutte le 10 SVM. Viene ancora eseguita un'istantanea sulla SVM di origine.

Se sono presenti quattro SVM con una SVM configurata per SMB, una configurata per NFS e le restanti due configurate per NFS e SMB, tutte le SVM verranno bloccate se l'attacco ha origine in una qualsiasi delle quattro SVM.

Prerequisiti per il blocco dell'accesso utente

Per il funzionamento di questa funzionalità sono necessarie credenziali a livello di cluster.

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni a workload Security per bloccare l'utente.

Per gli utenti csuser con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Assicurarsi di rivedere anche la sezione autorizzazioni della "Configurazione del Data Collector SVM di ONTAP" pagina.

Come attivare la funzione?

- In sicurezza del carico di lavoro, accedere a **sicurezza del carico di lavoro > Criteri > Criteri di risposta automatizzati**. Scegliere **+Criteri attacco**.
- Selezionare (selezionare) *Blocca accesso file utente*.

Come si imposta il blocco automatico degli accessi degli utenti?

- Creare una nuova policy di attacco o modificare una policy di attacco esistente.
- Selezionare le SVM su cui monitorare la policy di attacco.
- Fare clic sulla casella di controllo "Block User file Access" (Blocca accesso file utente). La funzione viene attivata quando viene selezionata.
- In "Time Period" (periodo di tempo), selezionare l'intervallo di tempo fino al quale applicare il blocco.
- Per testare il blocco automatico degli utenti, è possibile simulare un attacco tramite un "script simulato".

Come verificare se nel sistema sono presenti utenti bloccati?

- Nella pagina degli elenchi degli avvisi, viene visualizzato un banner nella parte superiore della schermata in caso di blocco di un utente.
- Facendo clic sul banner si accede alla pagina "utenti", in cui è possibile visualizzare l'elenco degli utenti bloccati.
- Nella pagina "utenti", all'interno di una colonna denominata "accesso utente/IP". In questa colonna viene visualizzato lo stato corrente di blocco dell'utente.

Limitare e gestire l'accesso utente manualmente

- È possibile accedere alla schermata dei dettagli degli avvisi o dei dettagli dell'utente, quindi bloccare o ripristinare manualmente un utente da tali schermate.

Cronologia delle limitazioni di accesso dell'utente

Nella pagina dei dettagli degli avvisi e dei dettagli dell'utente, nel pannello utente, è possibile visualizzare un audit della cronologia delle limitazioni di accesso dell'utente: Tempo, azione (blocco, sblocco), durata, azione intrapresa da, Manuale/automatico e IP interessati per NFS.

Come si disattiva la funzione?

È possibile disattivare la funzione in qualsiasi momento. Se nel sistema sono presenti utenti con restrizioni, è necessario ripristinarne l'accesso.

- In sicurezza del carico di lavoro, accedere a **sicurezza del carico di lavoro > Criteri > Criteri di risposta automatizzati**. Scegliere **+Criteri attacco**.
- Deselezionare *Blocca accesso al file utente*.

La funzione verrà nascosta da tutte le pagine.

Ripristinare manualmente gli IP per NFS

Attenersi alla seguente procedura per ripristinare manualmente gli IP da ONTAP se la versione di prova di workload Security scade o se l'agente/collector non è attivo.

1. Elencare tutti i criteri di esportazione su una SVM.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Eliminare le regole di tutti i criteri sulla SVM che hanno "cloudSecure_rule" come corrispondenza client specificando il rispettivo RuleIndex. La regola di sicurezza del carico di lavoro è solitamente 1.

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Assicurarsi che la regola di sicurezza del carico di lavoro sia
eliminata (passaggio facoltativo per confermare).
```

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
2 entries were displayed.
```

Ripristinare manualmente gli utenti per SMB

Attenersi alla seguente procedura per ripristinare manualmente gli utenti da ONTAP se la versione di prova di workload Security scade o se l'agente/collector non è attivo.

