工作負載安全

Data Infrastructure Insights

NetApp
February 19, 2026

目錄

工作負載安全

關於儲存工作負載安全

Data Infrastructure Insights儲存工作負載安全（以前稱為Cloud Secure）可協助您透過有關內部威脅的可操作情報來保護您的資料。它提供跨混合雲環境的所有公司資料存取的集中可視性和控制，以確保滿足安全性和合規性目標。

能見度

取得對使用者存取本機或雲端中儲存的關鍵公司資料的集中可見性和控制。

替換無法及時準確地提供資料存取和控制可見性的工具和手動流程。工作負載安全且獨特地在雲端和本地儲存系統上運行，為您提供惡意使用者行為的即時警報。

保護

透過先進的機器學習和異常檢測保護組織資料不被惡意或受感染的使用者濫用。

透過先進的機器學習和使用者行為異常檢測，向您發出任何異常資料存取警報。

遵守

透過審核用戶對儲存在本地或雲端中的關鍵公司資料的存取來確保公司合規性。

入門

工作負載安全入門

工作負載安全功能可協助您監控使用者活動並偵測儲存環境中的潛在安全威脅。在開始監控之前，您需要設定代理程式、資料收集器和目錄服務，為全面的安全監控奠定基礎。

工作負載安全系統使用代理從儲存系統收集存取資料並從目錄服務伺服器收集使用者資訊。

在開始收集資料之前，您需要配置以下內容：

任務	相關資訊
配置代理	"代理要求" "新增代理"
配置使用者目錄連接器	"新增使用者目錄連接器"
配置資料收集器	按一下*工作負載安全性>收集器*點選要設定的資料收集器。有關收集器信息，請參閱文件中的“資料收集器供應商參考”部分。

建立使用者帳戶	"管理用戶帳戶"

工作負載安全也可以與其他工具整合。例如，"請參閱本指南"與 Splunk 整合。

工作負載安全代理要求

在滿足最低作業系統、CPU、記憶體和磁碟空間要求的專用伺服器上部署 Workload Security Agent，以確保最佳的監控和威脅偵測效能。本指南詳細說明了"安裝 Workload Security Agent"前所需的硬體和網路要求，包括支援的 Linux 發行版、網路連接規則和系統容量規劃指南。

成分	**Linux** 需求
作業系統	執行下列任一授權版本的電腦：* AlmaLinux 9.4（64 位元）至 9.5（64 位元）、10（64 位元），包括 SELinux* CentOS Stream 9（64 位元）* Debian 11（64 位元）、12（64 位元），包括 SEL 8.10（64 位元）、9.1（64 位元）至 9.6（64 位元），包括 SELinux* Red Hat Enterprise Linux 8.10（64 位元）、9.1（64 位元）至 9.6（64 位元）、10（64 位元），包括 SELinux* Rock 15 SP4（64 位元）至 15 SP6（64 位元），包括 SELinux * Ubuntu 20.04 LTS（64 位元）、22.04 LTS（64 位元）、24.04 LTS（64 位元）此電腦不應執行其他應用程式級軟體。建議使用專用伺服器。
命令	安裝需要“unzip”。此外，安裝、執行腳本和卸載都需要「sudo su –」命令。
中央處理器	4 個 CPU 核心
記憶	16 GB 內存
可用磁碟空間	磁碟空間應按以下方式分配：/opt/netapp 36 GB（建立檔案系統後至少有 35 GB 的可用空間）注意：建議分配一些額外的磁碟空間以允許建立檔案系統。確保檔案系統中至少有 35 GB 的可用空間。如果 /opt 是從 NAS 儲存掛載的資料夾，請確保本機使用者可以存取該資料夾。如果本機使用者沒有存取此資料夾的權限，代理程式或資料收集器可能無法安裝。請參閱"故障排除"部分了解更多詳情。
網路	100 Mbps 到 1 Gbps 乙太網路連接、靜態 IP 位址、與所有設備的 IP 連接以及工作負載安全實例所需的連接埠（80 或 443）。

請注意：工作負載安全代理程式可以與Data Infrastructure Insights獲取單元和/或代理程式安裝在同一台機器上。但是，最佳做法是將它們安裝在單獨的機器上。如果將它們安裝在同一台機器上，請按如下所示指派磁碟空間：

可用磁碟空間	50-55 GB 對於 Linux，應以以下方式分配磁碟空間：/opt/netapp 25-30 GB /var/log/netapp 25 GB

其他建議

- 強烈建議使用*網路時間協定 (NTP)* 或*簡單網路時間協定 (SNTP)* 同步ONTAP系統和代理機器上的時間。

雲端網路存取規則

對於*美國*的工作負載安全環境：

協定	港口	來源	目的地	描述
TCP	443	工作負載安全代理	<網站名稱>.cs01.cloudinsights.netapp.com <網站名稱>.c01.cloudinsights.netapp.com <網站名稱>.c02.cloudinsights.netapp.com	存取Data Infrastructure Insights
TCP	443	工作負載安全代理	agentlogin.cs01.cloudinsights.netapp.com	存取身份驗證服務

對於*基於歐洲的*工作負載安全環境：

協定	港口	來源	目的地	描述
TCP	443	工作負載安全代理	<網站名稱>.cs01-eu-1.cloudinsights.netapp.com <網站名稱>.c01-eu-1.cloudinsights.netapp.com <網站名稱>.c02-eu-1.cloudinsights.netapp.com	存取Data Infrastructure Insights
TCP	443	工作負載安全代理	agentlogin.cs01-eu-1.cloudinsights.netapp.com	存取身份驗證服務

對於*基於亞太地區*的工作負載安全環境：

協定	港口	來源	目的地	描述
TCP	443	工作負載安全代理	<網站名稱>.cs01-ap-1.cloudinsights.netapp.com <網站名稱>.c01-ap-1.cloudinsights.netapp.com <網站名稱>.c02-ap-1.cloudinsights.netapp.com	存取Data Infrastructure Insights
TCP	443	工作負載安全代理	agentlogin.cs01-ap-1.cloudinsights.netapp.com	存取身份驗證服務

網路內規則

協定	港口	來源	目的地	描述
TCP	389（LDAP） 636（LDAP/啟動-tls）	工作負載安全代理	LDAP 伺服器 URL	連線到 LDAP
TCP	443	工作負載安全代理	叢集或 SVM 管理 IP 位址（取決於 SVM 收集器配置）	API 與ONTAP進行通信
TCP	35000 - 55000	SVM 資料 LIF IP 位址	工作負載安全代理	ONTAP與工作負載安全代理之間針對 Fpolicy 事件的通訊。必須向工作負載安全代理程式開啟這些端口，以便ONTAP向其發送事件，包括工作負載安全代理本身上的任何防火牆（如果存在）。請注意，您不需要保留所有這些端口，但為此保留的端口必須在此範圍內。建議先預留約 100 個端口，然後根據需要增加。
TCP	35000-55000	叢集管理IP	工作負載安全代理	從ONTAP叢集管理 IP 到工作負載安全代理程式的通信，用於 **EMS** 事件。必須向工作負載安全代理程式開啟這些端口，以便ONTAP向其發送 **EMS** 事件，包括工作負載安全代理本身上的任何防火牆（如果存在）。請注意，您不需要保留所有這些端口，但為此保留的端口必須在此範圍內。建議先預留約 100 個端口，然後根據需要增加。
SSH	22	工作負載安全代理	叢集管理	需要 CIFS/SMB 使用者阻止。

系統規模

查看"事件發生率檢查器"有關尺寸的資訊的文件。

部署工作負載安全代理

工作負載安全代理程式對於監控使用者活動和偵測儲存基礎架構中潛在的安全威脅至關重要。本指南提供逐步安裝說明、代理管理最佳實務（包括暫停/恢復和固定/取消固定功能）以及部署後設定要求。在開始之前，請確保您的代理伺服器符合以下條件： "系統需求"。

開始之前

- 安裝、執行腳本和解除安裝都需要 sudo 權限。
- 安裝代理程式時，會在機器上建立本機使用者_cssys_和本機群組_cssys_。如果權限設定不允許建立本機用戶，而是需要 Active Directory，則必須在 Active Directory 伺服器中建立使用者名為 *cssys* 的使用者。
- 您可以閱讀有關Data Infrastructure Insights安全性的文章"這裡"。

最佳實踐

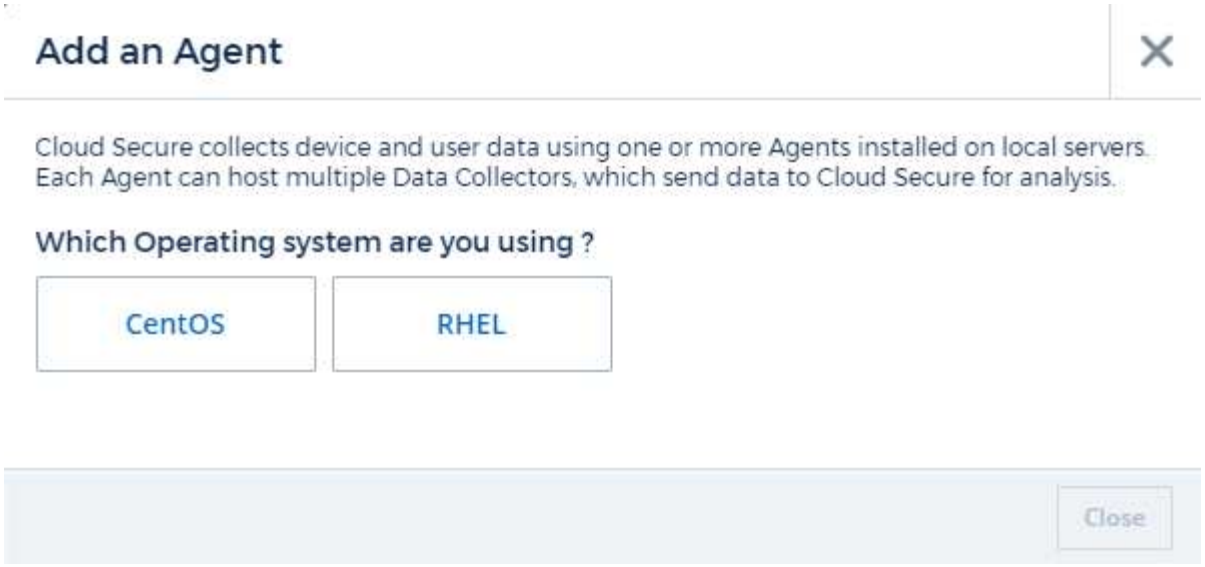
在配置工作負載安全代理之前，請記住以下事項。

暫停和恢復	暫停：從ONTAP移除 fpolicies。通常用於客戶執行可能需要大量時間的長時間維護活動，例如代理虛擬機器重新啟動或儲存更換。恢復：將 fpolicies 重新加入到ONTAP。
別針和拔針	Unpin 會立即取得最新版本（如果可用），並升級代理程式和收集器。在此升級過程中，fpolicies 將斷開連接並重新連接。此功能專為希望控制自動升級時間的客戶而設計。請見下文插針/拔針說明。
推薦方法	對於大型配置，建議使用引腳和引腳斷開操作，而不是暫停集電極。使用固定和取消固定功能時，無需暫停和恢復。客戶可以保留其代理商和收款員，並在收到有關新版本的電子郵件通知後，有 30 天的時間逐個選擇性地升級代理商。這種方法最大限度地減少了對 fpolicies 的延遲影響，並提供了對升級過程的更大控制。

