Sicurezza del carico di lavoro

Data Infrastructure Insights

NetApp
February 19, 2026

Sommario

Sicurezza del carico di lavoro

Informazioni sulla sicurezza del carico di lavoro di archiviazione

Data Infrastructure Insights Storage Workload Security (in precedenza Cloud Secure) aiuta a proteggere i tuoi dati con informazioni fruibili sulle minacce interne. Fornisce visibilità e controllo centralizzati di tutti gli accessi ai dati aziendali negli ambienti cloud ibridi, per garantire il raggiungimento degli obiettivi di sicurezza e conformità.

Visibilità

Ottieni visibilità e controllo centralizzati dell'accesso degli utenti ai dati aziendali critici archiviati in sede o nel cloud.

Sostituire gli strumenti e i processi manuali che non riescono a fornire una visibilità tempestiva e accurata dell'accesso e del controllo dei dati. Workload Security funziona in modo esclusivo sia sui sistemi di archiviazione cloud che su quelli on-premise per fornirti avvisi in tempo reale sui comportamenti dannosi degli utenti.

Protezione

Proteggi i dati aziendali dall'uso improprio da parte di utenti malintenzionati o compromessi tramite l'apprendimento automatico avanzato e il rilevamento delle anomalie.

Ti avvisa di eventuali accessi anomali ai dati tramite apprendimento automatico avanzato e rilevamento di anomalie nel comportamento dell'utente.

Conformità

Garantisci la conformità aziendale verificando l'accesso dei dati utente ai dati aziendali critici archiviati in sede o nel cloud.

Iniziare

Introduzione alla sicurezza del carico di lavoro

Workload Security ti aiuta a monitorare l'attività degli utenti e a rilevare potenziali minacce alla sicurezza nel tuo ambiente di archiviazione. Prima di poter iniziare il monitoraggio, è necessario configurare agenti, raccoglitori di dati e servizi di directory per gettare le basi per un monitoraggio completo della sicurezza.

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

Prima di poter iniziare a raccogliere dati, è necessario configurare quanto segue:

Compito	Informazioni correlate

Configurare un agente	"Requisiti dell'agente" "Aggiungi agente"
Configurare un connettore di directory utente	"Aggiungi connettore directory utente"
Configurare i raccoglitori di dati	Fare clic su **Sicurezza del carico di lavoro > Collettori**. Fare clic sul collettore dati che si desidera configurare. Per informazioni sul collettore, consultare la sezione Riferimento del fornitore del Data Collector della documentazione.
Crea account utente	"Gestisci account utente"

Workload Security può essere integrato anche con altri strumenti. Per esempio,"vedi questa guida" sull'integrazione con Splunk.

Requisiti dell'agente di sicurezza del carico di lavoro

Distribuisci gli agenti Workload Security su server dedicati che soddisfano i requisiti minimi di sistema operativo, CPU, memoria e spazio su disco per garantire prestazioni ottimali di monitoraggio e rilevamento delle minacce. Questa guida specifica i requisiti hardware e di rete necessari prima di "installazione del Workload Security Agent", incluse le distribuzioni Linux supportate, le regole di connettività di rete e le indicazioni sul dimensionamento del sistema.

Componente	Requisiti Linux
Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti: * AlmaLinux 9.4 (64 bit) fino a 9.5 (64 bit), 10 (64 bit), incluso SELinux * CentOS Stream 9 (64 bit) * Debian 11 (64 bit), 12 (64 bit), incluso SELinux * OpenSUSE Leap 15.3 (64 bit) fino a 15.6 (64 bit) * Oracle Linux 8.10 (64 bit), 9.1 (64 bit) fino a 9.6 (64 bit), incluso SELinux * Red Hat Enterprise Linux 8.10 (64 bit), 9.1 (64 bit) fino a 9.6 (64 bit), 10 (64 bit), incluso SELinux * Rocky 9.4 (64 bit) fino a 9.6 (64 bit), incluso SELinux * SUSE Linux Enterprise Server Da 15 SP4 (64 bit) a 15 SP6 (64 bit), incluso SELinux * Ubuntu 20.04 LTS (64 bit), 22.04 LTS (64 bit), 24.04 LTS (64 bit) Su questo computer non deve essere in esecuzione nessun altro software a livello di applicazione. Si consiglia un server dedicato.
Comandi	Per l'installazione è necessario 'unzip'. Inoltre, per l'installazione, l'esecuzione degli script e la disinstallazione è necessario il comando 'sudo su –'.
processore	4 core della CPU
Memoria	16 GB di RAM

Componente	Requisiti Linux
Spazio disponibile su disco	Lo spazio su disco dovrebbe essere allocato in questo modo: /opt/netapp 36 GB (minimo 35 GB di spazio libero dopo la creazione del file system) Nota: si consiglia di allocare un po' di spazio su disco extra per consentire la creazione del file system. Assicurarsi che ci siano almeno 35 GB di spazio libero nel file system. Se /opt è una cartella montata da un archivio NAS, assicurarsi che gli utenti locali abbiano accesso a questa cartella. L'installazione dell'agente o del raccoglitore dati potrebbe non riuscire se gli utenti locali non dispongono dell'autorizzazione per questa cartella. Vedere"Risoluzione dei problemi" sezione per maggiori dettagli.
Rete	Connessione Ethernet da 100 Mbps a 1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi e una porta obbligatoria per l'istanza di Workload Security (80 o 443).

Nota: l'agente Workload Security può essere installato nella stessa macchina di un'unità di acquisizione e/o di un agente Data Infrastructure Insights . Tuttavia, è buona norma installarli su macchine separate. Nel caso in cui siano installati sullo stesso computer, allocare lo spazio su disco come mostrato di seguito:

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

Ulteriori raccomandazioni

- Si consiglia vivamente di sincronizzare l'ora sia sul sistema ONTAP che sulla macchina dell'agente utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Regole di accesso alla rete cloud

Per ambienti di sicurezza del carico di lavoro con sede negli Stati Uniti:

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

Per ambienti di sicurezza dei carichi di lavoro **con sede in Europa**:

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

Per ambienti di sicurezza del carico di lavoro basati su **APAC**:

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

Regole in-network

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAP / start-tls)	Agente di sicurezza del carico di lavoro	URL del server LDAP	Connettiti a LDAP
TCP	443	Agente di sicurezza del carico di lavoro	Indirizzo IP di gestione del cluster o SVM (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000 - 55000	Indirizzi IP LIF dei dati SVM	Agente di sicurezza del carico di lavoro	Comunicazione da ONTAP al Workload Security Agent per gli eventi Fpolicy. Queste porte devono essere aperte verso il Workload Security Agent affinché ONTAP possa inviargli eventi, incluso qualsiasi firewall sul Workload Security Agent stesso (se presente). NOTA: non è necessario riservare **tutte** queste porte, ma le porte riservate a tale scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando circa 100 porte e di aumentarle se necessario.

Protocollo	Porta	Fonte	Destinazione	Descrizione
TCP	35000-55000	IP di gestione del cluster	Agente di sicurezza del carico di lavoro	Comunicazione dall'IP di gestione del cluster ONTAP al Workload Security Agent per **eventi EMS**. Queste porte devono essere aperte verso il Workload Security Agent affinché ONTAP possa inviargli **eventi EMS**, incluso qualsiasi firewall sul Workload Security Agent stesso (se presente). NOTA: non è necessario riservare **tutte** queste porte, ma le porte riservate a tale scopo devono essere comprese in questo intervallo. Si consiglia di iniziare riservando circa 100 porte e di aumentarle se necessario.
SSH	22	Agente di sicurezza del carico di lavoro	Gestione dei cluster	Necessario per il blocco degli utenti CIFS/SMB.

Dimensionamento del sistema

Vedi il"Verificatore del tasso di eventi" documentazione per informazioni sulle dimensioni.

Distribuisci agenti di sicurezza del carico di lavoro

Gli agenti Workload Security sono essenziali per monitorare l'attività degli utenti e rilevare potenziali minacce alla sicurezza nell'intera infrastruttura di storage. Questa guida fornisce istruzioni di installazione dettagliate, best practice per la gestione degli agenti (incluse le funzionalità di pausa/ripresa e blocco/sblocco) e requisiti di configurazione post-distribuzione. Prima di iniziare, assicurati che il tuo server agente soddisfi i requisiti "requisiti di sistema".

Prima di iniziare

- Il privilegio sudo è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
- Durante l'installazione dell'agente, sulla macchina vengono creati un utente locale *cssys* e un gruppo

locale *cssys*. Se le impostazioni delle autorizzazioni non consentono la creazione di un utente locale e richiedono invece Active Directory, è necessario creare un utente con il nome utente *cssys* nel server Active Directory.

- Puoi leggere informazioni sulla sicurezza Data Infrastructure Insights"Qui" .

Migliori pratiche

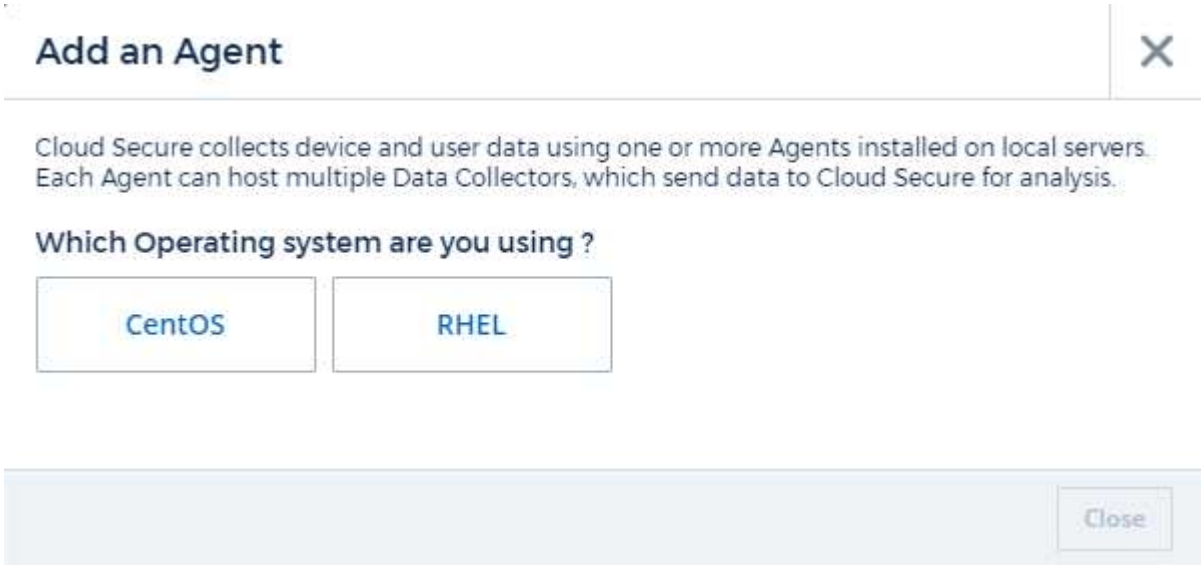
Prima di configurare l'agente Workload Security, tenere presente quanto segue.

Pausa e ripresa	Pausa: rimuove fpolicies da ONTAP. Solitamente utilizzato quando i clienti eseguono attività di manutenzione prolungate che potrebbero richiedere molto tempo, come riavvii di VM di agenti o sostituzioni di storage. Riprendi: aggiunge nuovamente fpolicies a ONTAP.
Fissare e sbloccare	Unpin recupera immediatamente la versione più recente (se disponibile) e aggiorna l'agente e il collettore. Durante questo aggiornamento, fpolicies si disconnetterà e si riconnetterà. Questa funzionalità è pensata per i clienti che desiderano controllare la tempistica degli aggiornamenti automatici. Vedi sotto peristruzioni per fissare/sganciare .
Approccio consigliato	Per configurazioni di grandi dimensioni, è consigliabile utilizzare Pin e Unpin anziché mettere in pausa i collettori. Non è necessario mettere in pausa e riprendere mentre si usa la funzione "blocca e sblocca". I clienti possono mantenere bloccati i propri agenti e collettori e, dopo aver ricevuto una notifica via e-mail relativa a una nuova versione, hanno una finestra di 30 giorni per aggiornare selettivamente gli agenti uno alla volta. Questo approccio riduce al minimo l'impatto della latenza sulle fpolicies e fornisce un maggiore controllo sul processo di aggiornamento.

Passaggi per installare l'agente

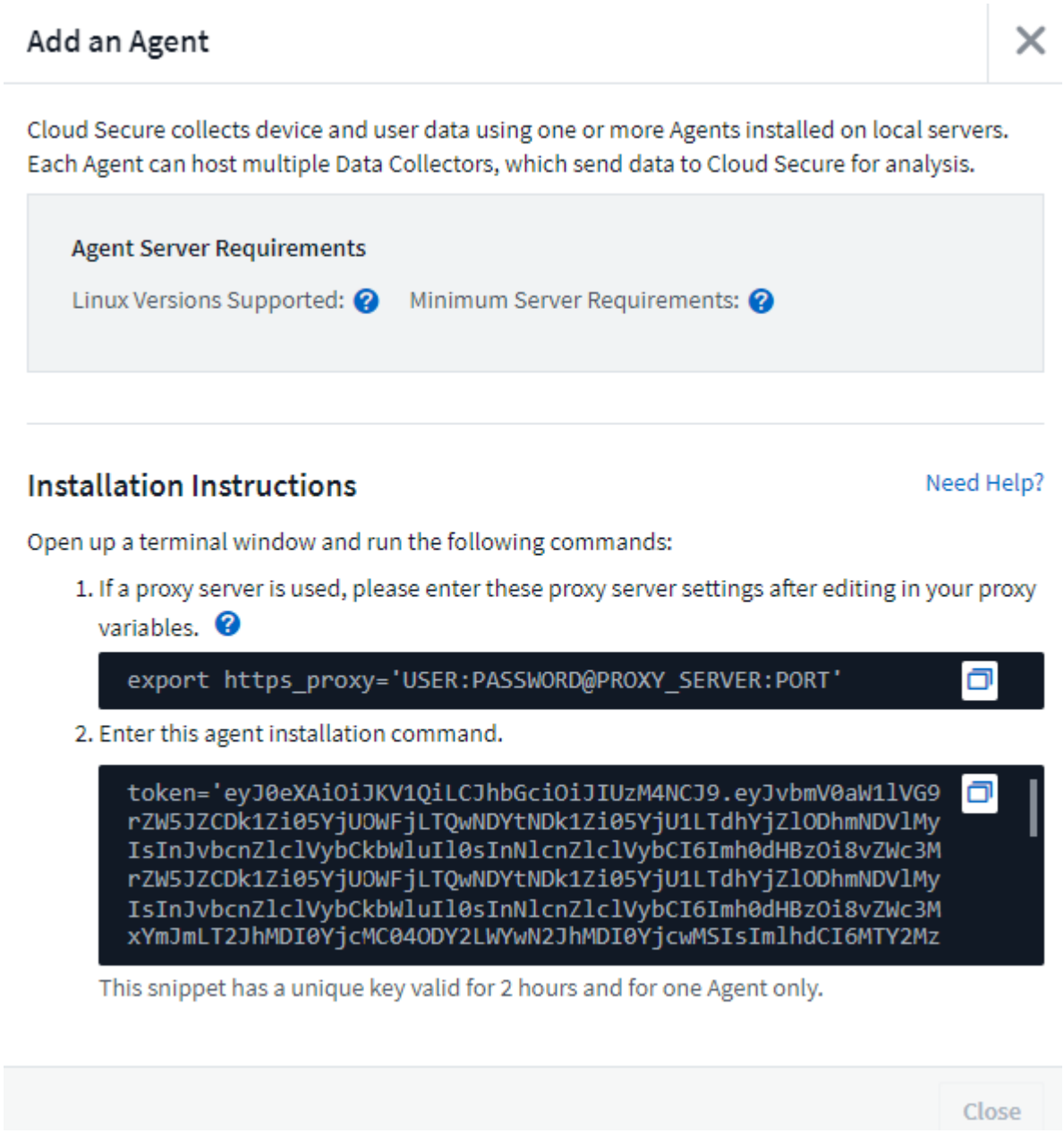
1. Accedi come amministratore o proprietario dell'account al tuo ambiente Workload Security.
2. Seleziona **Collezionisti > Agenti > +Agente**

   Il sistema visualizza la pagina Aggiungi un agente:



3. Verificare che il server agente soddisfi i requisiti minimi di sistema.

4. Per verificare che il server agente esegua una versione supportata di Linux, fare clic su *Versioni supportate (i)*.
5. Se la tua rete utilizza un server proxy, imposta 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. Una volta completata correttamente l'installazione, il sistema visualizza il seguente messaggio:

Dopo aver finito

1. È necessario configurare un"Raccoglitore di directory utente" .
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. Se l'intervallo di porte presenta problemi di sicurezza, è possibile utilizzare un intervallo di porte inferiore, ad esempio *35000:35100*. Ogni SVM utilizza due porte.

Passi

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

Segui i passaggi successivi in base alla tua piattaforma:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Esempio di output:

```
 -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)

Esempio di output:

```
35000-55000/tcp
```

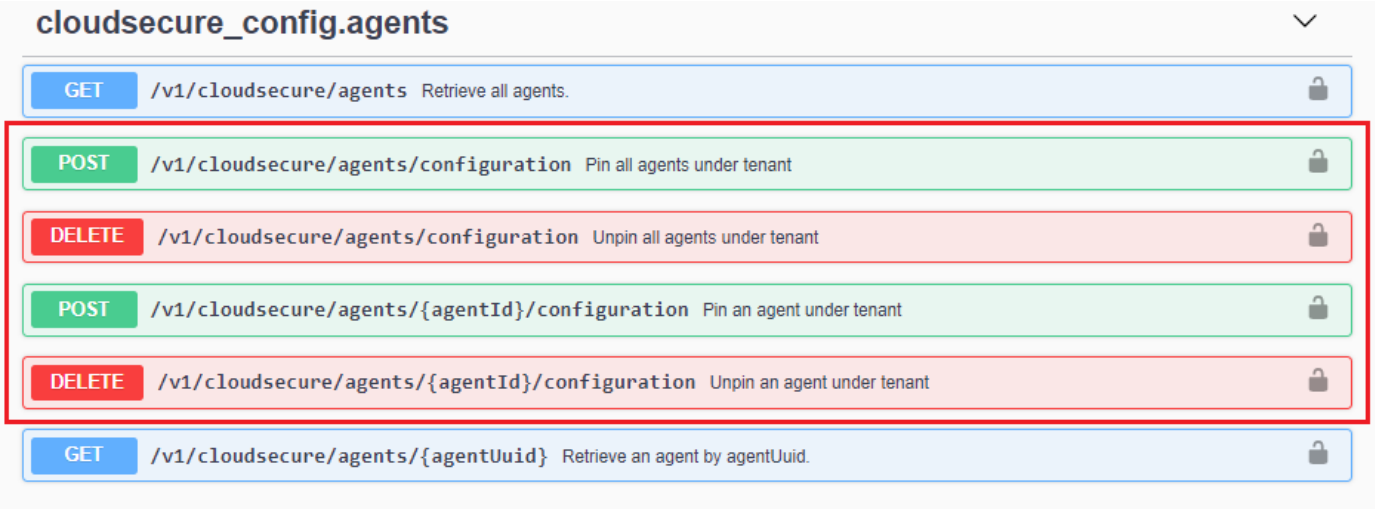
"Fissare" un agente alla versione corrente

Per impostazione predefinita, Data Infrastructure Insights Workload Security aggiorna automaticamente gli agenti. Alcuni clienti potrebbero voler sospendere l'aggiornamento automatico, lasciando un agente alla sua versione corrente finché non si verifica una delle seguenti situazioni:

- Il cliente riprende gli aggiornamenti automatici dell'agente.
- Sono trascorsi 30 giorni. Si noti che i 30 giorni iniziano il giorno dell'aggiornamento più recente dell'agente, non il giorno in cui l'agente è in pausa.

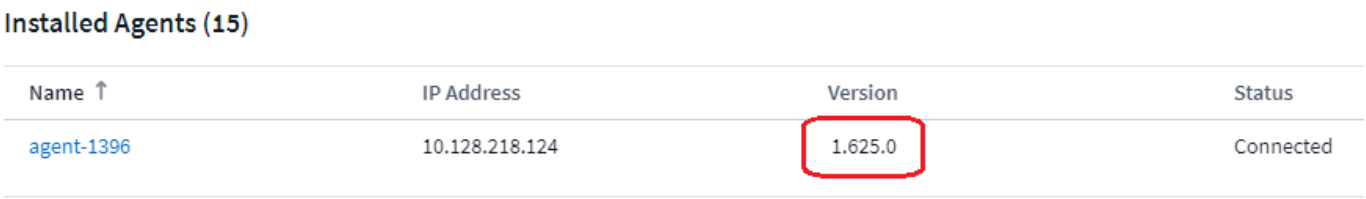
In ognuno di questi casi, l'agente verrà aggiornato al successivo aggiornamento di Workload Security.

Per sospendere o riprendere gli aggiornamenti automatici degli agenti, utilizzare le API *cloudsecure_config.agents*:



Tieni presente che potrebbero essere necessari fino a cinque minuti prima che l'azione di pausa o ripresa abbia effetto.

È possibile visualizzare le versioni correnti degli Agent nella pagina **Sicurezza del carico di lavoro > Collettori**, nella scheda **Agenti**.



Risoluzione dei problemi degli errori dell'agente

Nella tabella seguente sono descritti i problemi noti e le relative soluzioni.

Problema:	Risoluzione:
L'installazione dell'agente non riesce a creare la cartella /opt/netapp/cloudsecure/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 registro perché si verifica prima dell'inizializzazione del logger. L'errore viene reindirizzato all'output standard ed è visibile nel registro del servizio utilizzando `journalctl -u cloudsecure-agent.service` comando. Questo comando può essere utilizzato per risolvere ulteriormente il problema. est
L'installazione dell'agente fallisce con il messaggio "Questa distribuzione Linux non è supportata". Uscita dall'installazione.	Questo errore viene visualizzato quando si tenta di installare l'agente su un sistema non supportato. Vedere "Requisiti dell'agente" .

Problema:	Risoluzione:
L'installazione dell'agente non è riuscita con l'errore: "-bash: unzip: comando non trovato"	Installa unzip e poi esegui nuovamente il comando di installazione. Se Yum è installato sul computer, prova "yum install unzip" per installare il software di decompressione. Dopodiché, copia nuovamente il comando dall'interfaccia utente di installazione dell'agente e incollalo nella CLI per eseguire nuovamente l'installazione.
L'agente è stato installato ed è in esecuzione. Tuttavia l'agente si è fermato all'improvviso.	Eseguire l'SSH sulla macchina 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 daemon Workload Security". 2. Verificare se l'utente cssys esiste o meno nella macchina dell'agente. Eseguire i seguenti comandi uno alla volta con i permessi di root e verificare se l'utente e il gruppo cssys esistono. `sudo id cssys` `sudo groups cssys` 3. Se non ne esiste nessuno, è possibile che un criterio di monitoraggio centralizzato abbia eliminato l'utente cssys. 4. Creare manualmente l'utente e il gruppo cssys eseguendo i seguenti comandi. `sudo useradd cssys` `sudo groupadd cssys` 5. Successivamente riavviare il servizio agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service` 6. Se il problema persiste, controlla le altre opzioni di risoluzione dei problemi.
Impossibile aggiungere più di 50 raccoglitori di dati a un agente.	È possibile aggiungere solo 50 raccoglitori di dati a un agente. Può trattarsi di una combinazione di tutti i tipi di collettori, ad esempio Active Directory, SVM e altri collettori.
L'interfaccia utente mostra che l'agente è nello stato NOT_CONNECTED.	Passaggi per riavviare l'agente. 1. Eseguire l'SSH sulla macchina dell'agente. 2. Successivamente riavviare il servizio agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service` 3. Controllare lo stato del servizio agente tramite `sudo systemctl status cloudsecure-agent.service` . 4. L'agente dovrebbe passare allo stato CONNESSO.
L'agente VM si trova dietro il proxy Zscaler e l'installazione dell'agente non riesce. A causa dell'ispezione SSL del proxy Zscaler, i certificati di sicurezza del carico di lavoro vengono presentati così come sono firmati dalla CA Zscaler, quindi l'agente non si fida della comunicazione.	Disabilitare l'ispezione SSL nel proxy Zscaler per l'URL *.cloudinsights.netapp.com. Se Zscaler esegue l'ispezione SSL e sostituisce i certificati, Workload Security non funzionerà.

Problema:	Risoluzione:
Durante l’installazione dell’agente, l’installazione si blocca dopo la decompressione.	Il comando "chmod 755 -Rf" non funziona. Il comando fallisce 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 riuscito, il resto dell’installazione non viene eseguito. 1. Crea una nuova directory denominata “cloudsecure”. 2. Vai a quella directory. 3. Copia e incolla il comando di installazione completo “token=…… … ./cloudsecure-agent-install.sh" e premi Invio. 4. L’installazione dovrebbe poter procedere.
Se l’agente non riesce ancora a connettersi a Saas, aprire un caso con il supporto NetApp . Fornire il numero di serie Data Infrastructure Insights per aprire un caso e allegare i registri al caso come indicato.	Per allegare i registri alla custodia: 1. Eseguire lo script seguente con i permessi di 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 per uno con i permessi di root e condividere l’output. a. id cssys b. groups cssys c. cat /etc/os-release
Lo script cloudsecure-agent-symptom-collector.sh non riesce e restituisce il seguente errore. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Raccolta del registro di servizio Raccolta dei registri delle applicazioni Raccolta delle configurazioni degli agenti Acquisizione di uno snapshot dello stato del servizio Acquisizione di uno snapshot della struttura delle directory degli agenti ……. ……. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh: riga 52: zip: comando non trovato ERRORE: 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 nuovamente cloudsecure-agent-symptom-collector.sh.
L’installazione dell’agente fallisce con useradd: impossibile creare la directory /home/cssys	Questo errore può verificarsi se la directory di accesso dell’utente non può essere creata in /home, a causa della mancanza di autorizzazioni. La soluzione alternativa sarebbe quella di creare l’utente cssys e aggiungere manualmente la sua directory di accesso utilizzando il seguente comando: *sudo useradd user_name -m -d HOME_DIR* -m : crea la directory home 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 sua directory di accesso nella root.

Problema:	Risoluzione:
L'agente non è in esecuzione dopo l'installazione. *Systemctl status cloudsecure-agent.service* mostra quanto segue: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Servizio Daemon dell'agente di sicurezza del carico di lavoro Caricato: caricato (/usr/lib/systemd/system/cloudsecure-agent.service; abilitato; preimpostazione del fornitore: disabilitato) Attivo: attivazione (riavvio automatico) (Risultato: codice di uscita) da mar 2021-08-03 21:12:26 PDT; 2s fa Processo: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (codice=uscito stato=126) PID principale: 25889 (codice=uscito, stato=126), 03 ago 21:12:26 demo systemd[1]: cloudsecure-agent.service: processo principale uscito, codice=uscito, stato=126/n/d 03 ago 21:12:26 demo systemd[1]: l'unità cloudsecure-agent.service è entrata in stato di errore. 03 ago 21:12:26 demo systemd[1]: cloudsecure-agent.service non riuscito.	Questa operazione potrebbe non riuscire perché l'utente *cssys* potrebbe non avere l'autorizzazione per l'installazione. Se /opt/netapp è un mount NFS e se l'utente *cssys* non ha accesso a questa cartella, l'installazione non riuscirà. *cssys* è un utente locale creato dal programma di installazione di Workload Security che potrebbe non avere l'autorizzazione per accedere alla condivisione montata. È possibile verificarlo provando ad accedere a /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent utilizzando l'utente *cssys*. Se restituisce "Autorizzazione negata", l'autorizzazione all'installazione non è presente. Invece di una cartella montata, installa su una directory locale della macchina.
Inizialmente l'agente era connesso tramite un server proxy e il proxy è stato impostato durante l'installazione dell'agente. Ora il server proxy è cambiato. Come si può modificare la configurazione proxy dell'agente?	È possibile modificare agent.properties per aggiungere i dettagli del proxy. Seguire questi passaggi: 1. Passare alla cartella contenente il file delle proprietà: cd /opt/netapp/cloudsecure/conf 2. Utilizzando il tuo editor di testo preferito, apri il file *agent.properties* per modificarlo. 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. Salva il file. 5. Riavviare l'agente: sudo systemctl restart cloudsecure-agent.service

Eliminazione di un agente di sicurezza del carico di lavoro

Quando si elimina un Workload Security Agent, è necessario eliminare prima tutti i raccoglitori di dati 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 raccoglitori dati con un agente diverso, è necessario creare un backup delle configurazioni del raccoglitore dati prima di eliminare l'agente.

Prima di iniziare

1. Assicurarsi che tutti i raccoglitori di dati associati all'agente vengano eliminati dal portale Workload Security.

   Nota: ignorare questo passaggio se tutti i collettori associati sono nello stato STOPPED.

Passaggi per eliminare un agente:

1. Accedi tramite SSH alla VM dell'agente ed esegui 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 > Collettori > Agenti**

   Il sistema visualizza l'elenco degli agenti configurati.

3. Fare clic sul menu delle opzioni per l'agente che si desidera eliminare.
4. Fare clic su **Elimina**.

   Il sistema visualizza la pagina **Elimina agente**.

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

Configurazione di un raccoglitore di directory utente di Active Directory (AD)

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

Prima di iniziare

- Per eseguire questa attività, devi 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 Directory utente, è necessario configurare un agente.

Passaggi per configurare un raccoglitore di directory utente

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

   Il sistema visualizza la schermata Aggiungi directory utente.

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

Nome	Descrizione
Nome	Nome univoco per la directory utente. Ad esempio *GlobalADCollector*
Agente	Seleziona un agente configurato dall'elenco
IP del server/nome di dominio	Indirizzo IP o nome di dominio completo (FQDN) del server che ospita Active Directory

Nome della foresta	Livello foresta della struttura delle directory. Il nome della foresta consente entrambi i seguenti formati: *x.y.z* ⇒ nome di dominio diretto così come è presente sulla SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nomi distinti relativi [Esempio: DC=hq,DC= companyname,DC=com] Oppure puoi specificare come segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [per filtrare in base a OU engineering specifica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [per ottenere solo un utente specifico con <username> da OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [per ottenere tutti gli utenti Acrobat all'interno degli utenti di quell'organizzazione] Sono supportati anche i domini Active Directory attendibili.
Associa DN	Utente autorizzato a effettuare ricerche nella directory. Ad esempio: *username@companyname.com* oppure *username@domainname.com* Inoltre, è richiesta l'autorizzazione di sola lettura del dominio. L'utente deve essere membro del gruppo di sicurezza *Controller di dominio di sola lettura*.
Password BIND	Password del server di directory (ovvero password per il nome utente utilizzato in Bind DN)
Protocollo	ldap, ldaps, ldap-start-tls
porti	Seleziona la porta

Immettere i seguenti attributi obbligatori del Directory Server se i nomi degli attributi predefiniti sono stati modificati in Active Directory. Nella maggior parte dei casi i nomi di questi attributi *non* vengono modificati in Active Directory, nel qual caso è possibile procedere semplicemente con il nome di attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome da visualizzare	nome
SID	oggetti
Nome utente	sAMAccountName

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

Attributi	Nome attributo nel server directory
Indirizzo e-mail	posta
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato

Dipartimento	dipartimento
Foto	miniatura della foto
ManagerDN	manager
Gruppi	membroDi

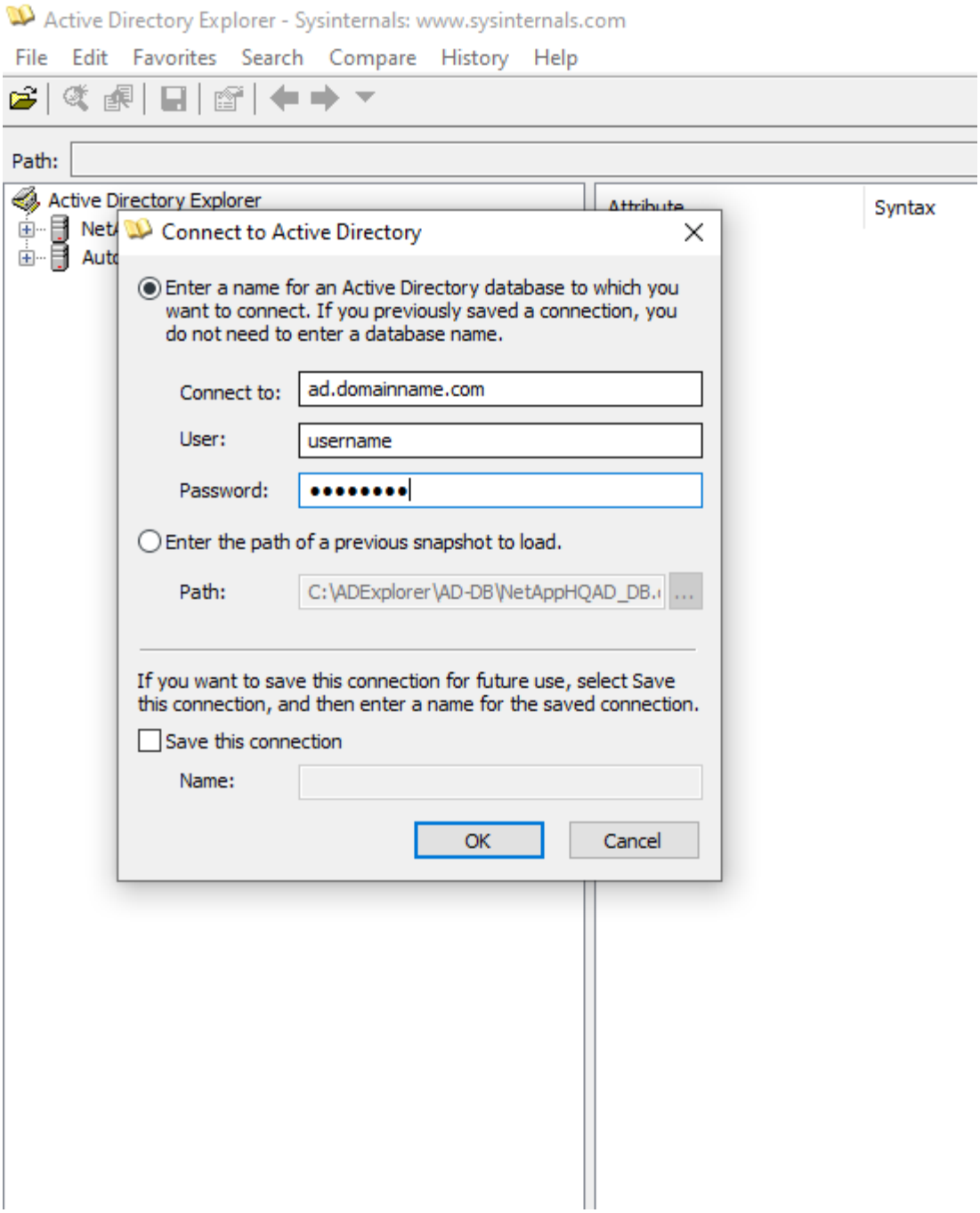
Test della configurazione del raccoglitore di directory utente

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

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP di Workload Security:

  ```
  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 e rieseguire.
  - Installare"Esploratore AD" su qualsiasi macchina Windows in grado di connettersi al server AD.
  - Connettersi al server AD utilizzando il nome utente/password del server della directory AD.