È possibile ottenere l'elenco degli utenti bloccati in workload Security dalla pagina dell'elenco utenti.

1. Accedere al cluster ONTAP (dove si desidera sbloccare gli utenti) con le credenziali *admin* del cluster. (Per Amazon FSX, accedi con le credenziali FSX).
2. Eseguire il seguente comando per elencare tutti gli utenti bloccati da workload Security per SMB in tutte le SVM:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                -                    Pattern: CSLAB\\US040
                                          Replacement:
2       -                -                    Pattern: CSLAB\\US030
                                          Replacement:
2 entries were displayed.
```

Nel suddetto output, 2 utenti sono stati bloccati (US030, US040) con il dominio CSLAB.

1. Una volta identificata la posizione dall'output precedente, eseguire il seguente comando per sbloccare l'utente:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Verificare che gli utenti siano sbloccati eseguendo il comando:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Non devono essere visualizzate voci per gli utenti precedentemente bloccati.

Risoluzione dei problemi

Problema	Provare
Alcuni utenti non sono soggetti a restrizioni, anche se si verifica un attacco.	1. Assicurarsi che Data Collector e Agent per le SVM siano in stato *running*. Workload Security non sarà in grado di inviare comandi se Data Collector e Agent vengono arrestati. 2. Ciò è dovuto al fatto che l'utente può avere accesso all'archivio da una macchina con un nuovo IP che non è stato utilizzato in precedenza. La limitazione avviene tramite l'indirizzo IP dell'host attraverso il quale l'utente accede allo storage. Controllare nell'interfaccia utente (Dettagli avviso > Cronologia limiti di accesso per questo utente > IP interessati) l'elenco degli indirizzi IP con restrizioni. Se l'utente accede allo storage da un host che ha un IP diverso dagli IP con restrizioni, l'utente potrà comunque accedere allo storage attraverso l'IP senza restrizioni. Se l'utente sta tentando di accedere dagli host i cui indirizzi IP sono limitati, lo storage non sarà accessibile.
Facendo clic manualmente su Restricate Access (limita accesso) si ottiene "gli indirizzi IP di questo utente sono già stati limitati".	L'IP da limitare è già stato limitato da un altro utente.
Impossibile modificare il criterio. Motivo: Non autorizzato per quel comando.	Controllare se si utilizza csuser, le autorizzazioni vengono assegnate all'utente come indicato in precedenza.

Problema	Provare
Il blocco dell'utente (indirizzo IP) per NFS funziona, ma per SMB / CIFS viene visualizzato un messaggio di errore: "Trasformazione SID in DomainName non riuscita. Timeout motivo: Socket non stabilito"	Ciò può accadere se *csuser* non dispone dell'autorizzazione per eseguire ssh. (Verificare la connessione a livello di cluster, quindi assicurarsi che l'utente possa eseguire ssh). il ruolo *csuser* richiede queste autorizzazioni. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Per *csuser* con credenziali cluster, effettuare le seguenti operazioni dalla riga di comando di ONTAP: Ruolo di accesso di sicurezza create -ruolo csrole -nomedesign"regola del criterio di esportazione vserver" -accedere a tutti i ruoli di accesso di sicurezza create -ruolo csruolo ONTAP
