Per iniziare

Cloud Insights

NetApp
July 12, 2024

Sommario

Per iniziare

Introduzione alla sicurezza del carico di lavoro

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

La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

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

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

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

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

Requisiti dell'agente per la sicurezza del carico di lavoro

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

La protezione del carico di lavoro dello storage non è disponibile nell'edizione federale di Cloud Insights.

Componente	Requisiti Linux
Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti componenti: Red Hat Enterprise Linux 7.x, 8.x 64 bit, SELinux CentOS 7.x a 64 bit, SELinux CentOS 8 Stream, SELinux Ubuntu 20 fino a 22 64 bit Rocky 8.x 64 bit, Rocky 9.x 64 bit, SELinux SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4, SELinux su SUSE 15 SP3 Questo computer non deve eseguire alcun altro software a livello di applicazione. Si consiglia di utilizzare un server dedicato.
Comandi	per l'installazione è necessario decomprimere. Inoltre, il comando 'sudo su –' è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
CPU	4 core CPU
Memoria	16 GB DI RAM
Spazio su disco disponibile	Lo spazio su disco deve 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 in più per consentire la creazione del filesystem. Assicurarsi che ci siano almeno 35 GB di spazio libero nel filesystem. Se /opt è una cartella montata da un dispositivo di archiviazione NAS, assicurarsi che gli utenti locali abbiano accesso a questa cartella. L'installazione dell'agente o del Data Collector potrebbe non riuscire se gli utenti locali non dispongono dell'autorizzazione per questa cartella. vedere "risoluzione dei problemi" per ulteriori dettagli.
Rete	Connessione Ethernet da 100 Mbps a 1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi e porta richiesta per l'istanza di workload Security (80 o 443).

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

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

Consigli aggiuntivi

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

Regole di accesso alla rete cloud

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

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

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

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

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

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

Regole in-network

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAPS / start-tls)	Agente di sicurezza del carico di lavoro	URL del server LDAP	Connettersi a LDAP
TCP	443	Agente di sicurezza del carico di lavoro	Cluster o SVM Management IP Address (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP
TCP	35000 - 55000	Indirizzi IP LIF dati SVM	Agente di sicurezza del carico di lavoro	Comunicazione da ONTAP all'agente di sicurezza del carico di lavoro per gli eventi Fpolicy. Affinché ONTAP possa inviarvi eventi, compresi eventuali firewall presenti nell'agente di protezione del carico di lavoro stesso (se presente), è necessario aprire queste porte verso l'agente di protezione del carico di lavoro.
TCP	7	Agente di sicurezza del carico di lavoro	Indirizzi IP LIF dati SVM	Eco dai Agent ai LIF dati SVM

Protocollo	Porta	Origine	Destinazione	Descrizione
SSH	22	Agente di sicurezza del carico di lavoro	Gestione del cluster	Necessario per il blocco degli utenti CIFS/SMB.

Dimensionamento del sistema

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

Installazione di workload Security Agent

Workload Security (in precedenza Cloud Secure) raccoglie i dati delle attività degli utenti utilizzando uno o più agenti. Gli agenti si connettono ai dispositivi del tuo ambiente e raccolgono i dati inviati al livello SaaS per la sicurezza del carico di lavoro per l'analisi. Vedere "Requisiti dell'agente" Per configurare una macchina virtuale dell'agente.