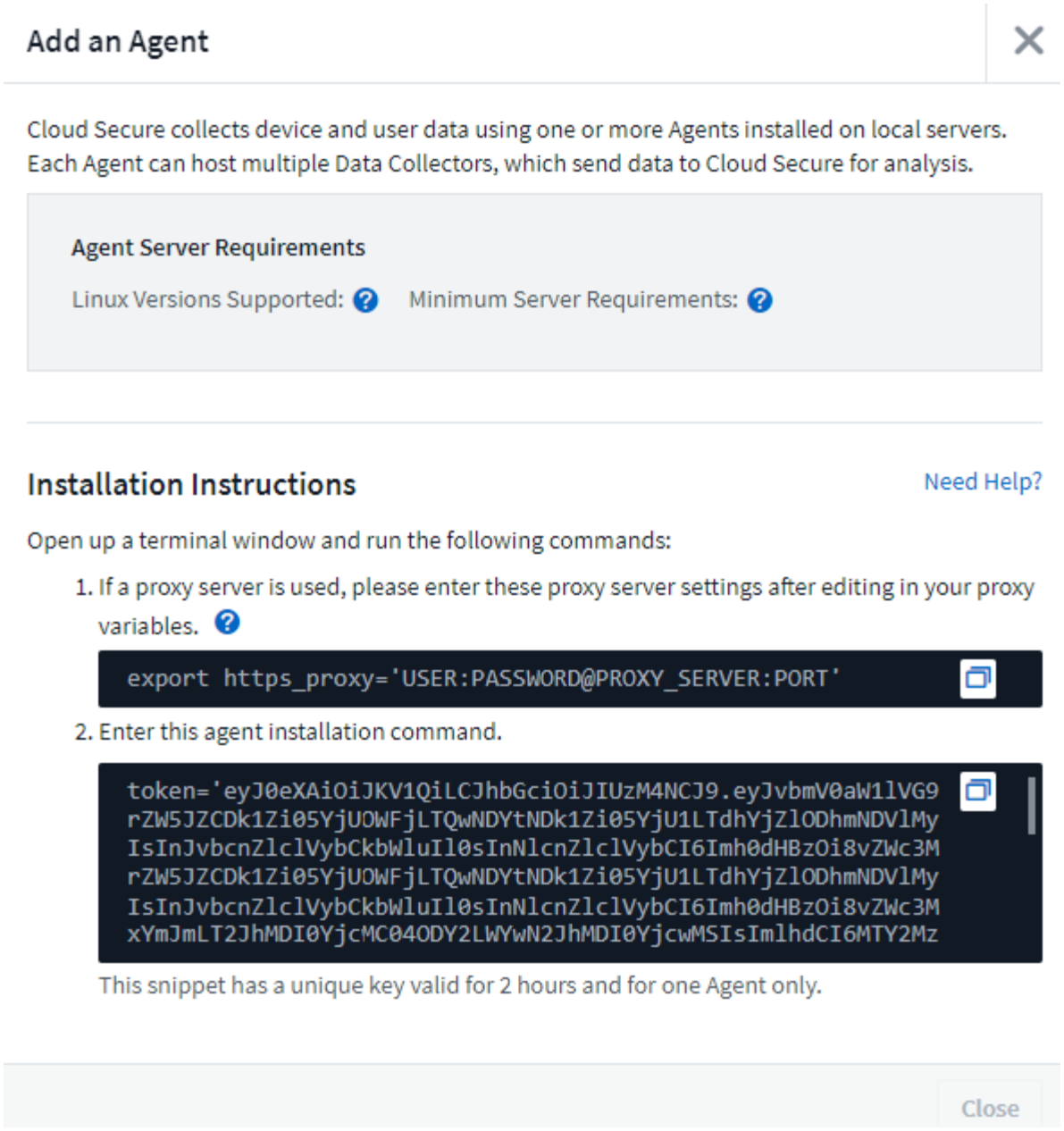
安裝代理的步驟

1. 以管理員或帳戶擁有者的身分登入您的工作負載安全環境。
2. 選擇*收藏家>代理商>+代理商*

   系統顯示「新增代理」頁面：



3. 驗證代理伺服器是否符合最低系統要求。
4. 若要驗證代理伺服器是否正在執行支援的 Linux 版本，請按一下_支援的版本 (i)_。
5. 如果您的網路使用代理伺服器，請按照代理程式部分中的說明設定代理伺服器詳細資訊。



6. 按一下「複製到剪貼簿」圖示以複製安裝命令。
7. 在終端機視窗中執行安裝命令。
8. 安裝成功完成後系統顯示以下訊息：

完成後

1. 您需要配置一個"使用者目錄收集器"。
2. 您需要配置一個或多個資料收集器。

網路設定

在本機系統上執行下列命令以開啟工作負載安全性將使用的連接埠。如果對連接埠範圍有安全性問題，則可以使用較小的連接埠範圍，例如 *35000:35100*。每個 SVM 使用兩個連接埠。

步驟

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

根據您的平台執行以下步驟：

CentOS 7.x / RHEL 7.x：

1. `sudo iptables-save | grep 35000`

範例輸出：

```
 -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`（適用於 CentOS 8）

範例輸出：