Ricevo il messaggio di errore *traduzione SID non riuscita. REASON:255:Error: Command failed: Not authorized for that commandError: "Access-check" is not a recognized command*, when a user would be blocked.	Questo può accadere quando *csuser* non dispone delle autorizzazioni corrette. Per ulteriori informazioni, vedere "Prerequisiti per il blocco dell'accesso utente" . Dopo aver applicato le autorizzazioni, si consiglia di riavviare il Data Collector di ONTAP e il Data Collector della directory utente. I comandi di autorizzazione richiesti sono elencati di seguito. ---- ruolo di accesso di sicurezza create -ruolo csrole -cmddirname "vserver export-policy rule" -accedi a tutto il ruolo di accesso di sicurezza create -ruolo csrole -cmddirname set -accedi a tutto il ruolo di accesso di sicurezza create -ruolo csrole -cmddirname "vserver cifs session" -accedi a tutto il ruolo di accesso di accesso di sicurezza create -ruolo csrole -cmddirname "vserver services access-check authentication translation" -accedi a tutto l'accesso di sicurezza creazione ruolo -ruolo csrole -cmddirname "vserver name-mapping" -access all ----

Sicurezza del carico di lavoro: Simulazione di un attacco

È possibile utilizzare le istruzioni riportate in questa pagina per simulare un attacco per il test o la dimostrazione di workload Security utilizzando lo script ransomware Simulation incluso.

Cose da notare prima di iniziare

- Lo script di simulazione ransomware funziona solo su Linux.
- Lo script viene fornito con i file di installazione dell'agente workload Security. È disponibile su qualsiasi computer su cui è installato un agente workload Security.
- È possibile eseguire lo script sul computer dell'agente workload Security; non è necessario preparare un'altra macchina Linux. Tuttavia, se si preferisce eseguire lo script su un altro sistema, è sufficiente copiare lo script ed eseguirlo.

Avere almeno 1,000 file di esempio

Questo script deve essere eseguito su una SVM con una cartella contenente file da crittografare. Si consiglia di avere almeno 1,000 file all'interno di tale cartella e di qualsiasi sottocartella. I file non devono essere vuoti. Non creare i file e crittografarli utilizzando lo stesso utente. Workload Security considera questa attività a basso rischio e pertanto non genera un avviso (ad esempio, lo stesso utente modifica i file appena creati).

Vedere di seguito le istruzioni per "creare a livello di codice file non vuoti".

Linee guida prima di eseguire il simulatore:

1. Assicurarsi che i file crittografati non siano vuoti.
2. Assicurarsi di crittografare > 50 file. Un numero limitato di file verrà ignorato.
3. Non eseguire più attacchi con lo stesso utente. Dopo alcune volte, workload Security apprenderà questo comportamento dell'utente e supporrà che si tratti del comportamento normale dell'utente.
4. Non crittografare i file creati dallo stesso utente. La modifica di un file appena creato da un utente non è considerata un'attività rischiosa. Utilizzare invece i file creati da un altro utente O attendere qualche ora tra la creazione e la crittografia dei file.

Preparare il sistema

Per prima cosa, montare il volume di destinazione sulla macchina. È possibile montare un montaggio NFS o un'esportazione CIFS.

Per montare l'esportazione NFS in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Non montare NFS versione 4.1; non è supportato da Fpolicy.

Per montare CIFS in Linux:

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
Quindi, configurare un Data Collector:
```