La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

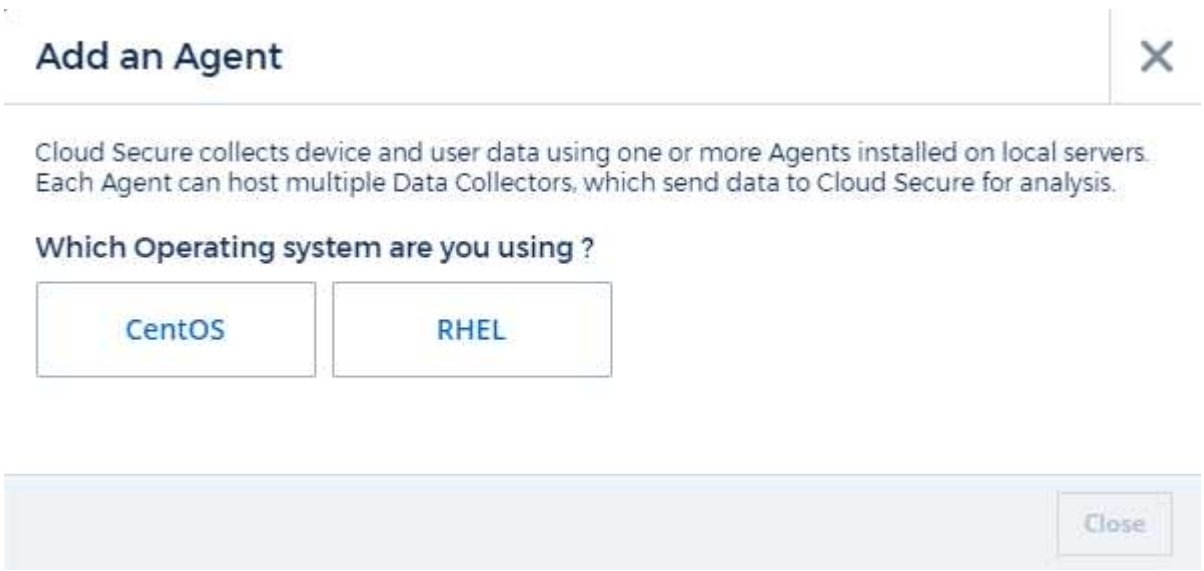
Prima di iniziare

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

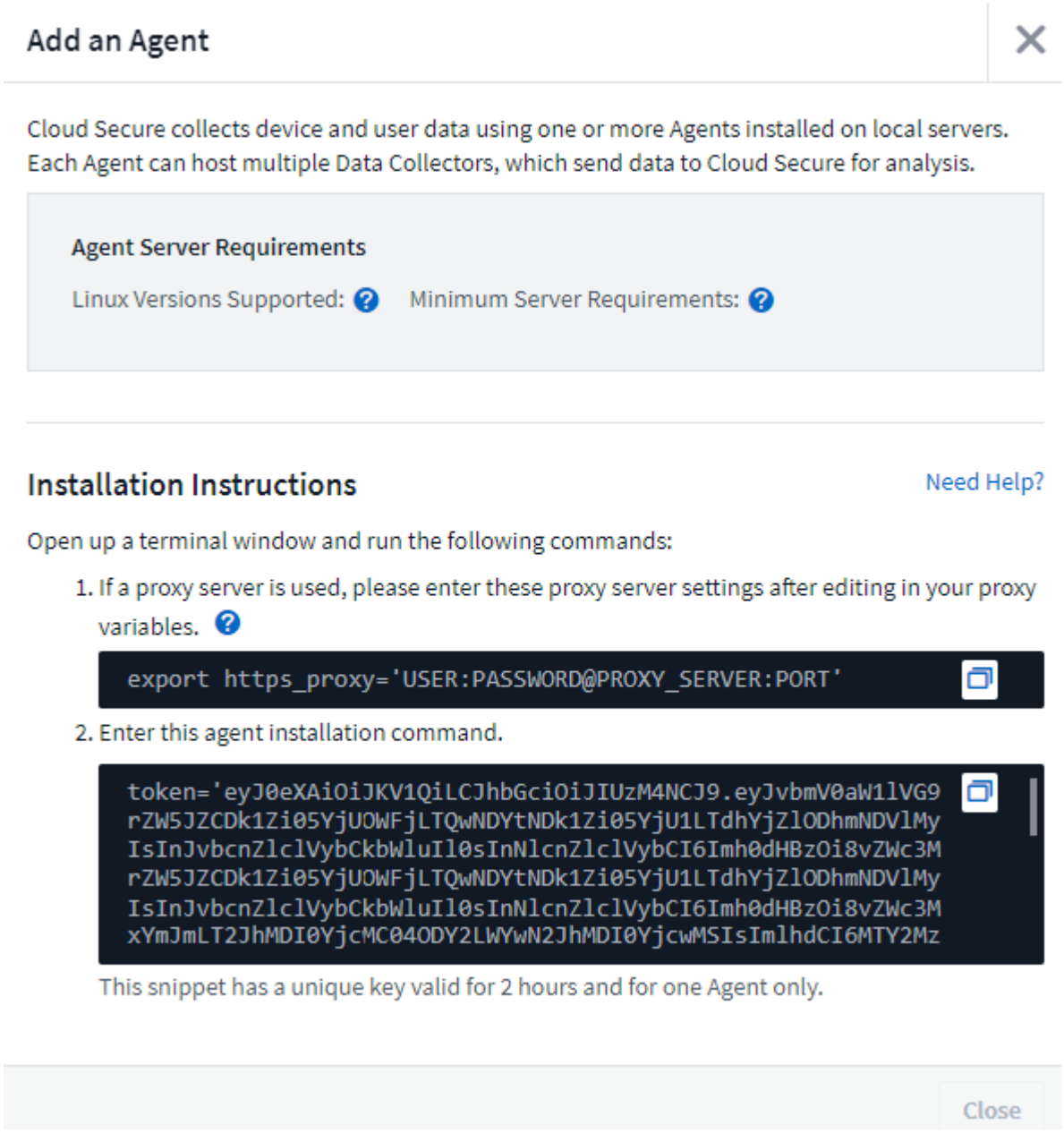
Procedura per l'installazione dell'agente

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

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



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



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

Una volta terminato

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

Configurazione di rete

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

Fasi

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

Segui i passaggi successivi in base alla piattaforma:

CentOS 7.x/RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Output di esempio:

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

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

Output di esempio:

```
35000-55000/tcp
```

Risoluzione dei problemi relativi agli errori dell'agente

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

Problema:	Risoluzione:
L'installazione dell'agente non riesce a creare la cartella /opt/netapp/cloudsecsicuro/Agent/logs/agent.log e il file install.log non fornisce informazioni rilevanti.	Questo errore si verifica durante il bootstrap dell'agente. L'errore non viene registrato nei file di log perché si verifica prima dell'inizializzazione del logger. L'errore viene reindirizzato all'output standard ed è visibile nel log di servizio utilizzando `journalctl -u cloudsecure-agent.service` comando. Questo comando può essere utilizzato per risolvere ulteriormente il problema.

Problema:	Risoluzione:
L’installazione dell’agente non riesce ‘questa distribuzione linux non è supportata. Uscire dall’installazione’.	Questo errore viene visualizzato quando si tenta di installare l’agente su un sistema non supportato. Vedere "Requisiti dell’agente".
Installazione dell’agente non riuscita con l’errore: "-bash: Unzip: Command not found"	Installare unzip ed eseguire nuovamente il comando di installazione. Se Yum è installato sul computer, provare a "yum install unzip" per installare il software unzip. Quindi, copiare nuovamente il comando dall’interfaccia utente di installazione dell’agente e incollarlo nell’interfaccia utente per eseguire nuovamente l’installazione.
L’agente è stato installato ed era in esecuzione. Tuttavia, l’agente si è arrestato improvvisamente.	SSH al computer dell’agente. Controllare lo stato del servizio dell’agente tramite `sudo systemctl status cloudsecure-agent.service`. 1. Controllare se nei registri viene visualizzato il messaggio "Impossibile avviare il servizio daemon di sicurezza workload" . 2. Controllare se l’utente cssys esiste o meno nel computer dell’agente. Eseguire i seguenti comandi uno alla volta con l’autorizzazione root e controllare se l’utente e il gruppo cssys esistono. `sudo id cssys` `sudo groups cssys`3. Se non ne esiste alcuna, è possibile che un criterio di monitoraggio centralizzato abbia eliminato l’utente cssys. 4. Creare manualmente un utente e un gruppo cssys eseguendo i seguenti comandi. `sudo useradd cssys` `sudo groupadd cssys`5. Riavviare il servizio dell’agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service`6. Se non è ancora in esecuzione, controllare le altre opzioni di risoluzione dei problemi.
Impossibile aggiungere più di 50 Data colleziones a un Agente.	È possibile aggiungere solo 50 Data colleziones a un Agente. Questa può essere una combinazione di tutti i tipi di collector, ad esempio Active Directory, SVM e altri tipi di raccolta.
L’interfaccia utente mostra che l’agente è in stato NOT_CONNECTED.	Procedura per riavviare l’agente. 1. SSH al computer dell’agente. 2. Riavviare il servizio dell’agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service`3. Controllare lo stato del servizio dell’agente tramite `sudo systemctl status cloudsecure-agent.service`. 4. L’agente deve passare allo stato CONNESSO.