Risoluzione dei problemi relativi agli errori di configurazione del raccoglitore directory utente

Nella tabella seguente vengono descritti i problemi noti e le relative soluzioni che possono verificarsi durante la configurazione del collettore:

Problema:	Risoluzione:
L'aggiunta di un connettore Directory utente genera lo stato "Errore". L'errore dice: "Credenziali non valide fornite per il server LDAP".	Nome utente o password forniti non corretti. Modifica e fornisci il nome utente e la password corretti.

Problema:	Risoluzione:
L’aggiunta di un connettore Directory utente genera lo stato "Errore". L’errore dice: "Impossibile ottenere l’oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome foresta".	Nome foresta fornito errato. Modifica e fornisci il nome corretto della foresta.
Gli attributi facoltativi dell’utente di dominio non vengono visualizzati nella pagina Profilo utente di Workload Security.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. Modifica e fornisci i nomi corretti degli attributi facoltativi.
Il raccoglitore dati è in stato di errore con "Impossibile recuperare gli utenti LDAP. Motivo dell’errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore cliccando sul pulsante *Riavvia*.
L’aggiunta di un connettore Directory utente genera lo stato "Errore".	Assicurati di aver fornito valori validi per i campi obbligatori (Server, nome foresta, DN di associazione, password di associazione). Assicurarsi che l’input bind-DN sia sempre fornito come 'Administrator@<domain_forest_name>' o come account utente con privilegi di amministratore di dominio.
L’aggiunta di un connettore Directory utente determina lo stato "RITIRO". Mostra l’errore "Impossibile definire lo stato del collettore, motivo per cui il comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] non è riuscito a causa di java.net.ConnectionException:Connessione rifiutata."	IP o FQDN non corretti forniti per il server AD. Modifica e fornisci l’indirizzo IP o il nome di dominio completo (FQDN) corretto.
L’aggiunta di un connettore Directory utente genera lo stato "Errore". L’errore dice: "Impossibile stabilire la connessione LDAP".	IP o FQDN non corretti forniti per il server AD. Modifica e fornisci l’indirizzo IP o il nome di dominio completo (FQDN) corretto.
L’aggiunta di un connettore Directory utente genera lo stato "Errore". L’errore dice: "Impossibile caricare le impostazioni. Motivo: la configurazione dell’origine dati presenta un errore. Motivo specifico: /connector/conf/application.conf: 70: ldap.ldap-port ha il tipo STRING anziché NUMBER”	Valore non corretto 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 ha funzionato. Dopo aver aggiunto quelli facoltativi, i dati degli attributi facoltativi non vengono recuperati da AD.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. Modifica e fornisci il nome corretto dell’attributo obbligatorio o facoltativo.
Dopo aver riavviato il collector, quando avverrà la sincronizzazione AD?	La sincronizzazione AD avverrà immediatamente dopo il riavvio del collector. Ci vorranno circa 15 minuti per recuperare i dati di circa 300.000 utenti e i dati vengono aggiornati automaticamente ogni 12 ore.

Problema:	Risoluzione:
I dati utente vengono sincronizzati da AD a CloudSecure. Quando verranno eliminati i dati?	In caso di mancato aggiornamento, i dati dell'utente vengono conservati per 13 mesi. Se l'inquilino viene eliminato, anche i dati verranno eliminati.
Il connettore della directory utente genera lo stato "Errore". "Il connettore è in stato di errore. Nome del servizio: usersLdap. Motivo dell'errore: impossibile recuperare gli utenti LDAP. Motivo dell'errore: 80090308: LdapErr: DSID-0C090453, commento: errore AcceptSecurityContext, dati 52e, v3839"	Nome foresta fornito errato. Per informazioni su come fornire il nome corretto della foresta, vedere sopra.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Molto probabilmente ciò è dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare lo specifico raccoglitore di Active Directory che recupera le informazioni dell'utente da Active Directory. 2. Si noti che tra gli attributi facoltativi è presente un campo denominato "Numero di telefono" mappato all'attributo di Active Directory "telephonenumber". 4. Ora, utilizzare lo strumento Active Directory Explorer come descritto sopra per esplorare Active Directory e visualizzare il nome corretto dell'attributo. 3. Assicurarsi che in Active Directory sia presente un attributo denominato "numero di telefono" che contenga effettivamente il numero di telefono dell'utente. 5. Supponiamo che in Active Directory sia stato modificato in "numero di telefono". 6. Quindi modifica il raccoglitore CloudSecure User Directory. Nella sezione degli attributi facoltativi, sostituire 'telephonenumber' con 'phonenumber'. 7. Salvare il raccoglitore di Active Directory, il raccoglitore verrà riavviato e otterrà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è abilitato sul server Active Directory (AD), Workload Security User Directory Collector non può connettersi al server AD.	Disattivare la crittografia del server AD prima di configurare un User Directory Collector. Una volta recuperati, i dati dell'utente rimarranno disponibili per 13 mesi. Se il server AD viene disconnesso dopo aver recuperato i dettagli dell'utente, gli utenti appena aggiunti in AD non verranno recuperati. Per effettuare nuovamente il recupero, il raccoglitore di directory utente deve essere connesso ad AD.
I dati di Active Directory sono presenti in CloudInsights Security. Vuoi 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 server di raccolta directory LDAP

È possibile configurare Workload Security per raccogliere gli attributi utente dai server della directory LDAP.

Prima di iniziare

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

Passaggi per configurare un raccoglitore di directory utente

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

   Il sistema visualizza la schermata Aggiungi directory utente.

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

Nome	Descrizione
Nome	Nome univoco per la directory utente. Ad esempio *GlobalLDAPCollector*
Agente	Seleziona un agente configurato dall'elenco
IP del server/nome di dominio	Indirizzo IP o nome di dominio completo (FQDN) del server che ospita il server di directory LDAP
Base di ricerca	Base di ricerca del server LDAP La base di ricerca consente entrambi i seguenti formati: *x.y.z* ⇒ nome di dominio diretto così come è presente sul tuo SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ Nomi distinti relativi [Esempio: DC=hq,DC= companyname,DC=com] Oppure puoi specificare come segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [per filtrare in base a OU engineering specifica] *CN=username,OU=engineering,DC=companyname, DC=netapp, DC=com* [per ottenere solo un utente specifico con <username> da OU <engineering>] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com ,O= companyname,L=Boston,S=MA,C=US* [per ottenere tutti gli utenti Acrobat all'interno degli utenti di quell'organizzazione]
Associa DN	Utente autorizzato a effettuare ricerche nella directory. Ad esempio: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=c ompanyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company ,dc=com per un utente john@dorp.company.com. dorp.company.com
--conti	--utenti
--Giovanni	--anna
Password BIND	Password del server di directory (ovvero password per il nome utente utilizzato in Bind DN)

Protocollo	ldap, ldaps, ldap-start-tls
porti	Seleziona la porta

Immettere i seguenti attributi obbligatori del Directory Server se i nomi degli attributi predefiniti sono stati modificati nel Directory Server LDAP. Nella maggior parte dei casi i nomi di questi attributi non vengono modificati in LDAP Directory Server, nel qual caso è possibile procedere semplicemente con il nome dell'attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome da visualizzare	nome
UNIXID	numero uid
Nome utente	fluido

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

Attributi	Nome attributo nel server directory
Indirizzo e-mail	posta
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato
Dipartimento	numerodipartimento
Foto	foto
ManagerDN	manager
Gruppi	membroDi

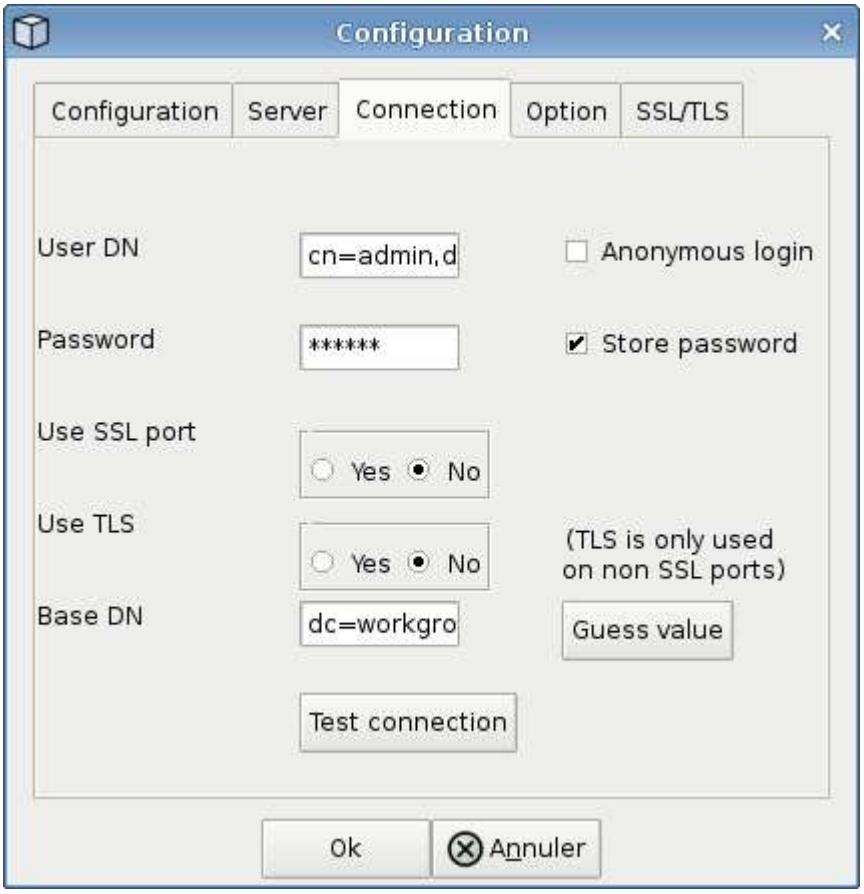
Test della configurazione del raccoglitore di directory utente

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

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP di Workload Security:

```
 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 e rieseguire.
```

- Installa LDAP Explorer(http://ldaptool.sourceforge.net/) o Java LDAP Explorer(http://jxplorer.org/) su qualsiasi macchina Windows in grado di connettersi al server LDAP.
- Connettersi al server LDAP utilizzando il nome utente/password del server di directory LDAP.



Risoluzione dei problemi di configurazione del raccoglitore directory LDAP

Nella tabella seguente vengono descritti i problemi noti e le relative soluzioni che possono verificarsi durante la configurazione del collettore:

Problema:	Risoluzione:
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Credenziali non valide fornite per il server LDAP".	Bind DN o Bind Password o Search Base forniti non corretti. Modifica e fornisci le informazioni corrette.
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Impossibile ottenere l'oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome foresta".	Base di ricerca fornita errata. Modifica e fornisci il nome corretto della foresta.
Gli attributi facoltativi dell'utente di dominio non vengono visualizzati nella pagina Profilo utente di Workload Security.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. I campi sono sensibili alle maiuscole e alle minuscole. Modifica e fornisci i nomi corretti degli attributi facoltativi.

Problema:	Risoluzione:
Il raccoglitore dati è in stato di errore con "Impossibile recuperare gli utenti LDAP. Motivo dell'errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore cliccando sul pulsante *Riavvia*.
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore".	Assicurati di aver fornito valori validi per i campi obbligatori (Server, nome foresta, DN di associazione, password di associazione). 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 "RITIRO". Mostra l'errore "Impossibile determinare lo stato del collettore, quindi 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 errore: "Impossibile determinare lo stato del collector entro 2 tentativi, provare a riavviare nuovamente il collector (codice errore: AGENT008)"	Assicurarsi che siano forniti l'IP del server e la base di ricerca corretti
L'aggiunta di un connettore di directory LDAP determina lo stato "RITIRO". Mostra l'errore "Impossibile definire lo stato del collettore, motivo per cui il comando TCP [Connect(localhost:35012,None,List(),Some(,seconds),true)] non è riuscito a causa di java.net.ConnectionException:Connessione rifiutata."	IP o FQDN non corretti forniti per il server AD. Modifica e fornisci l'indirizzo IP o il nome di dominio completo (FQDN) corretto. ////
L'aggiunta di un connettore di directory LDAP genera lo stato "Errore". L'errore dice: "Impossibile stabilire la connessione LDAP".	IP o FQDN non corretti forniti per il server LDAP. Modifica e fornisci l'indirizzo IP o il nome di dominio completo (FQDN) corretto. Oppure 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 genera lo stato "Errore". L'errore dice: "Impossibile caricare le impostazioni. Motivo: la configurazione dell'origine dati presenta un errore. Motivo specifico: /connector/conf/application.conf: 70: ldap.ldap-port ha il tipo STRING anziché NUMBER"	Valore non corretto 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 ha funzionato. Dopo aver aggiunto quelli facoltativi, i dati degli attributi facoltativi non vengono recuperati da AD.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi facoltativi aggiunti in CloudSecure e i nomi effettivi degli attributi in Active Directory. Modifica e fornisci il nome corretto dell'attributo obbligatorio o facoltativo.
Dopo aver riavviato il collector, quando avverrà la sincronizzazione LDAP?	La sincronizzazione LDAP avverrà immediatamente dopo il riavvio del collector. Ci vorranno circa 15 minuti per recuperare i dati di circa 300.000 utenti e i dati vengono aggiornati automaticamente ogni 12 ore.

Problema:	Risoluzione:
I dati utente vengono sincronizzati da LDAP a CloudSecure. Quando verranno eliminati i dati?	In caso di mancato aggiornamento, i dati dell'utente vengono conservati per 13 mesi. Se l'inquilino viene eliminato, anche i dati verranno eliminati.
Il connettore della directory LDAP genera lo stato "Errore". "Il connettore è in stato di errore. Nome del servizio: usersLdap. Motivo dell'errore: impossibile recuperare gli utenti LDAP. Motivo dell'errore: 80090308: LdapErr: DSID-0C090453, commento: errore AcceptSecurityContext, dati 52e, v3839"	Nome foresta fornito errato. Per informazioni su come fornire il nome corretto della foresta, vedere sopra.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Molto probabilmente ciò è dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare lo specifico raccoglitore di Active Directory che recupera le informazioni dell'utente da Active Directory. 2. Si noti che tra gli attributi facoltativi è presente un campo denominato "Numero di telefono" mappato all'attributo di Active Directory "telephonenumber". 4. Ora, utilizzare lo strumento Active Directory Explorer come descritto sopra per esplorare il server della directory LDAP e visualizzare il nome corretto dell'attributo. 3. Assicurarsi che nella directory LDAP sia presente un attributo denominato "numero di telefono" che contenga effettivamente il numero di telefono dell'utente. 5. Supponiamo che nella directory LDAP sia stato modificato in "numero di telefono". 6. Quindi modifica il raccoglitore CloudSecure User Directory. Nella sezione degli attributi facoltativi, sostituire 'telephonenumber' con 'phonenumber'. 7. Salvare il raccoglitore di Active Directory, il raccoglitore verrà riavviato e otterrà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è abilitato sul server Active Directory (AD), Workload Security User Directory Collector non può connettersi al server AD.	Disattivare la crittografia del server AD prima di configurare un User Directory Collector. Una volta recuperati, i dati dell'utente rimarranno disponibili per 13 mesi. Se il server AD viene disconnesso dopo aver recuperato i dettagli dell'utente, gli utenti appena aggiunti in AD non verranno recuperati. Per recuperare nuovamente la directory utente, è necessario connettersi ad AD.

Configurazione del raccoglitore dati ONTAP SVM

ONTAP SVM Data Collector consente a Workload Security di monitorare le attività di accesso ai file e agli utenti sulle macchine virtuali di storage (SVM) NetApp ONTAP . Questa guida illustra la configurazione e la gestione del raccoglitore dati SVM per garantire un monitoraggio completo della sicurezza del tuo ambiente ONTAP .

Prima di iniziare

- Questo raccoglitore di dati è supportato da quanto segue:
  - Data ONTAP 9.2 e versioni successive. Per prestazioni ottimali, utilizzare una versione Data ONTAP successiva alla 9.13.1.
  - Protocollo SMB versione 3.1 e precedenti.
  - Versioni NFS fino a NFS 4.1 inclusa (si noti che NFS 4.1 è supportato con ONTAP 9.15 o versioni successive).
  - Flexgroup è supportato da ONTAP 9.4 e versioni successive
  - FlexCache è supportato per NFS con ONTAP 9.7 e versioni successive.
  - FlexCache è supportato per SMB con ONTAP 9.14.1 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 raccoglitori di dati.
- Assicurati di avere configurato correttamente un connettore directory utente, altrimenti gli eventi mostreranno nomi utente codificati e non il nome effettivo dell'utente (come memorizzato in Active Directory) nella pagina "Attività forense".
- ONTAP Persistent Store è supportato dalla versione 9.14.1.
- Per prestazioni ottimali, è consigliabile configurare il server FPolicy in modo che si trovi sulla stessa subnet del sistema di archiviazione.
- Per le migliori pratiche e raccomandazioni complete riguardanti la configurazione di Workload Security FPolicy, vedere"Articolo della Knowledge Base sulle migliori pratiche di FPolicy" .
- 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 esattamente come mostrato in ONTAP e deve essere sensibile alle maiuscole e alle minuscole.
  - Utilizzando l'IP di gestione del server virtuale SVM, nome utente e password
  - Se non si è in grado o non si desidera utilizzare il nome utente e la password completi di gestione del cluster/SVM dell'amministratore, è possibile creare un utente personalizzato con privilegi inferiori come indicato in"Una nota sui permessi" sezione sottostante. Questo utente personalizzato può essere creato per l'accesso SVM o Cluster.
    - È anche possibile utilizzare un utente AD con un ruolo che abbia almeno le autorizzazioni di csrole, come indicato nella sezione "Nota sulle autorizzazioni" di seguito. Fare riferimento anche a"Documentazione ONTAP" .
- Assicurarsi che siano impostate le applicazioni corrette per l'SVM eseguendo il seguente comando:

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

Esempio di

output:

```
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.
```

- Assicurarsi che l'SVM abbia un server CIFS configurato: clustershell:> `vserver cifs show`

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

- Imposta una password per l'utente SVM vsadmin. Se si utilizza un utente personalizzato o un utente amministratore del cluster, saltare questo passaggio. clustershell:> `security login password -username vsadmin -vserver svmname`
- Sbloccare l'utente SVM vsadmin per l'accesso esterno. Se si utilizza un utente personalizzato o un utente amministratore del cluster, saltare questo passaggio. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Assicurarsi che la policy del firewall dei dati LIF sia impostata su 'mgmt' (non 'data'). Salta questo passaggio se utilizzi un lif di gestione dedicato per aggiungere l'SVM. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Quando un firewall è abilitato, è necessario definire un'eccezione per consentire il traffico TCP per la porta utilizzando Data ONTAP Data Collector.

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

- Quando un agente viene installato in un'istanza AWS EC2 per monitorare un Cloud ONTAP SVM, l'agente e lo storage devono trovarsi nella stessa VPC. Se si trovano in VPC separate, deve esserci un percorso valido tra le VPC.

Test di connettività per i collettori di dati

La funzionalità di test della connettività (introdotta a marzo 2025) ha lo scopo di aiutare gli utenti finali a identificare le cause specifiche dei guasti durante la configurazione dei raccoglitori di dati in Data Infrastructure Insights (DII) Workload Security. Ciò consente agli utenti di correggere autonomamente i problemi relativi alla comunicazione di rete o ai ruoli mancanti.

Questa funzionalità aiuterà gli utenti a determinare se tutti i controlli relativi alla rete sono stati eseguiti prima di configurare un raccoglitore dati. Inoltre, informerà gli utenti sulle funzionalità a cui possono accedere in base alla versione ONTAP , ai ruoli e alle autorizzazioni loro assegnate in ONTAP.

La connettività di prova non è supportata per i collettori di directory utente

Prerequisiti per il test di connessione

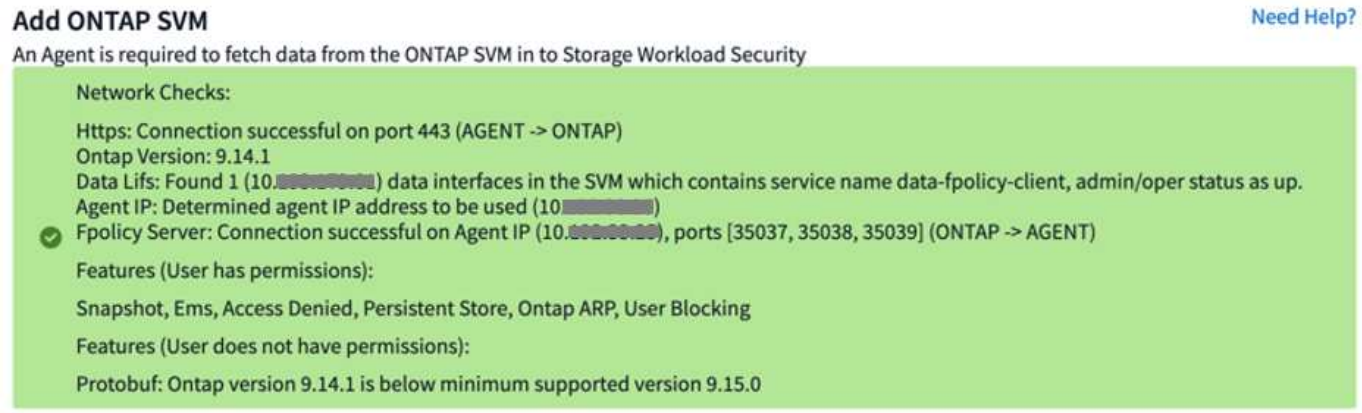
- Per il pieno funzionamento di questa funzionalità sono necessarie le credenziali a livello di cluster.
- Il controllo dell'accesso alle funzionalità non è supportato in modalità SVM.

- Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.
- Se si utilizza un utente personalizzato (ad esempio, *csuser*), fornire le autorizzazioni obbligatorie e le autorizzazioni specifiche per le funzionalità che si desidera utilizzare.

Assicurati di rivedere ilPermessi anche nella sezione sottostante.

Testare la connessione

L'utente può andare alla pagina Aggiungi/Modifica collettore, immettere i dettagli a livello di cluster (in modalità Cluster) o i dettagli a livello di SVM (in modalità SVM) e fare clic sul pulsante **Test connessione**. Workload Security elaborerà quindi la richiesta e visualizzerà un messaggio appropriato di successo o fallimento.



Cose da notare per ONTAP Multi Admin Verify (MAV)

Alcune funzionalità, come la creazione e l'eliminazione di snapshot o il blocco utente (SMB), potrebbero non funzionare in base ai comandi MAV aggiunti nella tua versione di ONTAP.

Seguire i passaggi indicati di seguito per aggiungere esclusioni ai comandi MAV che consentono a Workload Security di creare o eliminare snapshot e bloccare gli utenti.

Comandi per consentire la creazione e l'eliminazione di snapshot:

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Comando per consentire il blocco dell'utente:

```
multi-admin-verify rule delete -operation set
```

Prerequisiti per il blocco dell'accesso utente

Tieni presente quanto segue per"Blocco dell'accesso utente" :

Per il funzionamento di questa funzionalità sono necessarie le 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 concesse all'utente, seguire i passaggi in"Blocco dell'accesso utente" per concedere a Workload Security l'autorizzazione a bloccare l'utente.

Una nota sui permessi

Autorizzazioni durante l'aggiunta tramite IP di gestione cluster:

Se non è possibile utilizzare l'utente amministratore di gestione del cluster per consentire a Workload Security di accedere al raccoglitore dati ONTAP SVM, 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 raccoglitore dati Workload Security per utilizzare l'IP di gestione cluster.

Nota: è possibile creare un singolo ruolo da utilizzare per tutte le autorizzazioni delle funzionalità per un utente personalizzato. Se esiste già un utente, eliminare prima l'utente e il ruolo esistenti utilizzando questi comandi:

```
security login delete -user-or-group-name csuser -application *
security login role delete -role csrole -cmddirname *
security login rest-role delete -role csrestrole -api *
security login rest-role delete -role arwrole -api *
```

Per creare il nuovo utente, accedere a ONTAP con il nome utente/password dell'amministratore di 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 role create -role csrole -cmddirname "cluster application-
record" -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 durante l'aggiunta tramite IP di gestione Vserver:

Se non è possibile utilizzare l'utente amministratore di gestione del cluster per consentire a Workload Security di accedere al raccoglitore dati ONTAP SVM, 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 raccoglitore dati Workload Security per utilizzare l'IP di gestione Vserver.

Nota: è possibile creare un singolo ruolo da utilizzare per tutte le autorizzazioni delle funzionalità per un utente personalizzato. Se esiste già un utente, eliminare prima l'utente e il ruolo esistenti utilizzando questi comandi:

```
security login delete -user-or-group-name csuser -application * -vserver
<vservername>
security login role delete -role csrole -cmddirname * -vserver
<vservername>
security login rest-role delete -role csrestrole -api * -vserver
<vservername>
```

Per creare il nuovo utente, accedere a ONTAP con il nome utente e la password dell'amministratore di gestione del cluster ed eseguire i seguenti comandi sul server ONTAP . Per semplicità, copia questi comandi in un editor di testo e sostituisci <vservername> con il nome del tuo Vserver 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 abilitata nelle impostazioni *Configurazione avanzata* del raccoglitore. La modalità Protobuf è supportata nella versione ONTAP 9.15 e successive.

Maggiori dettagli su questa funzionalità possono essere trovati nel"Documentazione ONTAP" .

Per protobuf sono richieste autorizzazioni specifiche (alcune o tutte potrebbero già esistere):

Modalità cluster:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Modalità Vserver:
```

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

Autorizzazioni per la protezione autonoma da ransomware ONTAP e l'accesso negato a ONTAP

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

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi sottostanti per concedere a Workload Security le autorizzazioni per raccogliere informazioni relative ad ARP da ONTAP.

Per maggiori informazioni, leggi"Integrazione con ONTAP Accesso negato"

E"Integrazione con la protezione autonoma dai ransomware ONTAP"

Configurare il raccoglitore dati

Passaggi per la configurazione

1. Accedi come amministratore o proprietario dell'account al tuo ambiente Data Infrastructure Insights .
2. Fare clic su **Sicurezza del carico di lavoro > Collettori > +Collettori dati**

   Il sistema visualizza i Data Collector disponibili.

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

   Il sistema visualizza la pagina di configurazione ONTAP SVM. Inserisci i dati richiesti per ogni campo.

Campo	Descrizione
Nome	Nome univoco per il Data Collector
Agente	Selezionare un agente configurato dall'elenco.
Connettiti tramite IP di gestione per:	Selezionare l'IP del cluster o l'IP di gestione SVM
Indirizzo IP di gestione cluster/SVM	L'indirizzo IP per il cluster o l'SVM, a seconda della selezione effettuata sopra.
Nome SVM	Il nome dell'SVM (questo campo è obbligatorio quando ci si connette tramite IP del cluster)
Nome utente	Nome utente per accedere a SVM/Cluster Quando si aggiunge tramite IP del cluster, le opzioni sono: 1. Cluster-admin 2. 'csuser' 3. AD-user con ruolo simile a csuser. Quando si aggiunge tramite IP SVM le opzioni sono: 4. vsadmin 5. 'csuser' 6. AD-username ha un ruolo simile a csuser.
Password	Password per il nome utente sopra indicato
Filtra Condivisioni/Volumi	Scegli se includere o escludere Condivisioni/Volumi dalla raccolta eventi
Inserisci i nomi completi delle condivisioni da escludere/includere	Elenco separato da virgole delle azioni da escludere o includere (a seconda dei casi) dalla raccolta di eventi
Inserisci i nomi completi dei volumi da escludere/includere	Elenco separato da virgole dei volumi da escludere o includere (a seconda dei casi) dalla raccolta di eventi

Monitora l’accesso alle cartelle	Se selezionata, abilita gli eventi per il monitoraggio dell’accesso alle cartelle. Si noti che la creazione/rinomina e l’eliminazione delle cartelle verranno monitorate anche senza selezionare questa opzione. Abilitando questa opzione aumenterà il numero di eventi monitorati.
Imposta la dimensione del buffer di invio ONTAP	Imposta la dimensione del buffer di invio Fpolicy ONTAP . Se si utilizza una versione ONTAP precedente alla 9.8p7 e si riscontrano problemi di prestazioni, è possibile modificare la dimensione del buffer di invio ONTAP per ottenere prestazioni ONTAP migliori. Se non vedi questa opzione e desideri provarla, contatta l’assistenza NetApp .

Dopo aver finito

- Nella pagina Collettori dati installati, utilizzare il menu delle opzioni a destra di ciascun collettore per modificare il collettore dati. È possibile riavviare il raccoglitore dati o modificarne gli attributi di configurazione.

Configurazione consigliata per MetroCluster

Per MetroCluster si consiglia quanto segue:

1. Collegare due raccoglitori di dati, uno all’SVM di origine e l’altro all’SVM di destinazione.
2. I collettori di dati devono essere connessi tramite *Cluster IP*.
3. In qualsiasi momento, il raccoglitore dati dell’SVM attualmente in esecuzione verrà visualizzato come *In esecuzione*. Il raccoglitore dati dell’SVM attualmente 'arrestato' verrà visualizzato come *Arrestato*.
4. Ogni volta che si verifica un passaggio, lo stato del raccoglitore dati cambierà da *In esecuzione* a *Arrestato* e viceversa.
5. Ci vorranno fino a due minuti affinché il raccoglitore dati passi dallo stato *Arrestato* allo stato *In esecuzione*.

Politica di servizio

Se si utilizza la policy 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 9.9.1, non è necessario impostare *data-fpolicy-client*.

Raccolta dati di riproduzione e pausa

Se il Data Collector è in stato *In esecuzione*, è possibile mettere in pausa la raccolta. Aprire il menu "tre punti" del raccoglitore e selezionare PAUSA. Mentre il collettore è in pausa, nessun dato viene raccolto da ONTAP e

nessun dato viene inviato dal collettore a ONTAP. Ciò significa che nessun evento Fpolicy verrà trasmesso da ONTAP al raccoglitore dati e da lì a Data Infrastructure Insights.

Si noti che se vengono creati nuovi volumi, ecc. su ONTAP mentre il raccoglitore è in pausa, Workload Security non raccoglierà i dati e tali volumi, ecc. non verranno visualizzati nei dashboard o nelle tabelle.

Un collector non può essere messo in pausa se ha utenti limitati. Ripristinare l'accesso dell'utente prima di mettere in pausa il raccoglitore.

Tieni presente quanto segue:

- L'eliminazione degli snapshot non avverrà secondo le impostazioni configurate su un collector in pausa.
- Gli eventi EMS (come ONTAP ARP) non verranno elaborati su un collector in pausa. Ciò significa che se ONTAP identifica un attacco di manomissione dei file, Data Infrastructure Insights Workload Security non sarà in grado di acquisire quell'evento.
- Le email di notifica sullo stato di salute NON verranno inviate per un raccoglitore in pausa.
- Le azioni manuali o automatiche (ad esempio Snapshot o Blocco utente) non saranno supportate su un collector in pausa.
- Durante gli aggiornamenti dell'agente o del collettore, i riavvii/riavvii della VM dell'agente o il riavvio del servizio dell'agente, un collettore in pausa rimarrà nello stato *Paused*.
- Se il raccoglitore dati è nello stato *Errore*, non è possibile modificarlo nello stato *Pausa*. Il pulsante Pausa sarà abilitato solo se lo stato del raccoglitore è *In esecuzione*.
- Se l'agente è disconnesso, non è possibile modificare lo stato del collettore in *Pausa*. Il raccoglitore passerà allo stato *Arrestato* e il pulsante Pausa verrà disabilitato.

Archivio persistente

L'archivio persistente è supportato con ONTAP 9.14.1 e versioni successive. Si noti che le istruzioni relative al nome del volume variano da ONTAP 9.14 a 9.15.

È possibile abilitare Persistent Store 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 abilitare Persistent Store.

- Per ONTAP 9.14.1, è necessario creare il volume prima di abilitare la funzionalità e fornire lo stesso nome nel campo *Nome volume*. La dimensione consigliata del volume è 16 GB.
- Per ONTAP 9.15.1, il volume verrà creato automaticamente con una dimensione di 16 GB dal collettore, utilizzando il nome fornito nel campo *Nome volume*.

Per Persistent Store sono necessarie autorizzazioni specifiche (alcune o tutte potrebbero già esistere):

Modalità cluster:

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "job show" -access
readonly
```