```
35000-55000/tcp
```

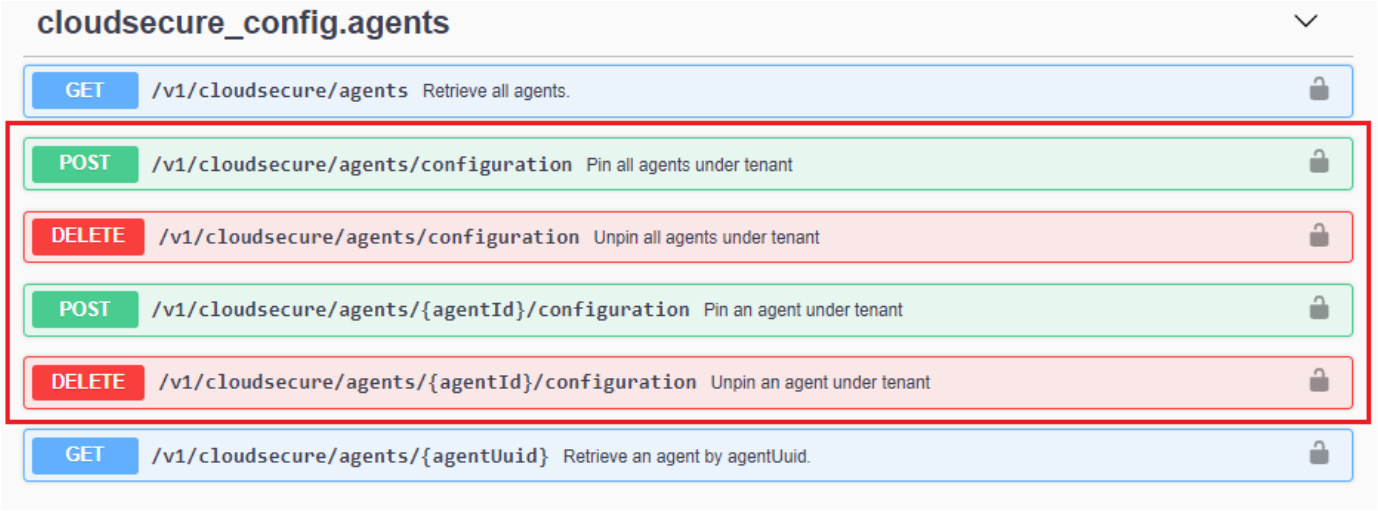
將代理程式“固定”在目前版本

預設情況下，Data Infrastructure Insights工作負載安全性會自動更新代理程式。一些客戶可能希望暫停自動更新，這將使代理商保持其當前版本，直到發生以下情況之一：

- 客戶恢復自動代理更新。
- 30天過去了。請注意，30 天從最近一次代理更新之日開始，而不是從代理暫停之日開始。

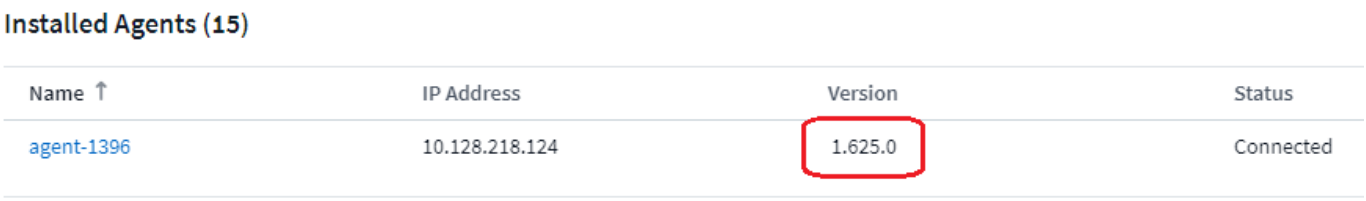
在每種情況下，代理程式都會在下一次工作負載安全刷新時更新。

若要暫停或恢復自動代理更新，請使用 *cloudsecure_config.agents* API：



請注意，暫停或恢復操作可能需要最多五分鐘才能生效。

您可以在「工作負載安全性 > 收集器」頁面的「代理」標籤中查看目前代理程式版本。



代理錯誤故障排除

下表描述了已知問題及其解決方法。

問題：	解決：
代理程式安裝無法建立 /opt/netapp/cloudsecure/agent/logs/agent.log 資料夾，且 install.log 檔案未提供相關資訊。	此錯誤發生在代理引導期間。該錯誤未記錄在日誌檔案中，因為它發生在記錄器初始化之前。錯誤被重定向到標準輸出，並可使用以下方式在服務日誌中查看 `journalctl -u cloudsecure-agent.service`命令。此命令可用於進一步解決問題。 est
代理安裝失敗，並顯示「不支援此 Linux 發行版」。退出安裝」。	當您嘗試在不支援的系統上安裝代理程式時會出現此錯誤。看"代理要求"。
代理安裝失敗，錯誤為：“-bash：unzip：未找到命令”	安裝unzip然後再次執行安裝命令。如果機器上安裝了 Yum，請嘗試「yum install unzip」來安裝解壓縮軟體。之後，從代理安裝 UI 重新複製命令並將其貼上到 CLI 中以再次執行安裝。

問題：	解決：
代理程式已安裝並正在運行。然而代理卻突然停止了。	透過 SSH 連接到代理機器。透過以下方式檢查代理服務的狀態 `sudo systemctl status cloudsecure-agent.service`。1.檢查日誌是否顯示訊息「無法啟動工作負載安全守護程序服務」。2.檢查代理機器中是否存在 cssys 使用者。以root權限逐一執行以下指令，並檢查cssys使用者和群組是否存在。 `sudo id cssys` `sudo groups cssys`3.如果不存在，則集中監控策略可能已刪除 `cssys` 使用者。4.透過執行以下命令手動建立 `cssys` 使用者和群組。 `sudo useradd cssys` `sudo groupadd cssys`5.然後透過執行以下命令重新啟動代理服務： `sudo systemctl restart cloudsecure-agent.service` 6.如果仍然無法運行，請檢查其他故障排除選項。
無法為代理程式新增超過 50 個資料收集器。	一個代理只能增加 50 個資料收集器。這可以是所有收集器類型的組合，例如 Active Directory、SVM 和其他收集器。
UI 顯示代理程式處於 NOT_CONNECTED 狀態。	重新啟動代理程式的步驟。1.透過 SSH 連接到代理機器。2.然後透過執行以下命令重新啟動代理服務： `sudo systemctl restart cloudsecure-agent.service` 3.透過以下方式檢查代理服務的狀態 `sudo systemctl status cloudsecure-agent.service`。4.代理應進入 CONNECTED 狀態。
代理 VM 位於 Zscaler 代理程式後面，且代理安裝失敗。由於 Zscaler 代理程式的 SSL 檢查，工作負載安全性憑證以 Zscaler CA 簽署的形式呈現，因此代理程式不信任該通訊。	停用 Zscaler 代理程式中 *.cloudinsights.netapp.com url 的 SSL 檢查。如果 Zscaler 進行 SSL 檢查並替換證書，工作負載安全將無法運作。
安裝代理程式時，解壓縮後安裝在掛起。	“chmod 755 -Rf”指令失敗。當代理安裝指令由非 root sudo 使用者執行，且工作目錄中有屬於另一個使用者的文件，且這些文件的權限無法變更時，指令將會失敗。由於 chmod 指令失敗，其餘安裝無法執行。1.建立一個名為「cloudsecure」的新目錄。2.轉到該目錄。3.複製並貼上完整的「token=… … ./cloudsecure-agent-install.sh」安裝指令並按下回車鍵。4.安裝應該可以繼續。
如果代理程式仍然無法連線到 Saas，請向NetApp支援部門提交案例。提供Data Infrastructure Insights序號以開啟案例，並按照說明將日誌附加到案例中。	將日誌附加到案例：1.使用 root 權限執行以下腳本並共用輸出檔案（cloudsecure-agent-symptoms.zip）。 a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2.使用 root 權限逐一執行以下命令並共用輸出。 a. id cssys b. groups cssys c. cat /etc/os-release

問題：	解決：
cloudsecure-agent-symptom-collector.sh 腳本失敗並出現下列錯誤。 [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 收集服務日誌 收集應用程式日誌收集代理程式設定 拍攝服務狀態快照 拍攝代理目錄結構快照…… …… /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh：第 52 行：zip：未找到指令錯誤：無法建立 /tmp/cloudsecure-agent-symptoms.zip	Zip 工具未安裝..透過執行指令“yum install zip”安裝zip工具。然後再次運行cloudsecure-agent-symptom-collector.sh。
代理安裝因 useradd 而失敗：無法建立目錄 /home/cssys	如果由於缺乏權限而無法在 /home 下建立使用者的登入目錄，則可能會發生此錯誤。解決方法是建立 cssys 使用者並使用以下命令手動新增其登入目錄：*sudo useradd user_name -m -d HOME_DIR* -m：如果不存在，則建立使用者的主目錄。 -d ：使用 HOME_DIR 作為使用者登入目錄的值來建立新使用者。例如 ，*sudo useradd cssys -m -d /cssys*，新增使用者 *cssys* 並在根目錄下建立其登入目錄。
安裝後代理未運行。 *Systemctl status cloudsecure-agent.service* 顯示以下內容：[root@demo ~]# systemctl status cloudsecure-agent.service agent.service – 工作負載安全代理守護程序服務已載入：已載入（/usr/lib/systemd/system/cloudsecure-agent. 啟用2021 年 8 月 3 日星期二 21:12:26 PDT 起；2 秒前 進程：25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent（代碼=exited status=126） 主21:12:26 demo systemd[1]：cloudsecure-agent.service：主進程已退出，代碼=exited，狀態=126/n/a 8 月 3 日 21:12:26 demo systemd[1]：單元 cloudsecure-agent.service 進入失敗狀態。 8 月 3 日 21:12:26 demo systemd[1]: cloudsecure-agent.service 失敗。	這可能會失敗，因為_cssys_使用者可能沒有安裝權限。如果 /opt/netapp 是 NFS 掛載，且 *cssys* 使用者無權存取此資料夾，則安裝將失敗。 *cssys* 是由 Workload Security 安裝程式建立的本機用戶，可能沒有權限存取已安裝的共用。您可以嘗試使用 *cssys* 使用者存取 /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent 來檢查這一點。如果傳回“權限被拒絕”，則表示不存在安裝權限。不要安裝在已安裝的資料夾中，而是安裝在機器本機的目錄中。
代理最初透過代理伺服器連接，並且代理程式是在代理安裝期間設定的。現在代理伺服器已經改變。如何更改代理的代理配置？	您可以編輯 agent.properties 來新增代理詳細資訊。請遵循以下步驟：1.變更為包含屬性檔案的資料夾：cd /opt/netapp/cloudsecure/conf 2.使用您喜歡的文字編輯器，開啟_agent.properties_檔案進行編輯。3.新增或修改下列一行 ：AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4.儲存文件。5.重新啟動代理程式：sudo systemctl restart cloudsecure-agent.service

刪除工作負載安全代理

刪除工作負載安全代理程式時，必須先刪除與該代理程式關聯的所有資料收集器。

刪除代理

刪除代理程式會刪除與該代理程式關聯的所有資料收集器。如果您打算使用不同的代理程式配置資料收集器，則應在刪除代理程式之前建立資料收集器配置的備份。

開始之前

1. 確保從工作負載安全入口網站中刪除與代理相關的所有資料收集器。

   注意：如果所有相關收集器都處於 STOPPED 狀態，請忽略此步驟。

刪除代理的步驟：

1. 透過 SSH 進入代理虛擬機器並執行以下命令。出現提示時，輸入“y”繼續。

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

2. 點選“工作負載安全性”>“收集器”>“代理”*

   系統顯示已配置的代理程式清單。

3. 按一下要刪除的代理程式的選項功能表。
4. 按一下“刪除”。

   系統顯示「刪除代理」頁面。

5. 點選“刪除”確認刪除。

設定 **Active Directory (AD)** 使用者目錄收集器

可以設定工作負載安全性以從 Active Directory 伺服器收集使用者屬性。

開始之前

- 您必須是Data Infrastructure Insights管理員或帳戶所有者才能執行此任務。
- 您必須擁有託管 Active Directory 伺服器的伺服器的 IP 位址。
- 在配置使用者目錄連接器之前，必須先配置代理程式。

配置使用者目錄收集器的步驟

1. 在「工作負載安全」功能表中，按一下：收集器 **>** 使用者目錄收集器 **> +** 使用者目錄收集器，然後選擇*Active Directory*

   系統顯示新增使用者目錄畫面。

透過在下表中輸入所需資料來設定使用者目錄收集器：

Name	描述
Name	使用者目錄的唯一名稱。例如_GlobalADColector_
代理人	從清單中選擇一個已配置的代理
伺服器IP/域名	託管活動目錄的伺服器的 IP 位址或完全限定網域名稱 (FQDN)