Problema:	Risoluzione:
La macchina virtuale dell'agente è dietro il proxy Zscaler e l'installazione dell'agente non riesce. A causa dell'ispezione SSL del proxy Zscaler, i certificati di workload Security vengono presentati in quanto firmati da Zscaler CA, in modo che l'agente non stia fidando della comunicazione.	Disattivare l'ispezione SSL nel proxy Zscaler per l'URL *.cloudinsights.netapp.com. Se Zscaler esegue l'ispezione SSL e sostituisce i certificati, la sicurezza del carico di lavoro non funzionerà.
Durante l'installazione dell'agente, l'installazione si blocca dopo la decompressione.	Il comando "chmod 755 -RF" non funziona correttamente. Il comando non riesce quando il comando di installazione dell'agente viene eseguito da un utente sudo non root che ha file nella directory di lavoro, appartenenti a un altro utente, e le autorizzazioni di tali file non possono essere modificate. A causa del comando chmod non funzionante, il resto dell'installazione non viene eseguito. 1. Creare una nuova directory denominata "cloudSecure". 2. Accedere alla directory. 3. Copiare e incollare il "token=…… completo … ./cloudsecure-agent-install.sh" e premere invio. 4. L'installazione dovrebbe essere in grado di procedere.
Se l'Agente non riesce ancora a connettersi a Saas, aprire un caso con il supporto NetApp. Fornire il numero di serie Cloud Insights per aprire un caso e allegare i registri al caso come indicato.	Per allegare i registri al caso: 1. Eseguire il seguente script con il permesso root e condividere il file di output (cloudSecure-Agent-symptoms.zip). a. /opt/netapp/cloudsecsicuro/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Eseguire i seguenti comandi uno alla volta con l'autorizzazione root e condividere l'output. a. id cssys b. gruppi cssys c. cat /etc/os-release
Lo script cloudsecure-agent-symptom-collector.sh non riesce e viene visualizzato il seguente errore. [Root@machine tmp] n. /opt/netapp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh raccolta log del servizio raccolta log dell'applicazione raccolta di configurazioni dell'agente acquisizione di snapshot dello stato del servizio acquisizione di snapshot della struttura della directory dell'agente …… . …… . /Opt/netapp/cloudsecura/Agent/bin/cloudsecura-Agent-Symptom-collector.sh: Riga 52: zip: Errore comando non trovato: Impossibile creare /tmp/cloudsecure-agent-symptoms.zip	Lo strumento ZIP non è installato. Installare lo strumento zip eseguendo il comando "yum install zip". Quindi eseguire di nuovo il file cloudsecure-agent-symptom-collector.sh.

Problema:	Risoluzione:
L'installazione dell'agente non riesce con useradd: Impossibile creare la directory /home/cssys	Questo errore può verificarsi se la directory di login dell'utente non può essere creata in /home, a causa della mancanza di permessi. La soluzione consiste nel creare un utente cssys e aggiungerne manualmente la directory di accesso utilizzando il seguente comando: *Sudo useradd user_name -m -d HOME_DIR* -m :creare la home directory dell'utente se non esiste. -D : il nuovo utente viene creato utilizzando HOME_DIR come valore per la directory di accesso dell'utente. Ad esempio, *sudo useradd cssys -m -d /cssys*, aggiunge un utente *cssys* e crea la directory di login sotto root.
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 – workload Security Agent Daemon Service Loaded: Loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: Disabled) Active: Attivazione (riavvio automatico) (risultato: Codice di uscita) dal mar 2021 26 alle 08-03 21:12 126 PDT; 2s fa processo: 25889 Start/unloopt/stato principale/unbin/unbin/aft/unbin/unload/unload/unbin/unload/unload/it/unbin/it/it/it/it/it/it/it/it/it/it 25889 (code=exited, status=126), 03 21 agosto:12:26 sistema dimostrativo[1]: cloudsecure-agent.service: processo principale terminato, code=exited, status=126/n/a 03 21 agosto:12:26 sistema dimostrativo[1]: L'unità cloudsecure-agent.service è entrata nello stato di errore. Agosto 03 21:12:26 sistema dimostrativo[1]: cloudsecure-agent.service non riuscito.	Questo potrebbe non riuscire perché l'utente *cssys* potrebbe non disporre dell'autorizzazione per l'installazione. Se /opt/netapp è un mount NFS e l'utente *cssys* non ha accesso a questa cartella, l'installazione avrà esito negativo. *Cssys* è un utente locale creato dal programma di installazione di workload Security che potrebbe non disporre dell'autorizzazione per accedere alla condivisione montata. Per verificarlo, tentare di accedere a /opt/netapp/cloudsecrect/Agent/bin/cloudsecrect-Agent utilizzando *cssys* user. Se restituisce "autorizzazione negata", l'autorizzazione all'installazione non è presente. Invece di una cartella montata, installarla in una directory locale del computer.
L'agente era inizialmente connesso tramite un server proxy e il proxy era impostato durante l'installazione dell'agente. Ora il server proxy è cambiato. Come si può modificare la configurazione del proxy dell'Agente?	È possibile modificare agent.properties per aggiungere i dettagli del proxy. Attenersi alla seguente procedura: 1. Passare alla cartella contenente il file di proprietà: cd /opt/netapp/cloudsecsicuro/conf 2. Utilizzando l'editor di testo preferito, aprire il file *agent.properties* per la modifica. 3. Aggiungere o modificare le seguenti righe: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Salvare il file. 5. Riavviare l'agente: Sudo systemctl riavviare cloudsecure-agent.service

Eliminazione di un agente di sicurezza del carico di lavoro

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

Eliminazione di un agente

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

Prima di iniziare

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

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

Procedura per l'eliminazione di un agente:

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

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

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

   Viene visualizzato l'elenco degli agenti configurati.