Modalità Vserver:

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"job show" -access readonly
```

Migrazione dei collezionisti

È possibile migrare facilmente un collettore Workload Security da un agente all'altro, consentendo un efficiente bilanciamento del carico dei collettori tra gli agenti.

Prerequisiti

- L'agente sorgente deve essere nello stato *connesso*.
- Il collector da migrare deve essere nello stato *running*.

Nota:

- La migrazione è supportata sia per i raccoglitori di dati che per quelli di directory utente.
- La migrazione di un collector non è supportata per i tenant gestiti manualmente.

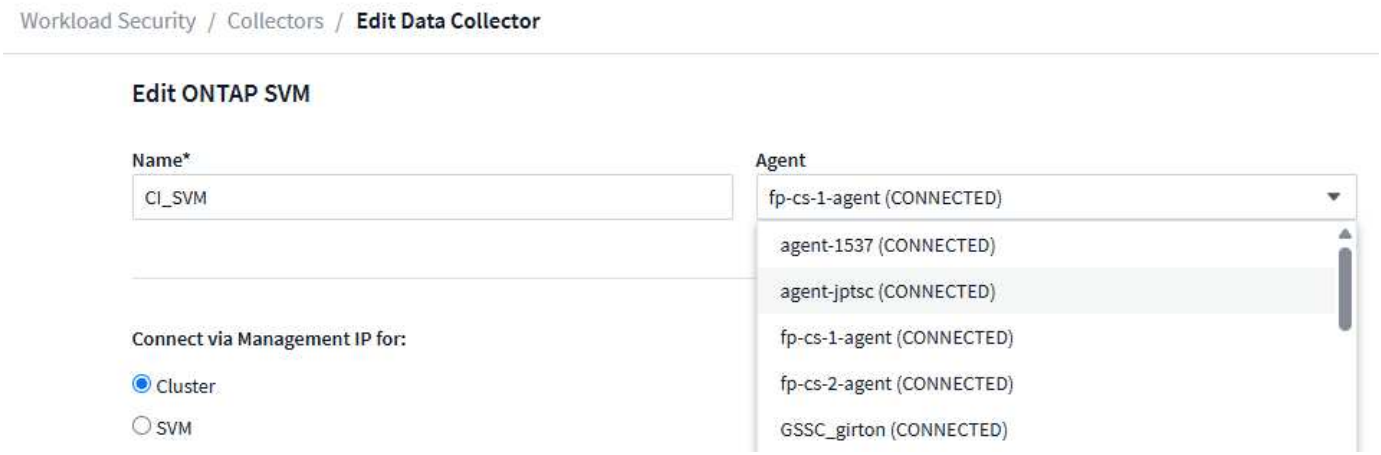
Migrare il raccoglitore

Per migrare un collector, seguire questi passaggi:

1. Vai alla pagina "Modifica raccoglitore".
2. Selezionare un agente di destinazione dal menu a discesa degli agenti.
3. Fare clic sul pulsante "Salva raccoglitore".

Workload Security elaborerà la richiesta. Una volta completata la migrazione, l'utente verrà reindirizzato alla pagina dell'elenco dei collezionisti. In caso di errore, verrà visualizzato un messaggio appropriato nella pagina di modifica.

Nota: tutte le modifiche alla configurazione apportate in precedenza nella pagina "Modifica raccoglitore" rimarranno applicate quando il raccoglitore verrà migrato correttamente all'agente di destinazione.



Risoluzione dei problemi

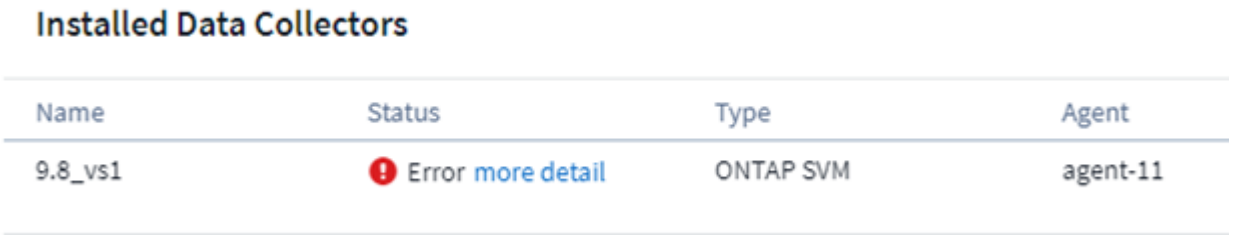
Vedi il"Risoluzione dei problemi del collettore SVM" pagina per suggerimenti sulla risoluzione dei problemi.

Risoluzione dei problemi del raccoglitore dati ONTAP SVM

Workload Security utilizza dei collettori di dati per raccogliere dati sui file e sugli accessi degli utenti dai dispositivi. Qui puoi trovare suggerimenti per la risoluzione dei problemi relativi a questo raccoglitore.

Vedi il"Configurazione del collettore SVM" pagina per le istruzioni sulla configurazione di questo raccoglitore.

In caso di errore, è possibile fare clic su *ulteriori dettagli* nella colonna *Stato* della pagina Collettori dati installati per ottenere maggiori dettagli sull'errore.



Di seguito vengono descritti i problemi noti e le relative soluzioni.

Problema: Data Collector funziona per un po' di tempo e si arresta dopo un tempo casuale, con il seguente messaggio di errore: "Messaggio di errore: il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno sovraccarico." **Prova questo:** la frequenza degli eventi di ONTAP era molto più alta di quella che la casella Agent può gestire. Di conseguenza la connessione è stata interrotta.

Controlla il picco di traffico in CloudSecure al momento della disconnessione. Puoi verificarlo dalla pagina **CloudSecure > Activity Forensics > Tutte le attività**.

Se il traffico aggregato di picco è superiore a quello che l'Agent Box può gestire, fare riferimento alla pagina Event Rate Checker per informazioni su come dimensionare la distribuzione del Collector in un Agent Box.

Se l'agente è stato installato nella casella Agente prima del 4 marzo 2021, eseguire i seguenti comandi nella casella Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Dopo il ridimensionamento, riavviare il raccoglitore dall'interfaccia utente.

{vuoto}

Problema: il Collector segnala il messaggio di errore: "Nessun indirizzo IP locale trovato sul connettore in

grado di raggiungere le interfacce dati dell'SVM". **Prova questo:** Molto probabilmente è dovuto a un problema di rete sul lato ONTAP . Si prega di seguire questi passaggi:

1. Assicurarsi che non vi siano firewall sulla vita dati SVM o sulla vita di gestione che bloccano la connessione dalla SVM.
2. Quando si aggiunge una SVM tramite un IP di gestione del cluster, assicurarsi che la vita dati e la vita di gestione della SVM siano pingabili dalla VM dell'agente. In caso di problemi, controllare il gateway, la netmask e i percorsi per lif.

   Puoi anche provare ad accedere al cluster tramite ssh utilizzando l'IP di gestione del cluster ed effettuare il ping dell'IP dell'agente. Assicurarsi che l'IP dell'agente sia pingabile:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

3. Se hai provato a connetterti tramite l'IP del cluster e non funziona, prova a connetterti direttamente tramite l'IP SVM. Per i passaggi necessari per connettersi tramite IP SVM, vedere quanto sopra.
4. Durante l'aggiunta del collettore tramite IP SVM e credenziali vsadmin, verificare se SVM Lif ha abilitato il ruolo Data plus Mgmt. In questo caso il ping all'SVM Lif funzionerà, ma l'SSH all'SVM Lif non funzionerà. In caso affermativo, creare un SVM Mgmt Only Lif e provare a connettersi tramite questo SVM Management Only Lif.
5. Se ancora non funziona, crea un nuovo SVM Lif e prova a connetterti tramite quel Lif. Assicurarsi che la subnet mask sia impostata correttamente.
6. Debug avanzato:
   a. Avvia una traccia dei pacchetti in ONTAP.
   b. Provare a connettere un data collector all'SVM dall'interfaccia utente di CloudSecure.
   c. Attendi finché non compare l'errore. Arresta la traccia dei pacchetti in ONTAP.
   d. Aprire la traccia del pacchetto da ONTAP. È disponibile in questa posizione

      ```
       https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
      .. Assicurarsi che ci sia un SYN da ONTAP alla casella Agent.
      .. Se non c'è SYN da ONTAP , allora c'è un problema con il firewall
      in ONTAP.
      .. Aprire il firewall in ONTAP, in modo che ONTAP possa connettersi
      alla casella agente.
      ```

7. Se il problema persiste, consultare il team di rete per accertarsi che nessun firewall esterno stia bloccando la connessione da ONTAP alla casella Agent.
8. Se nessuna delle soluzioni precedenti risolve il problema, apri un caso con"Supporto Netapp" per ulteriore assistenza.

{vuoto}

Problema: Messaggio: "Impossibile determinare il tipo ONTAP per [nome host: <indirizzo IP>. Motivo: Errore di connessione al sistema di archiviazione <Indirizzo IP>: Host non raggiungibile (Host non raggiungibile)
Prova questo:

1. Verificare che sia stato fornito l'indirizzo IP di gestione SVM o l'IP di gestione del cluster corretto.
2. Eseguire l'SSH sull'SVM o sul Cluster a cui si intende connettersi. Una volta effettuata la connessione, assicurarsi che il nome SVM o Cluster sia corretto.

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno terminato." **Prova questo:**

1. È molto probabile che un firewall stia bloccando le porte necessarie nella macchina dell'agente. Verificare che l'intervallo di porte 35000-55000/tcp sia aperto affinché la macchina agente possa connettersi dall'SVM. Assicurarsi inoltre che non vi siano firewall abilitati sul lato ONTAP che bloccano la comunicazione con la macchina agente.
2. Digitare il seguente comando nella casella Agente e assicurarsi che l'intervallo di porte sia aperto.

   ```
   sudo iptables-save | grep 3500*
   ```

   L'output di esempio dovrebbe apparire così:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Accedi a SVM, inserisci i seguenti comandi e verifica che non sia
   impostato alcun firewall per bloccare la comunicazione con ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Controlla i comandi del firewall"sul lato ONTAP .

3. Accedi tramite SSH all'SVM/Cluster che vuoi monitorare. Eseguire il ping della casella Agent dalla libreria dati SVM (con supporto dei protocolli CIFS e NFS) e assicurarsi che il ping funzioni:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

4. Se un singolo SVM viene aggiunto due volte a un tenant tramite 2 collettori dati, verrà visualizzato questo errore. Eliminare uno dei collettori di dati tramite l'interfaccia utente. Quindi riavviare l'altro raccoglitore dati

tramite l'interfaccia utente. Quindi il raccoglitore dati mostrerà lo stato "IN ESECUZIONE" e inizierà a ricevere eventi da SVM.

In pratica, in un tenant, 1 SVM dovrebbe essere aggiunto una sola volta, tramite 1 data collector. 1 SVM non dovrebbe essere aggiunto due volte tramite 2 collettori di dati.

5. Nei casi in cui lo stesso SVM è stato aggiunto in due diversi ambienti Workload Security (tenant), l'ultimo riuscirà sempre. Il secondo collettore configurerà fpolicy con il proprio indirizzo IP ed espellerà il primo. Quindi il collettore nel primo smetterà di ricevere eventi e il suo servizio di "audit" entrerà in stato di errore. Per evitare ciò, configurare ogni SVM su un singolo ambiente.
6. Questo errore può verificarsi anche se i criteri di servizio non sono configurati correttamente. Con ONTAP 9.8 o versioni successive, per connettersi al Data Source Collector, è necessario il servizio data-fpolicy-client insieme al servizio dati data-nfs e/o data-cifs. Inoltre, il servizio data-fpolicy-client deve essere associato ai dati lif per l'SVM monitorato.

{vuoto}

Problema: Nessun evento visualizzato nella pagina delle attività. **Prova questo:**

1. Verificare se il collettore ONTAP è nello stato "IN ESECUZIONE". In caso affermativo, assicurarsi che alcuni eventi cifs vengano generati sulle VM client cifs aprendo alcuni file.
2. Se non vengono rilevate attività, effettuare l'accesso all'SVM e immettere il seguente comando.

   ```
   <SVM>event log show -source fpolicy
   ```

   Assicurati che non ci siano errori relativi a fpolicy.

3. Se non vengono visualizzate attività, effettuare l'accesso all'SVM. Immettere il seguente comando:

   ```
   <SVM>fpolicy show
   ```

   Verificare se la policy fpolicy denominata con prefisso "cloudsecure_" è stata impostata e lo stato è "on". Se non è impostato, molto probabilmente l'agente non è in grado di eseguire i comandi nell'SVM. Si prega di assicurarsi che siano stati rispettati tutti i prerequisiti descritti all'inizio della pagina.

{vuoto}

Problema: SVM Data Collector è in stato di errore e il messaggio di errore è "L'agente non è riuscito a connettersi al raccoglitore". **Prova questo:**

1. Molto probabilmente l'agente è sovraccarico e non riesce a connettersi ai collettori dell'origine dati.
2. Controllare quanti collettori di origini dati sono connessi all'agente.
3. Controllare anche la velocità del flusso di dati nella pagina "Tutte le attività" nell'interfaccia utente.
4. Se il numero di attività al secondo è significativamente elevato, installare un altro agente e spostare alcuni dei Data Source Collector sul nuovo agente.

{vuoto}

Problema: SVM Data Collector mostra il messaggio di errore "fpolicy.server.connectError: il nodo non è riuscito a stabilire una connessione con il server FPolicy "12.195.15.146" (motivo: "Selezione scaduta")" **Prova questo:** il firewall è abilitato in SVM/Cluster. Quindi il motore fpolicy non è in grado di connettersi al server fpolicy. Le CLI in ONTAP che possono essere utilizzate per ottenere maggiori informazioni sono:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Controlla i comandi del firewall"sul lato ONTAP .

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Nessuna interfaccia dati valida (ruolo: dati, protocolli dati: NFS o CIFS o entrambi, stato: attivo) trovata sull'SVM." **Prova questo:** assicurati che ci sia un'interfaccia operativa (che abbia il ruolo di dati e protocollo dati come CIFS/NFS).

{vuoto}

Problema: il raccoglitore dati entra nello stato di errore e poi, dopo un po' di tempo, passa allo stato di esecuzione, per poi tornare nuovamente allo stato di errore. Questo ciclo si ripete. **Prova questo:** Questo accade in genere nel seguente scenario:

1. Sono stati aggiunti più raccoglitori di dati.
2. Ai collettori di dati che mostrano questo tipo di comportamento verrà aggiunto 1 SVM. Ciò significa che 2 o più collettori di dati sono collegati a 1 SVM.
3. Assicurarsi che 1 raccoglitore dati si connetta a 1 solo SVM.
4. Eliminare gli altri raccoglitori di dati connessi allo stesso SVM.

{vuoto}

Problema: Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare (policy su SVM svmname. Motivo: Valore non valido specificato per l'elemento 'shares-to-include' in 'fpolicy.policy.scope-modify: "Federal' **Prova questo:** *I nomi delle condivisioni devono essere specificati senza virgolette. Modificare la configurazione DSC ONTAP SVM per correggere i nomi delle condivisioni.

Includi ed escludi azioni non è pensato per un lungo elenco di nomi di azioni. Se hai un gran numero di azioni da includere o escludere, utilizza il filtro per volume.

{vuoto}

Problema: Nel cluster sono presenti fpolicies esistenti che non sono utilizzati. Cosa si dovrebbe fare prima di installare Workload Security? **Prova questo:** Si consiglia di eliminare tutte le impostazioni fpolicy esistenti e non utilizzate, anche se sono in stato disconnesso. Workload Security creerà fpolicy con il prefisso "cloudsecure_". Tutte le altre configurazioni fpolicy non utilizzate possono essere eliminate.

Comando CLI per visualizzare l'elenco fpolicy:

```
 fpolicy show
Passaggi per eliminare le configurazioni fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vuoto}

Problema: Dopo aver abilitato Workload Security, le prestazioni ONTAP risultano compromesse: la latenza diventa sporadicamente elevata, mentre gli IOPS diventano sporadicamente bassi. **Prova questo:** Durante l'utilizzo di ONTAP con Workload Security, a volte si possono verificare problemi di latenza in ONTAP. Le possibili cause di ciò sono molteplici, come indicato di seguito:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tutti questi problemi sono stati risolti in ONTAP 9.13.1 e versioni successive; si consiglia vivamente di utilizzare una di queste versioni successive.

{vuoto}

Problema: Data Collector mostra il messaggio di errore: "Errore: impossibile determinare lo stato del collector entro 2 tentativi, provare a riavviare nuovamente il collector (codice errore: AGENT008)". **Prova questo:**

1. Nella pagina dei raccoglitori di dati, scorrere verso destra del raccoglitore di dati che ha generato l'errore e fare clic sul menu con i 3 puntini. Selezionare *Modifica*. Inserire nuovamente la password del raccoglitore dati. Salvare il raccoglitore dati premendo il pulsante *Salva*. Data Collector verrà riavviato e l'errore dovrebbe essere risolto.
2. La macchina dell'agente potrebbe non avere abbastanza CPU o RAM, ecco perché i DSC non funzionano. Controllare il numero di Data Collector aggiunti all'agente nella macchina. Se è superiore a 20, aumentare la capacità della CPU e della RAM della macchina agente. Una volta aumentata la CPU e la RAM, i DSC entreranno automaticamente nello stato di inizializzazione e poi in quello di esecuzione. Consulta la guida alle taglie su"questa pagina" .

{vuoto}

Problema: il Data Collector genera un errore quando è selezionata la modalità SVM. **Prova questo:** durante

la connessione in modalità SVM, se per la connessione viene utilizzato l'IP di gestione del cluster anziché l'IP di gestione SVM, la connessione genererà un errore. Assicurarsi che venga utilizzato l'IP SVM corretto.

{vuoto}

Problema: Il raccoglitore dati mostra un messaggio di errore quando la funzione Accesso negato è abilitata: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: impossibile configurare fpolicy su SVM test_svm. Motivo: L'utente non è autorizzato." **Prova questo:** L'utente potrebbe non disporre delle autorizzazioni REST necessarie per la funzionalità Accesso negato. Si prega di seguire le istruzioni su"questa pagina" per impostare i permessi.

Una volta impostate le autorizzazioni, riavviare il raccoglitore.

{vuoto}

Problema: Il collettore è in stato di errore con il messaggio: Il connettore è in stato di errore. Motivo dell'errore: impossibile configurare l'archivio persistente su SVM <Nome SVM>. Motivo: impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova il comando. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare l'archivio persistente su SVM <SVM Name>. Motivo: Impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova a eseguire il comando.

Prova questo: attendi qualche minuto e poi riavvia il Collector.

{vuoto}

Se riscontri ancora problemi, contatta l'assistenza tramite i link indicati nella pagina **Aiuto > Assistenza**.

Configurazione di Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP

Monitora l'accesso ai file e agli utenti nell'intera infrastruttura di archiviazione cloud configurando i raccoglitori di dati Workload Security per Cloud Volumes ONTAP e Amazon FSx for NetApp ONTAP. Questa guida fornisce istruzioni dettagliate per distribuire gli agenti in AWS e connetterli alle istanze di archiviazione cloud.

Configurazione di archiviazione Cloud Volumes ONTAP

Consultare la documentazione di OnCommand Cloud Volumes ONTAP per configurare un'istanza AWS a nodo singolo/HA per ospitare Workload Security Agent:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Una volta completata la configurazione, segui i passaggi per impostare la tua SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Piattaforme supportate

- Cloud Volumes ONTAP, supportato da tutti i provider di servizi cloud disponibili, ove disponibili. Ad esempio: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Configurazione della macchina agente

La macchina agente deve essere configurata 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 passaggi equivalenti, a seconda del provider di servizi cloud, in Azure o Google Cloud.

In AWS, attenersi alla seguente procedura per configurare la macchina da utilizzare come agente di sicurezza del carico di lavoro:

Per configurare la macchina da utilizzare come Workload Security Agent, attenersi alla seguente procedura:

Passi

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

Installare l'agente di sicurezza del carico di lavoro

1. Accedi come amministratore o proprietario dell'account al tuo ambiente Data Infrastructure Insights .
2. Passare a **Collectors** di Workload Security e fare clic sulla scheda **Agents**.
3. Fare clic su **+Agente** e specificare RHEL come piattaforma di destinazione.
4. Copiare il comando Installazione agente.
5. Incolla il comando Agent Installation nell'istanza RHEL EC2 a cui hai effettuato l'accesso. Questo installa l'agente Workload Security, fornendo tutti i"Prerequisiti dell'agente" sono soddisfatte.

Per i passaggi dettagliati, fare riferimento a questo collegamento: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Risoluzione dei problemi

Nella tabella seguente sono descritti i problemi noti e le relative soluzioni.

Problema	Risoluzione

Il Data Collector mostra l'errore "Sicurezza del carico di lavoro: impossibile determinare il tipo di ONTAP per il raccoglitore dati Amazon FxSN". Il cliente non è in grado di aggiungere un nuovo raccoglitore dati Amazon FSxN in Workload Security. La connessione al cluster FSxN sulla porta 443 dall'agente è in timeout. Il firewall e i gruppi di sicurezza AWS hanno le regole necessarie abilitate per consentire la comunicazione. Un agente è già distribuito e si trova anche nello stesso account AWS. Questo stesso agente viene utilizzato per connettere e monitorare i restanti dispositivi NetApp (e tutti funzionano).	Risolvi questo problema aggiungendo il segmento di rete LIF di fsxadmin alla regola di sicurezza dell'agente. Se non sei sicuro delle porte, consenti tutte le porte.

Gestione degli utenti

Gli account utente di Workload Security 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 utenti e assegnare a ciascun utente uno dei seguenti ruoli di sicurezza del carico di lavoro:

Ruolo	Accesso alla sicurezza del carico di lavoro
Amministratore	Può eseguire tutte le funzioni di sicurezza del carico di lavoro, comprese quelle per avvisi, analisi forense, raccoglitori di dati, criteri di risposta automatizzati e API per la sicurezza del carico di lavoro. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di sicurezza del carico di lavoro.
Utente	Può visualizzare e gestire gli avvisi e visualizzare le analisi forensi. Il ruolo utente può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot e limitare l'accesso utente.
Ospite	È possibile visualizzare avvisi e analisi forensi. Il ruolo ospite non può modificare lo stato dell'avviso, aggiungere una nota, acquisire manualmente snapshot o limitare l'accesso degli utenti.

Passi

1. Accedi a Workload Security
2. Nel menu, fare clic su **Amministrazione > Gestione utenti**

   Verrai indirizzato alla pagina Gestione utenti di Data Infrastructure Insights.

3. Selezionare il ruolo desiderato per ciascun utente.

Quando si aggiunge un nuovo utente, è sufficiente selezionare il ruolo desiderato (solitamente Utente o Ospite).

Ulteriori informazioni sugli account utente e sui ruoli sono disponibili in Data Infrastructure Insights"Ruolo utente" documentazione.

Event Rate Checker: Guida alle dimensioni degli agenti

Determina il dimensionamento ottimale delle macchine Agent misurando le frequenze degli eventi NFS e SMB generate dalle tue SVM prima di distribuire i data collector. Lo script Event Rate Checker ti aiuta a comprendere i limiti di capacità (massimo 50 data collector per Agent) e garantisce che la tua infrastruttura Agent possa gestire il volume di eventi previsto per un rilevamento affidabile delle minacce.

Requisiti:

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

Quando si esegue questo script, non deve essere in esecuzione alcun ONTAP SVM Data Collector per l'SVM per cui si sta determinando la frequenza degli eventi.

Passaggi:

1. Installare l'agente 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 che _sshpass_ sia installato sulla macchina
Linux.  Ci sono due modi per installarlo:
```

   a. Esegui il seguente comando:

```
 linux_prompt> yum install sshpass
.. Se ciò non funziona, scarica _sshpass_ dal web sul computer Linux
ed esegui il seguente comando:
```

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

3. Fornire i valori corretti quando richiesto. Di seguito è riportato un esempio.
4. L'esecuzione dello script richiederà circa 5 minuti.
5. Una volta completata l'esecuzione, lo script stamperà la frequenza degli eventi dall'SVM. È possibile controllare la frequenza degli eventi per SVM nell'output della console:

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

Ogni Ontap SVM Data Collector può essere associato a un singolo SVM, il che significa che ogni data collector sarà in grado di ricevere il numero di eventi generati da un singolo SVM.

Tieni presente quanto segue:

A) Utilizzare questa tabella come guida generale alle taglie. È possibile aumentare il numero di core e/o di memoria per aumentare il numero di collettori dati supportati, fino a un massimo di 50 collettori dati:

Configurazione della macchina agente	Numero di collettori di dati SVM	Frequenza massima degli eventi che la macchina agente può gestire
4 core, 16 GB	10 raccoglitori di dati	20K eventi/sec
4 core, 32 GB	20 raccoglitori di dati	20K eventi/sec

B) Per calcolare il totale degli eventi, sommare gli eventi generati per tutti gli SVM per quell'agente.

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

B + C Dovrebbe essere minore di A, altrimenti la macchina agente non riuscirà a monitorare.

In altre parole, il numero di collettori di dati che possono essere aggiunti a una singola macchina agente dovrebbe essere conforme alla formula seguente:

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

Esempio

Supponiamo di avere tre SVMS che generano frequenze 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 dell'agente nel nome file *fpolicy_stat_<Nome SVM>.log* nella directory di lavoro corrente.

Lo script potrebbe dare risultati errati nei seguenti casi:

- Sono state fornite credenziali, IP o nome SVM errati.
- Una fpolicy già esistente con lo stesso nome, numero di sequenza, ecc. genererà un errore.
- Lo script si interrompe bruscamente durante l'esecuzione.

Di seguito è riportato un esempio di esecuzione dello 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
```

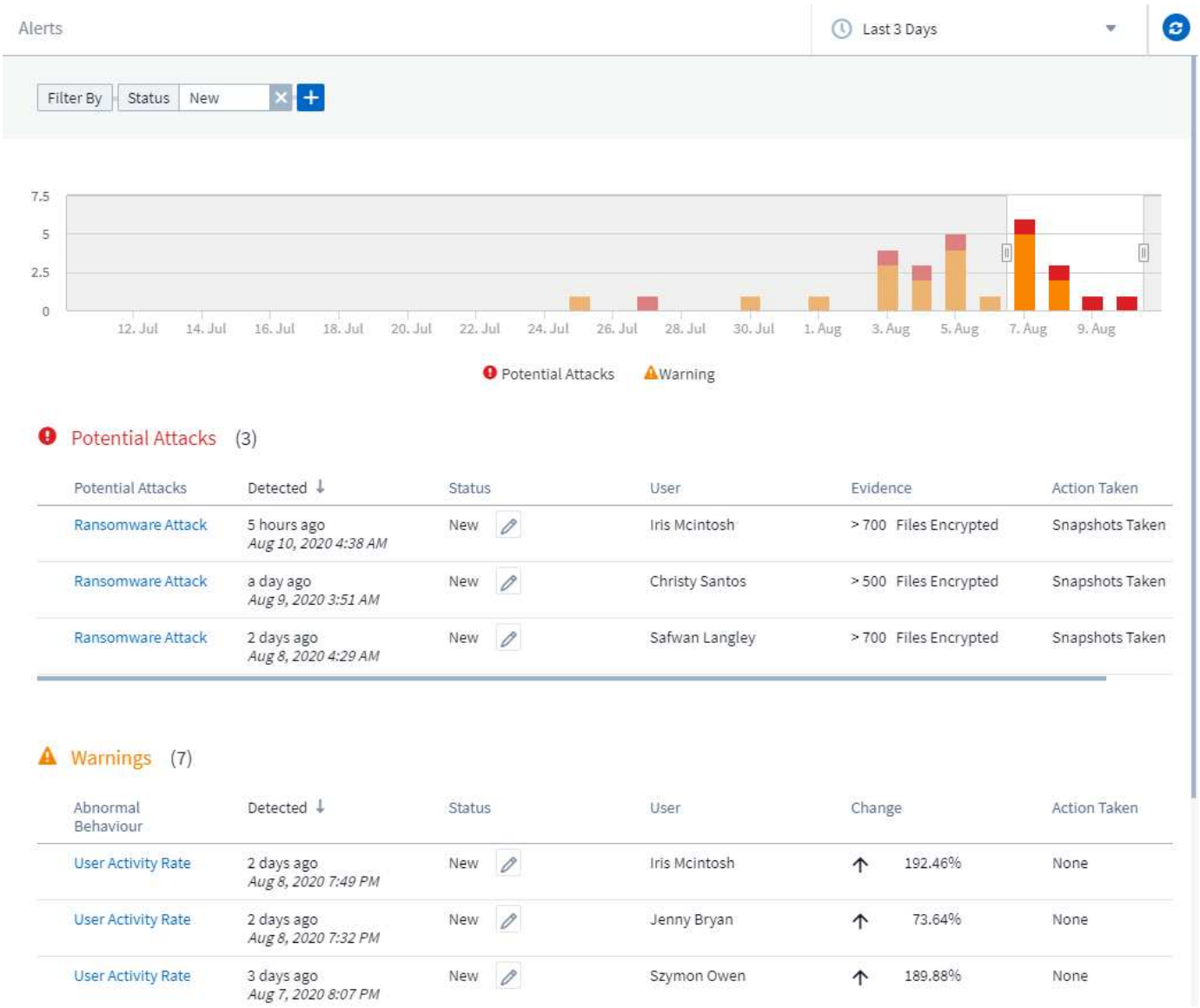
```
[root@ci-cs-data agent]#
```

Risoluzione dei problemi

Domanda	Risposta
Se eseguo questo script su una SVM già configurata per Workload Security, utilizza semplicemente la configurazione fpolicy esistente sulla SVM oppure ne imposta una temporanea ed esegue il processo?	Event Rate Checker può funzionare correttamente anche per una SVM già configurata per Workload Security. Non dovrebbe esserci alcun impatto.
Posso aumentare il numero di SVM su cui può essere eseguito lo script?	Sì. Basta modificare lo script e cambiare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se aumento il numero di SVM, aumenterà il tempo di esecuzione dello script?	No. Lo script verrà eseguito per un massimo di 5 minuti, anche se il numero di SVM viene aumentato.
Posso aumentare il numero di SVM su cui può essere eseguito lo script?	Sì. È necessario modificare lo script e cambiare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se aumento il numero di SVM, aumenterà il tempo di esecuzione dello script?	No. Lo script verrà eseguito per un massimo di 5 minuti, anche se il numero di SVM viene aumentato.
Cosa succede se eseguo Event Rate Checker con un agente esistente?	L'esecuzione di Event Rate Checker su un agente già esistente potrebbe causare un aumento della latenza sull'SVM. Questo aumento sarà di natura temporanea mentre è in esecuzione Event Rate Checker.

Comprendere e indagare gli avvisi

La pagina Avvisi sulla sicurezza del carico di lavoro fornisce una cronologia completa delle minacce e degli avvisi rilevati, con strumenti di indagine dettagliati. Visualizza i dettagli degli avvisi, gestisci gli aggiornamenti di stato, filtra in base a criteri e monitora le attività degli utenti per indagare e rispondere in modo efficiente agli incidenti di sicurezza.



Attenzione

L'elenco degli avvisi visualizza un grafico che mostra il numero totale di potenziali attacchi e/o avvisi emessi nell'intervallo di tempo selezionato, seguito da un elenco degli attacchi e/o avvisi verificatisi in tale intervallo di tempo. È possibile modificare l'intervallo di tempo regolando i cursori dell'ora di inizio e dell'ora di fine nel grafico.

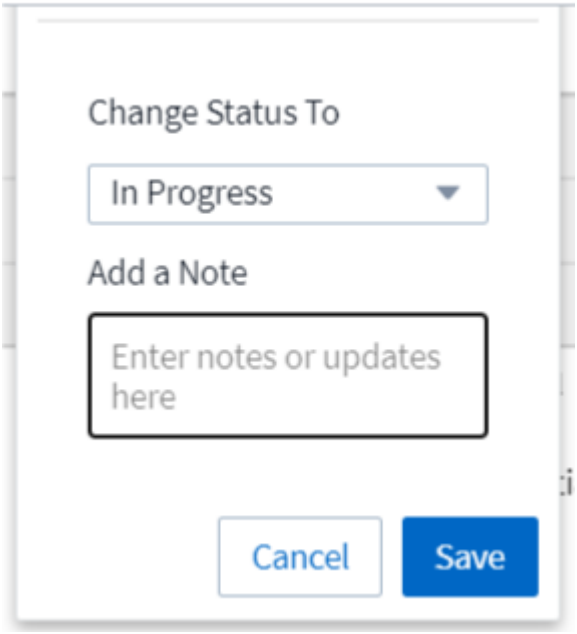
Per ogni avviso viene visualizzato quanto segue:

Potenziali attacchi:

- Il tipo di *Potenziale attacco* (ad esempio, manomissione di file o sabotaggio)
- Data e ora in cui è stato rilevato il potenziale attacco
- Lo *Stato* dell'avviso:
  - **Nuovo**: questa è l'impostazione predefinita per i nuovi avvisi.
  - **In corso**: l'avviso è in fase di analisi da parte di uno o più membri del team.
  - **Risolto**: l'avviso è stato contrassegnato come risolto da un membro del team.