森林名稱	目錄結構的森林層級。森林名稱允許以下兩種格式：*x.y.z* ⇒ 直接域名，與您在 SVM 上的一樣。 [範例：hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 相對可分辨名稱 [範例：DC=hq,DC=companyname,DC=com] 或您可以指定如下：*OU=engineering,DC=hq,DC=companyname=DC=com* [按特定 name eng DC=netapp, DC=com_ [從 OU <engineering> 取得具有 <username> 的特定使用者] _CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com,O= companyname,L=Boston,Scro=MA 的
綁定 DN	允許使用者搜尋目錄。例如：*username@companyname.com* 或 *username@domainname.com* 另外，還需要網域唯讀權限。使用者必須是安全性群組「只讀網域控制站」的成員。
綁定密碼	目錄伺服器密碼（即綁定 DN 中使用的使用者名稱的密碼）
協定	ldap、ldaps、ldap-start-tls
連接埠	選擇連接埠

如果在 Active Directory 中修改了預設屬性名稱，請輸入下列 Directory Server 所需的屬性。大多數情況下，這些屬性名稱在 Active Directory 中不會被修改，在這種情況下，您可以簡單地使用預設屬性名稱。

屬性	目錄伺服器中的屬性名稱
顯示名稱	姓名
SID	物件標識符
使用者名稱	sAM帳戶名稱

按一下「包括可選屬性」以新增下列任意屬性：

屬性	目錄伺服器中的屬性名稱
電子郵件	郵件
電話號碼	電話號碼
角色	標題
國家	公司
狀態	狀態
部門	部門

照片	縮圖
經理DN	主管
團體	成員

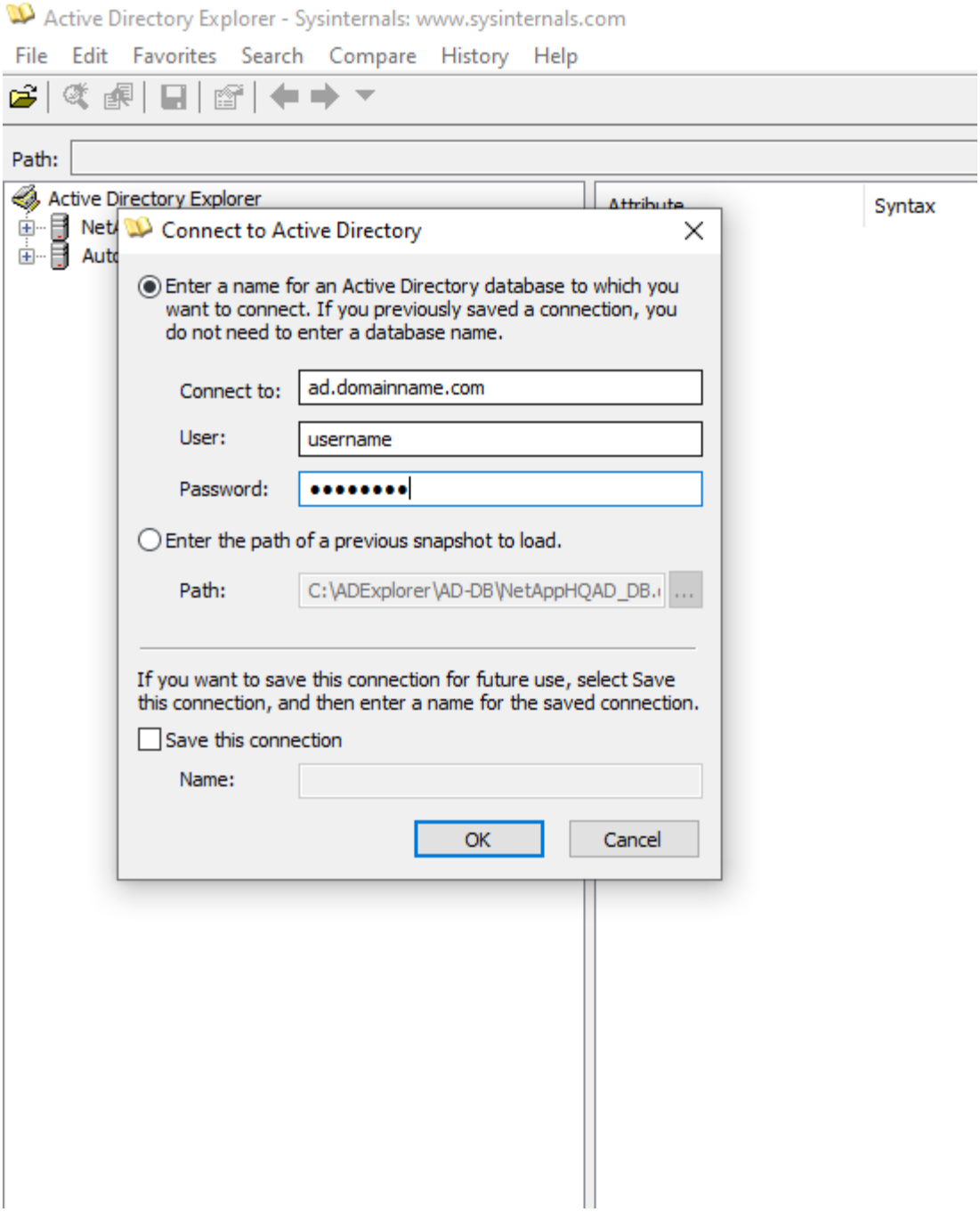
測試您的使用者目錄收集器配置

您可以使用下列步驟驗證 LDAP 使用者權限和屬性定義：

- 使用下列指令驗證 Workload Security LDAP 使用者權限：

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

- 使用 AD Explorer 瀏覽 AD 資料庫、查看物件屬性和特性、檢視權限、檢視物件的模式、執行可以儲存和重新執行的複雜搜尋。
  - 安裝"AD 瀏覽器"在任何可以連接到 AD 伺服器的 Windows 機器上。
  - 使用 AD 目錄伺服器的使用者名稱/密碼連線到 AD 伺服器。



排除使用者目錄收集器配置錯誤

下表描述了收集器配置期間可能出現的已知問題和解決方法：

問題：	解決：
新增使用者目錄連接器會導致「錯誤」狀態。錯誤提示「為 LDAP 伺服器提供的憑證無效」。	提供的使用者名稱或密碼不正確。編輯並提供正確的使用者名稱和密碼。
新增使用者目錄連接器會導致「錯誤」狀態。錯誤提示：“無法取得與作為林名稱提供的 DN=DC=hq,DC=domainname,DC=com 對應的物件。”	提供的森林名稱不正確。編輯並提供正確的森林名稱。

問題：	解決：
網域使用者的選用屬性未出現在工作負載安全使用者設定檔頁面中。	這可能是由於 CloudSecure 中新增的可選屬性名稱與 Active Directory 中的實際屬性名稱不符所造成的。編輯並提供正確的可選屬性名稱。
資料收集器處於錯誤狀態，顯示「無法檢索 LDAP 使用者。失敗原因：無法連接到伺服器，連接為空”	點選“重新啟動”按鈕重新啟動收集器。
新增使用者目錄連接器會導致「錯誤」狀態。	確保您已為必填欄位（伺服器、林名稱、綁定 DN、綁定密碼）提供了有效值。確保 bind-DN 輸入始終以「Administrator@<domain_forest_name>」或具有網域管理員權限的使用者帳戶的形式提供。
新增使用者目錄連接器會導致「重試」狀態。顯示錯誤“無法定義收集器的狀態，原因 Tcp 命令 [Connect(localhost:35012,None,List(),Some(,seconds),true)] 因 java.net.ConnectionException:Connection 被拒絕而失敗。”	為 AD 伺服器提供的 IP 或 FQDN 不正確。編輯並提供正確的 IP 位址或 FQDN。
新增使用者目錄連接器會導致「錯誤」狀態。錯誤提示「無法建立 LDAP 連線」。	為 AD 伺服器提供的 IP 或 FQDN 不正確。編輯並提供正確的 IP 位址或 FQDN。
新增使用者目錄連接器會導致「錯誤」狀態。錯誤提示：「無法載入設定。原因：資料來源配置錯誤。具體原因：/connector/conf/application.conf: 70: ldap.ldap-port 的類型為 STRING 而非 NUMBER”	提供的連接埠值不正確。嘗試使用 AD 伺服器的預設連接埠值或正確的連接埠號碼。
我從強制屬性開始，並且它起作用了。新增可選項後，可選屬性資料不會從 AD 中取得。	這可能是由於 CloudSecure 中新增的可選屬性與 Active Directory 中的實際屬性名稱不符所造成的。編輯並提供正確的強製或可選屬性名稱。
重新啟動收集器後，AD 同步何時發生？	收集器重新啟動後，AD 同步將立即發生。取得約30萬用戶的用戶資料大約需要15分鐘，並且每12小時自動刷新一次。
使用者資料從 AD 同步到 CloudSecure。數據何時會被刪除？	如果沒有刷新，用戶資料將保留13個月。如果租戶被刪除，那麼資料也將被刪除。
使用者目錄連接器導致“錯誤”狀態。 「連接器處於錯誤狀態。服務名稱：usersLdap。失敗原因：無法檢索 LDAP 使用者。失敗原因：80090308：LdapErr：DSID-0C090453，註：AcceptSecurityContext 錯誤，資料 52e，v3839”	提供的森林名稱不正確。請參閱上文，了解如何提供正確的森林名稱。

問題：	解決：
用戶資料頁面中未填寫電話號碼。	這很可能是由於 Active Directory 的屬性對映問題所造成的。1.編輯從 Active Directory 取得使用者資訊的特定 Active Directory 收集器。2.請注意，在選用屬性下，有一個欄位名稱「電話號碼」會對應到 Active Directory 屬性「telephonenumber」。4.現在，請使用上述所述的 Active Directory Explorer 工具瀏覽 Active Directory 並查看正確的屬性名稱。3.確保 Active Directory 中有一個名為「telephonenumber」的屬性，其中確實包含使用者的電話號碼。5.假設在 Active Directory 中它已被修改為「電話號碼」。6.然後編輯 CloudSecure 使用者目錄收集器。在可選屬性部分，將“telephonenumber”替換為“phonenumber”。7.儲存 Active Directory 收集器，收集器將重新啟動並取得使用者的電話號碼，並將其顯示在使用者個人資料頁面中。
如果在 Active Directory (AD) 伺服器上啟用了加密憑證 (SSL)，則 Workload Security User Directory Collector 無法連線到 AD 伺服器。	在設定使用者目錄收集器之前停用 AD 伺服器加密。一旦獲取用戶詳細信息，它將保留 13 個月。如果 AD 伺服器在取得使用者詳細資訊後斷開連接，則不會取得 AD 中新新增的使用者。要再次獲取，用戶目錄收集器需要連接到 AD。
CloudInsights Security 中存在來自 Active Directory 的資料。想要從 CloudInsights 中刪除所有使用者資訊。	無法僅從 CloudInsights Security 中刪除 Active Directory 使用者資訊。為了刪除用戶，需要刪除整個租戶。

設定 **LDAP** 目錄伺服器收集器

您設定工作負載安全性以從 LDAP 目錄伺服器收集使用者屬性。

開始之前

- 您必須是Data Infrastructure Insights管理員或帳戶所有者才能執行此任務。
- 您必須擁有託管 LDAP 目錄伺服器的伺服器的 IP 位址。
- 在設定 LDAP 目錄連接器之前，必須先設定代理程式。

配置使用者目錄收集器的步驟

1. 在工作負載安全性選單中，按一下：收集器 **>** 使用者目錄收集器 **> +** 使用者目錄收集器，然後選擇*LDAP 目錄伺服器*

   系統顯示新增使用者目錄畫面。

透過在下表中輸入所需資料來設定使用者目錄收集器：

Name	描述
Name	使用者目錄的唯一名稱。例如 *GlobalLDAPCollector*
代理人	從清單中選擇一個已配置的代理
伺服器IP/域名	託管 LDAP 目錄伺服器的伺服器的 IP 位址或完全限定網域名稱 (FQDN)

搜尋基礎	LDAP 伺服器的搜尋基礎搜尋基礎允許以下兩種格式：*x.y.z* ⇒ 直接域名，就像您在 SVM 上擁有的那樣。 [範例：hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ 相對可分辨名稱 [範例：DC=hq,DC=companyname,DC=com] 或您可以指定如下：*OU=engineering,DC=hq,DC=companyname=DC=com* [按特定 name eng DC=netapp, DC=com_ [從 OU <engineering> 取得具有 <username> 的特定使用者] *CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com,O= companyname,L=Boston,S=MA,C=US* [取得該組織內使用者的所有 Acroanyname,L=Boston,S=MA,C=US_ [取得該組織內使用者的所有 Acroanyname, Bcroston,S=MA,C=US_ [取得該組織內使用者的所有 Acroanyname, Bcroston,S=MA,C=US_ [取得該組織內使用者的所有 Acroanyname, 4croston,S=MAs]
綁定 DN	允許使用者搜尋目錄。例如：uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com 給使用者 john@dorp.company.com。dorp.company.com
--帳戶	--用戶
--約翰	--安娜
綁定密碼	目錄伺服器密碼（即綁定 DN 中使用的使用者名稱的密碼）
協定	ldap、ldaps、ldap-start-tls
連接埠	選擇連接埠

如果 LDAP 目錄伺服器中的預設屬性名稱已被修改，請輸入下列目錄伺服器所需的屬性。大多數情況下，這些屬性名稱在 LDAP 目錄伺服器中不會被修改，在這種情況下，您可以簡單地使用預設屬性名稱。

屬性	目錄伺服器中的屬性名稱
顯示名稱	姓名
UNIXID	uid 號
使用者名稱	uid

按一下「包括可選屬性」以新增下列任意屬性：

屬性	目錄伺服器中的屬性名稱
電子郵件	郵件
電話號碼	電話號碼
角色	標題
國家	公司

狀態	狀態
部門	部門編號
照片	照片
經理DN	主管
團體	成員

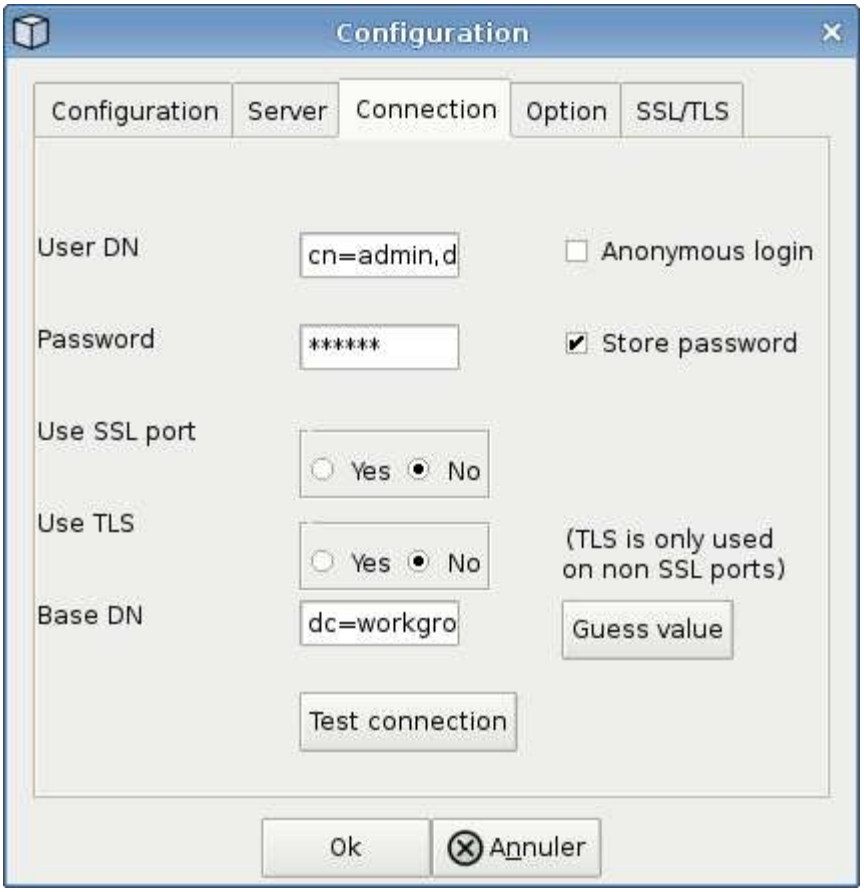
測試您的使用者目錄收集器配置

您可以使用下列步驟驗證 LDAP 使用者權限和屬性定義：

- 使用下列指令驗證 Workload Security LDAP 使用者權限：