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

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

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

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

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

Prima di iniziare

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

Procedura per la configurazione di un servizio di raccolta directory utente

1. Nel menu workload Security (sicurezza del carico di lavoro), fare clic su:
   Collector > User Directory Collector > + User Directory Collector e selezionare **Active Directory**

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

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

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

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

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

Nome utente	SAMAccountName

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

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

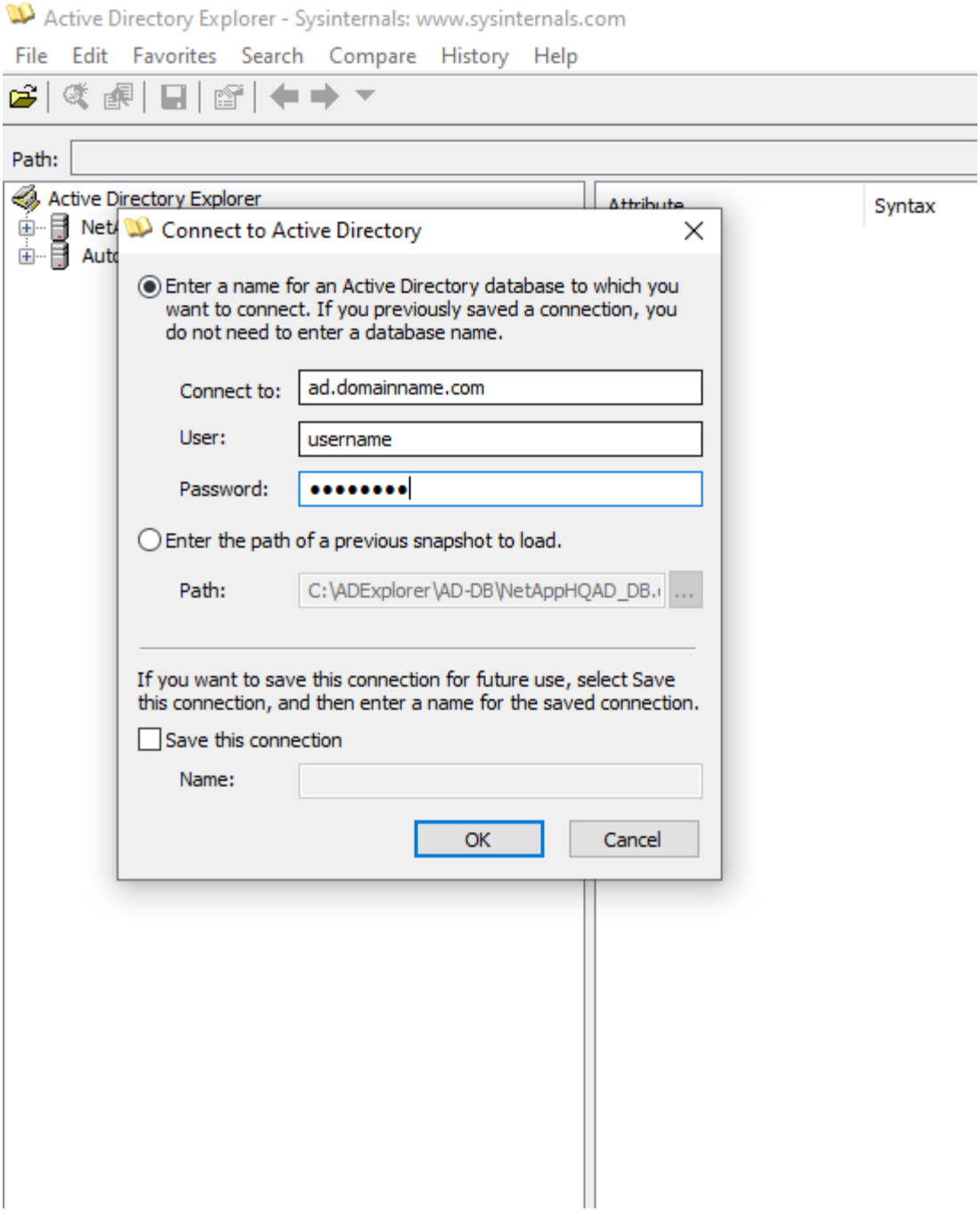
Verifica della configurazione di User Directory Collector

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

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

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

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



Risoluzione degli errori di configurazione di User Directory Collector

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

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

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

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

Configurazione di un servizio di raccolta LDAP Directory Server

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

Prima di iniziare

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

Procedura per la configurazione di un servizio di raccolta directory utente

1. Nel menu workload Security (sicurezza del carico di lavoro), fare clic su: **Collector > User Directory Collector > + User Directory Collector** e selezionare **LDAP Directory Server**