- **Ignorato**: l'avviso è stato ignorato come falso positivo o comportamento previsto.

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



- 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 un'istantanea)

Avvertenze:

- Il *comportamento anomalo* che ha attivato l'avviso
- La data e l'ora in cui il comportamento è stato *Rilevato*
- Lo *Stato* dell'avviso (Nuovo, In corso, ecc.)
- L'*Utente* il cui comportamento ha attivato l'avviso
- Una descrizione della *Modifica* (ad esempio, un aumento anomalo dell'accesso ai file)
- L'azione intrapresa

Opzioni filtro

Puoi filtrare gli avvisi in base a quanto segue:

- Lo *Stato* dell'avviso
- Testo specifico nella *Nota*
- Il tipo di *Attacchi/Avvisi*
- L'*Utente* le cui azioni hanno attivato l'avviso/segnalazione

La pagina Dettagli avviso

È possibile fare clic sul collegamento di un avviso nella pagina dell'elenco degli avvisi per aprire una pagina dei dettagli dell'avviso. I dettagli dell'avviso possono variare a seconda del tipo di attacco o di avviso. Ad

esempio, una pagina con i dettagli di un attacco di manomissione di file potrebbe mostrare le seguenti informazioni:

Sezione riassuntiva:

- Tipo di attacco (manomissione di file, sabotaggio) e ID avviso (assegnato da Workload Security)
- Data e ora in cui è stato rilevato l'attacco
- Azione intrapresa (ad esempio, è stata scattata un'istantanea automatica). L'ora dello snapshot è mostrata immediatamente sotto la sezione di riepilogo))
- Stato (Nuovo, In corso, ecc.)

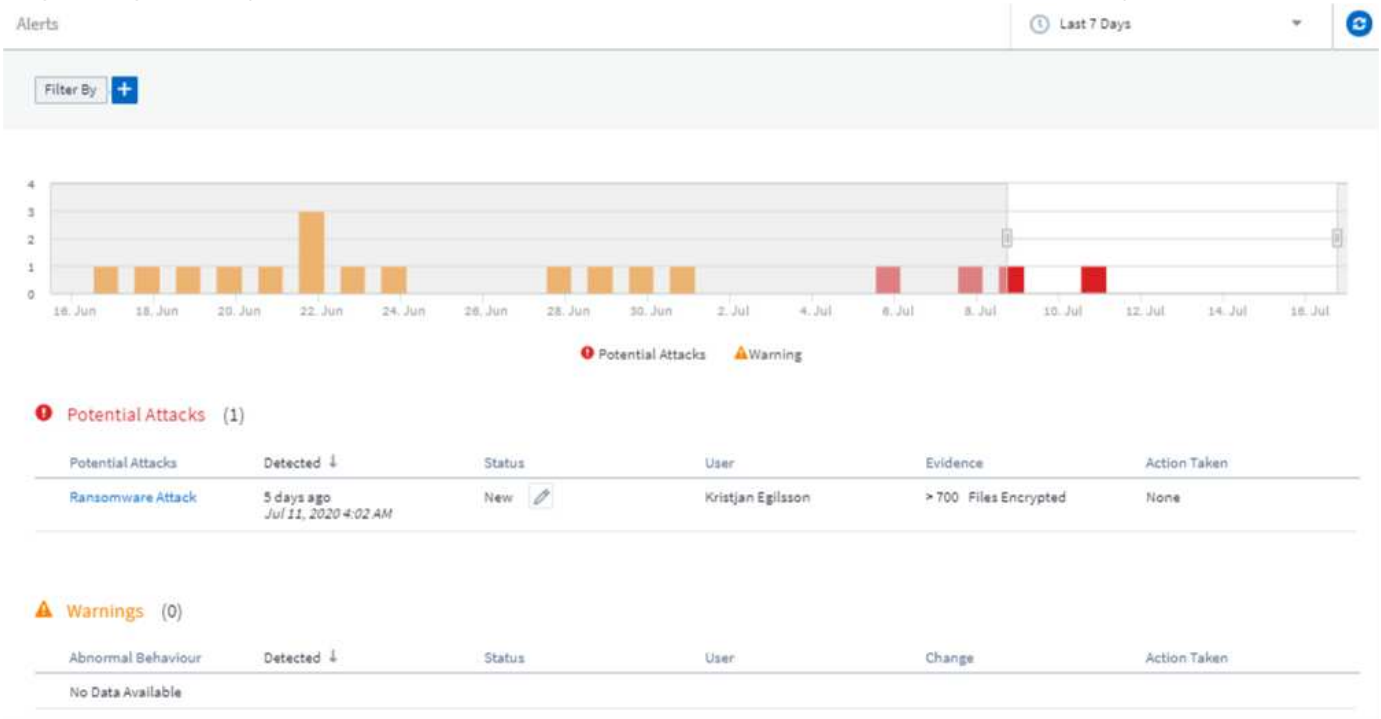
Sezione Risultati dell'attacco:

- Conteggio dei volumi e dei file interessati
- Un riassunto allegato del rilevamento
- Un grafico che mostra l'attività del file durante l'attacco

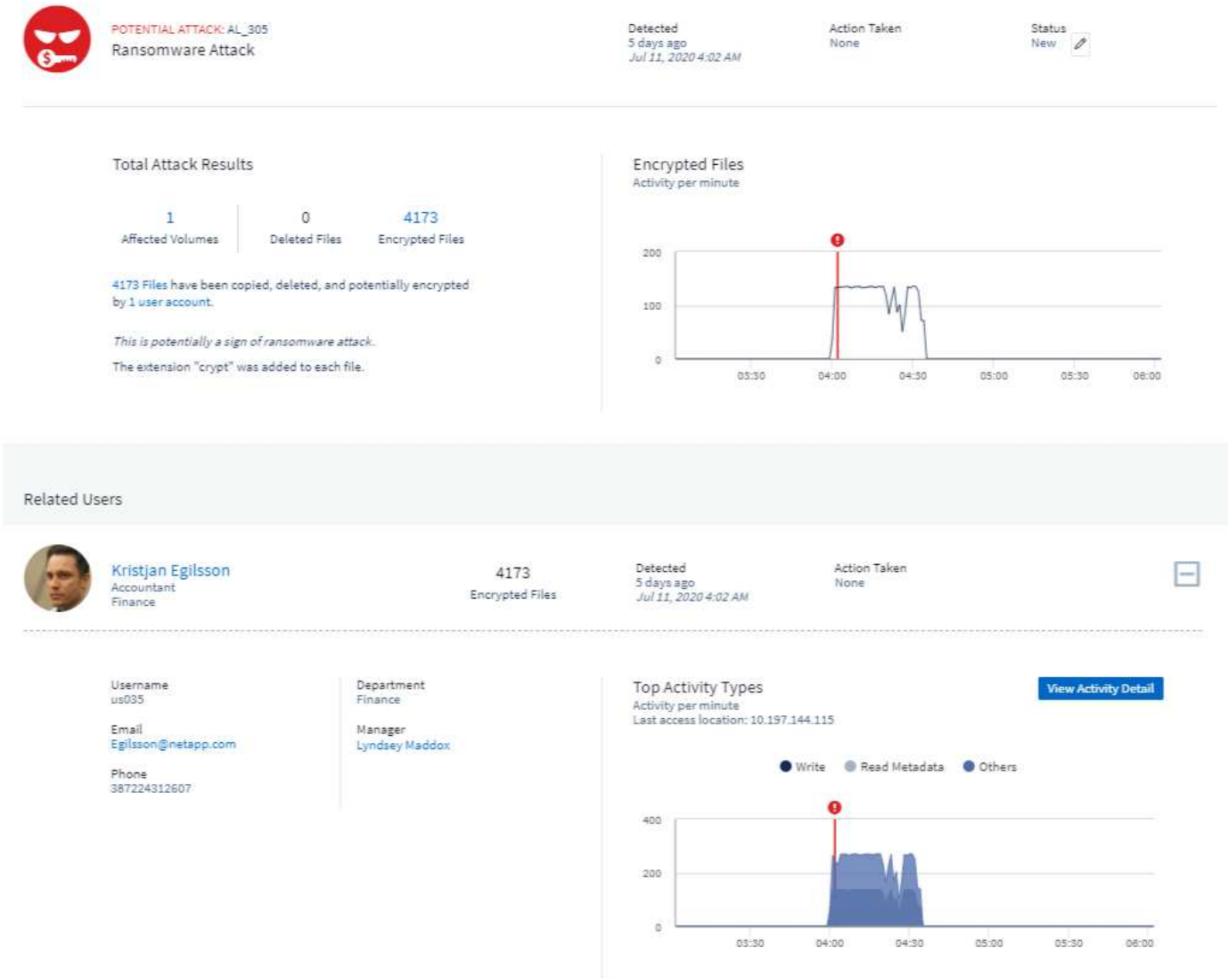
Sezione Utenti correlati:

Questa sezione mostra i dettagli sull'utente coinvolto nel potenziale attacco, incluso un grafico delle principali attività dell'utente.

Pagina degli avvisi (questo esempio mostra un potenziale attacco di manomissione dei file):



Pagina dei dettagli (questo esempio mostra un potenziale attacco di manomissione dei file):

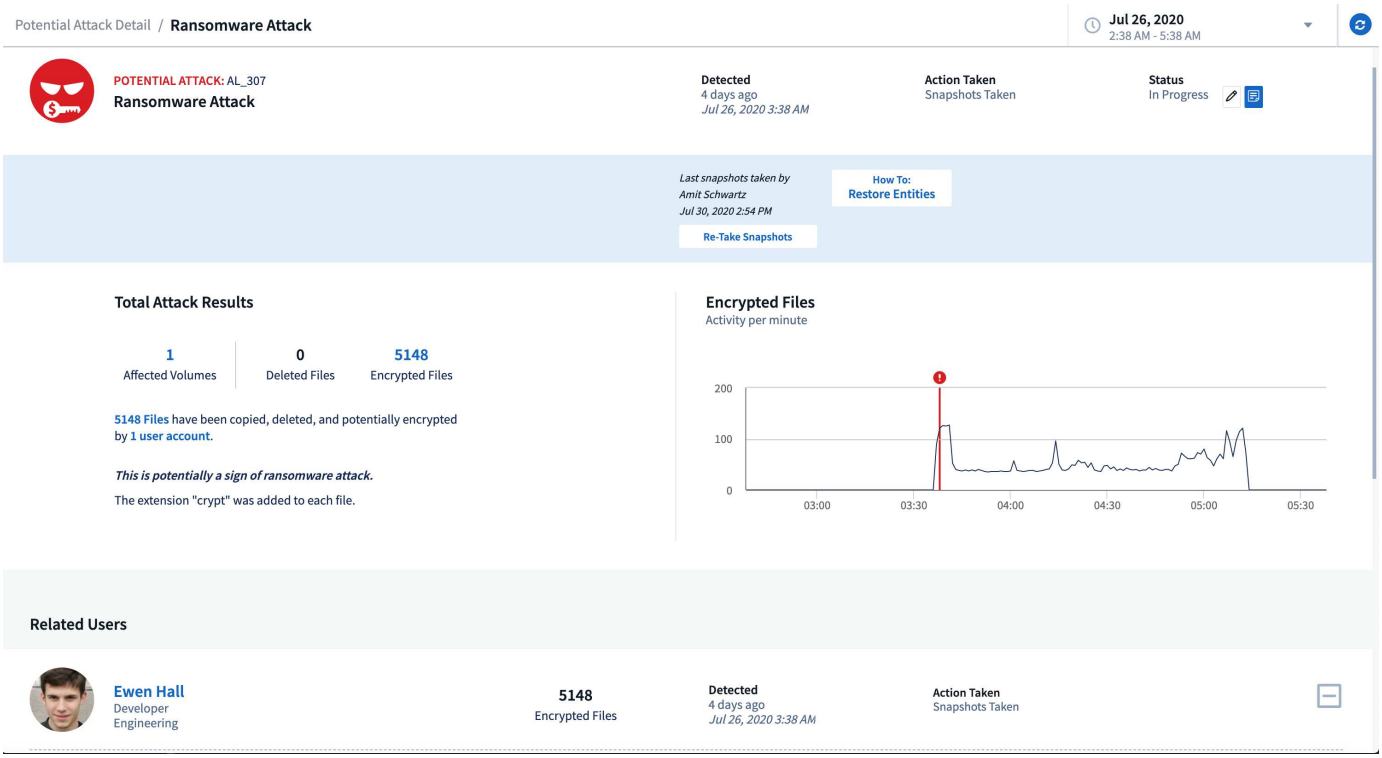


Scatta un'istantanea **Azione**

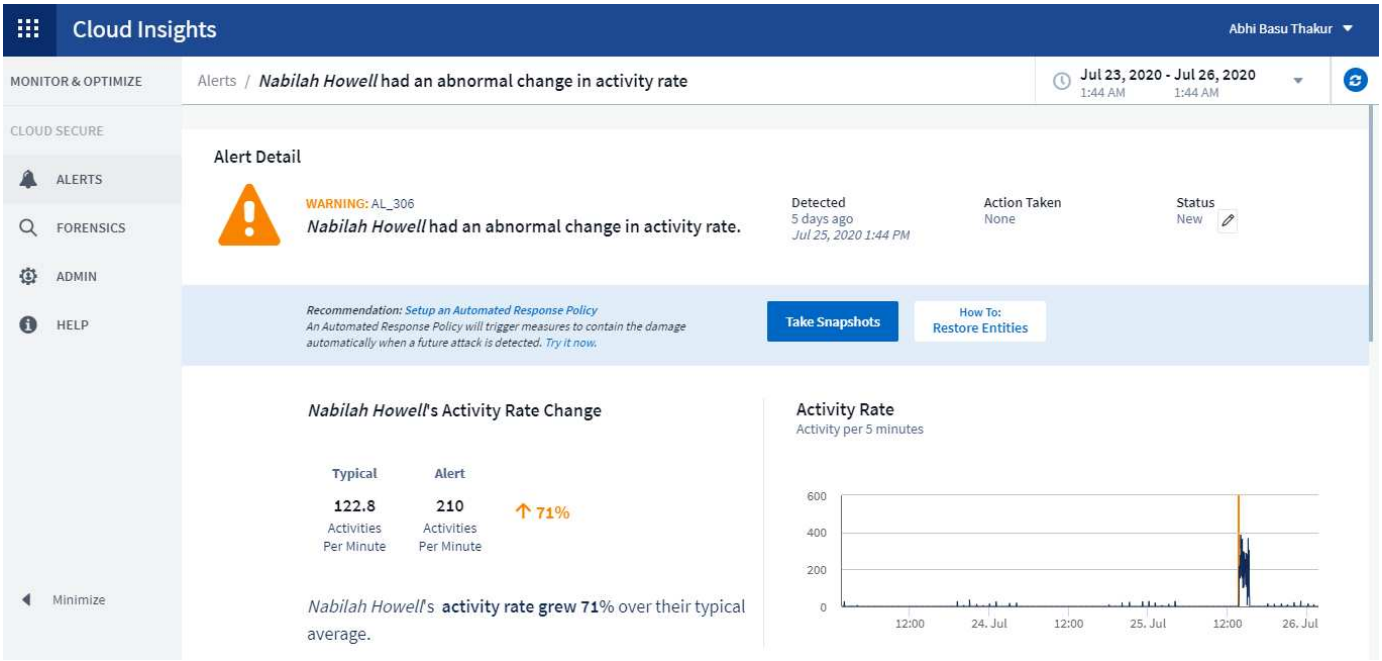
Workload Security protegge i tuoi dati eseguendo automaticamente uno snapshot quando viene rilevata un'attività dannosa, garantendo così che i tuoi dati vengano sottoposti a backup in modo sicuro.

Puoi definire "politiche di risposta automatizzate" che scattano un'istantanea quando viene rilevato un attacco di manomissione dei file o altre attività anomale dell'utente. È anche possibile acquisire manualmente uno snapshot dalla pagina di avviso.

Istantanea automatica
scattata:



Istantanea manuale:



Notifiche di avviso

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

Politica di conservazione

Gli avvisi e le segnalazioni vengono conservati per 13 mesi. Gli avvisi e le segnalazioni più vecchi di 13 mesi

verranno eliminati. Se l'ambiente Workload Security viene eliminato, vengono eliminati anche tutti i dati associati all'ambiente.

Risoluzione dei problemi

Problema:	Prova questo:
Esiste una situazione in cui ONTAP acquisisce snapshot orari al giorno. Gli snapshot di Workload Security (WS) avranno ripercussioni? Lo snapshot WS sostituirà lo snapshot orario? Lo snapshot orario predefinito verrà interrotto?	Gli snapshot di Workload Security non influiranno sugli snapshot orari. Gli snapshot WS non occuperanno lo spazio degli snapshot orari e la situazione dovrebbe continuare come prima. Lo snapshot orario predefinito non verrà interrotto.
Cosa succede se viene raggiunto il numero massimo di snapshot in ONTAP?	Se viene raggiunto il numero massimo di snapshot, l'acquisizione successiva degli snapshot non riuscirà e Workload Security mostrerà un messaggio di errore che indica che lo snapshot è pieno. L'utente deve definire criteri di snapshot per eliminare gli snapshot più vecchi, altrimenti gli snapshot non verranno acquisiti. 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 ONTAP per informazioni su"impostazione della politica di eliminazione degli snapshot" .
Workload Security non è in grado di acquisire snapshot.	Assicurarsi che il ruolo utilizzato per creare snapshot abbia il collegamento: https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [diritti appropriati assegnati]. Assicurarsi che *csrole* sia stato creato con i diritti di accesso appropriati per l'acquisizione di snapshot: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Gli snapshot non funzionano per gli avvisi più vecchi sulle SVM che sono state rimosse da Workload Security e successivamente aggiunte di nuovo. Per i nuovi avvisi che si verificano dopo aver aggiunto nuovamente SVM, vengono creati degli snapshot.	Si tratta di uno scenario raro. Nel caso in cui si verifichi questo problema, accedere a ONTAP ed eseguire manualmente gli snapshot per gli avvisi più vecchi.
Nella pagina *Dettagli avviso*, sotto il pulsante *Acquisisci istantanea* viene visualizzato il messaggio di errore "Ultimo tentativo fallito". Passando il mouse sopra l'errore viene visualizzato il messaggio "Il comando Invoke API è scaduto per il raccoglitore dati con ID".	Ciò può accadere quando un data collector viene aggiunto a Workload Security tramite SVM Management IP, se il LIF dell'SVM è nello stato *disabilitato* in ONTAP. Abilitare il LIF specifico in ONTAP e attivare *Esegui snapshot manualmente* da Workload Security. L'azione Snapshot avrà quindi esito positivo.

Medicina legale

Analisi forense - Tutte le attività

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

Esame di tutti i dati di attività

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

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

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

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

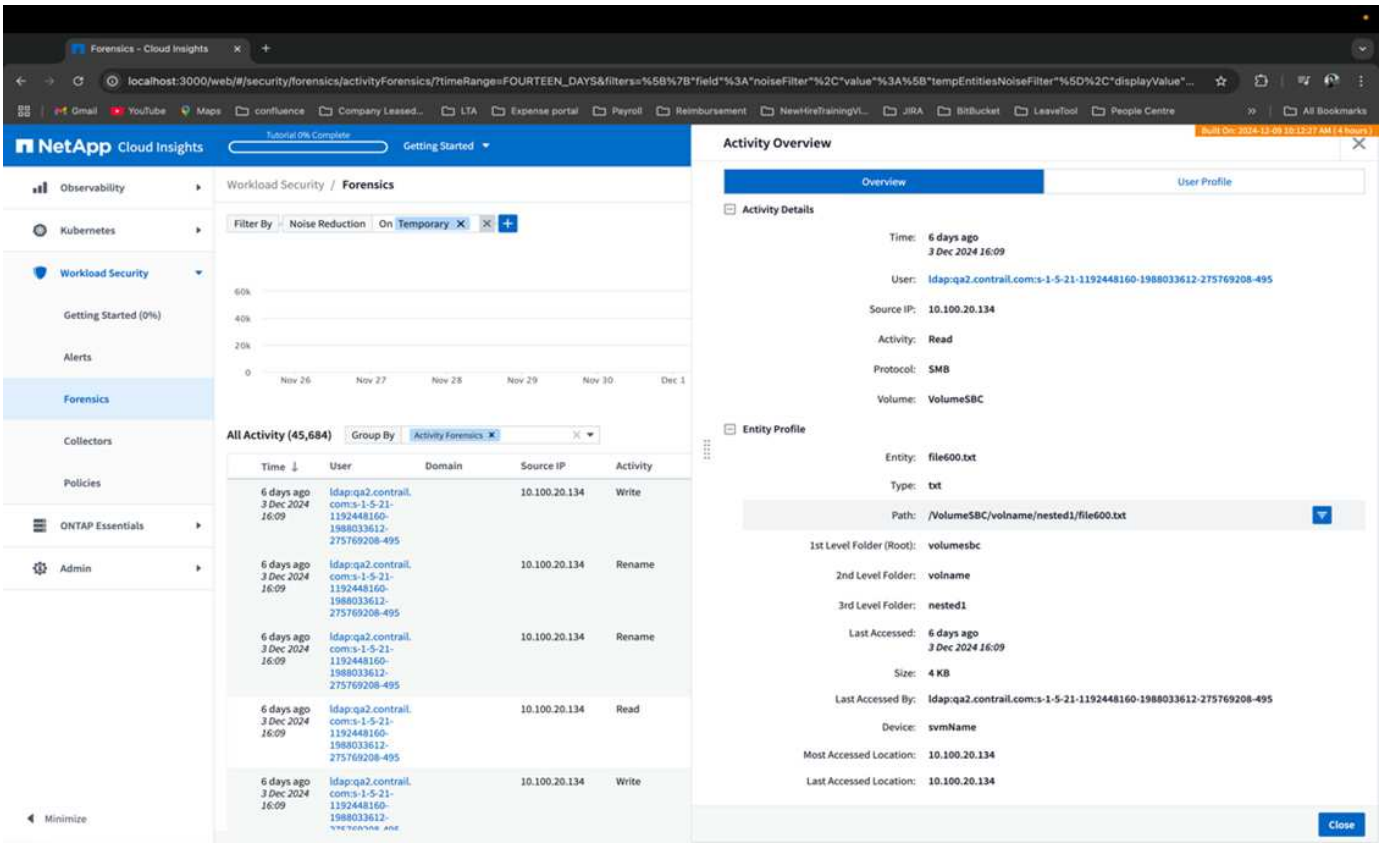
La tabella **Tutte le attività** mostra le seguenti informazioni. Si noti che non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare cliccando sull'icona "ingranaggio".

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

"*/home/userX/nested1/nested2/abc.txt*") OPPURE la parte di directory del percorso per la ricerca ricorsiva (ad esempio, "*/home/userX/nested1/nested2/*"). NOTA: i modelli di percorso regex (ad esempio, *nested*) NON sono consentiti qui. In alternativa, è possibile specificare anche filtri individuali a livello di cartella del percorso, come indicato di seguito, per il filtraggio del percorso.

- La **Cartella di 1° livello (Radice)** è la directory radice del percorso dell'entità in minuscolo.
- La **Cartella di secondo livello** è la directory di secondo livello del percorso dell'entità in minuscolo.
- La **Cartella di terzo livello** è la directory di terzo livello del percorso dell'entità in minuscolo.
- La **Cartella di 4° livello** è la directory di quarto livello del percorso dell'entità in minuscolo.
- **Tipo di entità**, inclusa l'estensione dell'entità (ad esempio file) (.doc, .docx, .tmp, ecc.).
- Il **Dispositivo** in cui risiedono le entità.
- Il **Protocollo** utilizzato per recuperare gli eventi.
- Il **Percorso originale** utilizzato per gli eventi di ridenominazione quando il file originale è stato rinominato. Per impostazione predefinita, questa colonna non è visibile nella tabella. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- Il **Volume** in cui risiedono le entità. Per impostazione predefinita, questa colonna non è visibile nella tabella. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- **Nome entità** è l'ultimo componente del percorso dell'entità; per il tipo di entità come file, è il nome del file.

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



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

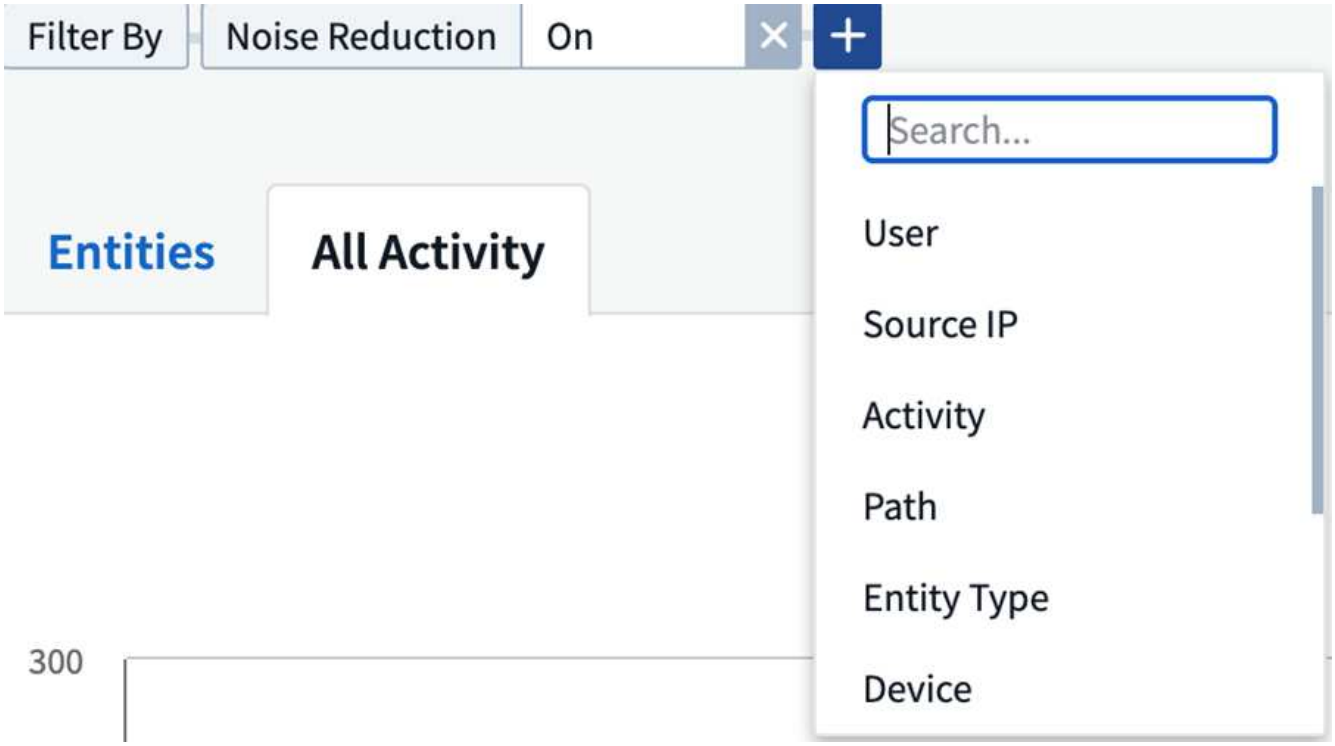
- Il conteggio delle attività viene visualizzato come collegamento ipertestuale; selezionando questa opzione, il raggruppamento selezionato verrà aggiunto come filtro. La tabella delle attività verrà aggiornata in base a quel filtro.
- Tieni presente che se modifichi il filtro, modifichi l'intervallo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

Filtraggio dei dati della cronologia delle attività forensi

Esistono due metodi per filtrare i dati.

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

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



  Inserisci il testo da cercare

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

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

- Il tipo **Attività**.
- **Protocollo** per recuperare attività specifiche del protocollo.
- **Nome utente** dell'utente che esegue l'attività. Per filtrare è necessario fornire il nome utente esatto. La ricerca con nome utente parziale o con nome utente parziale preceduto o suffisso '*' non funzionerà.
- **Riduzione rumore** per filtrare i file creati nelle ultime 2 ore dall'utente. Viene utilizzato anche per filtrare i

file temporanei (ad esempio, i file .tmp) a cui accede l'utente.

- **Dominio** dell'utente che esegue l'attività. Per filtrare è necessario fornire il **dominio esatto**. La ricerca di domini parziali o di domini parziali con prefisso o suffisso con carattere jolly ('*') non funzionerà. È possibile specificare *None* per cercare il dominio mancante.

I seguenti campi sono soggetti a regole di filtraggio speciali:

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

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

- Il valore esatto deve essere racchiuso tra virgolette: Esempio: "searchtext"
- Le stringhe jolly non devono contenere virgolette: Esempio: searchtext, *searchtext*, filtrerà tutte le stringhe contenenti 'searchtext'.
- Stringa con un prefisso, ad esempio: searchtext* , cercherà tutte le stringhe che iniziano con 'searchtext'.

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

Esempi di filtri forensi per l'attività:

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

NOTA:

1. Il conteggio delle attività visualizzato accanto all'icona Tutte le attività viene arrotondato a 30 minuti quando

l'intervallo di tempo selezionato si estende per più di 3 giorni. Ad esempio, un intervallo di tempo dal 1° settembre alle 10:15 al 7 settembre alle 10:15 mostrerà i conteggi delle attività dal 1° settembre alle 10:00 al 7 settembre alle 10:30.

2. Allo stesso modo, le metriche di conteggio mostrate nel grafico Cronologia attività vengono arrotondate a 30 minuti quando l'intervallo di tempo selezionato si estende per più di 3 giorni.

Ordinamento dei dati della cronologia delle attività forensi

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

Guida utente per le esportazioni asincrone

Panoramica

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

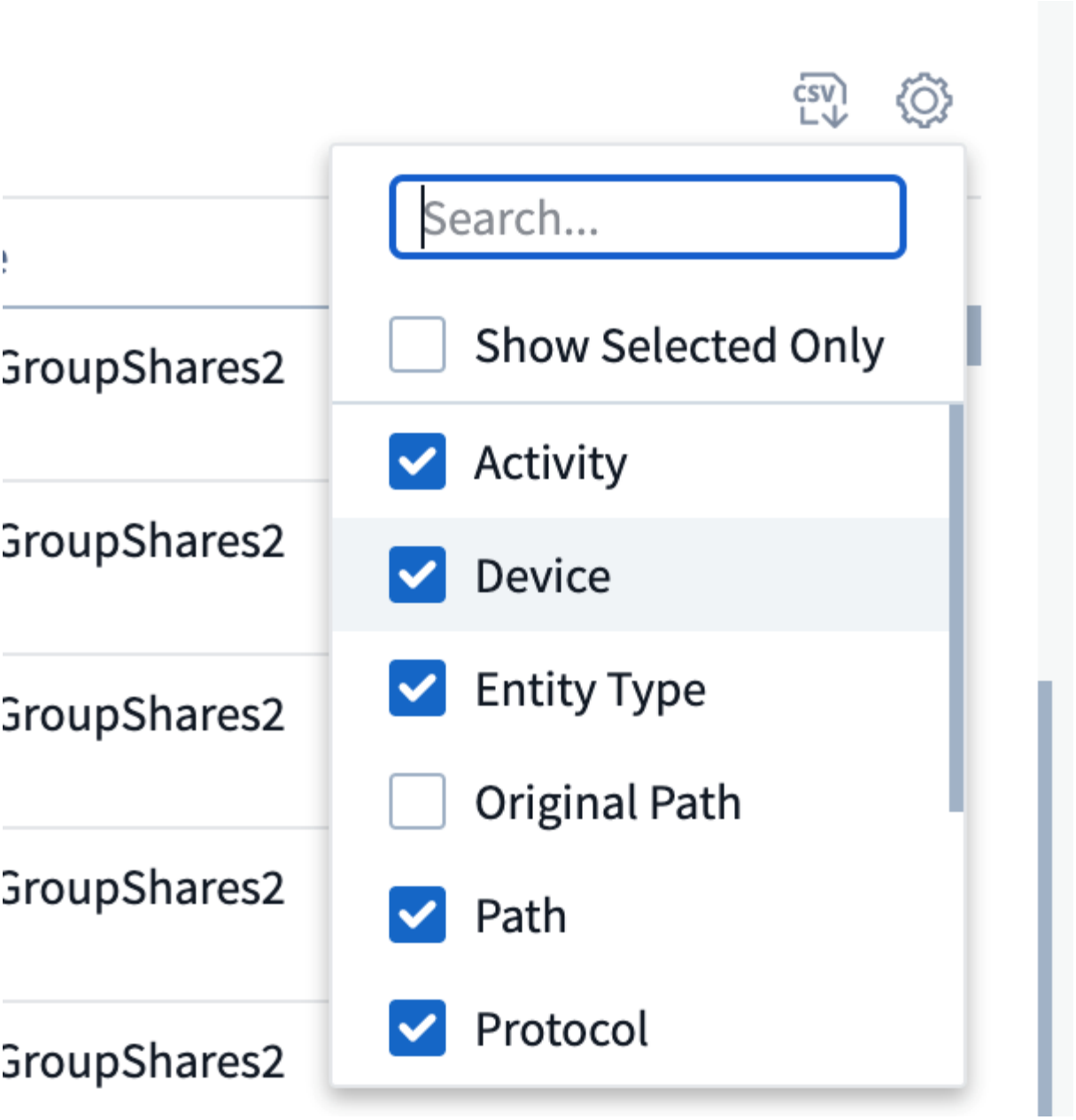
Guida passo passo: esportazione di dati con esportazioni asincrone

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

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

Selezione della colonna per tutte le attività

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



Conservazione della cronologia delle attività

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

Applicabilità dei filtri nella pagina forense

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

Ricerca percorso

I risultati della ricerca con e senza / saranno diversi

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

Modifiche all'attività dell'utente SVM radice locale

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

Per esempio:

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

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

Risoluzione dei problemi

Problema	Prova questo

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

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

Panoramica utente forense

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

Profilo utente

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

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

Comportamento dell’utente

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

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

Intervallo di aggiornamento

L’elenco degli utenti viene aggiornato ogni 12 ore.