```
 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
* 使用 LDAP Explorer 瀏覽 LDAP
資料庫、檢視物件屬性和特性、檢視權限、檢視物件的模式、執行可以儲存和重新執行的複雜搜尋
。
```

  - 安裝 LDAP Explorer(http://ldaptool.sourceforge.net/ ）或 Java LDAP 資源管理器(http://jxplorer.org/) 在任何可以連接到 LDAP 伺服器的 Windows 機器上。
  - 使用 LDAP 目錄伺服器的使用者名稱/密碼連線到 LDAP 伺服器。



排除 **LDAP** 目錄收集器設定錯誤

下表描述了收集器配置期間可能出現的已知問題和解決方法：

問題：	解決：
新增 LDAP 目錄連接器會導致「錯誤」狀態。錯誤提示「為 LDAP 伺服器提供的憑證無效」。	提供的綁定 DN、綁定密碼或搜尋基礎不正確。編輯並提供正確的資訊。
新增 LDAP 目錄連接器會導致「錯誤」狀態。錯誤提示：“無法取得與作為林名稱提供的 DN=DC=hq,DC=domainname,DC=com 對應的物件。”	提供的搜尋基礎不正確。編輯並提供正確的森林名稱。
網域使用者的選用屬性未出現在工作負載安全使用者設定檔頁面中。	這可能是由於 CloudSecure 中新增的可選屬性名稱與 Active Directory 中的實際屬性名稱不符所造成的。字段區分大小寫。編輯並提供正確的可選屬性名稱。
資料收集器處於錯誤狀態，顯示「無法檢索 LDAP 使用者。失敗原因：無法連接到伺服器，連接為空”	點選“重新啟動”按鈕重新啟動收集器。
新增 LDAP 目錄連接器會導致「錯誤」狀態。	確保您已為必填欄位（伺服器、林名稱、綁定 DN、綁定密碼）提供了有效值。確保綁定 DN 輸入始終為 uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com。
新增 LDAP 目錄連接器會導致「重試」狀態。顯示錯誤“無法確定收集器的健康狀況，因此請重試”	確保提供正確的伺服器 IP 和搜尋庫 ////

問題：	解決：
新增 LDAP 目錄時顯示下列錯誤：“無法在 2 次重試內確定收集器的健康狀況，請嘗試重新啟動收集器（錯誤代碼：AGENT008）”	確保提供正確的伺服器 IP 和搜尋庫
新增 LDAP 目錄連接器會導致「重試」狀態。顯示錯誤“無法定義收集器的狀態，原因 Tcp 命令 [Connect(localhost:35012,None,List(),Some(,seconds),true)] 因 java.net.ConnectionException:Connection 被拒絕而失敗。”	為 AD 伺服器提供的 IP 或 FQDN 不正確。編輯並提供正確的 IP 位址或 FQDN。 ////
新增 LDAP 目錄連接器會導致「錯誤」狀態。錯誤提示「無法建立 LDAP 連線」。	為 LDAP 伺服器提供的 IP 或 FQDN 不正確。編輯並提供正確的 IP 位址或 FQDN。或提供的連接埠值不正確。嘗試使用 LDAP 伺服器的預設連接埠值或正確的連接埠號碼。
新增 LDAP 目錄連接器會導致「錯誤」狀態。錯誤提示：「無法載入設定。原因：資料來源配置錯誤。具體原因：/connector/conf/application.conf: 70: ldap.ldap-port 的類型為 STRING 而非 NUMBER”	提供的連接埠值不正確。嘗試使用 AD 伺服器的預設連接埠值或正確的連接埠號碼。
我從強制屬性開始，並且它起作用了。新增可選項後，可選屬性資料不會從 AD 中取得。	這可能是由於 CloudSecure 中新增的可選屬性與 Active Directory 中的實際屬性名稱不符所造成的。編輯並提供正確的強製或可選屬性名稱。
重新啟動收集器後，LDAP 同步何時發生？	收集器重新啟動後，LDAP 同步將立即發生。取得約30萬用戶的用戶資料大約需要15分鐘，並且每12小時自動刷新一次。
使用者資料從 LDAP 同步到 CloudSecure。數據何時會被刪除？	如果沒有刷新，用戶資料將保留13個月。如果租戶被刪除，那麼資料也將被刪除。
LDAP 目錄連接器導致「錯誤」狀態。 「連接器處於錯誤狀態。服務名稱：usersLdap。失敗原因：無法檢索 LDAP 使用者。失敗原因：80090308：LdapErr：DSID-0C090453，註：AcceptSecurityContext 錯誤，資料 52e，v3839”	提供的森林名稱不正確。請參閱上文，了解如何提供正確的森林名稱。
用戶資料頁面中未填寫電話號碼。	這很可能是由於 Active Directory 的屬性對映問題所造成的。1.編輯從 Active Directory 取得使用者資訊的特定 Active Directory 收集器。2.請注意，在選用屬性下，有一個欄位名稱「電話號碼」會對應到 Active Directory 屬性「telephonenumber」。4.現在，請使用上面描述的 Active Directory Explorer 工具瀏覽 LDAP 目錄伺服器並查看正確的屬性名稱。3.確保 LDAP 目錄中有一個名為「telephonenumber」的屬性，其中確實包含使用者的電話號碼。5.假設在 LDAP 目錄中它已被修改為「電話號碼」。6.然後編輯 CloudSecure 使用者目錄收集器。在可選屬性部分，將“telephonenumber”替換為“phonenumber”。7.儲存 Active Directory 收集器，收集器將重新啟動並取得使用者的電話號碼，並將其顯示在使用者個人資料頁面中。

問題：	解決：
如果在 Active Directory (AD) 伺服器上啟用了加密憑證 (SSL)，則 Workload Security User Directory Collector 無法連線到 AD 伺服器。	在設定使用者目錄收集器之前停用 AD 伺服器加密。一旦獲取用戶詳細信息，它將保留 13 個月。如果 AD 伺服器在取得使用者詳細資訊後斷開連接，則不會取得 AD 中新新增的使用者。若要再次取得使用者目錄收集器，需要連接到 AD。

配置**ONTAP SVM** 資料收集器

ONTAP SVM 資料收集器使工作負載安全能夠監控NetApp ONTAP儲存虛擬機器 (SVM) 上的檔案和使用者存取活動。本指南將引導您完成 SVM 資料收集器的設定和管理，以便為您的ONTAP環境提供全面的安全監控。

開始之前

- 此數據收集器支援以下功能：
  - Data ONTAP 9.2 及更高版本。為了獲得最佳效能，請使用高於 9.13.1 的Data ONTAP版本。
  - SMB 協定版本 3.1 及更早版本。
  - NFS 版本最高可達 NFS 4.1（請注意， ONTAP 9.15 或更高版本支援 NFS 4.1）。
  - ONTAP 9.4 及更高版本支援 Flexgroup
  - ONTAP 9.7 及更高版本的 NFS 支援FlexCache 。
  - ONTAP 9.14.1 及更高版本的 SMB 支援FlexCache 。
  - 支援ONTAP Select
- 僅支援資料類型 SVM。不支援具有無限磁碟區的 SVM。
- SVM 有幾種子類型。其中，僅支援_default_、*sync_source*_和_*sync_destination*。
- 一名特務"必須配置"然後才可以配置資料收集器。
- 確保您具有正確配置的使用者目錄連接器，否則事件將在「活動取證」頁面中顯示編碼的使用者名稱而不是使用者的實際名稱（儲存在 Active Directory 中）。
- ONTAP持久性儲存從 9.14.1 版本開始支援。
- 為了獲得最佳效能，您應該將 FPolicy 伺服器配置為與儲存系統位於相同子網路。
- 有關工作負載安全性原則配置的全面最佳實務和建議，請參閱"知識庫文章：FPolicy最佳實踐"。
- 您必須使用以下兩種方法之一新增 SVM：
  - 透過使用叢集 IP、SVM 名稱以及叢集管理使用者名稱和密碼。 _這是推薦的方法。 _
    - SVM 名稱必須與ONTAP中顯示的完全一致，並且區分大小寫。
  - 使用 SVM Vserver 管理 IP、使用者名稱和密碼
  - 如果您無法或不願意使用完整的管理員叢集/SVM 管理使用者名稱和密碼，您可以建立一個具有較低權限的自訂用戶，如“關於權限的說明”下面的部分。可以為 SVM 或叢集存取權建立此自訂使用者。
    - 您也可以使用具有至少 csrole 權限的角色的 AD 用戶，如下面的「關於權限的說明」部分所述。另請參閱"ONTAP 文件"。

- 透過執行以下命令確保為 SVM 設定了正確的應用程式：

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

範例輸出