1. Configurare l'agente workload Security, se non è già stato fatto.
2. Configurare il data collector SVM se non è già stato fatto.

Eseguire lo script ransomware Simulator

1. Accedere (ssh) al computer dell'agente workload Security.
2. Accedere a: */opt/netapp/cloudSecure/Agent/install*
3. Chiamare lo script del simulatore senza parametri per visualizzare l'utilizzo:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

Crittografare i file di test

Per crittografare i file, eseguire il seguente comando:

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

Ripristinare i file

Per decrittare, eseguire il seguente comando:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

Eseguire lo script più volte

Dopo aver generato un attacco ransomware per un utente, passare a un altro utente per generare un attacco aggiuntivo. Workload Security apprende il comportamento dell'utente e non avvisa in caso di ripetuti attacchi ransomware entro un breve periodo di tempo per lo stesso utente.

Creare file a livello di codice

Prima di creare i file, è necessario interrompere o sospendere l'elaborazione del Data Collector. Prima di aggiungere il data collector all'agente, attenersi alla procedura riportata di seguito. Se è già stato aggiunto il data collector, è sufficiente modificare il data collector, inserire una password non valida e salvarla. In questo modo, il data collector viene temporaneamente messo in stato di errore. NOTA: Annotare la password originale.

L'opzione consigliata è a "mettere in pausa il raccoglitore" prima di creare i file.]

Prima di eseguire la simulazione, è necessario aggiungere i file da crittografare. È possibile copiare manualmente i file da crittografare nella cartella di destinazione oppure utilizzare uno script (vedere l'esempio seguente) per creare i file a livello di programmazione. Copiare almeno 1,000 file, indipendentemente dal metodo utilizzato.

Se si sceglie di creare i file a livello di programmazione, attenersi alla seguente procedura:

1. Accedere alla casella Agente.
2. Montare un'esportazione NFS dalla SVM del filer alla macchina Agent. Su tale cartella.
3. In tale cartella creare un file denominato createfiles.sh
4. Copiare le seguenti righe nel file.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Salvare il file.
6. Assicurarsi che il permesso di esecuzione sul file sia:

```
 chmod 777 ./createfiles.sh
. Eseguire lo script:
```

```
./createfiles.sh
```

   nella cartella corrente verranno creati 1000 file.

7. Riattivare il data collector

   Se il data collector è stato disattivato al punto 1, modificare il data collector, inserire la password corretta e salvare. Assicurarsi che il data collector sia nuovamente in esecuzione.

8. Se il raccoglitore è stato messo in pausa prima di procedere come indicato di seguito, assicurarsi di selezionare "riprendere il raccoglitore".

Configurazione delle notifiche e-mail per gli avvisi, gli avvisi e lo stato del servizio di raccolta origine dati/agente

Per configurare i destinatari degli avvisi di workload Security, fare clic su **Admin > Notifiche** e inserire gli indirizzi e-mail nelle sezioni appropriate per ciascun destinatario.

Avvisi e avvisi di potenziali attacchi

Per inviare notifiche di avviso di *potenziali attacchi*, inserire gli indirizzi e-mail dei destinatari nella sezione *Invia avvisi potenziali attacchi*. Le notifiche e-mail vengono inviate all'elenco dei destinatari degli avvisi per ogni azione dell'avviso.

Per inviare notifiche di tipo *Warning*, inserire gli indirizzi e-mail dei destinatari nella sezione *Send Warning Alerts*.

Monitoraggio dello stato di salute di Agent e Data Collector

È possibile monitorare lo stato degli agenti e delle origini dati attraverso le notifiche.

Per ricevere notifiche in caso di mancato funzionamento di un agente o di un Data Source Collector, inserire gli indirizzi e-mail dei destinatari nella sezione *Data Collection Health Alerts*.

Tenere presente quanto segue:

- Gli avvisi sullo stato di salute verranno inviati solo dopo che l'agente/raccoglitore ha interrotto la segnalazione per almeno un'ora.
- Viene inviata una sola notifica via email ai destinatari in un dato periodo di 24 ore, anche se l'agente o il Data Collector sono disconnessi per un periodo di tempo più lungo.
- In caso di guasto di un Agente, verrà inviato un avviso (non uno per raccoglitore). L'e-mail includerà un elenco di tutte le SVM interessate.
- Un errore di raccolta Active Directory viene segnalato come avviso e non influisce sul rilevamento ransomware.
- L'elenco di configurazione per iniziare ora include una nuova fase di *Configurazione delle notifiche e-mail*.

Ricezione delle notifiche di aggiornamento dell'agente e del Data Collector

- Immettere gli ID e-mail in "Data Collection Health Alerts" (Avvisi integrità raccolta dati).
- La casella di controllo "Abilita notifiche di aggiornamento" diventa attiva.
- Le notifiche e-mail di aggiornamento dell'agente e di Data Collector vengono inviate agli ID e-mail un giorno prima dell'aggiornamento pianificato.