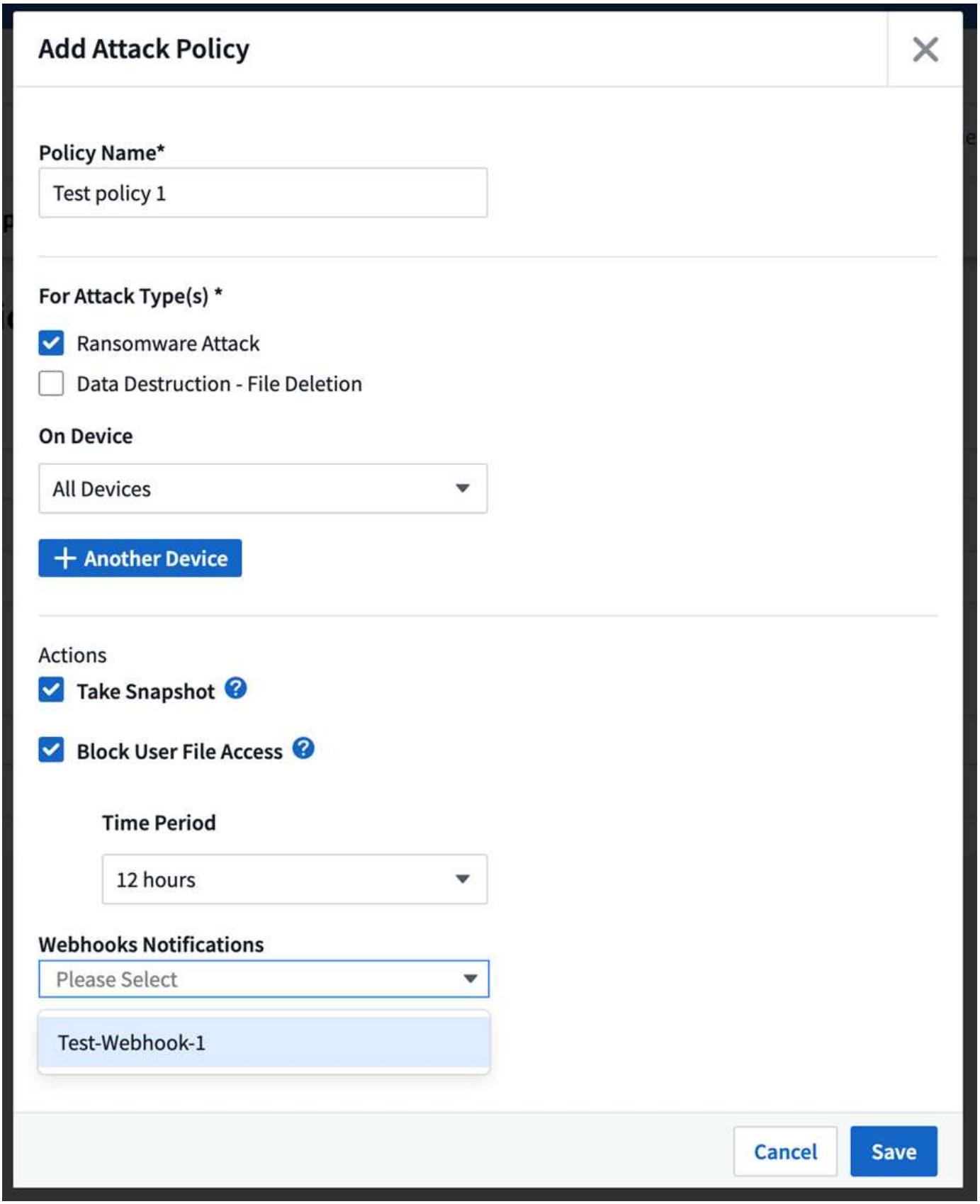
Politica di conservazione

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

Criteri di risposta automatizzati

I criteri di risposta attivano azioni quali l'acquisizione 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, seleziona **Amministrazione > Criteri di risposta automatica** e fai clic sul pulsante **+Criterio** appropriato. È possibile creare policy per gli attacchi o per gli avvisi.



È necessario salvare la policy con un nome univoco.

Per disattivare un'azione di risposta automatica (ad esempio, Acquisisci snapshot), è sufficiente deselezionare l'azione e salvare il criterio.

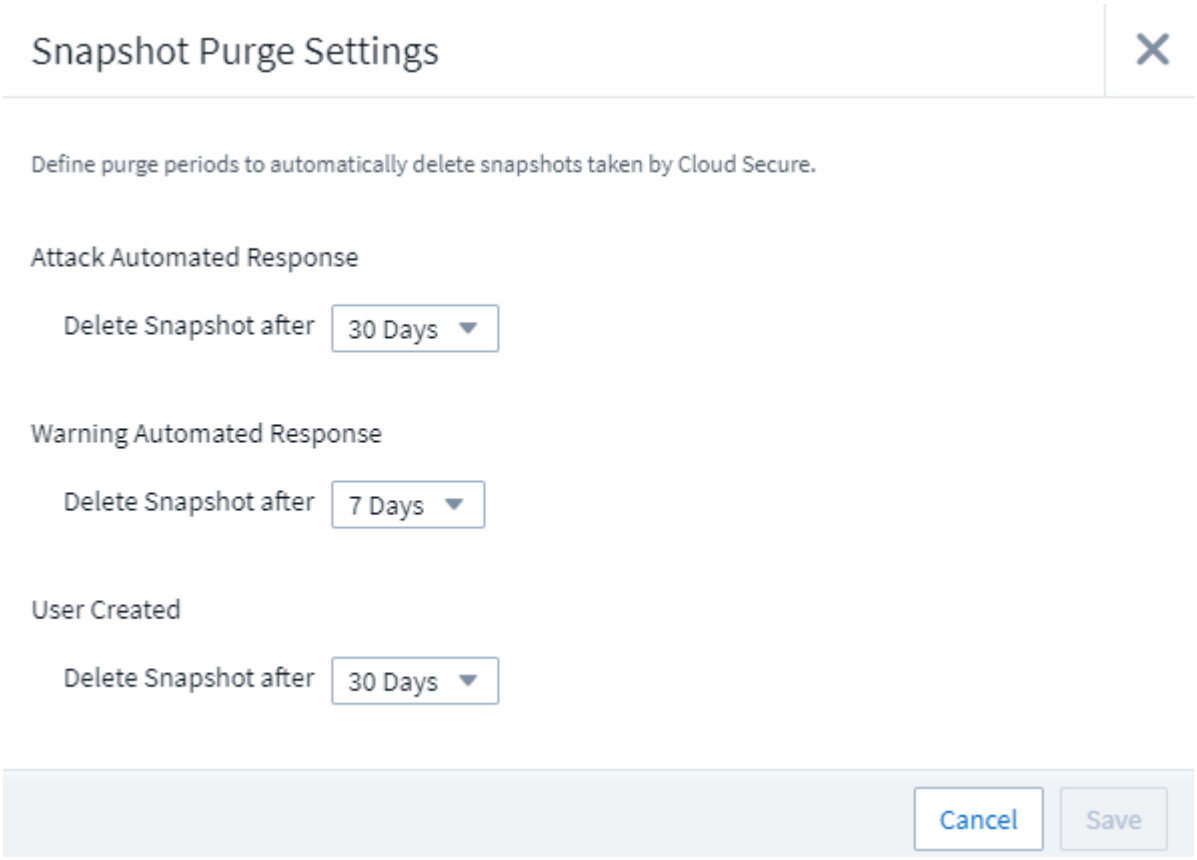
Quando viene attivato un avviso sui dispositivi specificati (o su tutti i dispositivi, se selezionati), il criterio di risposta automatica acquisisce un'istantanea dei dati. È possibile visualizzare lo stato dell'istantanea su"Pagina dei dettagli dell'avviso" .

Vedi il"Limita l'accesso degli utenti" pagina per maggiori dettagli sulla limitazione dell'accesso degli utenti tramite IP.

È possibile allegare uno o più webhook a un criterio per ricevere una notifica quando viene creato un avviso e viene intrapresa un'azione. Si consiglia di aggiungere non più di 10 webhook a una policy. Tenere presente che se una policy viene sospesa, le notifiche webhook non verranno attivate.

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

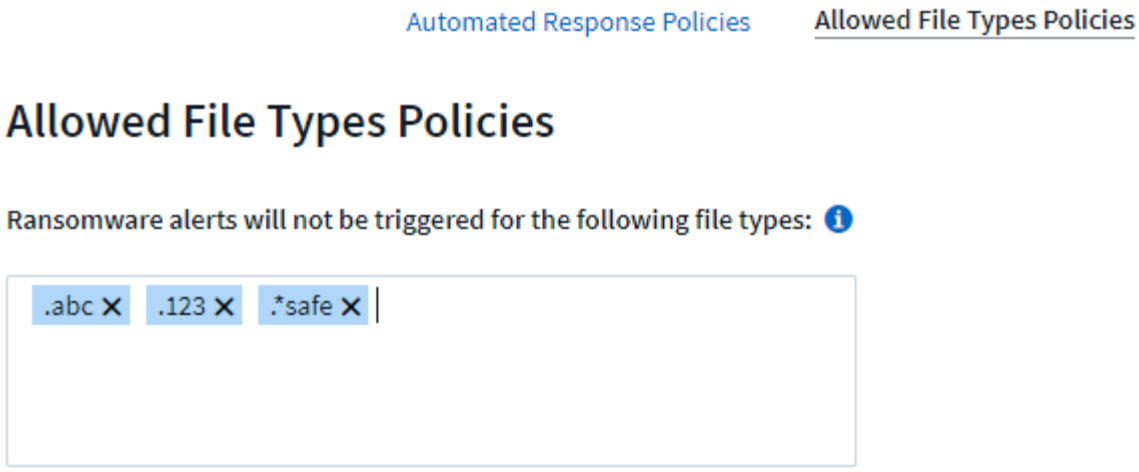
Workload Security eliminerà automaticamente gli snapshot una volta al giorno in base alle impostazioni di Snapshot Purge.



Criteri sui tipi di file consentiti

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

Passare a **Sicurezza del carico di lavoro > Criteri** e andare alla scheda *Criteri sui tipi di file consentiti*.



Una volta aggiunto all'elenco dei *tipi di file consentiti*, non verrà generato alcun avviso di attacco di manomissione dei file per quel tipo di file consentito. Si noti che la politica *Tipi di file consentiti* è applicabile solo per il rilevamento di manomissioni di file.

Ad esempio, se un file denominato *test.txt* viene rinominato in *test.txt.abc* e Workload Security rileva un attacco di manomissione del file a causa dell'estensione *.abc*, l'estensione *.abc* può essere aggiunta all'elenco dei *tipi di file consentiti*. Dopo l'aggiunta all'elenco, gli attacchi di manomissione dei file non verranno più generati contro i 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 autonoma dai ransomware ONTAP

La funzionalità di protezione autonoma ONTAP utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e segnalare attività anomale nei file che potrebbero indicare attacchi dannosi o modifiche non autorizzate dei dati.

Ulteriori dettagli e requisiti di licenza su ARP possono essere trovati"Qui" .

Workload Security 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 ed esegue le seguenti azioni:

1. Correla gli eventi di crittografia del volume con l'attività dell'utente per identificare chi sta causando il danno.
2. Implementa politiche di risposta automatica (se definite)
3. Fornisce funzionalità forensi:
    - Consentire ai clienti di condurre indagini sulle violazioni dei dati.
    - Identificare i file interessati, contribuendo a un recupero più rapido e a condurre indagini sulle violazioni dei dati.

Prerequisiti

1. Versione minima ONTAP : 9.11.1
2. Volumi abilitati ARP. I dettagli sull'abilitazione di ARP possono essere trovati"Qui" . ARP deve essere abilitato tramite OnCommand System Manager. Workload Security non può abilitare ARP.
3. Il collettore di sicurezza del carico di lavoro deve essere aggiunto tramite l'IP del cluster.
4. Per il funzionamento di questa funzionalità sono necessarie le credenziali a livello di cluster. In altre parole, quando si aggiunge l'SVM è necessario utilizzare le credenziali a livello di cluster.

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 concesse all'utente, seguire i passaggi sottostanti per concedere a Workload Security le autorizzazioni per raccogliere informazioni relative ad ARP da ONTAP.

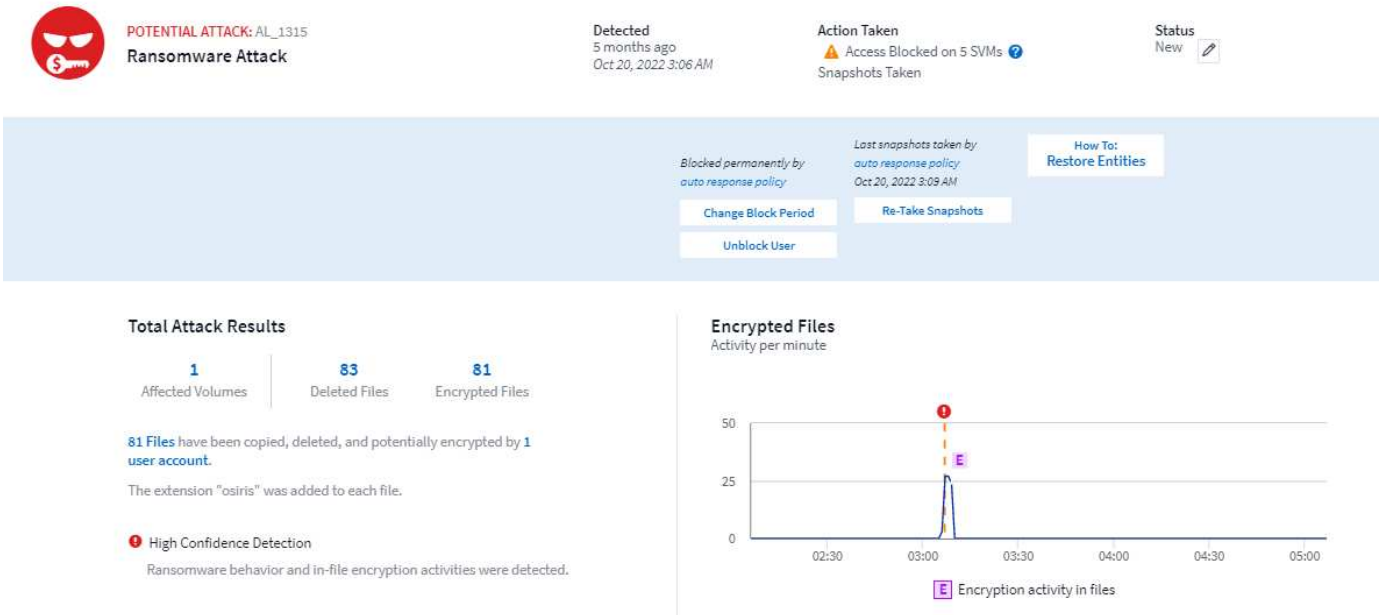
Per *csuser* con credenziali del cluster, procedere come segue dalla riga di comando ONTAP :

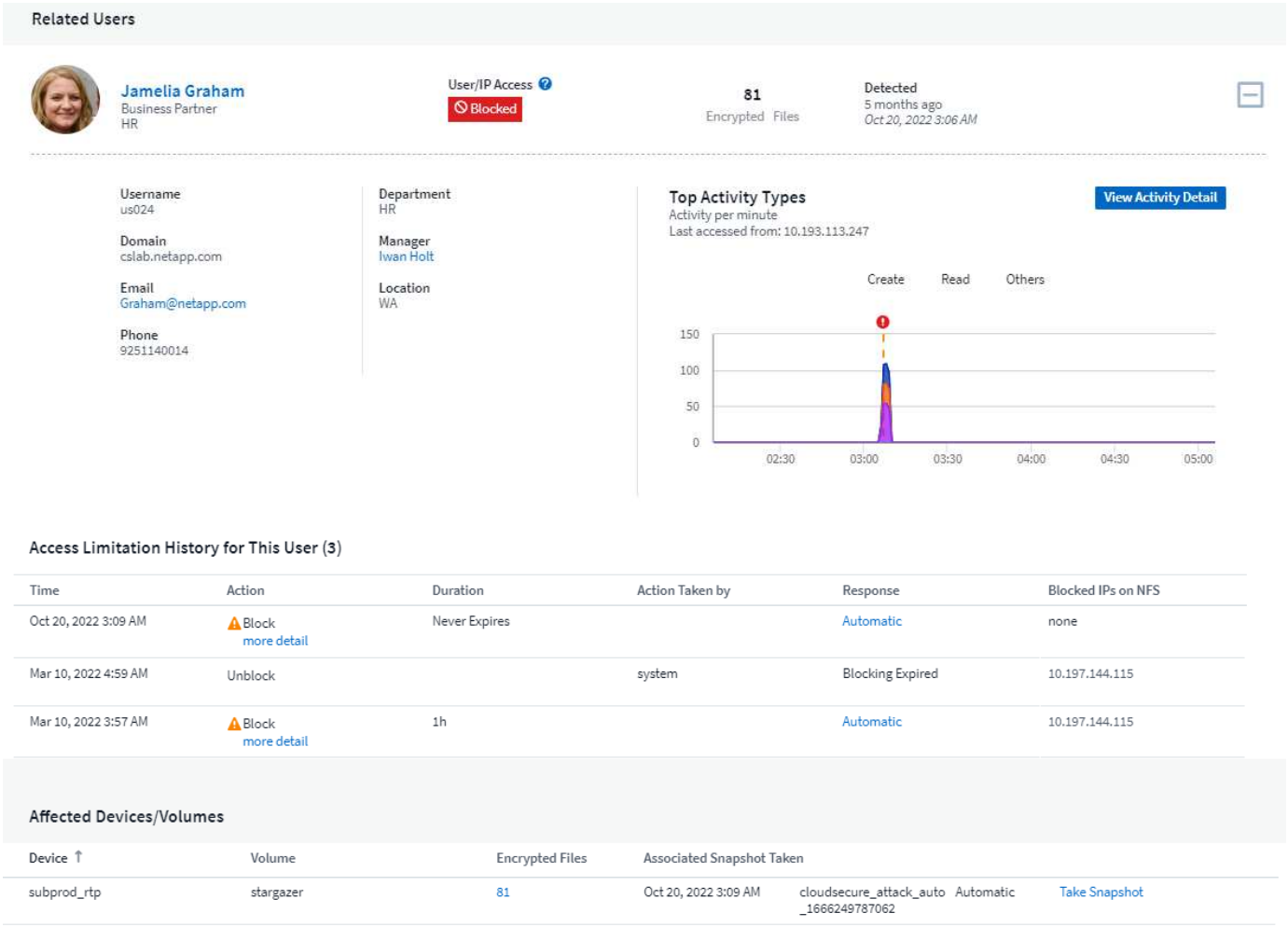
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

Per saperne di più sulla configurazione di altri"Autorizzazioni ONTAP" .

Esempio di avviso

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





Un banner di alta affidabilità indica che l'attacco ha mostrato un comportamento di manomissione dei file insieme ad attività di crittografia dei file. Il grafico dei file crittografati indica il timestamp in cui l'attività di crittografia del volume è stata rilevata dalla soluzione ARP.

Limitazioni

Nel caso in cui un SVM non sia monitorato da Workload Security, ma vi siano eventi ARP generati da ONTAP, gli eventi verranno comunque ricevuti e visualizzati da Workload Security. Tuttavia, le informazioni forensi relative all'avviso, così come la mappatura degli utenti, non verranno acquisite o mostrate.

Risoluzione dei problemi

Nella tabella seguente sono descritti i problemi noti e le relative soluzioni.

Problema:	Risoluzione:
Gli avvisi via e-mail vengono ricevuti 24 ore dopo il rilevamento di un attacco. Nell'interfaccia utente, gli avvisi vengono visualizzati 24 ore prima che le e-mail vengano ricevute da Data Infrastructure Insights Workload Security.	Quando ONTAP invia l'evento *Ransomware Detected* a Data Infrastructure Insights Workload Security (ovvero Workload Security), l'e-mail viene inviata. L'evento contiene un elenco degli attacchi e i relativi timestamp. L'interfaccia utente di Workload Security visualizza il timestamp dell'avviso del primo file attaccato. ONTAP invia l'evento *Ransomware Detected* a Data Infrastructure Insights quando viene codificato un certo numero di file. Potrebbe quindi esserci una differenza tra l'orario in cui l'avviso viene visualizzato nell'interfaccia utente e l'orario in cui viene inviata l'e-mail.

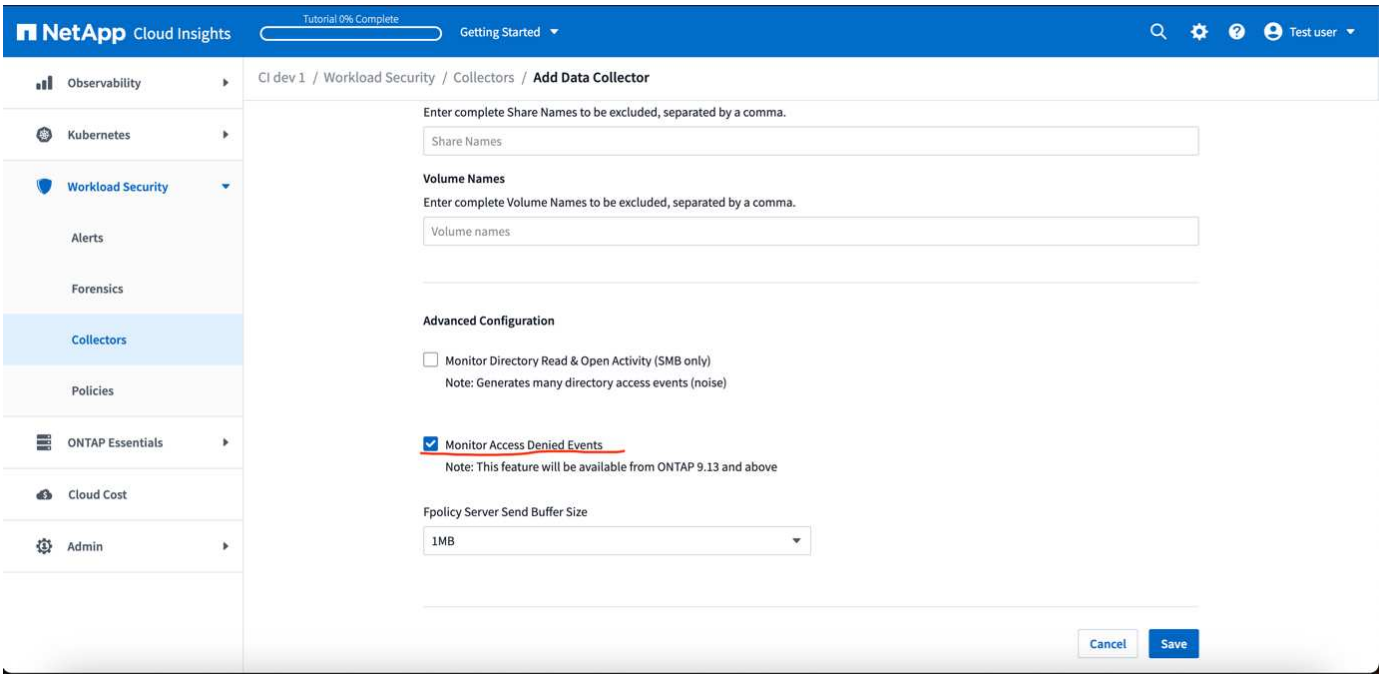
Integrazione con ONTAP Accesso negato

La funzionalità ONTAP Access Denied utilizza l'analisi del carico di lavoro negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e avvisare in caso di operazioni sui file non riuscite (ad esempio, un utente che tenta di eseguire un'operazione per la quale non ha l'autorizzazione). Queste notifiche di operazioni sui file non riuscite, soprattutto in caso di errori legati alla sicurezza, aiuteranno ulteriormente a bloccare gli attacchi interni nelle fasi iniziali.

Data Infrastructure Insights Workload Security si integra con ONTAP per ricevere eventi di accesso negato e fornire un ulteriore livello di risposta automatica e analitica.

Prerequisiti

- Versione minima ONTAP : 9.13.0.
- Un amministratore di Workload Security deve abilitare la funzionalità Accesso negato durante l'aggiunta di un nuovo collector o la modifica di un collector esistente, selezionando la casella di controllo *Monitora eventi di accesso negato* in Configurazione avanzata.



Autorizzazioni utente richieste

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

Se il Collector viene aggiunto tramite un utente personalizzato (ad esempio, *csuser*) con autorizzazioni concesse all'utente, seguire i passaggi sottostanti per concedere a Workload Security l'autorizzazione necessaria per registrarsi per gli eventi di accesso negato con ONTAP.

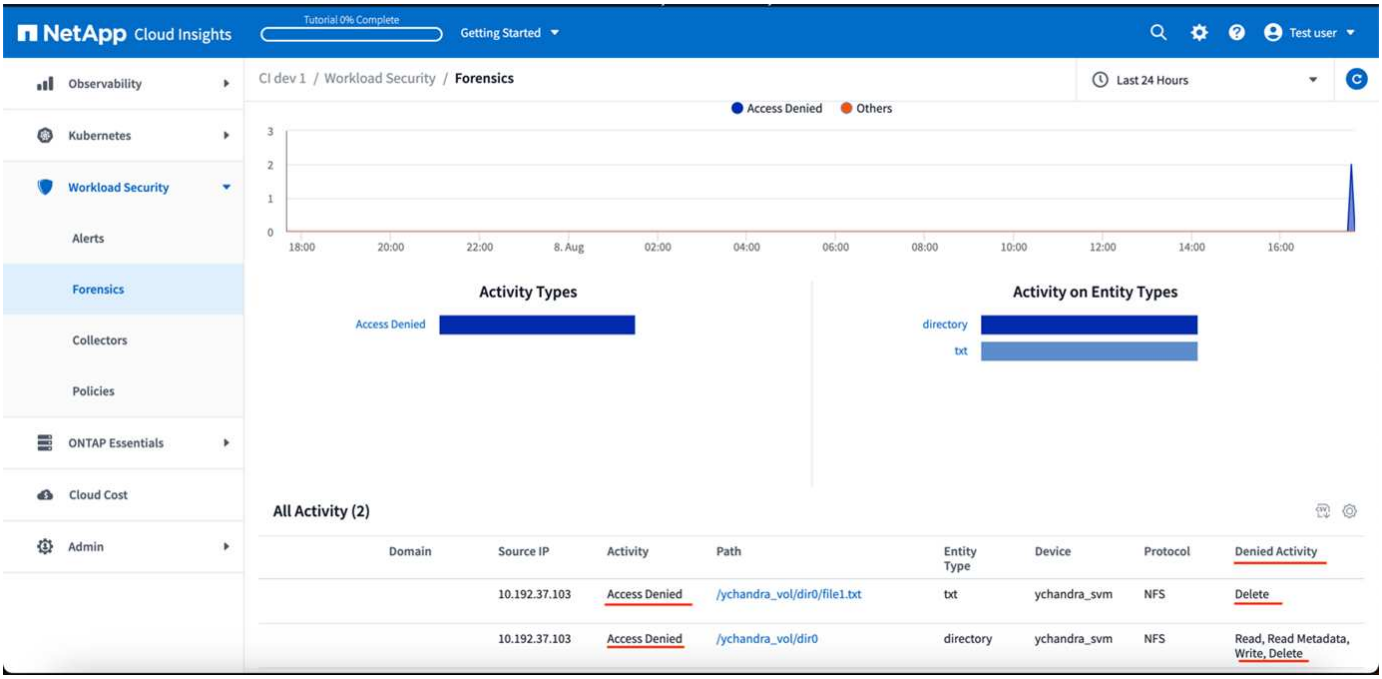
Per csuser con credenziali *cluster*, eseguire i seguenti comandi dalla riga di comando ONTAP . Si noti che questa autorizzazione potrebbe già esistere.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Per csuser con credenziali _SVM_, eseguire i seguenti comandi dalla riga
di comando ONTAP .  Si noti che questa autorizzazione potrebbe già
esistere.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
Per saperne di più sulla configurazione di
altrilink:task_add_collector_svm.html["Autorizzazioni ONTAP"] .
```

Eventi di accesso negato

Una volta acquisiti gli eventi dal sistema ONTAP , la pagina Workload Security Forensics mostrerà gli eventi di accesso negato. Oltre alle informazioni visualizzate, è possibile visualizzare le autorizzazioni utente mancanti per una particolare operazione aggiungendo la colonna *Attività desiderata* alla tabella tramite l'icona a forma di ingranaggio.



Blocco dell'accesso degli utenti per fermare gli attacchi

Interrompere immediatamente gli attacchi rilevati bloccando l'accesso degli utenti compromessi per impedire ulteriori danni ai dati o l'esfiltrazione. Workload Security consente sia il blocco automatico tramite criteri di risposta automatizzati sia l'intervento manuale dalle pagine di avviso o dei dettagli dell'utente, offrendoti un controllo flessibile sulla tua risposta di sicurezza. Le restrizioni di accesso si applicano automaticamente a tutti i volumi di archiviazione monitorati e sono limitate nel tempo per il ripristino automatico.

L'utente viene bloccato direttamente per SMB e l'indirizzo IP delle macchine host che causano l'attacco verrà bloccato per NFS. A tali indirizzi IP delle macchine verrà impedito l'accesso a qualsiasi Storage Virtual Machine (SVM) monitorata da Workload Security.

Ad esempio, supponiamo che Workload Security gestisca 10 SVM e che la politica di risposta automatica sia configurata per quattro di queste SVM. Se l'attacco ha origine in una delle quattro SVM, l'accesso dell'utente verrà bloccato in tutte e 10 le SVM. Viene comunque eseguito uno snapshot sull'SVM di origine.

Se sono presenti quattro SVM, di cui una configurata per SMB, una per NFS e le restanti due configurate sia per NFS che per 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 le 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 concesse all'utente, seguire i passaggi seguenti per concedere a Workload Security le autorizzazioni per bloccare l'utente.

Per csuser con credenziali cluster, procedere come segue 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
```

Assicurati di rivedere la sezione Autorizzazioni del"Configurazione del raccoglitore dati ONTAP SVM" anche la pagina.

Come abilitare la funzionalità?

- In Workload Security, vai a **Workload Security > Criteri > Criteri di risposta automatica**. Seleziona **+Politica di attacco**.
- Selezionare (selezionare) *Blocca accesso file utente*.

Come impostare il blocco automatico dell'accesso degli utenti?

- Crea una nuova politica di attacco o modifica una politica di attacco esistente.
- Selezionare le SVM su cui monitorare la policy di attacco.
- Fare clic sulla casella di controllo "Blocca accesso file utente". La funzionalità verrà abilitata quando questa opzione è selezionata.
- In "Periodo di tempo" seleziona l'orario fino al quale deve essere applicato il blocco.
- Per testare il blocco automatico degli utenti, puoi simulare un attacco tramite un"sceneggiatura simulata" .

Come sapere se ci sono utenti bloccati nel sistema?

- Nella pagina degli elenchi di avvisi, verrà visualizzato un banner nella parte superiore dello schermo nel caso in cui un utente venga bloccato.
- Cliccando sul banner verrai indirizzato alla pagina "Utenti", dove potrai vedere l'elenco degli utenti bloccati.
- Nella pagina "Utenti", c'è una colonna denominata "Accesso utente/IP". In quella colonna verrà visualizzato lo stato attuale del blocco dell'utente.

Limitare e gestire manualmente l'accesso degli utenti

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

Cronologia delle limitazioni di accesso utente

Nella pagina dei dettagli dell'avviso e dei dettagli dell'utente, nel pannello utente, è possibile visualizzare un controllo della cronologia delle limitazioni di accesso dell'utente: ora, azione (blocca, sblocca), durata, azione intrapresa da, manuale/automatica e IP interessati per NFS.

Come disattivare la funzione?

Puoi disattivare questa funzione in qualsiasi momento. Se nel sistema sono presenti utenti con restrizioni, è necessario prima ripristinare il loro accesso.