```
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.
```

- 確保 SVM 已配置 CIFS 伺服器：clustershell:> `vserver cifs show`

  系統傳回 Vserver 名稱、CIFS 伺服器名稱和其他欄位。

- 為 SVM vsadmin 使用者設定密碼。如果使用自訂用戶或叢集管理員用戶，請跳過此步驟。 clustershell:> `security login password -username vsadmin -vserver svmname`
- 解鎖 SVM vsadmin 使用者以進行外部存取。如果使用自訂用戶或叢集管理員用戶，請跳過此步驟。 clustershell:> `security login unlock -username vsadmin -vserver svmname`
- 確保資料 LIF 的防火牆策略設定為“mgmt”（而不是“資料”）。如果使用專用管理生命週期來新增 SVM，請跳過此步驟。 clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall -policy mgmt`
- 啟用防火牆後，您必須定義例外值以允許使用Data ONTAP資料收集器的連接埠的 TCP 流量。

  看"代理要求"取得配置資訊。這適用於本地代理和安裝在雲端的代理。

- 當在 AWS EC2 執行個體中安裝代理程式以監控 Cloud ONTAP SVM 時，代理程式和儲存必須位於同一個 VPC 中。如果它們位於不同的 VPC 中，則 VPC 之間必須有有效的路由。

測試資料收集器的連通性

測試連線功能（於 2025 年 3 月推出）旨在協助最終用戶在Data Infrastructure Insights(DII) 工作負載安全性中設定資料收集器時識別故障的具體原因。這使得用戶能夠自行修正與網路通訊或缺失角色相關的問題。

此功能將幫助用戶在設定資料收集器之前確定所有與網路相關的檢查是否已到位。此外，它還會根據ONTAP版本、角色以及在ONTAP中分配給他們的權限，告知使用者可以存取的功能。

使用者目錄收集器不支援測試連接

連接測試的先決條件

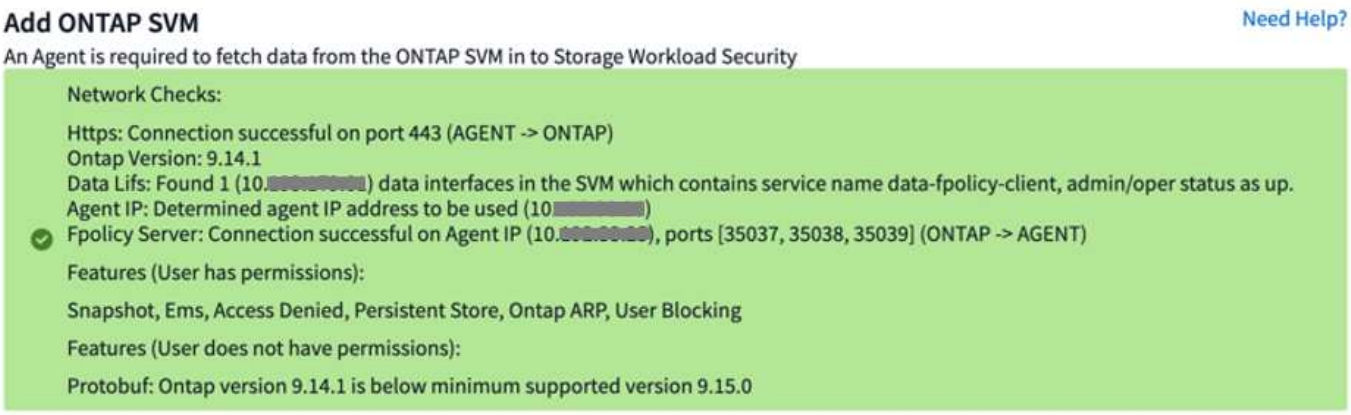
- 此功能要完全發揮作用，需要集群級憑證。

- SVM 模式不支援功能存取檢查。
- 如果您使用叢集管理憑證，則不需要新的權限。
- 如果您使用自訂使用者（例如，*csuser*），請為您想要使用的功能提供強制權限和特定功能權限。

請務必查看權限下面的部分也是如此。

測試連接

使用者可以前往新增/編輯收集器頁面，輸入叢集層級詳細資料（在叢集模式下）或 SVM 層級詳細資料（在 SVM 模式下），然後按一下 測試連線 按鈕。然後，工作負載安全性將處理該請求並顯示適當的成功或失敗訊息。



ONTAP 多重管理員驗證 **(MAV)** 注意事項

某些功能（例如建立和刪除快照或使用者封鎖（SMB））可能無法運作，這取決於您的 ONTAP 版本中新增的 MAV 命令。

請依照下列步驟為 MAV 指令新增排除項，以便 Workload Security 能夠建立或刪除快照並封鎖使用者。

允許建立和刪除快照的命令：

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

允許使用者封鎖的命令：

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

使用者存取阻止的先決條件

請記住以下幾點"使用者存取阻止"：

此功能需要集群級憑證才能運作。

如果您使用叢集管理憑證，則不需要新的權限。

如果您使用自訂使用者（例如 *csuser*）並賦予該使用者權限，請依照"使用者存取阻止"授予 Workload Security 阻止使用者的權限。

關於權限的說明

透過*群集管理 **IP***新增時的權限：

如果您無法使用叢集管理員用戶允許工作負載安全地存取ONTAP SVM 資料收集器，則可以建立名為「csuser」的新用戶，並使用以下命令所示的角色。設定工作負載安全資料收集器以使用叢集管理 IP 時，請使用使用者名稱「csuser」和密碼「csuser」。

注意：您可以建立一個角色來用於自訂使用者的所有功能權限。如果存在現有用戶，則首先使用以下命令刪除現有用戶和角色：