Risoluzione dei problemi

Problema:	Provare questo:
Gli ID e-mail sono presenti in "Data Collector Health Alerts" (Avvisi integrità del Data Collector), tuttavia non si ricevono notifiche.	Le e-mail di notifica vengono inviate dal dominio di approfondimento dell'infrastruttura dati NetApp, ad esempio da_accounts@service.cledy dintevises.NetApp.com_. Alcune aziende bloccano le e-mail in arrivo se provengono da un dominio esterno. Assicurarsi che le notifiche esterne dai domini di NetApp Data Infrastructure Insights siano inserite nella whitelist.

API per la sicurezza del carico di lavoro

L'API workload Security consente ai clienti NetApp e ai vendor di software indipendenti (ISV) di integrare workload Security con altre applicazioni, come CMDB o altri sistemi di ticketing.

Requisiti per l'accesso API:

- Per concedere l'accesso viene utilizzato un modello API Access Token.
- La gestione del token API viene eseguita dagli utenti di workload Security con il ruolo di Amministratore.

Documentazione API (Swagger)

Le informazioni API più recenti si trovano accedendo a workload Security e accedendo a **Admin > API Access**. Fare clic sul collegamento **documentazione API**. La documentazione API è basata su Swagger, che fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provarla sul tenant.

Se si chiama l'API Forensics Activity, utilizzare l'API cloudSecure_forensics.activities.**v2**. Se si effettuano più chiamate a questa API, assicurarsi che le chiamate vengano eseguite in sequenza, non in parallelo. Più chiamate parallele possono causare il timeout dell'API.

Token di accesso API

Prima di utilizzare l'API workload Security, è necessario creare uno o più **API Access Token**. I token di accesso concedono le autorizzazioni di lettura. È inoltre possibile impostare la scadenza per ciascun token di accesso.

Per creare un token di accesso:

- Fare clic su **Admin > API Access** (Amministratore > accesso API)
- Fare clic su **+token di accesso API**
- Inserire **Nome token**
- Specificare **scadenza token**

Il token sarà disponibile solo per la copia negli Appunti e il salvataggio durante il processo di creazione. I token non possono essere recuperati dopo la loro creazione, pertanto si consiglia vivamente di copiarli e salvarli in una posizione sicura. Viene richiesto di fare clic sul pulsante Copy API Access Token (Copia token di accesso API) prima di chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. È possibile attivare i token disattivati.

I token concedono un accesso generico alle API dal punto di vista del cliente, gestendo l'accesso alle API nell'ambito del proprio tenant.

L'applicazione riceve un token di accesso dopo che un utente ha autenticato e autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token passato informa l'API che la portante del token è stata autorizzata ad accedere all'API ed eseguire azioni specifiche in base all'ambito concesso durante l'autorizzazione.

L'intestazione HTTP in cui viene passato il token di accesso è **X-CloudInsights-apiKey:**

Ad esempio, utilizzare quanto segue per recuperare le risorse di storage:

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
Dove _<API_Access_Token>_ è il token salvato durante la creazione della
chiave di accesso API.
```

Informazioni dettagliate sono disponibili nel link *documentazione API* sotto **Admin > accesso API**.

Script per estrarre i dati tramite l'API

Gli agenti di sicurezza workload includono uno script di esportazione per facilitare le chiamate parallele all'API v2 dividendo l'intervallo di tempo richiesto in batch più piccoli.

Lo script si trova in */opt/NetApp/cloudSecure/Agent/export-script*. Un file README nella stessa directory fornisce istruzioni per l'uso.

Ecco un esempio di comando per richiamare lo script:

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --access_key %ACCESS_KEY% --path_filter
"<dir path>" --user_name "<user>" --from_time "01-08-2024 00:00:00"
--to_time "31-08-2024 23:59:59" --iteration_interval 12 --num_workers 3
```

Key Parameters: - `--iteration_interval 12`: Divide l'intervallo di tempo richiesto in intervalli di 12 ore. - `--num_workers 3`: Esegue il fetch di questi intervalli in parallelo utilizzando 3 filettature.

Informazioni sul copyright

Informazioni sul marchio commerciale