- In Workload Security, vai a **Workload Security > Criteri > Criteri di risposta automatica**. Seleziona **+Politica di attacco**.
- Deseleziona (deseleziona) *Blocca accesso file utente*.

La funzionalità verrà nascosta da tutte le pagine.

Ripristina manualmente gli IP per NFS

Per ripristinare manualmente gli IP da ONTAP se il periodo di prova di Workload Security scade o se l'agente/collettore è inattivo, attenersi alla seguente procedura.

1. Elenca tutte le policy 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 in tutti i criteri sull'SVM che hanno "cloudsecure_rule" come corrispondenza client specificando il rispettivo RuleIndex. La regola di sicurezza del carico di lavoro sarà solitamente impostata su 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Assicurarsi che la regola Workload Security sia stata eliminata
(passaggio facoltativo per la conferma).
```

```
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.
```

Ripristina manualmente gli utenti per SMB

Per ripristinare manualmente gli utenti da ONTAP se il periodo di prova di Workload Security scade o se l'agente/collector è inattivo, procedere come segue.

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

1. Accedi al cluster ONTAP (in cui desideri 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.
```

Nell'output sopra riportato, 2 utenti sono stati bloccati (US030, US040) con dominio CSLAB.

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

```
 vserver name-mapping delete -direction win-unix -position <position>
. Per confermare che gli utenti siano sbloccati, eseguire il comando:
```

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

Non devono essere visualizzate voci per gli utenti precedentemente bloccati.

Risoluzione dei problemi

Problema	Prova questo
Alcuni utenti non sono soggetti a restrizioni, nonostante ci sia un attacco.	1. Assicurarsi che il Data Collector e l'agente per le SVM siano nello stato *In esecuzione*. Workload Security non sarà in grado di inviare comandi se Data Collector e Agent sono arrestati. 2. Ciò accade perché l'utente potrebbe aver avuto accesso all'archiviazione da una macchina con un nuovo IP mai utilizzato in precedenza. La limitazione avviene tramite l'indirizzo IP dell'host tramite il quale l'utente accede allo storage. Controllare nell'interfaccia utente (Dettagli avviso > Cronologia limitazioni di accesso per questo utente > IP interessati) l'elenco degli indirizzi IP soggetti a restrizioni. Se l'utente accede allo storage da un host con un IP diverso dagli IP con restrizioni, potrà comunque accedere allo storage tramite l'IP senza restrizioni. Se l'utente tenta di accedere dagli host i cui IP sono limitati, l'archiviazione non sarà accessibile.
Cliccando manualmente su Limita accesso si ottiene il messaggio "Gli indirizzi IP di questo utente sono già stati limitati".	L'IP da limitare è già limitato a un altro utente.
La politica non può essere modificata. Motivo: non autorizzato per quel comando.	Controllare se si utilizza csuser, che le autorizzazioni siano concesse all'utente come indicato sopra.

Problema	Prova questo
Il blocco dell'utente (indirizzo IP) per NFS funziona, ma per SMB/CIFS vedo un messaggio di errore: "La trasformazione da SID a DomainName non è riuscita. Motivo del timeout: il socket non è stato stabilito"	Ciò può accadere se *csuser* non ha l'autorizzazione per eseguire ssh. (Assicurarsi che la connessione sia 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, procedere come segue 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 Se *csuser* non viene utilizzato e se viene utilizzato l'utente amministratore a livello di cluster, assicurarsi che l'utente amministratore disponga dell'autorizzazione SSH per ONTAP.
Ricevo il messaggio di errore *SID translate failed. Reason:255:Error: command failed: not authorized for that commandError: "access-check" is not a recognized command*, quando un utente avrebbe dovuto essere bloccato.	Ciò può accadere quando *csuser* non dispone delle autorizzazioni corrette. Vedere "Prerequisiti per il blocco dell'accesso utente" per maggiori informazioni. Dopo aver applicato le autorizzazioni, si consiglia di riavviare il raccoglitore dati ONTAP e il raccoglitore dati della directory utente. Di seguito sono elencati i comandi di autorizzazione richiesti. ---- creazione ruolo di accesso di sicurezza -role csrole -cmddirname "regola policy di esportazione vserver" -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname set -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname "sessione cifs vserver" -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname "traduzione autenticazione controllo accesso servizi vserver" -access all creazione ruolo di accesso di sicurezza -role csrole -cmddirname "mappatura nome vserver" -access all ----

Sicurezza del carico di lavoro: simulazione della manomissione dei file

È possibile utilizzare le istruzioni presenti in questa pagina per simulare la manomissione dei file a scopo di test o dimostrazione della sicurezza del carico di lavoro utilizzando lo script di simulazione della manomissione dei file incluso.

Cose da notare prima di iniziare

- Lo script di simulazione della manomissione dei file funziona solo su Linux. Lo script di simulazione dovrebbe anche generare avvisi di elevata affidabilità nel caso in cui l'utente abbia integrato ONTAP ARP con Workload Security.
- Workload Security rileverà gli eventi e gli avvisi generati con NFS 4.1 solo se la versione ONTAP è 9.15 o successiva.
- Lo script è fornito con i file di installazione dell'agente Workload Security. È disponibile su qualsiasi macchina su cui sia installato un agente Workload Security.
- È possibile eseguire lo script direttamente sulla macchina dell'agente Workload Security; non è necessario preparare un'altra macchina Linux. Tuttavia, se preferisci eseguire lo script su un altro sistema, ti basterà copiarlo ed eseguirlo lì.
- Gli utenti possono scegliere tra Python o script shell in base alle proprie preferenze e ai requisiti di sistema.
- Lo script Python richiede installazioni preliminari. Se non vuoi usare Python, usa lo script shell.

Linee guida:

Questo script dovrebbe essere eseguito su una SVM contenente una cartella con un numero considerevole di file da crittografare, idealmente 100 o più, inclusi i file nelle sottocartelle. Assicurarsi che i file non siano vuoti.

Per generare l'avviso, mettere temporaneamente in pausa il raccoglitore prima di creare i dati di prova. Una volta generati i file di esempio, riavviare il raccoglitore e avviare il processo di crittografia.

Passaggi:

Preparare il sistema:

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

Abilita ONTAP Autonomous Ransomware Protection (facoltativo):

Se la versione del cluster ONTAP è 9.11.1 o successiva, è possibile abilitare il servizio ONTAP Ransomware Protection eseguendo il seguente comando sulla console di comando ONTAP .

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Successivamente, configura un Data Collector:
```

1. Configurare l'agente Workload Security se non è già stato fatto.
2. Se non è già stato fatto, configurare un raccoglitore dati SVM.
3. Assicurarsi che il protocollo di montaggio sia selezionato durante la configurazione del raccoglitore dati.

Generare i file di esempio a livello di programmazione:

Prima di creare i file, è necessario prima arrestare o"mettere in pausa il raccoglitore dati" elaborazione.

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 degli script inclusi per creare i file in modo programmatico. Qualunque sia il metodo utilizzato, assicurati che siano presenti almeno 100 file da crittografare.

Se si sceglie di creare i file a livello di programmazione, è possibile utilizzare Shell o Python:

Conchiglia:

1. Accedi alla casella Agente.
2. Montare una condivisione NFS o CIFS dall'SVM del filer alla macchina dell'agente. Vai a quella cartella.
3. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) nella posizione di montaggio di destinazione.
4. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per creare la cartella e i file del set di dati di prova:

```
 './create_dataset.sh'
. Verranno creati 100 file non vuoti con varie estensioni all'interno
della cartella di montaggio, in una directory denominata "test_dataset".
```

Pitone:

Prerequisito per lo script Python:

- Installa Python (se non è già installato).
  - Scarica Python 3.5.2 o versione successiva da https://www.python.org/ .
  - Per verificare l'installazione di Python, eseguire `python --version` .
  - Lo script Python è stato testato a partire dalla versione 3.5.2.
- Installare pip se non è già installato:
  - Scarica lo script get-pip.py da https://bootstrap.pypa.io/ .
  - Installa pip usando `python get-pip.py` .

- Verificare l'installazione del pip con `pip --version` .

- Libreria PyCryptodome:
  - Lo script utilizza la libreria PyCryptodome.
  - Installa PyCryptodome con `pip install pycryptodome` .
  - Confermare l'installazione di PyCryptodome eseguendo `pip show pycryptodome` .

Script di creazione file Python:

1. Accedi alla casella Agente.
2. Montare una condivisione NFS o CIFS dall'SVM del filer alla macchina dell'agente. Vai a quella cartella.
3. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) nella posizione di montaggio di destinazione.
4. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per creare la cartella e i file del set di dati di prova:

```
 'python create_dataset.py'
. Questo creerà 100 file non vuoti con varie estensioni all'interno
della cartella di montaggio sotto una directory chiamata "test_dataset"
```

Riprendi il collezionista

Se hai messo in pausa il raccoglitore prima di seguire questi passaggi, assicurati di riavviarlo una volta creati i file di esempio.

Generare i file di esempio a livello di programmazione:

Prima di creare i file, è necessario prima arrestare o"mettere in pausa il raccoglitore dati" elaborazione.

Per generare un avviso di manomissione di file, è possibile eseguire lo script incluso che simulerà un avviso di manomissione di file in Workload Security.

Conchiglia:

1. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) nella posizione di montaggio di destinazione.
2. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per crittografare il set di dati di prova:

```
 './simulate_attack.sh'
. In questo modo verranno crittografati i file di esempio creati nella
directory "test_dataset".
```

Pitone:

1. Copiare lo script dalla directory di installazione dell'agente (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) nella posizione di montaggio di destinazione.
2. Si prega di notare che i prerequisiti Python sono installati come da sezione Prerequisiti dello script Python
3. Eseguire il seguente comando utilizzando gli script all'interno della directory montata (ad esempio /root/demo) per crittografare il set di dati di prova:

```
 'python simulate_attack.py'
. In questo modo verranno crittografati i file di esempio creati nella
directory "test_dataset".
```

Genera un avviso in Workload Security

Una volta terminata l'esecuzione dello script del simulatore, entro pochi minuti verrà visualizzato un avviso sull'interfaccia utente Web.

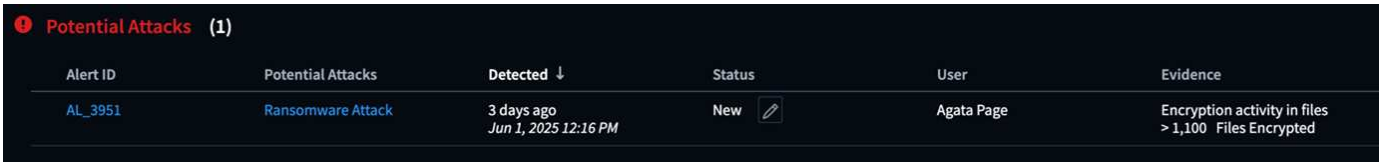
Nota: nel caso in cui siano soddisfatte tutte le seguenti condizioni, verrà generato un avviso di elevata affidabilità.

1. Versione ONTAP di SVM monitorata superiore a 9.11.1
2. Protezione autonoma dal ransomware ONTAP configurata
3. Il raccoglitore di dati di sicurezza del carico di lavoro è stato aggiunto in modalità Cluster.

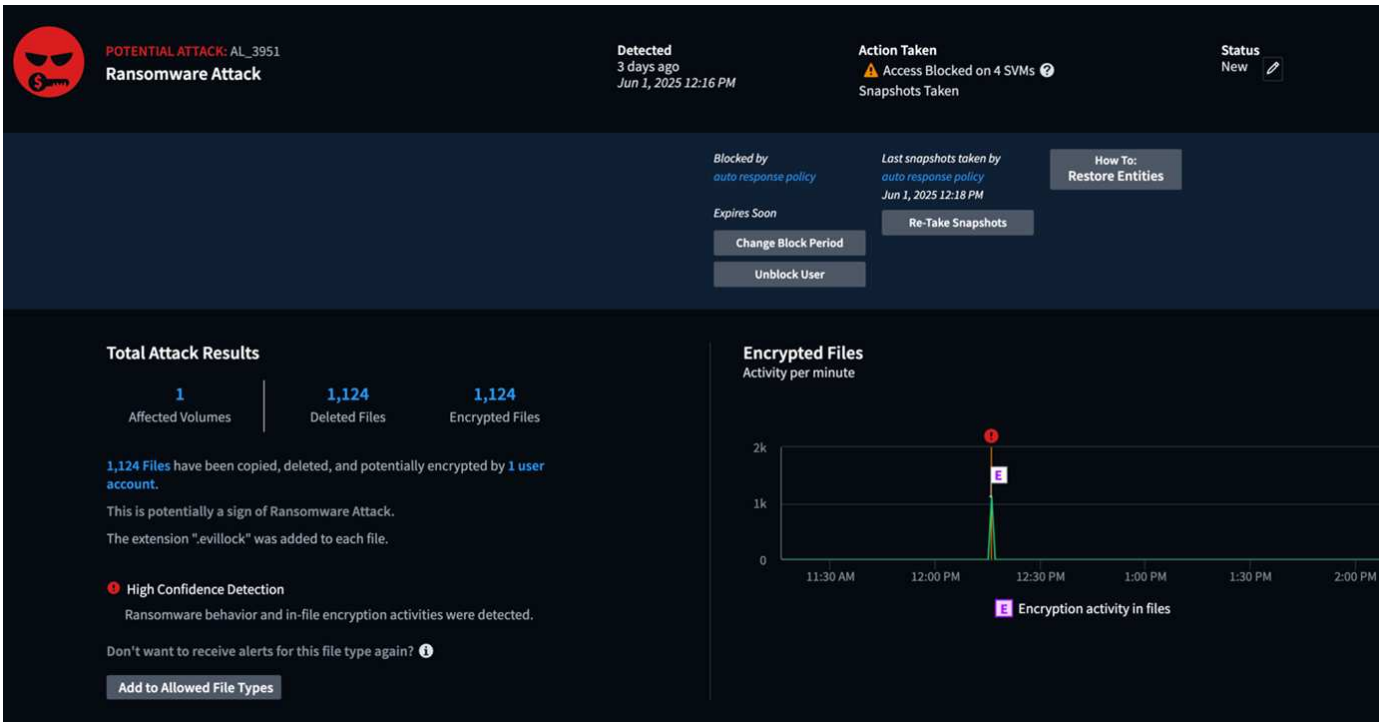
Workload Security rileva i modelli di manomissione dei file in base al comportamento dell'utente, mentre ONTAP ARP rileva le attività di manomissione dei file in base alle attività di crittografia nei file.

Se le condizioni sono soddisfatte, Workload Security contrassegna gli avvisi come avviso di elevata affidabilità.

Esempio di avviso di elevata affidabilità nella pagina dell'elenco degli avvisi:



Esempio di dettaglio dell'avviso di elevata affidabilità:



Attivazione dell'avviso più volte

Workload Security apprende il comportamento dell'utente e non genererà avvisi in caso di ripetuti attacchi di manomissione dei file entro 24 ore per lo stesso utente.

Per generare un nuovo avviso con un utente diverso, ripetere gli stessi passaggi (creazione dei dati di prova e successiva crittografia dei dati di prova).

Configurazione delle notifiche e-mail per avvisi, avvertenze e stato di integrità dell'agente/collettore dell'origine dati

Le notifiche e-mail ti consentono di rimanere informato su potenziali attacchi, avvisi di sicurezza e problemi di integrità dell'infrastruttura non appena si verificano. Configura gli indirizzi email dei destinatari nelle impostazioni Amministrazione > Notifiche per ricevere avvisi in tempo reale personalizzati in base alle responsabilità di ciascun destinatario.

Avvisi e avvisi di potenziali attacchi

Per inviare notifiche di avviso di *Potenziale attacco*, inserisci gli indirizzi email dei destinatari nella sezione *Invia avvisi di potenziale attacco*. Per ogni azione sull'avviso vengono inviate notifiche e-mail all'elenco dei destinatari dell'avviso.

Per inviare notifiche di *Avviso*, inserisci gli indirizzi email dei destinatari nella sezione *Invia avvisi di avviso*.

Monitoraggio dello stato di salute dell'agente e del raccoglitore dati

È possibile monitorare lo stato di salute degli agenti e delle origini dati tramite notifiche.

Per ricevere notifiche nel caso in cui un agente o un raccoglitore di origini dati non funzioni, immettere gli indirizzi e-mail dei destinatari nella sezione *Avvisi sullo stato di integrità della raccolta dati*.

Tieni presente quanto segue:

- Gli avvisi sanitari verranno inviati solo dopo che l'agente/esattore avrà smesso di segnalare per almeno un'ora.
- Viene inviata una sola notifica e-mail ai destinatari previsti in un dato periodo di 24 ore, anche se l'agente o il raccoglitore dati sono disconnessi per un periodo di tempo più lungo.
- In caso di errore dell'agente, verrà inviato un avviso (non uno per ogni collettore). L'e-mail conterrà un elenco di tutti gli SVM interessati.
- L'errore di raccolta di Active Directory viene segnalato come avviso; non influisce sul rilevamento delle minacce.
- L'elenco di configurazione introduttiva ora include una nuova fase *Configura notifiche e-mail*.

Ricezione di notifiche di aggiornamento dell'agente e del raccoglitore dati

- Inserire l'ID e-mail in "Avvisi sanitari sulla raccolta dati".
- La casella di controllo "Abilita notifiche di aggiornamento" diventa abilitata.
- Le notifiche e-mail relative all'aggiornamento di Agent e Data Collector vengono inviate agli ID e-mail un giorno prima dell'aggiornamento pianificato.

Risoluzione dei problemi

Problema:	Prova questo:
Gli ID e-mail sono presenti negli "Avvisi sullo stato di salute del Data Collector", tuttavia non ricevo notifiche.	Le email di notifica vengono inviate dal dominio NetApp Data Infrastructure Insights , ovvero da *accounts@service.cloudinsights.netapp.com*. Alcune aziende bloccano le email in arrivo se provengono da un dominio esterno. Assicurarsi che le notifiche esterne provenienti dai domini NetApp Data Infrastructure Insights siano inserite nella whitelist.

Notifiche webhook

Notifiche di sicurezza del carico di lavoro tramite webhook

I webhook consentono agli utenti di inviare notifiche di avviso critiche o di avvertimento a varie applicazioni utilizzando un canale webhook personalizzato.

Molte applicazioni commerciali supportano i webhook come interfaccia di input standard, ad esempio: Slack, PagerDuty, Teams e Discord. Supportando un canale webhook generico e personalizzabile, Workload Security può supportare molti di questi canali di distribuzione. Le informazioni sulla configurazione dei webhook sono disponibili sui siti web delle rispettive applicazioni. Ad esempio, Slack fornisce"questa guida utile" .

È possibile creare più canali webhook, ognuno dei quali è destinato a uno scopo diverso, ad applicazioni separate, a destinatari diversi, ecc.

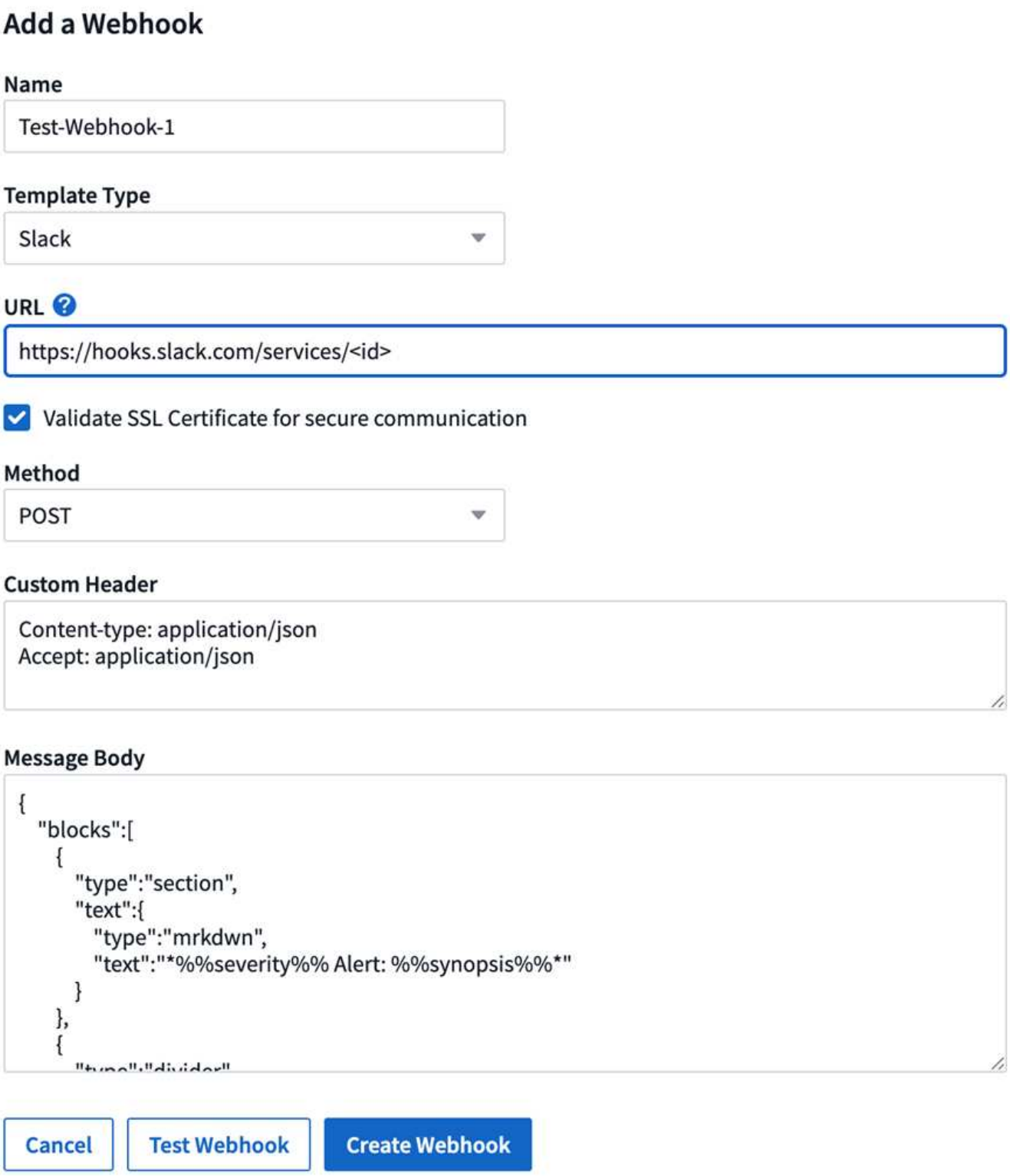
L'istanza del canale webhook è composta dai seguenti elementi

Nome	Descrizione
URL	URL di destinazione del webhook, incluso il prefisso http:// o https:// insieme ai parametri URL
Metodo	GET/POST - Il valore predefinito è POST
Intestazione personalizzata	Specifica qui eventuali intestazioni personalizzate
Corpo del messaggio	Inserisci qui il corpo del tuo messaggio
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri e i segreti personalizzati consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook di sicurezza del carico di lavoro, vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". L'immagine seguente mostra un esempio di schermata di creazione di un webhook Slack.

Nota: per creare e gestire i webhook di Workload Security, l'utente deve essere un amministratore di Workload Security.



- Inserisci le informazioni appropriate per ciascun campo e fai clic su "Salva".
- Puoi anche cliccare sul pulsante "Test Webhook" per testare la connessione. Si noti che in questo modo verrà inviato il "Corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.
- I webhook SWS comprendono una serie di parametri predefiniti. Inoltre, puoi creare parametri o segreti personalizzati.

Parametri: cosa sono e come utilizzarli?

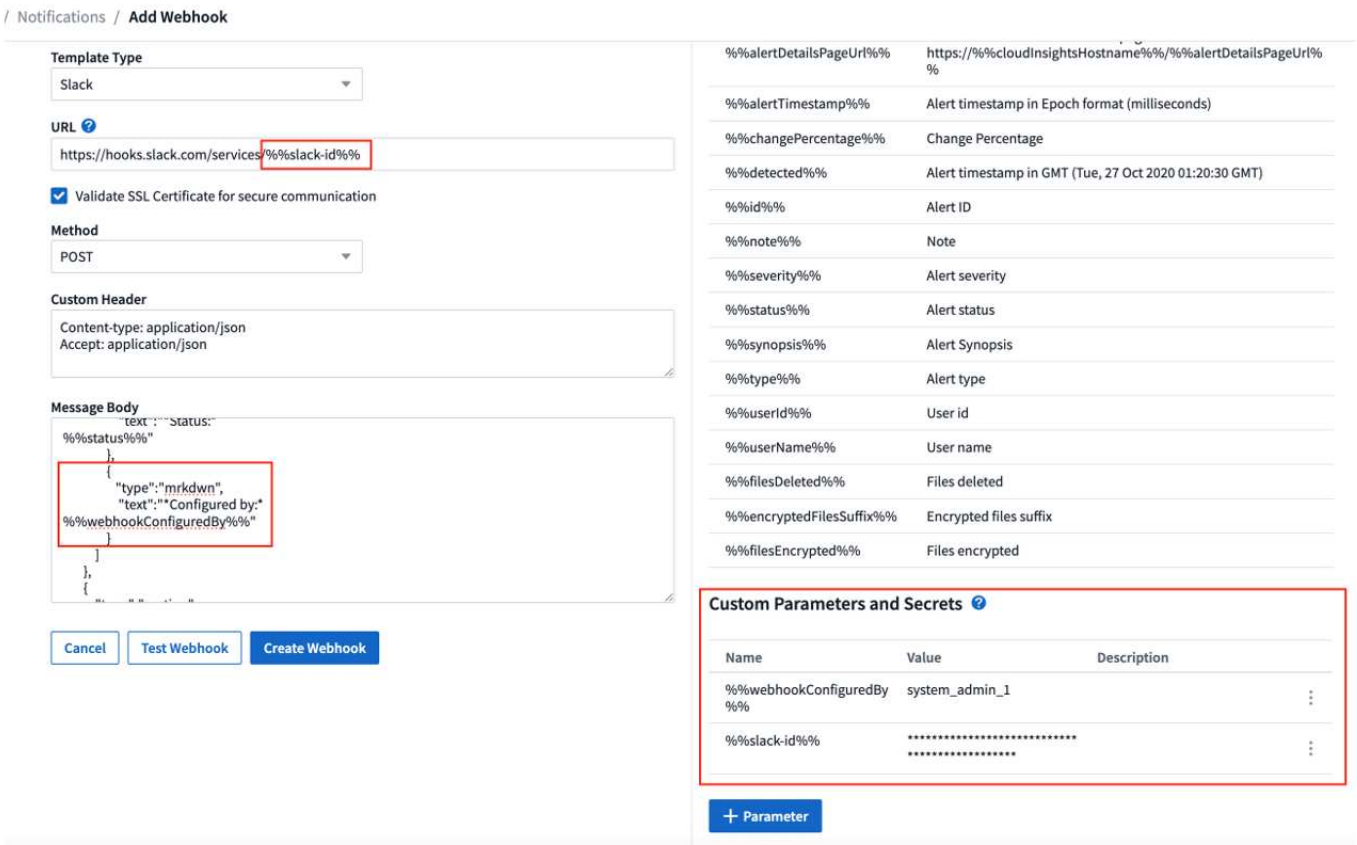
I parametri di avviso sono valori dinamici popolati per avviso. Ad esempio, il parametro *%%severity%%* verrà sostituito con il tipo di gravità dell'avviso.

Si noti che le sostituzioni non vengono eseguite quando si fa clic sul pulsante "Test Webhook"; il test invia un payload che mostra i segnaposto del parametro (*%%<param-name>%%*) ma non li sostituisce con i dati.

Parametri e segreti personalizzati

In questa sezione puoi aggiungere tutti i parametri personalizzati e/o segreti che desideri. Un parametro personalizzato o un segreto può essere presente nell'URL o nel corpo del messaggio. I segreti consentono all'utente di configurare un parametro personalizzato sicuro come password, apiKey ecc.

L'immagine di esempio seguente mostra come vengono utilizzati i parametri personalizzati nella creazione di webhook.



Pagina elenco webhook sicurezza carico di lavoro

Nella pagina dell'elenco dei webhook vengono visualizzati i campi Nome, Creato da, Creato il, Stato, Sicuro e Ultimo segnalato. Nota: il valore della colonna "stato" continuerà a cambiare in base al risultato dell'ultimo trigger del webhook. Di seguito sono riportati alcuni esempi di risultati di stato.

Stato	Descrizione
OK	Notifica inviata correttamente.
403	Vietato.
404	URL non trovato.

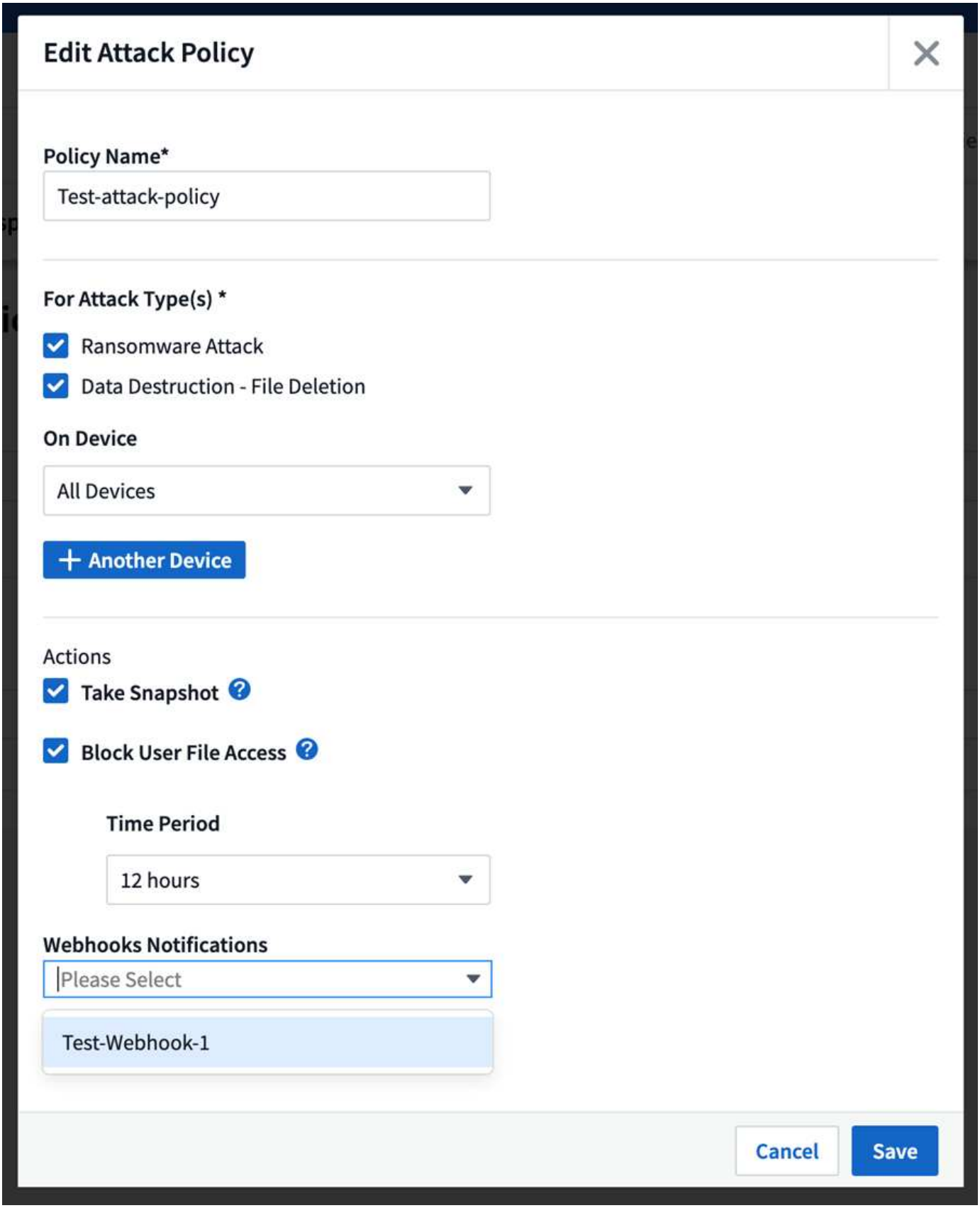
400	Brutta richiesta. Potresti visualizzare questo stato se c'è un errore nel corpo del messaggio, ad esempio: • JSON formattato male. • Fornito valore non valido per le chiavi riservate. Ad esempio, PagerDuty accetta solo informazioni critiche/avviso/errore/informazioni per "Gravità". Qualsiasi altro risultato potrebbe comportare lo stato 400. • Errori di convalida specifici dell'applicazione. Ad esempio, Slack consente un massimo di 10 campi all'interno di una sezione. Includerne più di 10 può comportare lo stato 400.
410	La risorsa non è più disponibile

La colonna "Ultimo segnalato" indica l'ora in cui il webhook è stato attivato l'ultima volta.

Dalla pagina dell'elenco dei webhook gli utenti possono anche modificare/duplicare/eliminare i webhook.

Configurare la notifica Webhook nel criterio di avviso

Per aggiungere una notifica webhook a un criterio di avviso, vai su -Sicurezza del carico di lavoro > Criteri- e seleziona un criterio esistente o aggiungine uno nuovo. Nella sezione *Azioni* > menu a discesa *Notifiche webhook*, seleziona i webhook richiesti.



Le notifiche webhook sono collegate alle policy. Quando si verifica l'attacco (RW/DD/WARN), verrà eseguita l'azione configurata (Scatta snapshot/blocco utente) e verrà quindi attivata la notifica webhook associata.

Nota: le notifiche e-mail sono indipendenti dalle policy e verranno attivate come di consueto.

- Se una policy viene sospesa, le notifiche webhook non verranno attivate.
- È possibile associare più webhook a una singola policy, ma si consiglia di non associarne più di 5.

Esempi di webhook sulla sicurezza del carico di lavoro

Webhook per"Slack"

Webhook per"PagerDuty" Webhook per"Squadre" Webhook per"Discordia"

Esempio di webhook di sicurezza del carico di lavoro per Discord

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Discord.

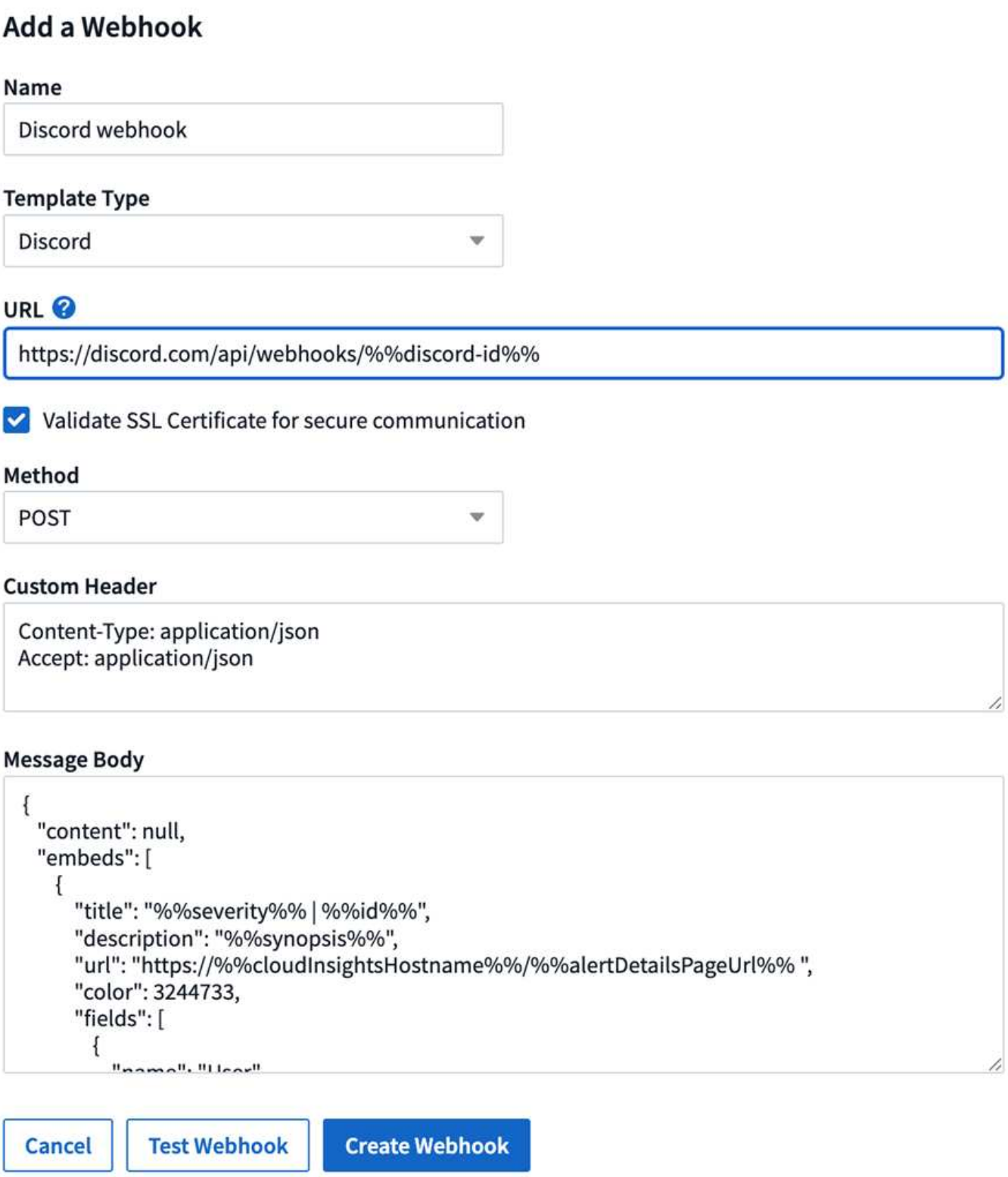
Questa pagina fa riferimento a istruzioni di terze parti, che sono soggette a modifiche. Fare riferimento al"Documentazione Discord" per le informazioni più aggiornate.

Configurazione Discord:

- In Discord, seleziona il server, in Canali di testo, seleziona Modifica canale (icona a forma di ingranaggio)
- Seleziona **Integrazioni > Visualizza webhook** e fai clic su **Nuovo webhook**
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook sulla sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Fare clic su '+ Webhook' per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Discord**.
4. Incolla l'URL di Discord riportato sopra nel campo *URL*.



Per testare il webhook, sostituisci temporaneamente il valore URL nel corpo del messaggio con un URL valido (ad esempio *https://netapp.com*), quindi fai clic sul pulsante *Test Webhook*. Per far funzionare la funzionalità Test Webhook, Discord richiede che venga fornito un URL valido.

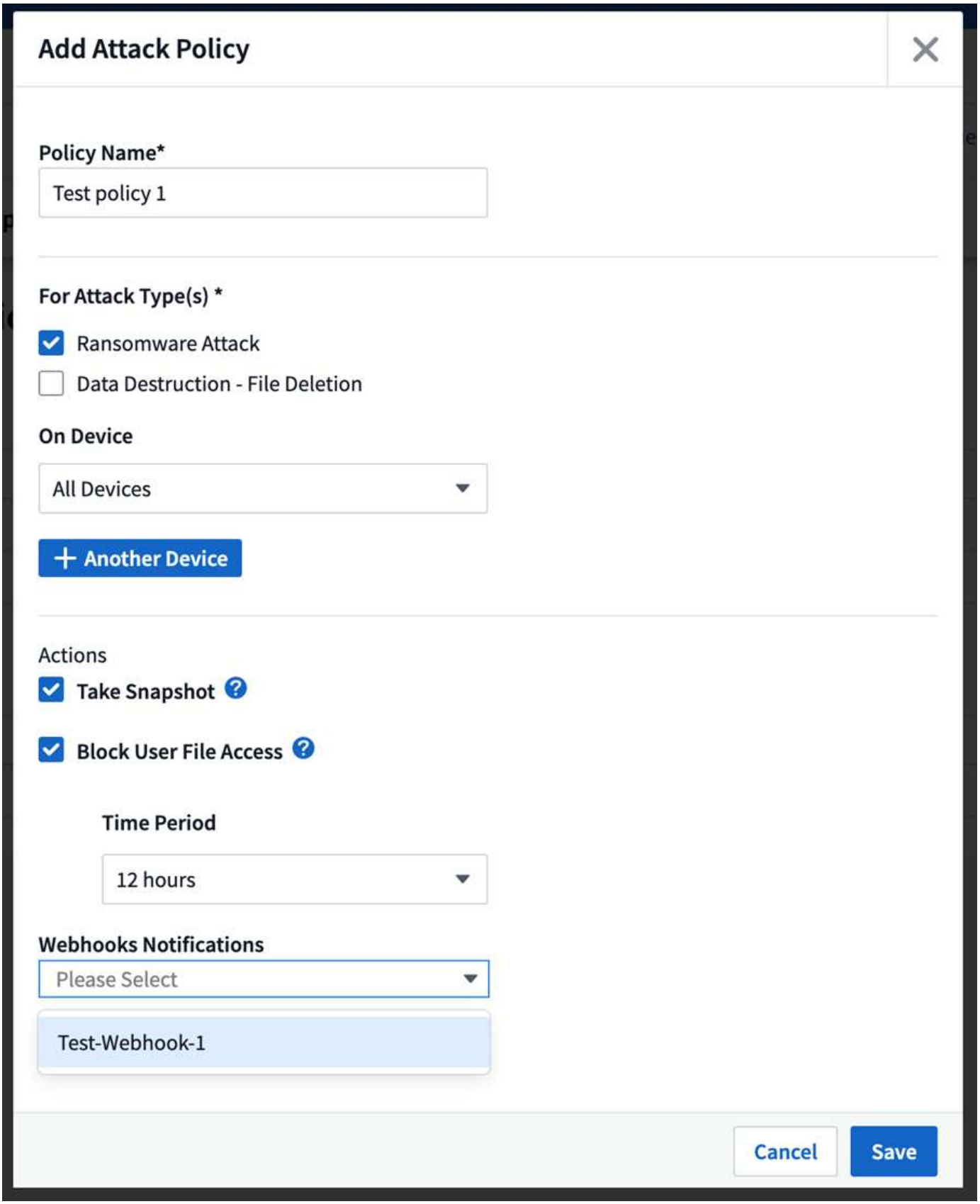
Una volta completato il test, assicurati di reimpostare il corpo del messaggio.

Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui associare la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook Discord desiderati e salva.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



Esempio di webhook di sicurezza del carico di lavoro per PagerDuty

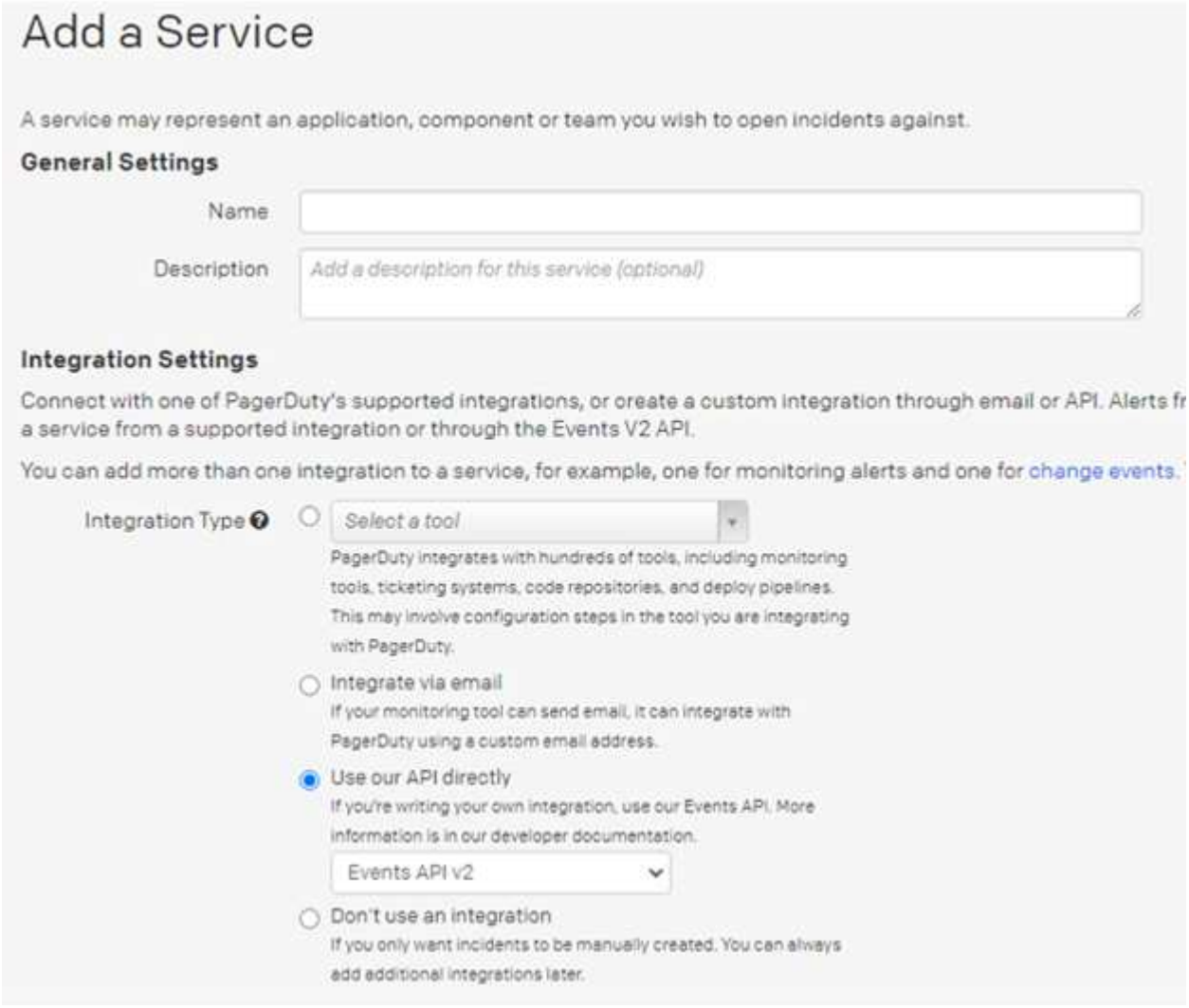
I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per

impostare webhook per PagerDuty.

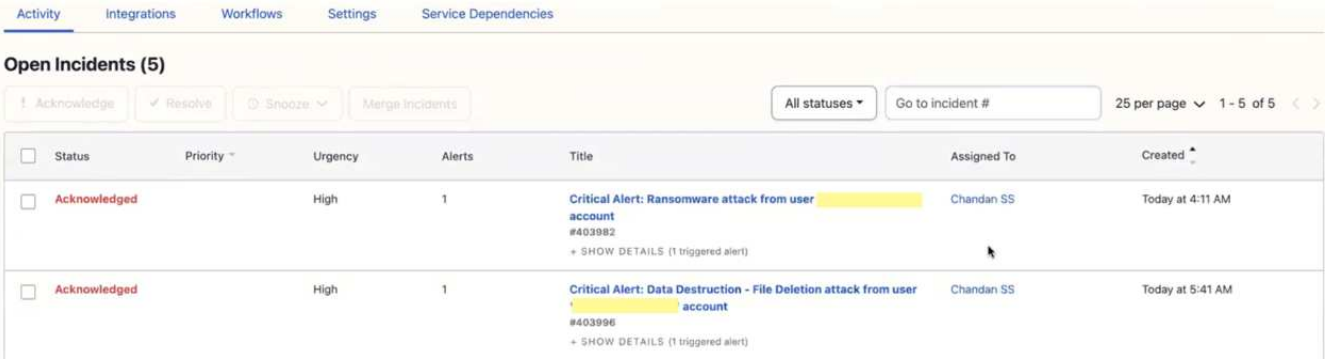
Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento al"Documentazione PagerDuty" per le informazioni più aggiornate.

Configurazione PagerDuty:

1. In PagerDuty, vai su **Servizi > Directory dei servizi** e clicca sul pulsante **+Nuovo servizio**.
2. Inserisci un *Nome* e seleziona *Usa direttamente la nostra API*. Selezionare *Aggiungi servizio*.

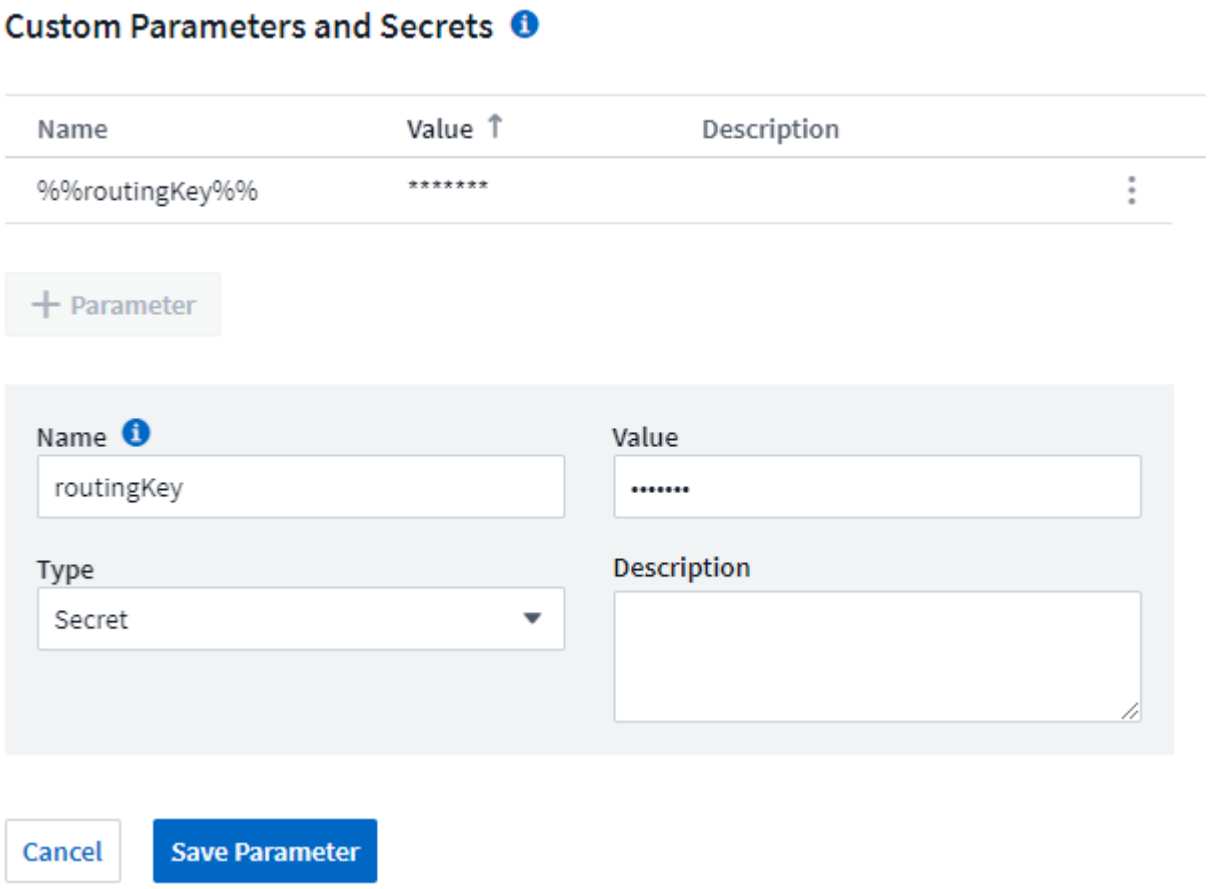


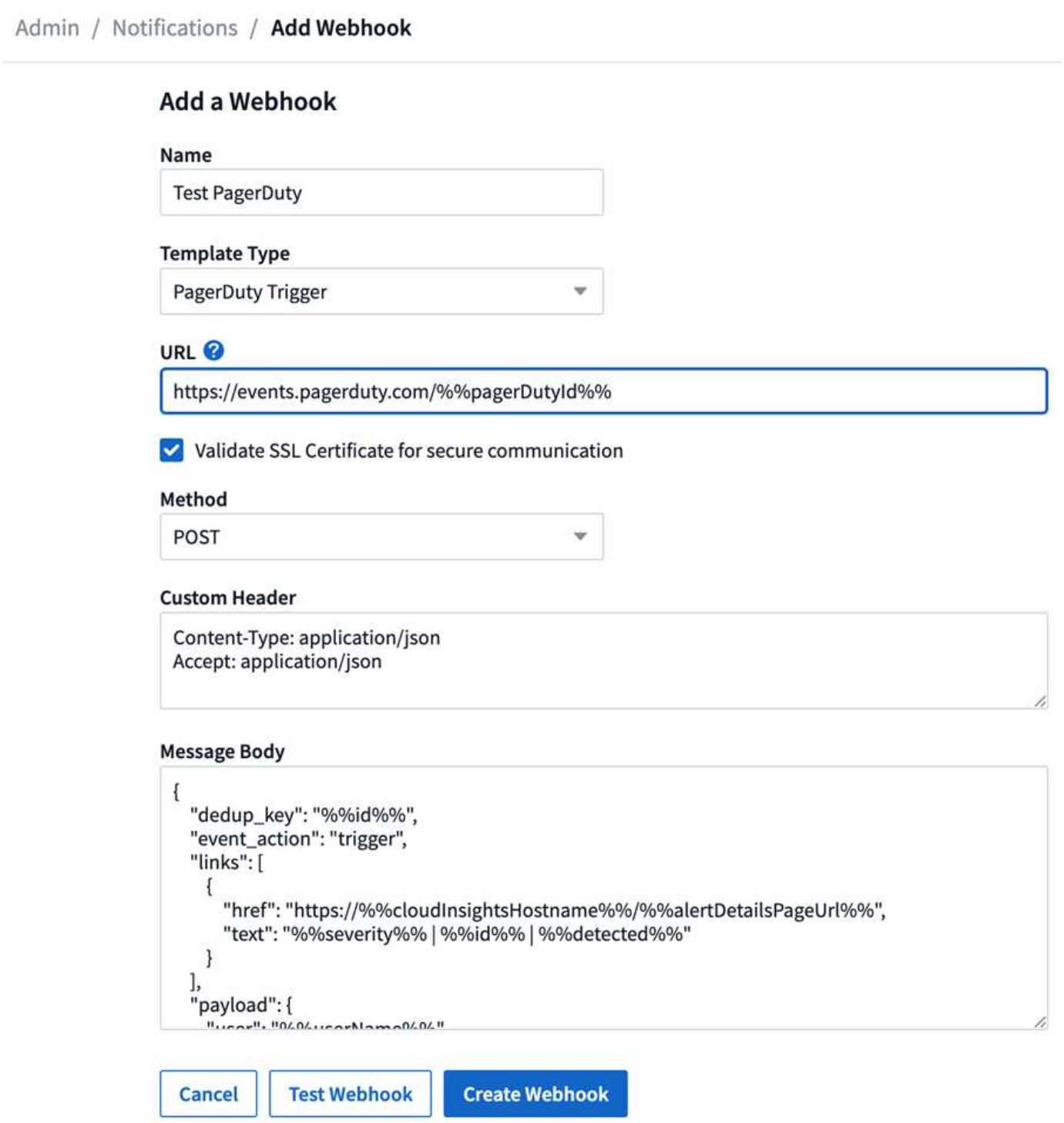
3. Selezionare la scheda *Integrazioni* per visualizzare la **Chiave di integrazione**. Questa chiave ti servirà quando creerai il webhook Workload Security qui sotto.
4. Vai a **Incidenti** o **Servizi** per visualizzare gli avvisi.



Crea webhook Workload Security PagerDuty:

- Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare '+ Webhook' per creare un nuovo webhook.
- Assegnare al webhook un nome significativo.
- Nel menu a discesa *Tipo di modello*, seleziona *Trigger PagerDuty*.
- Crea un parametro segreto personalizzato denominato *routingKey* e imposta il valore sulla *Chiave di integrazione* PagerDuty creata in precedenza.

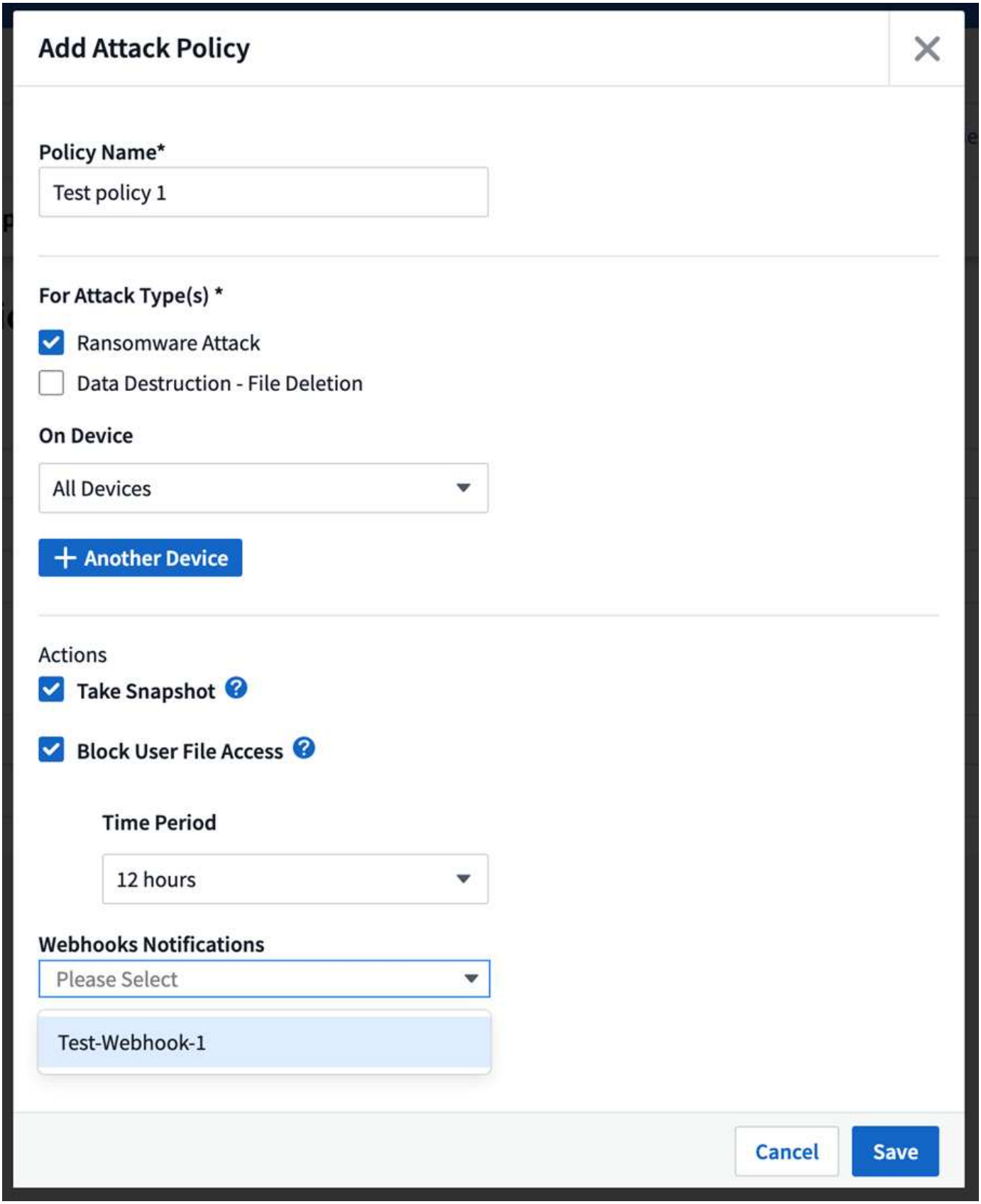




Notifiche tramite Webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro > Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.
- Nel menu a discesa *Notifiche webhook*, seleziona i webhook PagerDuty desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



Esempio di webhook di sicurezza del carico di lavoro per Slack

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni

utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Slack.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Per informazioni più aggiornate, consultare la documentazione di Slack.

Esempio di Slack

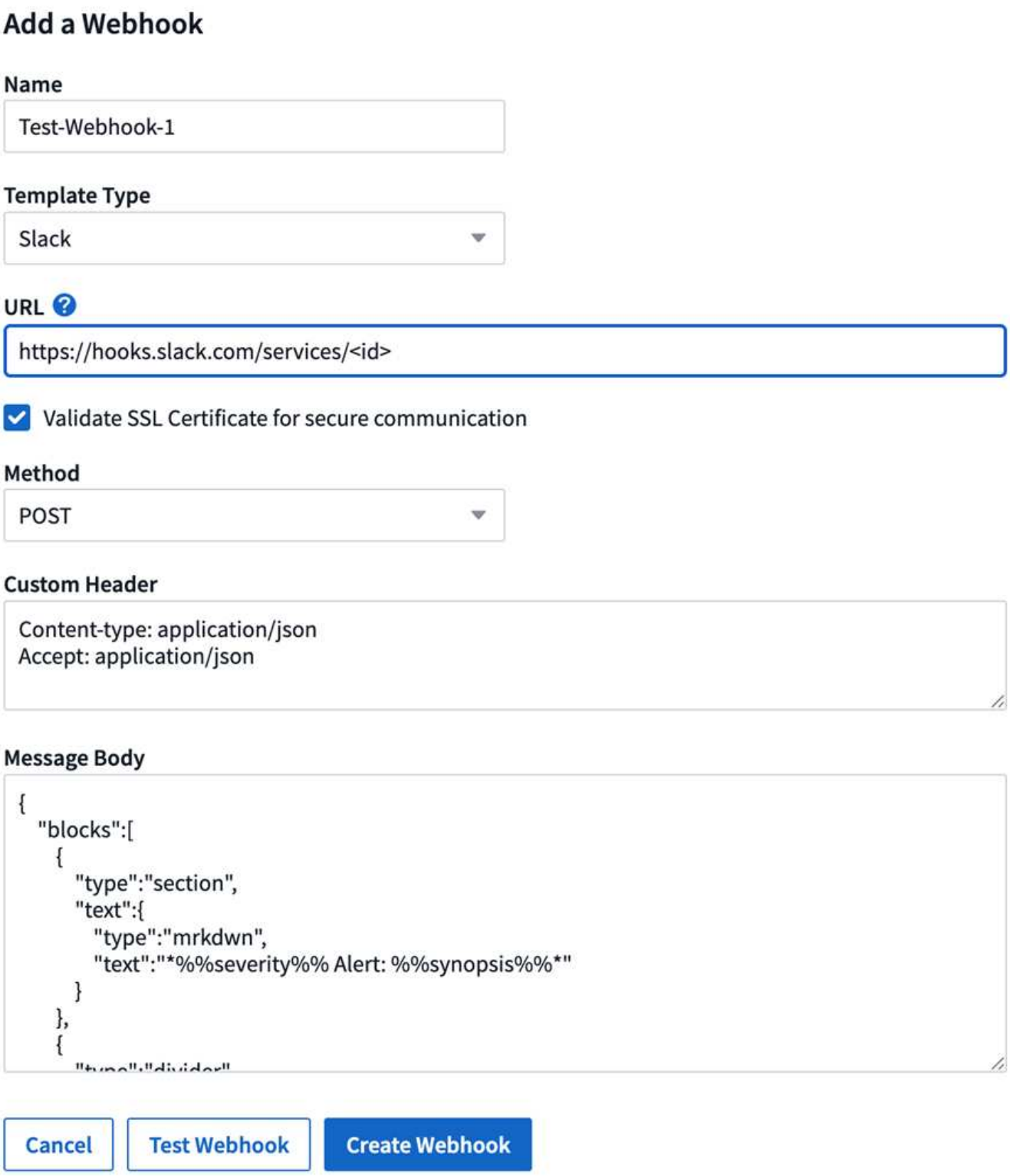
- Vai a https://api.slack.com/apps e crea una nuova app. Assegnagli un nome significativo e seleziona un'area di lavoro.

- Vai a Webhook in arrivo, clicca su *Attiva webhook in arrivo*, seleziona *Aggiungi nuovo webhook* e seleziona il canale su cui pubblicare.
- Copia l'URL del webhook. Questo URL verrà fornito durante la creazione di un webhook di Workload

Security.

Crea un webhook Slack per la sicurezza del carico di lavoro

1. Vai su Amministrazione > Notifiche e seleziona la scheda *Webhook di sicurezza del carico di lavoro*. Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona *Slack*.
4. Incolla l'URL copiato sopra.

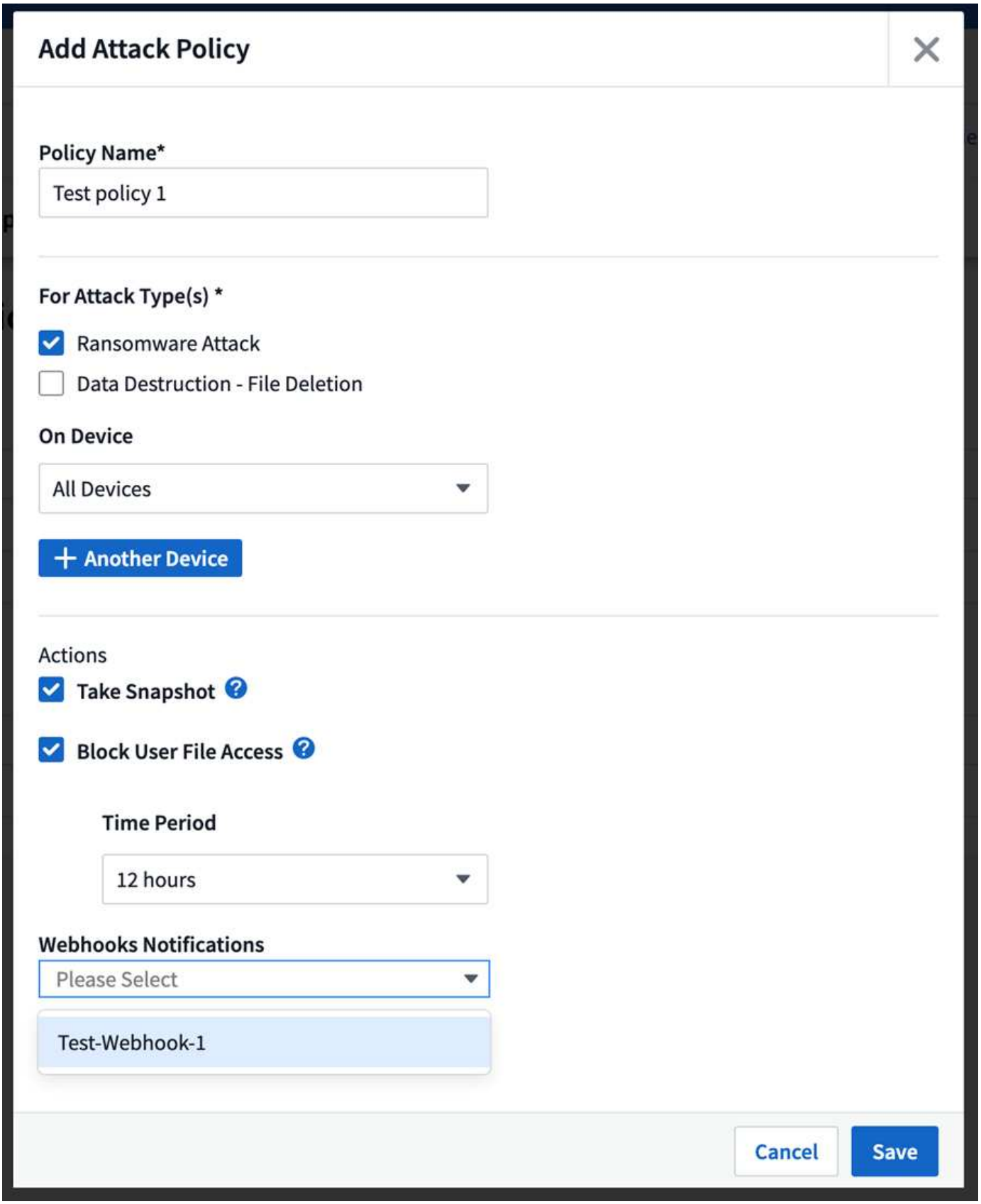


Notifiche tramite webhook

- Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Fare clic su *+Criterio di attacco* o *+Criterio di avviso*.
- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.

- Nel menu a discesa *Notifiche webhook*, seleziona i webhook desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



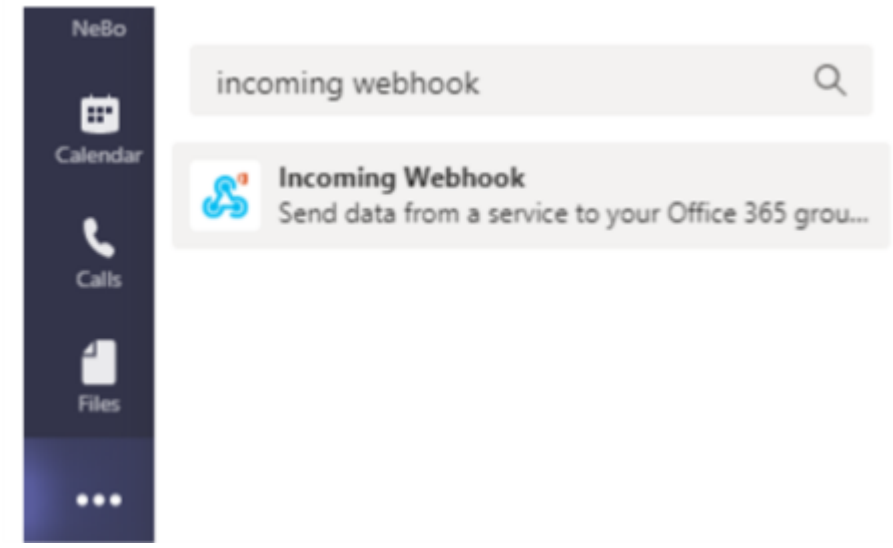
Esempio di webhook di sicurezza del carico di lavoro per Microsoft Teams

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per la configurazione di webhook per Teams.

Questa pagina fa riferimento a istruzioni di terze parti, soggette a modifiche. Fare riferimento al"Documentazione dei team" per le informazioni più aggiornate.

Configurazione delle squadre:

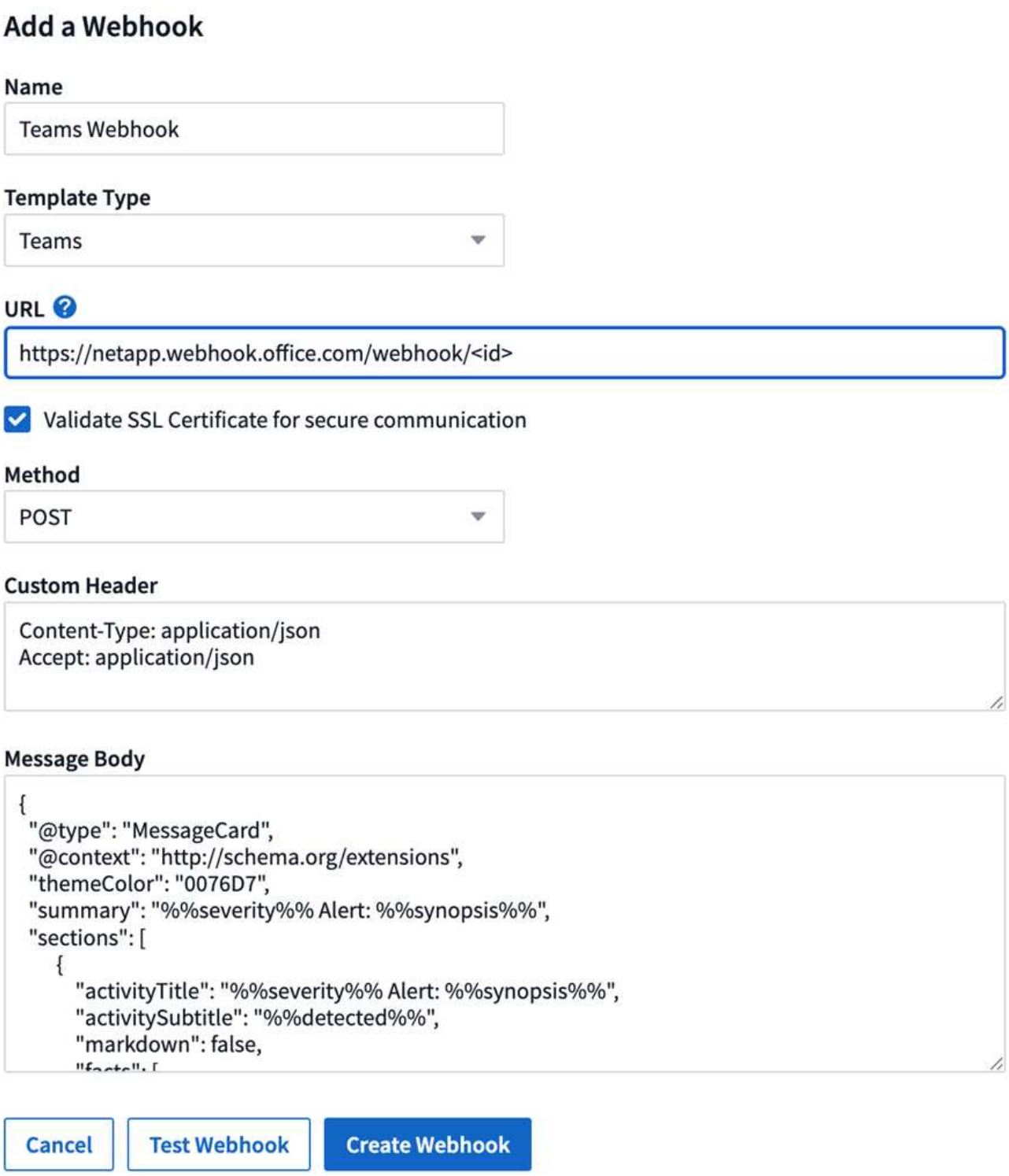
1. In Teams, seleziona il kebab e cerca Webhook in arrivo.



2. Seleziona **Aggiungi a un team > Seleziona un team > Imposta un connettore**.
3. Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Workload Security.

Crea webhook per i team di sicurezza del carico di lavoro:

1. Vai su Amministrazione > Notifiche e seleziona la scheda "Webhook di sicurezza del carico di lavoro". Selezionare + *Webhook* per creare un nuovo webhook.
2. Assegnare al webhook un nome significativo.
3. Nel menu a discesa *Tipo di modello*, seleziona **Team**.



4. Incolla l'URL sopra nel campo *URL*.

Passaggi per creare notifiche Teams con il modello Adaptive Card

1. Sostituisci il corpo del messaggio con il seguente template:

```
{
"type": "message",
"attachments": [
```

```
{
  "contentType": "application/vnd.microsoft.card.adaptive",
  "content": {
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "type": "AdaptiveCard",
    "version": "1.2",
    "body": [
      {
        "type": "TextBlock",
        "text": "%%severity%% Alert: %%synopsis%%",
        "wrap": true,
        "weight": "Bolder",
        "size": "Large"
      },
      {
        "type": "TextBlock",
        "text": "%%detected%%",
        "wrap": true,
        "isSubtle": true,
        "spacing": "Small"
      },
      {
        "type": "FactSet",
        "facts": [
          {
            "title": "User",
            "value": "%%userName%%"
          },
          {
            "title": "Attack/Abnormal Behavior",
            "value": "%%type%%"
          },
          {
            "title": "Action taken",
            "value": "%%actionTaken%%"
          },
          {
            "title": "Files encrypted",
            "value": "%%filesEncrypted%%"
          },
          {
            "title": "Encrypted files suffix",
            "value": "%%encryptedFilesSuffix%%"
          },
          {
            "title": "Files deleted",
```

```
                "value": "%%filesDeleted%%"
              },
              {
                "title": "Activity Change Rate",
                "value": "%%changePercentage%%"
              },
              {
                "title": "Severity",
                "value": "%%severity%%"
              },
              {
                "title": "Status",
                "value": "%%status%%"
              },
              {
                "title": "Notes",
                "value": "%%note%%"
              }
            ]
          }
        ],
        "actions": [
          {
            "type": "Action.OpenUrl",
            "title": "View Details",
            "url":
"https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%"
          }
        ]
      }
    }
  ]
}
```

2. Se si utilizzano i flussi di Power Automate, i parametri di query nell'URL sono in formato codificato. È necessario decodificare l'URL prima di inserirlo.
3. Fare clic su "Test Webhook" per assicurarsi che non vi siano errori.
4. Salva il webhook.

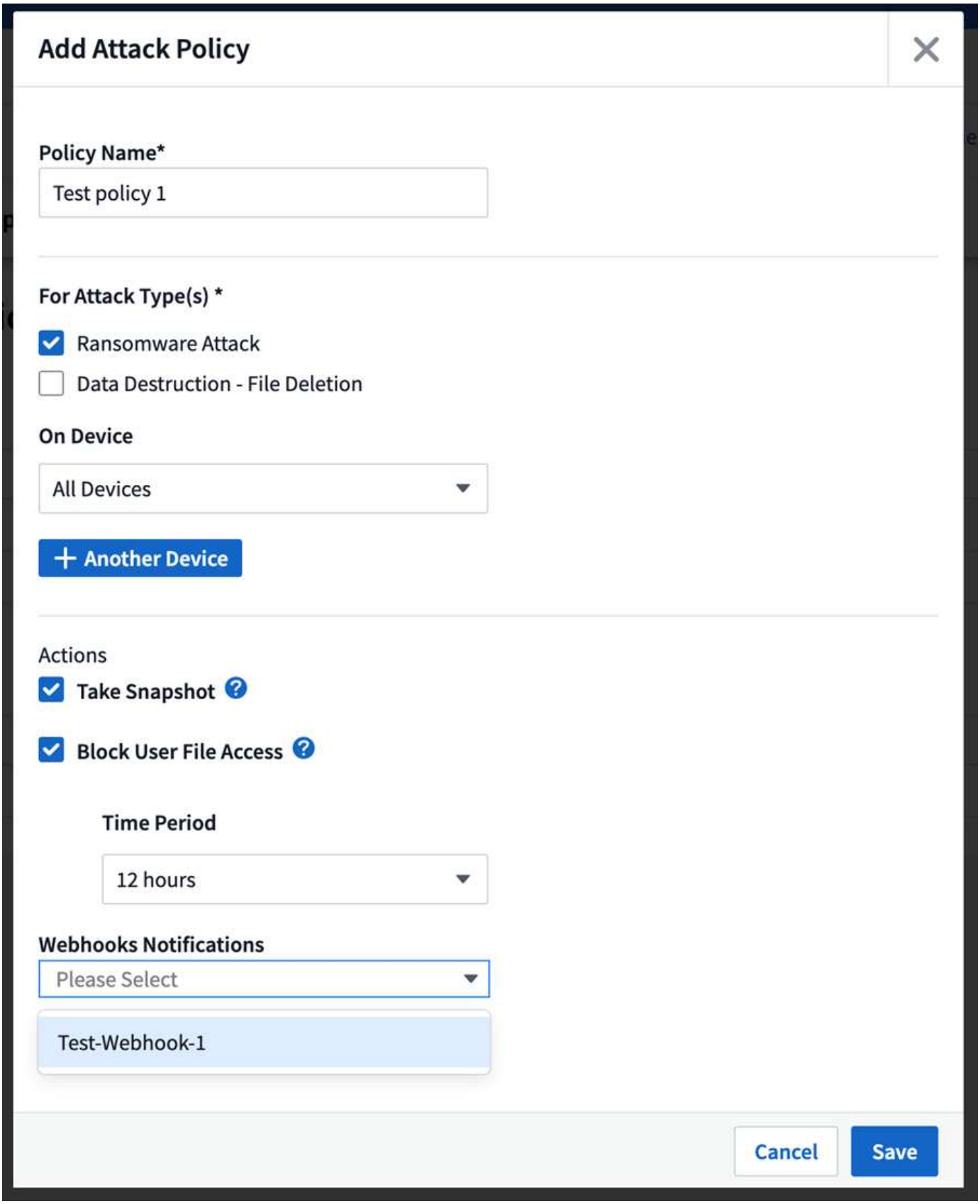
Notifiche tramite Webhook

Per ricevere notifiche sugli eventi tramite webhook, vai su *Sicurezza del carico di lavoro* > *Criteri*. Selezionare *+Criterio di attacco* o *+Criterio di avviso*.

- Immettere un nome significativo per la policy.
- Selezionare i tipi di attacco richiesti, i dispositivi a cui deve essere associata la policy e le azioni richieste.

- Nel menu a discesa *Notifiche webhook*, seleziona i webhook di Teams desiderati. Salva la polizza.

Nota: i webhook possono anche essere allegati a policy esistenti modificandole.



API di sicurezza del carico di lavoro

Integra Workload Security con il tuo ecosistema aziendale utilizzando un'API REST protetta da un'autenticazione sicura basata su token. Recupera dati di attività forensi, gestisci i token di accesso alle API e sviluppa integrazioni personalizzate con CMDB, sistemi di ticketing e altre applicazioni. La documentazione interattiva Swagger fornisce specifiche API complete e consente di testare direttamente gli endpoint.

Requisiti per l'accesso all'API:

- Per concedere l'accesso viene utilizzato un modello di token di accesso API.
- La gestione dei token API viene eseguita dagli utenti di Workload Security con il ruolo di amministratore.

Documentazione API (Swagger)

Per reperire le informazioni API più recenti, accedere a Workload Security e andare su **Amministrazione > Accesso API**. 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 proprio tenant.

Se si richiama l'API Forensics Activity, utilizzare l'API cloudsecure_forensics.activities.**v2**. Se si effettuano più chiamate a questa API, assicurarsi che le chiamate avvengano in sequenza e non in parallelo. Più chiamate parallele potrebbero causare il timeout dell'API.

Token di accesso API

Prima di utilizzare l'API Workload Security, è necessario creare uno o più **token di accesso API**. I token di accesso concedono permessi di lettura. È anche possibile impostare la scadenza per ciascun token di accesso.

Per creare un token di accesso:

- Fare clic su **Amministrazione > Accesso API**
- Fai clic su **+Token di accesso API**
- Inserisci **Nome token**
- Specifica **Scadenza token**

Il tuo token potrà essere copiato negli appunti e salvato solo durante il processo di creazione. Una volta creati, i token non possono essere recuperati, pertanto si consiglia vivamente di copiarli e salvarli in un luogo sicuro. Ti verrà chiesto di fare clic sul pulsante Copia token di accesso API prima di poter chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. I token disabilitati possono essere abilitati.

I token garantiscono l'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 si è autenticato e ha autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token trasmesso informa l'API che il portatore del token è stato autorizzato 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 archiviazione:

```
 curl https://<Workload Security tenant>/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 e _<Workload Security Tenant>_ è l'URL del tenant
del tuo ambiente Workload Security.
```

Informazioni dettagliate sono disponibili nel link *Documentazione API* in **Amministrazione > Accesso API**.

Script per estrarre dati tramite API

Gli agenti Workload Security includono uno script di esportazione per facilitare le chiamate parallele all'API v2 suddividendo 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 le istruzioni per l'uso.

Ecco un comando di esempio per richiamare lo script:

```
python3 data-export.py --tenant_url <Workload Security tenant>
--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
```

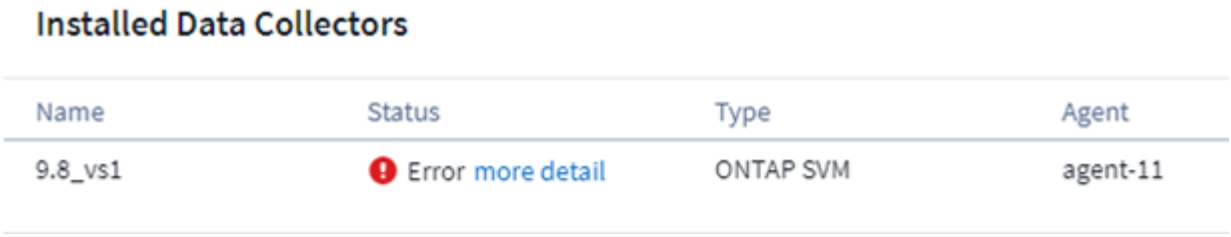
Parametri chiave: - `--iteration_interval 12` : Suddivide l'intervallo di tempo richiesto in intervalli di 12 ore. - `--num_workers 3` : Recupera questi intervalli in parallelo utilizzando 3 thread.

Risoluzione dei problemi del raccoglitore dati ONTAP SVM

Workload Security utilizza dei collettori di dati per raccogliere dati sui file e sugli accessi degli utenti dai dispositivi. Qui puoi trovare suggerimenti per la risoluzione dei problemi relativi a questo raccoglitore.

Vedi il"Configurazione del collettore SVM" pagina per le istruzioni sulla configurazione di questo raccoglitore.

In caso di errore, è possibile fare clic su *ulteriori dettagli* nella colonna *Stato* della pagina Collettori dati installati per ottenere maggiori dettagli sull'errore.



Di seguito vengono descritti i problemi noti e le relative soluzioni.

Problema: Data Collector funziona per un po' di tempo e si arresta dopo un tempo casuale, con il seguente messaggio di errore: "Messaggio di errore: il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno sovraccarico." **Prova questo:** la frequenza degli eventi di ONTAP era molto più alta di quella che la casella Agent può gestire. Di conseguenza la connessione è stata interrotta.

Controlla il picco di traffico in CloudSecure al momento della disconnessione. Puoi verificarlo dalla pagina **CloudSecure > Activity Forensics > Tutte le attività**.

Se il traffico aggregato di picco è superiore a quello che l'Agent Box può gestire, fare riferimento alla pagina Event Rate Checker per informazioni su come dimensionare la distribuzione del Collector in un Agent Box.

Se l'agente è stato installato nella casella Agente prima del 4 marzo 2021, eseguire i seguenti comandi nella casella Agente:

```
echo 'net.core.rmem_max=8388608' >> /etc/sysctl.conf
echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf
sysctl -p
```

Dopo il ridimensionamento, riavviare il raccoglitore dall'interfaccia utente.

{vuoto}

Problema: il Collector segnala il messaggio di errore: "Nessun indirizzo IP locale trovato sul connettore in grado di raggiungere le interfacce dati dell'SVM". **Prova questo:** Molto probabilmente è dovuto a un problema di rete sul lato ONTAP . Si prega di seguire questi passaggi:

1. Assicurarsi che non vi siano firewall sulla vita dati SVM o sulla vita di gestione che bloccano la connessione dalla SVM.
2. Quando si aggiunge una SVM tramite un IP di gestione del cluster, assicurarsi che la vita dati e la vita di gestione della SVM siano pingabili dalla VM dell'agente. In caso di problemi, controllare il gateway, la netmask e i percorsi per lif.

   Puoi anche provare ad accedere al cluster tramite ssh utilizzando l'IP di gestione del cluster ed effettuare il ping dell'IP dell'agente. Assicurarsi che l'IP dell'agente sia pingabile:

```
network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
Name> -show-detail
```

Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

3. Se hai provato a connetterti tramite l'IP del cluster e non funziona, prova a connetterti direttamente tramite l'IP SVM. Per i passaggi necessari per connettersi tramite IP SVM, vedere quanto sopra.
4. Durante l'aggiunta del collettore tramite IP SVM e credenziali vsadmin, verificare se SVM Lif ha abilitato il ruolo Data plus Mgmt. In questo caso il ping all'SVM Lif funzionerà, ma l'SSH all'SVM Lif non funzionerà. In caso affermativo, creare un SVM Mgmt Only Lif e provare a connettersi tramite questo SVM Management Only Lif.
5. Se ancora non funziona, crea un nuovo SVM Lif e prova a connetterti tramite quel Lif. Assicurarsi che la subnet mask sia impostata correttamente.
6. Debug avanzato:
   a. Avvia una traccia dei pacchetti in ONTAP.
   b. Provare a connettere un data collector all'SVM dall'interfaccia utente di CloudSecure.
   c. Attendi finché non compare l'errore. Arresta la traccia dei pacchetti in ONTAP.
   d. Aprire la traccia del pacchetto da ONTAP. È disponibile in questa posizione

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Assicurarsi che ci sia un SYN da ONTAP alla casella Agent.
.. Se non c'è SYN da ONTAP , allora c'è un problema con il firewall
in ONTAP.
.. Aprire il firewall in ONTAP, in modo che ONTAP possa connettersi
alla casella agente.
```

7. Se il problema persiste, consultare il team di rete per accertarsi che nessun firewall esterno stia bloccando la connessione da ONTAP alla casella Agent.
8. Se nessuna delle soluzioni precedenti risolve il problema, apri un caso con"Supporto Netapp" per ulteriore assistenza.

{vuoto}

Problema: Messaggio: "Impossibile determinare il tipo ONTAP per [nome host: <indirizzo IP>. Motivo: Errore di connessione al sistema di archiviazione <Indirizzo IP>: Host non raggiungibile (Host non raggiungibile)
Prova questo:

1. Verificare che sia stato fornito l'indirizzo IP di gestione SVM o l'IP di gestione del cluster corretto.
2. Eseguire l'SSH sull'SVM o sul Cluster a cui si intende connettersi. Una volta effettuata la connessione, assicurarsi che il nome SVM o Cluster sia corretto.

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: server fpolicy esterno terminato." **Prova questo:**

1. È molto probabile che un firewall stia bloccando le porte necessarie nella macchina dell'agente. Verificare che l'intervallo di porte 35000-55000/tcp sia aperto affinché la macchina agente possa connettersi dall'SVM. Assicurarsi inoltre che non vi siano firewall abilitati sul lato ONTAP che bloccano la comunicazione con la macchina agente.
2. Digitare il seguente comando nella casella Agente e assicurarsi che l'intervallo di porte sia aperto.

   ```
   sudo iptables-save | grep 3500*
   ```

   L'output di esempio dovrebbe apparire così:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Accedi a SVM, inserisci i seguenti comandi e verifica che non sia
   impostato alcun firewall per bloccare la comunicazione con ONTAP.
   ```

   ```
   system services firewall show
   system services firewall policy show
   ```

   "Controlla i comandi del firewall"sul lato ONTAP .

3. Accedi tramite SSH all'SVM/Cluster che vuoi monitorare. Eseguire il ping della casella Agent dalla libreria dati SVM (con supporto dei protocolli CIFS e NFS) e assicurarsi che il ping funzioni:

   ```
   network ping -vserver <vserver name> -destination <Agent IP> -lif <Lif
   Name> -show-detail
   ```

   Se non è possibile effettuare il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che la macchina dell'agente sia pingabile.

4. Se un singolo SVM viene aggiunto due volte a un tenant tramite 2 collettori dati, verrà visualizzato questo errore. Eliminare uno dei collettori di dati tramite l'interfaccia utente. Quindi riavviare l'altro raccoglitore dati tramite l'interfaccia utente. Quindi il raccoglitore dati mostrerà lo stato "IN ESECUZIONE" e inizierà a ricevere eventi da SVM.

   In pratica, in un tenant, 1 SVM dovrebbe essere aggiunto una sola volta, tramite 1 data collector. 1 SVM non dovrebbe essere aggiunto due volte tramite 2 collettori di dati.

5. Nei casi in cui lo stesso SVM è stato aggiunto in due diversi ambienti Workload Security (tenant), l'ultimo riuscirà sempre. Il secondo collettore configurerà fpolicy con il proprio indirizzo IP ed espellerà il primo. Quindi il collettore nel primo smetterà di ricevere eventi e il suo servizio di "audit" entrerà in stato di errore. Per evitare ciò, configurare ogni SVM su un singolo ambiente.
6. Questo errore può verificarsi anche se i criteri di servizio non sono configurati correttamente. Con ONTAP 9.8 o versioni successive, per connettersi al Data Source Collector, è necessario il servizio data-fpolicy-

client insieme al servizio dati data-nfs e/o data-cifs. Inoltre, il servizio data-fpolicy-client deve essere associato ai dati lif per l'SVM monitorato.

{vuoto}

Problema: Nessun evento visualizzato nella pagina delle attività. **Prova questo:**

1. Verificare se il collettore ONTAP è nello stato "IN ESECUZIONE". In caso affermativo, assicurarsi che alcuni eventi cifs vengano generati sulle VM client cifs aprendo alcuni file.
2. Se non vengono rilevate attività, effettuare l'accesso all'SVM e immettere il seguente comando.

   ```
   <SVM>event log show -source fpolicy
   ```

   Assicurati che non ci siano errori relativi a fpolicy.

3. Se non vengono visualizzate attività, effettuare l'accesso all'SVM. Immettere il seguente comando:

   ```
   <SVM>fpolicy show
   ```

   Verificare se la policy fpolicy denominata con prefisso "cloudsecure_" è stata impostata e lo stato è "on". Se non è impostato, molto probabilmente l'agente non è in grado di eseguire i comandi nell'SVM. Si prega di assicurarsi che siano stati rispettati tutti i prerequisiti descritti all'inizio della pagina.

{vuoto}

Problema: SVM Data Collector è in stato di errore e il messaggio di errore è "L'agente non è riuscito a connettersi al raccoglitore". **Prova questo:**

1. Molto probabilmente l'agente è sovraccarico e non riesce a connettersi ai collettori dell'origine dati.
2. Controllare quanti collettori di origini dati sono connessi all'agente.
3. Controllare anche la velocità del flusso di dati nella pagina "Tutte le attività" nell'interfaccia utente.
4. Se il numero di attività al secondo è significativamente elevato, installare un altro agente e spostare alcuni dei Data Source Collector sul nuovo agente.

{vuoto}

Problema: SVM Data Collector mostra il messaggio di errore "fpolicy.server.connectError: il nodo non è riuscito a stabilire una connessione con il server FPolicy "12.195.15.146" (motivo: "Selezione scaduta")" **Prova questo:** il firewall è abilitato in SVM/Cluster. Quindi il motore fpolicy non è in grado di connettersi al server fpolicy. Le CLI in ONTAP che possono essere utilizzate per ottenere maggiori informazioni sono:

```
event log show -source fpolicy which shows the error
event log show -source fpolicy -fields event,action,description which
shows more details.
```

"Controlla i comandi del firewall"sul lato ONTAP .

{vuoto}

Problema: Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Nessuna interfaccia dati valida (ruolo: dati, protocolli dati: NFS o CIFS o entrambi, stato: attivo) trovata sull'SVM." **Prova questo:** assicurati che ci sia un'interfaccia operativa (che abbia il ruolo di dati e protocollo dati come CIFS/NFS).

{vuoto}

Problema: il raccoglitore dati entra nello stato di errore e poi, dopo un po' di tempo, passa allo stato di esecuzione, per poi tornare nuovamente allo stato di errore. Questo ciclo si ripete. **Prova questo:** Questo accade in genere nel seguente scenario:

1. Sono stati aggiunti più raccoglitori di dati.
2. Ai collettori di dati che mostrano questo tipo di comportamento verrà aggiunto 1 SVM. Ciò significa che 2 o più collettori di dati sono collegati a 1 SVM.
3. Assicurarsi che 1 raccoglitore dati si connetta a 1 solo SVM.
4. Eliminare gli altri raccoglitori di dati connessi allo stesso SVM.

{vuoto}

Problema: Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare (policy su SVM svmname. Motivo: Valore non valido specificato per l'elemento 'shares-to-include' in 'fpolicy.policy.scope-modify: "Federal' **Prova questo:** *I nomi delle condivisioni devono essere specificati senza virgolette. Modificare la configurazione DSC ONTAP SVM per correggere i nomi delle condivisioni.

Includi ed escludi azioni non è pensato per un lungo elenco di nomi di azioni. Se hai un gran numero di azioni da includere o escludere, utilizza il filtro per volume.

{vuoto}

Problema: Nel cluster sono presenti fpolicies esistenti che non sono utilizzati. Cosa si dovrebbe fare prima di installare Workload Security? **Prova questo:** Si consiglia di eliminare tutte le impostazioni fpolicy esistenti e non utilizzate, anche se sono in stato disconnesso. Workload Security creerà fpolicy con il prefisso "cloudsecure_". Tutte le altre configurazioni fpolicy non utilizzate possono essere eliminate.

Comando CLI per visualizzare l'elenco fpolicy:

```
 fpolicy show
Passaggi per eliminare le configurazioni fpolicy:
```

```
fpolicy disable -vserver <svmname> -policy-name <policy_name>
fpolicy policy scope delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy delete -vserver <svmname> -policy-name <policy_name>
fpolicy policy event delete -vserver <svmname> -event-name <event_list>
fpolicy policy external-engine delete -vserver <svmname> -engine-name
<engine_name>
```

{vuoto}

Problema: Dopo aver abilitato Workload Security, le prestazioni ONTAP risultano compromesse: la latenza diventa sporadicamente elevata, mentre gli IOPS diventano sporadicamente bassi. **Prova questo:** Durante l'utilizzo di ONTAP con Workload Security, a volte si possono verificare problemi di latenza in ONTAP. Le possibili cause di ciò sono molteplici, come indicato di seguito:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" . Tutti questi problemi sono stati risolti in ONTAP 9.13.1 e versioni successive; si consiglia vivamente di utilizzare una di queste versioni successive.

{vuoto}

Problema: Data Collector mostra il messaggio di errore: "Errore: impossibile determinare lo stato del collector entro 2 tentativi, provare a riavviare nuovamente il collector (codice errore: AGENT008)". **Prova questo:**

1. Nella pagina dei raccoglitori di dati, scorrere verso destra del raccoglitore di dati che ha generato l'errore e fare clic sul menu con i 3 puntini. Selezionare *Modifica*. Inserire nuovamente la password del raccoglitore dati. Salvare il raccoglitore dati premendo il pulsante *Salva*. Data Collector verrà riavviato e l'errore dovrebbe essere risolto.
2. La macchina dell'agente potrebbe non avere abbastanza CPU o RAM, ecco perché i DSC non funzionano. Controllare il numero di Data Collector aggiunti all'agente nella macchina. Se è superiore a 20, aumentare la capacità della CPU e della RAM della macchina agente. Una volta aumentata la CPU e la RAM, i DSC entreranno automaticamente nello stato di inizializzazione e poi in quello di esecuzione. Consulta la guida alle taglie su"questa pagina" .

{vuoto}

Problema: il Data Collector genera un errore quando è selezionata la modalità SVM. **Prova questo:** durante la connessione in modalità SVM, se per la connessione viene utilizzato l'IP di gestione del cluster anziché l'IP di gestione SVM, la connessione genererà un errore. Assicurarsi che venga utilizzato l'IP SVM corretto.

{vuoto}

Problema: Il raccoglitore dati mostra un messaggio di errore quando la funzione Accesso negato è abilitata: "Il connettore è in stato di errore. Nome del servizio: audit. Motivo dell'errore: impossibile configurare fpolicy su SVM test_svm. Motivo: L'utente non è autorizzato." **Prova questo:** L'utente potrebbe non disporre delle autorizzazioni REST necessarie per la funzionalità Accesso negato. Si prega di seguire le istruzioni su"questa pagina" per impostare i permessi.

Una volta impostate le autorizzazioni, riavviare il raccoglitore.

{vuoto}

Problema: Il collettore è in stato di errore con il messaggio: Il connettore è in stato di errore. Motivo dell'errore: impossibile configurare l'archivio persistente su SVM <Nome SVM>. Motivo: impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova il comando. Nome del servizio: audit. Motivo dell'errore: Impossibile configurare l'archivio persistente su SVM <SVM Name>. Motivo: Impossibile trovare un aggregato adatto per il volume "<volumeName>" in SVM "<SVM Name>". Motivo: le informazioni sulle prestazioni per l'aggregato "<aggregateName>" non sono attualmente disponibili. Attendi qualche minuto e riprova a eseguire il comando.

Prova questo: attendi qualche minuto e poi riavvia il Collector.

{vuoto}

Se riscontri ancora problemi, contatta l'assistenza tramite i link indicati nella pagina **Aiuto > Assistenza**.

Informazioni sul copyright

Informazioni sul marchio commerciale