```
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 *
```

若要建立新用戶，請使用叢集管理管理員使用者名稱/密碼登入ONTAP ，然後在ONTAP伺服器上執行下列命令：

```
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
```

透過 **Vserver** 管理 **IP** 新增時的權限：

如果您無法使用叢集管理員用戶允許工作負載安全地存取ONTAP SVM 資料收集器，則可以建立名為「csuser」的新用戶，並使用以下命令所示的角色。設定工作負載安全資料收集器以使用 Vserver 管理 IP 時，請使用使用者名稱「csuser」和密碼「csuser」。

注意：您可以建立一個角色來用於自訂使用者的所有功能權限。如果存在現有用戶，則首先使用以下命令刪除現有用戶和角色：

```
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>
```

若要建立新用戶，請使用叢集管理管理員使用者名稱/密碼登入ONTAP ，然後在ONTAP伺服器上執行下列命令。為方便起見，請將這些命令複製到文字編輯器，然後將 <vservername> 替換為您的 Vserver 名稱，然後在ONTAP上執行這些命令：

```
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>
```

Protobuf模式

當在收集器的「進階配置」設定中啟用此選項時，工作負載安全性將在 protobuf 模式下配置 FPolicy 引擎。ONTAP 9.15 及更高版本支援 Protobuf 模式。

關於此功能的更多詳細信息，請參閱"ONTAP 文件"。

protobuf 需要特定的權限（其中一些或全部可能已經存在）：

集群模式：

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

虛擬伺服器模式：

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

ONTAP自主勒索軟體防護和**ONTAP**存取的權限被拒絕

如果您使用叢集管理憑證，則不需要新的權限。

如果您使用具有指定權限的自訂使用者（例如 *csuser*），請依照下列步驟授予 Workload Security 從ONTAP收集 ARP 相關資訊的權限。

欲了解更多信息，請閱讀"與ONTAP整合存取被拒絕"

和"與ONTAP自主勒索軟體防護集成"

配置資料收集器

設定步驟

1. 以管理員或帳戶擁有者的身分登入您的Data Infrastructure Insights環境。
2. 按一下“工作負載安全性**>**收集器**>+**資料收集器”

   系統顯示可用的資料收集器。

3. 將滑鼠懸停在 * NetApp SVM 圖塊上，然後按一下 **+Monitor**。

   系統顯示ONTAP SVM 設定頁面。為每個欄位輸入所需的資料。

場地	描述
Name	資料收集器的唯一名稱
代理人	從清單中選擇一個已配置的代理程式。
透過管理 IP 連線：	選擇叢集 IP 或 SVM 管理 IP
叢集/SVM 管理 IP 位址	叢集或 SVM 的 IP 位址，取決於您上面的選擇。
SVM 名稱	SVM 的名稱（透過 Cluster IP 連線時需要此欄位）
使用者名稱	用於存取 SVM/叢集的使用者名稱透過叢集 IP 新增時，選項為：1.集群管理員 2。 'csuser' 3. AD 使用者俱有與 csuser 類似的角色。透過 SVM IP 新增時，選項為：4. vsadmin 5. 'csuser' 6. AD 使用者名稱具有與 csuser 類似的角色。
密碼	上述使用者名稱的密碼
篩選股份/交易量	選擇是否在事件收集中包含或排除股票/交易量
輸入要排除/包含的完整共享名稱	以逗號分隔的共享列表，用於從事件收集中排除或包含（視情況而定）
輸入要排除/包含的完整磁碟區名稱	以逗號分隔的捲列表，用於從事件收集中排除或包含（視情況而定）
監控資料夾訪問	選取後，啟用資料夾存取監控事件。請注意，即使未選擇此選項，資料夾的建立/重新命名和刪除也會受到監控。啟用此功能將增加監控的事件數量。

設定ONTAP發送緩衝區大小	設定ONTAP Fpolicy 發送緩衝區大小。如果使用 9.8p7 之前的ONTAP版本並發現效能問題，則可以變更ONTAP發送緩衝區大小以提高ONTAP效能。如果您沒有看到此選項並希望探索它，請聯絡NetApp支援。

完成後

- 在已安裝的資料收集器頁面中，使用每個收集器右側的選項功能表來編輯資料收集器。您可以重新啟動資料收集器或編輯資料收集器配置屬性。

MetroCluster的推薦配置

以下是針對MetroCluster的建議：

1. 連接兩個資料收集器，一個連接到來源 SVM，另一個連接到目標 SVM。
2. 資料收集器應透過_集群 IP_ 連接。
3. 在任何時間點，目前「正在運行」的 SVM 的資料收集器將顯示為「正在運行」。目前「停止」的 SVM 資料收集器將顯示為「已停止」。
4. 每當發生切換時，資料收集器的狀態將從_Running_變為_Stopped，反之亦然。
5. 資料收集器從_停止_狀態轉變為_運行_狀態最多需要兩分鐘。

服務政策

如果使用ONTAP **9.9.1** 版或更新版本 的服務策略，為了連接到資料來源收集器，需要 *data-fpolicy-client* 服務以及資料服務 *data-nfs* 和/或 *data-cifs*。

範例：

```
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)
```

在ONTAP 9.9.1 之前的版本中，無需設定 *data-fpolicy-client* 。

播放-暫停數據收集器

如果資料收集器處於_運行_狀態，您可以暫停收集。打開收集器的“三個點”選單並選擇暫停。當收集器暫停時，不會從ONTAP收集任何數據，也不會從收集器向ONTAP發送任何數據。這意味著沒有 Fpolicy 事件會從ONTAP流向資料收集器，再從那裡流向Data Infrastructure Insights。

請注意，如果在收集器暫停時在ONTAP上建立任何新磁碟區等，則工作負載安全性將不會收集數據，並且這些磁碟區等將不會反映在儀表板或表格中。

如果收集器有限制用戶，則無法暫停收集器。在暫停收集器之前恢復使用者存取權限。

請記住以下幾點：

- 快照清除不會按照暫停收集器上配置的設定進行。
- EMS 事件（例如 ONTAP ARP）將不會在暫停的收集器上處理。這意味著如果 ONTAP 識別出檔案竄改攻擊，Data Infrastructure Insights Workload Security 將無法取得該事件。
- 對於已暫停的收集器，將不會發送健康通知電子郵件。
- 暫停的收集器不支援手動或自動操作（例如快照或使用者封鎖）。
- 當代理程式或收集器升級、代理 VM 重新啟動/重新啟動或代理服務重新啟動時，暫停的收集器將保持_暫停_狀態。
- 如果資料收集器處於_Error_狀態，則收集器無法變更為_Paused_狀態。只有當收集器的狀態為「正在運作」時，「暫停」按鈕才會啟用。
- 如果代理程式斷開連接，則收集器無法變更為_Paused_狀態。收集器將進入_停止_狀態並且暫停按鈕將被停用。

持久性儲存

ONTAP 9.14.1 及更高版本支援持久性儲存。請注意，磁碟區名稱說明從ONTAP 9.14 到 9.15 有所不同。

可以透過選取收集器編輯/新增頁面中的複選框來啟用持久性儲存。勾選方塊後，將顯示一個用於接受磁碟區名稱的文字欄位。磁碟區名稱是啟用持久性儲存的必填欄位。

- 對於ONTAP 9.14.1，您必須在啟用該功能之前建立卷，並在「卷宗名稱」欄位中提供相同的名稱。建議的磁碟區大小為 16GB。
- 對於ONTAP 9.15.1，收集器將使用「磁碟區名稱」欄位中提供的名稱自動建立大小為 16 GB 的磁碟區。

持久性儲存需要特定權限（其中一些或全部可能已經存在）：

集群模式：

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

虛擬伺服器模式：

```
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
```

遷移收集器

您可以輕鬆地將工作負載安全收集器從一個代理遷移到另一個代理，從而實現跨代理的收集器的有效負載平衡。

先決條件

- 來源代理必須處於_連線_狀態。
- 要遷移的收集器必須處於_running_狀態。

筆記：

- 資料和使用者目錄收集器均支援遷移。
- 不支援手動管理的租戶遷移收集器。

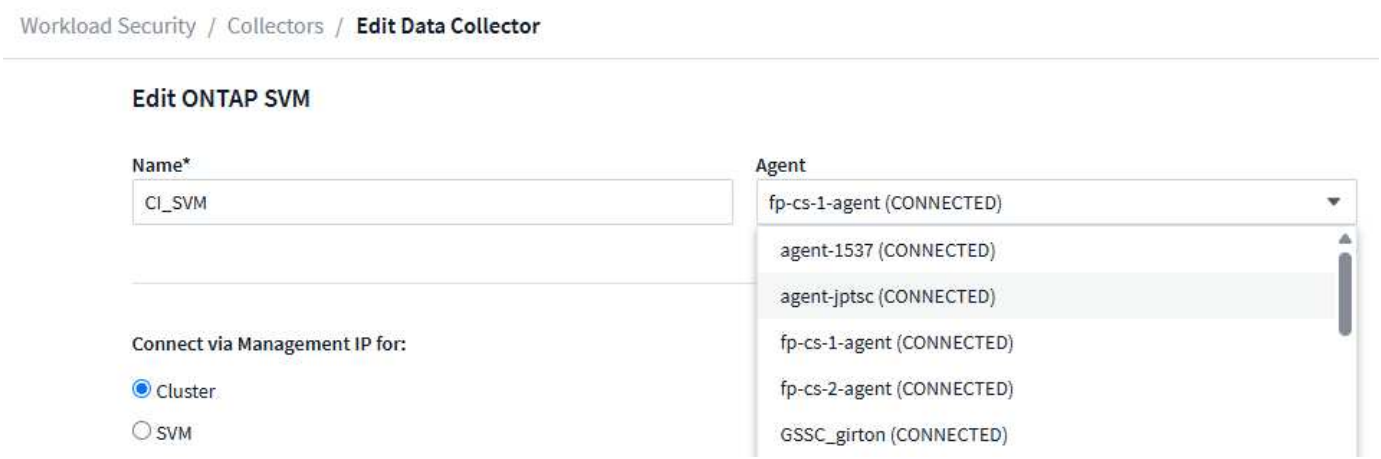
遷移收集器

若要遷移收集器，請依照下列步驟操作：

1. 前往“編輯收藏家”頁面。
2. 從代理下拉選單中選擇目標代理。
3. 點選「儲存收集器」按鈕。

工作負載安全性將處理該請求。遷移成功後，使用者將被重定向到收藏家清單頁面。如果失敗，編輯頁面上將顯示相應的訊息。

注意：當收集器成功移轉到目標代理程式時，「編輯收集器」頁面上先前所做的任何設定變更都會保留應用程式。



故障排除

查看"SVM 收集器故障排除"頁面以取得故障排除提示。

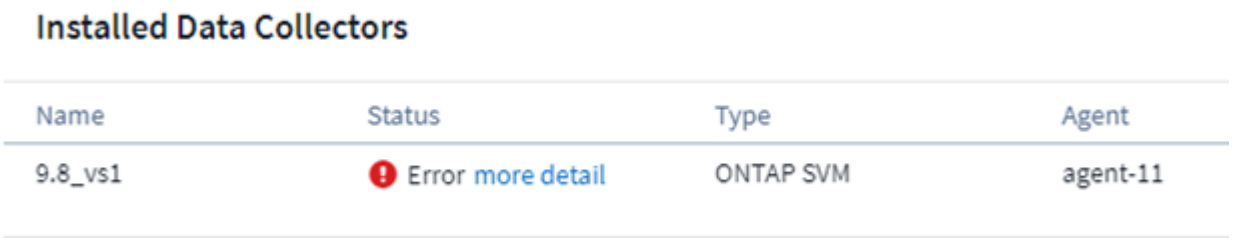
ONTAP SVM 資料收集器故障排除

工作負載安全使用資料收集器從設備收集文件和使用者存取資料。您可以在這裡找到解決此收集器問題的提示。

查看"配置 SVM 收集器"頁面以取得有關配置此收集器的說明。

如果發生錯誤，您可以按一下「已安裝的資料收集器」頁面的「狀態」列中的「詳細資訊」以了解有關錯誤的詳

細資訊。



已知問題及其解決方案如下所述。

問題：*資料收集器運作一段時間後在隨機時間後停止，並發生故障：「錯誤訊息：連接器處於錯誤狀態。服務名稱：審計。失敗原因：外部 **fpolicy** 伺服器超載。 」*試試看： ONTAP的事件率遠高於代理盒可以處理的事件率。因此連線被終止。

檢查斷開連接時 CloudSecure 中的峰值流量。您可以從 **CloudSecure > Activity Forensics > All Activity** 頁面進行檢查。

如果峰值聚合流量高於代理箱可以處理的流量，請參閱事件速率檢查器頁面，以了解如何確定代理箱中收集器的部署規模。

如果代理程式是在 2021 年 3 月 4 日之前安裝在代理框中的，請在代理框中執行以下命令：

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

調整大小後從 UI 重新啟動收集器。

{空的}

*問題：*收集器報告錯誤訊息：「在連接器上找不到可以到達 SVM 資料介面的本機 IP 位址」。 *試試看：*這很可能是由於ONTAP端的網路問題造成的。請依照以下步驟操作：

1. 確保 SVM 資料生命週期或管理生命週期上沒有防火牆阻止來自 SVM 的連線。
2. 透過叢集管理 IP 新增 SVM 時，請確保 SVM 的資料 lif 和管理 lif 可以從代理 VM ping 通。如果出現問題，請檢查網關、網路遮罩和路由。

   您也可以嘗試使用集群管理 IP 透過 ssh 登入集群，並 ping 代理 IP。確保代理 IP 可 ping 通：

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

   如果無法 ping 通，請確保ONTAP中的網路設定正確，以便 Agent 機器可以 ping 通。

3. 如果您嘗試透過 Cluster IP 連線但不成功，請嘗試直接透過 SVM IP 連線。請參閱上文以了解透過 SVM IP 連線的步驟。
4. 透過 SVM IP 和 vsadmin 憑證新增收集器時，檢查 SVM Lif 是否啟用了資料加管理角色。在這種情況下，ping 到 SVM Lif 將會起作用，但是 SSH 到 SVM Lif 將不起作用。如果是，請建立 SVM Mgmt Only Lif 並嘗試透過此 SVM 管理專用 Lif 進行連線。
5. 如果仍然不起作用，請建立新的 SVM Lif 並嘗試透過該 Lif 進行連線。確保子網路遮罩設定正確。
6. 進階調試：
   a. 在ONTAP中啟動資料包追蹤。
   b. 嘗試從 CloudSecure UI 將資料收集器連接到 SVM。
   c. 等待直到錯誤出現。在ONTAP中停止資料包追蹤。
   d. 從ONTAP開啟資料包追蹤。可在此位置取得