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

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

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

Protocollo	ldap, ldaps, ldap-start-tls
Porte	Selezionare la porta

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

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

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

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

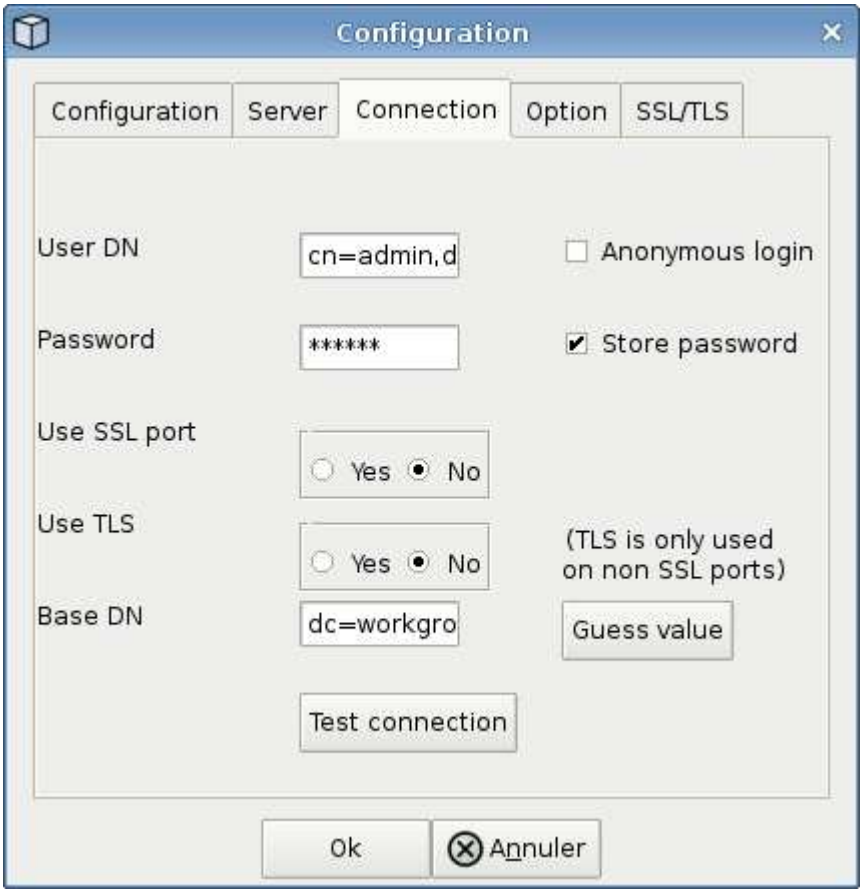
Verifica della configurazione di User Directory Collector

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

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

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

- Installare LDAP Explorer (http://ldaptool.sourceforge.net/) O Java LDAP Explorer (http://jxplorer.org/) Su qualsiasi computer Windows in grado di connettersi al server LDAP.
- Connettersi al server LDAP utilizzando il nome utente/la password del server di directory LDAP.



Risoluzione degli errori di configurazione di LDAP Directory Collector

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

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

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

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

Configurazione del Data Collector SVM di ONTAP

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

Prima di iniziare

- Questo data collector è supportato con i seguenti elementi:
  - Data ONTAP 9.2 e versioni successive. Per prestazioni ottimali, utilizzare una versione Data ONTAP superiore a 9.13.1.
  - Protocollo SMB versione 3.1 e precedenti.
  - Protocollo NFS versione 4.0 e precedenti
  - FlexGroup è supportato da ONTAP 9.4 e versioni successive
  - ONTAP Select è supportato
- Sono supportati solo i tipi di dati SVM. Le SVM con volumi infiniti non sono supportate.
- SVM ha diversi sottotipi. Di questi, sono supportati solo *default*, *Sync_source* e *Sync_destination*.
- Un Agente "deve essere configurato" prima di poter configurare i data colleziones.
- Assicurarsi di disporre di un connettore User Directory configurato correttamente, altrimenti gli eventi mostreranno i nomi utente codificati e non il nome effettivo dell'utente (come memorizzato in Active Directory) nella pagina "Activity Forensics" (analisi delle attività).
- • ONTAP Persistent Store è supportato da 9.15.1.
- Per ottenere prestazioni ottimali, è necessario configurare il server FPolicy in modo che si trova sulla stessa subnet del sistema di storage.
- È necessario aggiungere una SVM utilizzando uno dei due metodi seguenti:
  - Utilizzando l'IP del cluster, il nome SVM e il nome utente e la password di gestione del cluster. ***questo è il metodo consigliato.***
    - Il nome SVM deve essere identico a quello mostrato in ONTAP ed è sensibile al maiuscolo/minuscolo.
  - Utilizzando SVM Vserver Management IP, Username e Password
  - Se non si è in grado o non si è disposti a utilizzare il nome utente e la password completi di Administrator Cluster/SVM Management, è possibile creare un utente personalizzato con privilegi inferiori, come indicato nella "Nota sulle autorizzazioni" di seguito. Questo utente personalizzato può essere creato per l'accesso a SVM o Cluster.
    - o è anche possibile utilizzare un utente ad con un ruolo che disponga almeno delle autorizzazioni di csrole, come indicato nella sezione "A note about permissions" (Nota sulle autorizzazioni) riportata di seguito. Consultare anche la "Documentazione ONTAP".
- Assicurarsi che siano impostate le applicazioni corrette per SVM eseguendo il seguente comando:

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

Output di esempio:

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

- Assicurarsi che la SVM abbia un server CIFS configurato: Clustershell::> `vserver cifs show`

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

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

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

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

Prerequisiti per il blocco dell'accesso utente

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

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

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

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

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

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

Nota sulle autorizzazioni

Autorizzazioni per l'aggiunta tramite Cluster Management IP:

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

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

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

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

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

Autorizzazioni per l'aggiunta tramite Vserver Management IP:

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

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

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

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

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

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

Autorizzazioni per la protezione autonoma da ransomware 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 assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni alla sicurezza del carico di lavoro per raccogliere

informazioni relative all'ARP da ONTAP.

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

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

Per ulteriori informazioni, consultare la sezione "Integrazione con la protezione ransomware autonoma di ONTAP"

Autorizzazioni per accesso ONTAP negate

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

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

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

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

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

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

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

Configurare il data collector

Procedura per la configurazione

1. Accedere come amministratore o come proprietario dell'account all'ambiente Cloud Insights.
2. Fare clic su **sicurezza del carico di lavoro > Collector > +Data Collector**

   Il sistema visualizza i Data Collector disponibili.

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

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

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

Al termine

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

Configurazione consigliata per Metro Cluster

Per Metro Cluster si consiglia quanto segue:

1. Collegare due data collettori, uno alla SVM di origine e l'altro alla SVM di destinazione.
2. I data collezioner devono essere collegati da *Cluster IP*.
3. In qualsiasi momento, un data collector dovrebbe essere in esecuzione, un altro potrebbe essere in errore.

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

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

Policy di servizio

Se si utilizza la policy di servizio di ONTAP versione 9.9.1, per connettersi al servizio di raccolta origine dati, è necessario il servizio *data-fpolicy-client* insieme al servizio dati *data-nfs* e/o *data-cifs*.

Esempio:

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

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

Riproduci-Pausa Data Collector

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

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

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

Tenere presente quanto segue:

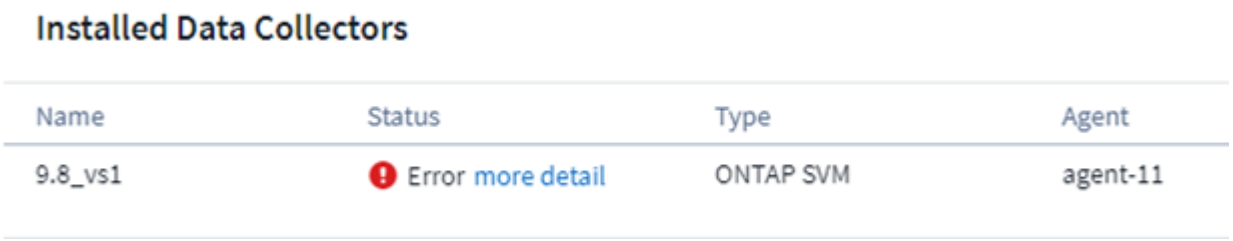
- L'eliminazione degli snapshot non avviene in base alle impostazioni configurate su un raccoglitore in pausa.
- Gli eventi EMS (come ONTAP ARP) non verranno elaborati su un raccoglitore in pausa. Ciò significa che se ONTAP identifica un attacco ransomware, Cloud Insights workload Security non sarà in grado di acquisire quell'evento.
- Le e-mail di notifica dello stato NON verranno inviate per un raccoglitore in pausa.

- Le azioni manuali o automatiche (come Snapshot o blocco utente) non sono supportate in un raccoglitore in pausa.
- In caso di aggiornamenti dell'agente o del raccoglitore, di riavvio/riavvio della VM dell'agente o di riavvio del servizio dell'agente, un raccoglitore in pausa rimarrà nello stato *Paused*.
- Se il data collector si trova nello stato *Error*, il collector non può essere modificato nello stato *Paused*. Il pulsante Pausa viene attivato solo se lo stato del raccoglitore è *in esecuzione*.
- Se l'agente è disconnesso, non è possibile modificare lo stato del collettore in *Paused*. Il raccoglitore passerà allo stato *Stopped* e il pulsante Pausa verrà disattivato.
- Non è possibile eliminare un Data Collector in pausa.
- In pausa, le impostazioni di fpolicy in ONTAP sono disattivate ma non vengono eliminate. Al momento della ripresa, le impostazioni fpolicy in ONTAP vengono nuovamente attivate.

Risoluzione dei problemi

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

In caso di errore, fare clic su *More Detail* nella colonna *Status* per informazioni dettagliate sull'errore.



Problema:	Risoluzione:
Data Collector viene eseguito per un certo periodo di tempo e si arresta dopo un periodo di tempo casuale, con il messaggio di errore: "Messaggio di errore: Connettore in stato di errore. Nome del servizio: Audit. Motivo del guasto: Server fpolicy esterno sovraccarico."	La percentuale di eventi di ONTAP era molto superiore a quella che la casella Agente è in grado di gestire. Di conseguenza, la connessione è stata interrotta. Controllare il picco di traffico in CloudSecure quando si è verificata la disconnessione. Questa opzione è disponibile nella pagina **CloudSecure > Activity Forensics > All Activity**. Se il picco di traffico aggregato è superiore a quello che Agent Box è in grado di gestire, fare riferimento alla pagina Event Rate Checker per informazioni su come dimensionare l'implementazione di Collector in un Agent Box. Se l'agente è stato installato nella casella Agent prima del 4 marzo 2021, eseguire i seguenti comandi nella casella Agent: ECHO 'net.core.rmem_max=8388608' >> /etc/sysctl.conf echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p riavviare il raccoglitore dall'interfaccia utente dopo il ridimensionamento.

Problema:	Risoluzione:
"Collector riporta il messaggio di errore "Nessun indirizzo IP locale trovato sul connettore che può raggiungere le interfacce dati della SVM"."	Questo è probabilmente dovuto a un problema di rete sul lato ONTAP. Attenersi alla seguente procedura: 1. Assicurarsi che non vi siano firewall sui dati della SVM lif o sul lif di gestione che bloccano la connessione dalla SVM. 2. Quando si aggiunge una SVM tramite un IP di gestione del cluster, assicurarsi che il file di dati e il file di gestione della SVM siano in grado di eseguire il ping dalla macchina virtuale dell'agente. In caso di problemi, controllare il gateway, la netmask e i percorsi per la lif. È anche possibile provare ad accedere al cluster tramite ssh utilizzando l'IP di gestione del cluster e ping dell'IP dell'agente. Verificare che l'indirizzo IP dell'agente sia associabile: *Ping di rete -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail* Se non è possibile eseguire il ping, verificare che le impostazioni di rete in ONTAP siano corrette, in modo che il computer dell'agente possa essere collegato. 3. Se hai provato a connetterti tramite Cluster IP e non funziona, prova a connetterti direttamente tramite SVM IP. Vedere sopra per la procedura di connessione tramite SVM IP. 4. Durante l'aggiunta del collector tramite le credenziali SVM IP e vsadmin, controllare se il ruolo Data Plus Mgmt di SVM LIF è attivato. In questo caso il ping alla LIF SVM funzionerà, tuttavia SSH alla LIF SVM non funzionerà. In caso affermativo, creare una LIF solo gestione SVM e provare a connettersi tramite questa LIF solo gestione SVM. 5. Se il problema persiste, creare una nuova LIF SVM e provare a connettersi tramite tale LIF. Assicurarsi che la subnet mask sia impostata correttamente. 6. Debug avanzato: A) avviare una traccia di pacchetto in ONTAP. b) provare a collegare un data collector alla SVM dall'interfaccia utente di CloudSecure. c) attendere che venga visualizzato l'errore. Interrompere la traccia dei pacchetti in ONTAP. d) aprire la traccia del pacchetto da ONTAP. È disponibile in questa località *https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/p*

Problema:	Risoluzione:
Messaggio: "Impossibile determinare il tipo di ONTAP per [hostname: <IP Address>. Motivo: Errore di connessione al <IP Address> del sistema di storage: Host irraggiungibile (host irraggiungibile)"	1. Verificare che sia stato fornito l'indirizzo IP di gestione SVM o l'IP di gestione del cluster corretto. 2. SSH alla SVM o al cluster a cui si intende connettersi. Una volta stabilita la connessione, assicurarsi che il nome SVM o il nome del cluster sia corretto.
Messaggio di errore: "Il connettore è in stato di errore. Service.name: Audit. Motivo del guasto: Server fpolicy esterno terminato."	1. È molto probabile che un firewall blocchi le porte necessarie nel computer dell'agente. Verificare che l'intervallo di porte 35000-55000/tcp sia aperto affinché il computer dell'agente si connetta da SVM. Assicurarsi inoltre che non vi siano firewall abilitati dal lato ONTAP che bloccano la comunicazione con il computer dell'agente. 2. Digitare il seguente comando nella casella Agente e verificare che l'intervallo di porte sia aperto. _Sudo iptables-Save

Problema:	Risoluzione:
grep 3500*_ l'output di esempio dovrebbe essere simile a: *-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT* 3. Accedere a SVM, immettere i seguenti comandi e verificare che nessun firewall sia impostato per bloccare la comunicazione con ONTAP. *visualizzazione firewall servizi di sistema visualizzazione policy firewall servizi di sistema_"Controllare i comandi del firewall" Sul lato ONTAP. 4. SSH alla SVM/Cluster che si desidera monitorare. Eseguire il ping della casella Agent dal file di dati SVM (con il supporto dei protocolli CIFS e NFS) e assicurarsi che il ping funzioni: _Ping di rete -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail* se non è possibile eseguire il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che il computer dell'agente possa eseguire il ping. 5.se una singola SVM viene aggiunta due volte a un tenant tramite 2 data collettori, viene visualizzato questo errore. Eliminare uno dei data collezionisti attraverso l'interfaccia utente. Quindi riavviare l'altro data collector tramite l'interfaccia utente. Il data collector mostrerà lo stato "IN ESECUZIONE" e inizierà a ricevere gli eventi da SVM. In sostanza, in un tenant, 1 SVM deve essere aggiunto una sola volta, tramite 1 data collector. 1 SVM non deve essere aggiunto due volte tramite 2 data collezioner. 6. Nei casi in cui la stessa SVM è stata aggiunta in due diversi ambienti di workload Security (tenant), l'ultimo avrà sempre successo. Il secondo collector configurerà fpolicy con il proprio indirizzo IP e eseguirà il kick out del primo. In questo modo, il collector del primo interrompe la ricezione degli eventi e il servizio di "audit" entra in stato di errore. Per evitare questo problema, configurare ogni SVM in un singolo ambiente. 7. Questo errore può verificarsi anche se le policy di servizio non sono configurate correttamente. Con ONTAP 9.8 o versione successiva, per connettersi al Data Source Collector, è necessario il servizio client data-fpolicy insieme al servizio dati data-nfs e/o data-cifs. Inoltre, il servizio data-fpolicy-client deve essere associato ai lif di dati per la SVM monitorata.	Nessun evento visualizzato nella pagina delle attività.

Problema:	Risoluzione:
1. Verificare che ONTAP Collector sia in esecuzione. In caso affermativo, assicurarsi che alcuni eventi cifs vengano generati sulle macchine virtuali del client cifs aprendo alcuni file. 2. Se non vengono visualizzate attività, accedere a SVM e immettere il seguente comando. *<SVM> ftllog show -source fpolicy* assicurarsi che non ci siano errori relativi a fpolicy. 3. Se non vengono visualizzate attività, accedere a SVM. Immettere il seguente comando *<SVM> policy show* controllare se la policy fpolicy denominata con il prefisso "cloudSecure_" è stata impostata e lo stato è "on". Se non impostato, molto probabilmente l'agente non è in grado di eseguire i comandi nella SVM. Assicurarsi di aver seguito tutti i prerequisiti descritti all'inizio della pagina.	SVM Data Collector si trova in stato di errore e il messaggio di errore indica che l'agente non è riuscito a connettersi al collector.
1. Molto probabilmente l'Agente è sovraccarico e non riesce a connettersi ai Data Source collettori. 2. Verificare quanti Data Source collettori sono connessi all'Agente. 3. Controllare anche la velocità di flusso dei dati nella pagina "All Activity" (tutte le attività) dell'interfaccia utente. 4. Se il numero di attività al secondo è significativamente elevato, installare un altro Agent e spostare alcuni Data Source Collector nel nuovo Agent.	SVM Data Collector visualizza il messaggio di errore "fpolicy.server.connectError: Node failed to stabiling a Connection with the FPolicy server "12.195.15.146" (Reason: "Select Timed out")"
Il firewall è attivato in SVM/Cluster. Pertanto, il motore fpolicy non è in grado di connettersi al server fpolicy. I CLIS in ONTAP che possono essere utilizzati per ottenere ulteriori informazioni sono: Registro eventi show -source fpolicy che mostra il registro eventi di errore show -source fpolicy -fields event,action,description che mostra ulteriori dettagli."Controllare i comandi del firewall" Sul lato ONTAP.	Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio:audit. Motivo del guasto: Nessuna interfaccia dati valida (ruolo: Dati, protocolli dati: NFS o CIFS o entrambi, stato: Up) trovata su SVM."
Assicurarsi che sia presente un'interfaccia operativa (con ruolo di protocollo dati e dati come CIFS/NFS).	Il data collector passa allo stato di errore, quindi PASSA ALLO stato DI ESECUZIONE dopo un certo periodo di tempo, quindi torna a Error. Questo ciclo si ripete.
Ciò si verifica in genere nel seguente scenario: 1. Sono stati aggiunti più data colleziones. 2. I data collezioner che mostrano questo tipo di comportamento avranno 1 SVM aggiunto a questi data collezioner. Ciò significa che 2 o più data collezioner sono collegati a 1 SVM. 3. Assicurarsi che 1 data collector si connetta a una sola SVM. 4. Eliminare gli altri data collezioner collegati alla stessa SVM.	Il connettore è in stato di errore. Nome del servizio: Audit. Motivo dell'errore: Configurazione non riuscita (policy su SVM svmname. Motivo: Valore non valido specificato per l'elemento 'shares-to-include' all'interno di 'fpolicy.policy.scope-modify: "Federal"

Problema:	Risoluzione:
I nomi delle condivisioni devono essere forniti senza virgolette. Modificare la configurazione DSC SVM ONTAP per correggere i nomi delle condivisioni. *Include ed exclude share* non è destinato a un lungo elenco di nomi di share. Utilizzare invece il filtraggio per volume se si dispone di un elevato numero di condivisioni da includere o escludere.	Nel cluster sono presenti fpolicy inutilizzate. Cosa fare con quelli prima dell'installazione di workload Security?
Si consiglia di eliminare tutte le impostazioni fpolicy inutilizzate esistenti anche se si trovano in stato disconnesso. Workload Security creerà fpolicy con il prefisso "cloudSecure_". Tutte le altre configurazioni fpolicy inutilizzate possono essere eliminate. Comando CLI per visualizzare l'elenco fpolicy: *Fpolicy show* passi per eliminare le configurazioni fpolicy: *Fpolicy disable -vserver <svmname> -policy-name <policy_name> fpolicy policy policy policy scope delete -vserver <svmname> -policy-name <policy_name> fpolicy policy policy delete -vserver <svmname> <event_list> -policy-name <policy_name> <svmname>* _fpolicy policy policy event delete -vserver <svmname> <engine_name> -nome-motore-esterno -server_vpolicy	Dopo aver attivato la sicurezza dei workload, le performance di ONTAP ne risentono: La latenza diventa sporadicamente elevata, gli IOPS diventano sporadicamente bassi.
Mentre si utilizza ONTAP con sicurezza del carico di lavoro, a volte i problemi di latenza possono essere riscontrati in ONTAP. Le ragioni possibili sono diverse, 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.	Data Collector in error, visualizza questo messaggio di errore. "Errore: Il connettore è in stato di errore. Nome del servizio: Audit. Motivo dell'errore: Impossibile configurare il criterio su SVM svm_test. Motivo: Valore mancante per il campo zapi: Eventi. "
Inizia con una nuova SVM con solo il servizio NFS configurato. Aggiungere un data collector SVM ONTAP in sicurezza del carico di lavoro. CIFS viene configurato come protocollo consentito per SVM mentre si aggiunge il Data Collector SVM ONTAP in sicurezza del carico di lavoro. Attendere che il Data Collector in workload Security visualizzi un errore. Poiché il server CIFS NON è configurato su SVM, questo errore, come mostrato a sinistra, viene visualizzato da workload Security. Modificare il data collector ONTAP SVM e deselezionare CIFS come protocollo consentito. Salvare il data collector. Verrà avviato solo con il protocollo NFS attivato.	Data Collector visualizza il messaggio di errore: "Errore: Impossibile determinare lo stato di salute del raccoglitore entro 2 tentativi, provare a riavviare nuovamente il Collector (codice di errore: AGENT008)".

Problema:	Risoluzione:
1. Nella pagina Data Collector, scorrere a destra del data collector che indica l'errore e fare clic sul menu a 3 punti. Selezionare *Edit*. Immettere nuovamente la password del data collector. Salvare il data collector premendo il pulsante *Save*. Data Collector verrà riavviato e l'errore dovrebbe essere risolto. 2. Il computer dell'agente potrebbe non disporre di spazio sufficiente per la CPU o la RAM, motivo per cui i DSC si guastano. Verificare il numero di Data Collector aggiunti all'Agente nel computer. Se è superiore a 20, aumentare la capacità della CPU e della RAM del computer dell'agente. Una volta aumentate la CPU e la RAM, i DSC entrano automaticamente in Inizializzazione e quindi in esecuzione. Consultare la guida al dimensionamento su "questa pagina".	Il Data Collector genera un errore quando viene selezionata la modalità SVM.

Se i problemi persistono, accedere ai collegamenti di supporto indicati nella pagina **Guida > supporto**.

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

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

Configurazione dello storage Cloud Volumes ONTAP

Consultare la documentazione di OnCommand Cloud Volumes ONTAP per configurare un'istanza di ha AWS a nodo singolo per ospitare l'agente di sicurezza del carico di lavoro:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

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

Piattaforme supportate

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

Configurazione del computer dell'agente

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

Di seguito sono riportati i passaggi per l'installazione dell'agente in AWS. Per l'installazione, è possibile seguire

procedure equivalenti, applicabili al provider di servizi cloud, in Azure o Google Cloud.

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

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

Fasi

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

Installare Workload Security Agent

1. Accedere come amministratore o come proprietario dell'account all'ambiente Cloud Insights.
2. Accedere a sicurezza del carico di lavoro **Collectors** e fare clic sulla scheda **Agenti**.
3. Fare clic su **+Agent** e specificare RHEL come piattaforma di destinazione.
4. Copiare il comando Installazione agente.
5. Incollare il comando Installazione agente nell'istanza RHEL EC2 a cui si è connessi. In questo modo viene installato l'agente workload Security, fornendo tutte le funzioni di "Prerequisiti dell'agente" sono soddisfatti.

Per informazioni dettagliate, fare riferimento a questo xref:./ https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Risoluzione dei problemi

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

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

Gestione utenti

Workload gli account utente di sicurezza vengono gestiti tramite Cloud Insights.

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

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

Fasi

1. Accedere a workload Security
2. Nel menu, fare clic su **Admin > User Management**

   Sarai inoltrato alla pagina User Management di Cloud Insights.

3. Selezionare il ruolo desiderato per ciascun utente.

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

Ulteriori informazioni sugli account utente e sui ruoli sono disponibili in Cloud Insights "Ruolo dell'utente" documentazione.

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

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

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

Requisiti:

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

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

Fasi:

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

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

   a. Eseguire il seguente comando:

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

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

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

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

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

Tenere presente quanto segue:

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

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

4 core, 32 GB	20 raccolta di dati	20.000 eventi/sec

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

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

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

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

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

Esempio

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

Applichiamo la formula:

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

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

Lo script può fornire risultati errati nei seguenti casi:

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

Di seguito è riportato un esempio di esecuzione di script:

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

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

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

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

Risoluzione dei problemi

Domanda	Risposta

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