```
https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
. . 確保從ONTAP到代理框有一個 SYN。
. . 如果沒有來自ONTAP的 SYN，那麼這是ONTAP中的防火牆有問題。
. . 在ONTAP中開啟防火牆，以便ONTAP能夠連接代理盒。
```

7. 如果仍然不起作用，請諮詢網路團隊，以確保沒有外部防火牆阻止從ONTAP到代理盒的連線。
8. 如果以上方法都無法解決問題，請提交案例"Netapp 支持"以獲得進一步的幫助。

{空的}

問題：*訊息：「無法確定 **[**主機名稱：**<IP** 位址**>]** 的**ONTAP**類型。原因：與儲存系統 **<IP** 位址**>** 的連線錯誤：主機無法存取（主機無法存取）」*嘗試此操作：

1. 驗證是否提供了正確的 SVM IP 管理位址或叢集管理 IP。
2. 透過 SSH 連接到您要連接的 SVM 或叢集。連接後，請確保 SVM 或叢集名稱正確。

{空的}

問題：*錯誤訊息：「連接器處於錯誤狀態。服務名稱：審計。失敗原因：外部 **fpolicy** 伺服器終止。」 *試試這個：

1. 最有可能的是防火牆阻止了代理機器中的必要連接埠。驗證連接埠範圍 35000-55000/tcp 是否已打開，以便代理電腦從 SVM 進行連線。也要確保ONTAP端沒有啟用防火牆來阻止與代理機器的通訊。
2. 在代理框中輸入以下命令並確保連接埠範圍是開放的。

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

   範例輸出應如下圖所示：

```
 -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
NEW -j ACCEPT
```
. 登入 SVM，輸入以下命令並檢查是否沒有設定防火牆來阻止與ONTAP 的通訊。

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

"檢查防火牆命令"在ONTAP方面。

3. 透過 SSH 連接到您要監控的 SVM/叢集。從 SVM 資料生命週期 (支援 CIFS、NFS 協定) 對代理程式盒執行 ping 操作，並確保 ping 操作正常：

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

如果無法 ping 通，請確保ONTAP中的網路設定正確，以便 Agent 機器可以 ping 通。

4. 如果透過 2 個資料收集器將單一 SVM 兩次新增至租用戶，則會顯示此錯誤。透過 UI 刪除其中一個資料收集器。然後透過 UI 重新啟動其他資料收集器。然後資料收集器將顯示“RUNNING”狀態並開始從 SVM 接收事件。

基本上，在一個租用戶中，應該只透過 1 個資料收集器添加 1 個 SVM 一次。 1 個 SVM 不應透過 2 個資料收集器添加兩次。

5. 如果在兩個不同的工作負載安全環境（租用戶）中新增了相同的 SVM，則最後一個 SVM 總是會成功。第二個收集器將使用自己的 IP 位址配置 fpolicy，並踢出第一個收集器。因此第一個收集器將停止接收事件，並且其「稽核」服務將進入錯誤狀態。為防止這種情況，請在單一環境上配置每個 SVM。
6. 如果服務策略配置不正確，也可能會出現此錯誤。使用ONTAP 9.8 或更高版本時，為了連接到資料來源收集器，需要 data-fpolicy-client 服務以及資料服務 data-nfs 和/或 data-cifs 。此外，data-fpolicy-client 服務必須與受監控 SVM 的資料生命週期相關聯。

{空的}

問題：*活動頁面中未顯示任何事件。 *試試這個：

1. 檢查ONTAP收集器是否處於「正在運作」狀態。如果是，則透過開啟一些檔案確保在 cifs 用戶端虛擬機器上產生一些 cifs 事件。
2. 如果沒有看到任何活動，請登入 SVM 並輸入以下命令。

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

請確保沒有與 fpolicy 相關的錯誤。

---

3. 如果沒有看到任何活動，請登入 SVM。輸入以下命令：

```
<SVM>fpolicy show
```

檢查以「cloudsecure_」為前綴的 fpolicy 政策是否已設定且狀態為「on」。如果未設置，那麼代理程式很可能無法執行 SVM 中的命令。請確保已遵循頁面開頭所述的所有先決條件。

{空的}

問題： SVM 資料收集器處於錯誤狀態，錯誤訊息為「代理無法連線到收集器」 嘗試下列操作：

1. 最有可能的是代理超載並且無法連接到資料來源收集器。
2. 檢查有多少個資料來源收集器連接到代理程式。
3. 也可以檢查 UI 中「所有活動」頁面的資料流量。
4. 如果每秒的活動數量非常高，請安裝另一個代理並將一些資料來源收集器移至新的代理程式。

{空的}

問題： SVM 資料收集器顯示錯誤訊息為「fpolicy.server.connectError：節點無法與 FPolicy 伺服器「12.195.15.146」建立連線（原因：「選擇逾時」）」 嘗試此操作： SVM/Cluster 中啟用了防火牆。因此 fpolicy 引擎無法連接到 fpolicy 伺服器。 ONTAP中可用於取得更多資訊的 CLI 包括：

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

"檢查防火牆命令"在ONTAP方面。

{空的}

*問題：*錯誤訊息：「連接器處於錯誤狀態。服務名稱：審計。失敗原因：在 SVM 上找不到有效的資料介面（角色：資料、資料協定：NFS 或 CIFS 或兩者、狀態：啟動）。 *試試看：*確保有一個操作介面（具有資料角色和 CIFS/NFS 資料協定）。

{空的}

---

*問題：*資料收集器進入錯誤狀態，一段時間後進入運作狀態，然後再次傳回錯誤狀態。如此循環往復。 *試試看：*這通常發生在以下場景：

1. 新增了多個數據收集器。

2. 表現出這種行為的資料收集器將會有 1 個 SVM 加入這些資料收集器。意思是 2 個或更多資料收集器連接到 1 個 SVM。
3. 確保 1 個資料收集器僅連接到 1 個 SVM。
4. 刪除連接到相同 SVM 的其他資料收集器。

{空的}

問題：*連接器處於錯誤狀態。服務名稱：審計。失敗原因：無法設定（**SVM svmname** 上的策略）。原因：在「**fpolicy.policy.scope-modify: “Federal”**中為**“shares-to-include”**元素指定的值無效*嘗試此操作： *共享名稱需要不帶任何引號。編輯ONTAP SVM DSC 配置以更正共享名稱。

_包括和排除共享_不適用於較長的共享名稱清單。如果您需要包含或排除大量股票，請使用按數量過濾。

{空的}

---

*問題：*集群中存在未使用的現有 fpolicies。在安裝 Workload Security 之前該做什麼？ *試試看：*建議刪除所有現有的未使用的 fpolicy 設置，即使它們處於斷開連接狀態。工作負載安全性將建立帶有前綴“cloudsecure_”的 fpolicy。所有其他未使用的 fpolicy 配置都可以刪除。

顯示 fpolicy 清單的 CLI 指令：

```
 fpolicy show
```

刪除 `fpolicy` 配置的步驟：

```
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>
```

{空的}

---

*問題：*啟用工作負載安全後， ONTAP效能受到影響：延遲偶爾會升高，IOPS 偶爾會降低。 *試試看這個：*在使用ONTAP和工作負載安全時，有時會在ONTAP中看到延遲問題。造成這種情況可能有以下幾個原因："1372994" ， "1415152" ， "1438207" ， "1479704" ， "1354659" 。所有這些問題均已在ONTAP 9.13.1 及更高版本中修復；強烈建議使用其中一個更高版本。

{空的}

問題：*資料收集器顯示錯誤訊息：「錯誤：兩次重試後無法確定收集器的健康狀況，請嘗試重新啟動收集器（錯誤代碼：**AGENT008**）」。 *試試這個：

1. 在資料收集器頁面上，捲動到出現錯誤的資料收集器的右側，然後按一下 3 個點選單。選擇“編輯”。再次輸入資料擷取器的密碼。按下「儲存」按鈕儲存資料收集器。數據收集器將重新啟動並且錯誤應該解決。
2. 代理機器可能沒有足夠的 CPU 或 RAM 空間，這就是 DSC 失敗的原因。請檢查機器中新增到代理程式的資料收集器的數量。如果超過20，請增加Agent機器的CPU和RAM容量。一旦 CPU 和 RAM 增加，DSC 將自動進入初始化狀態，然後進入運作狀態。查看尺寸指南"本頁"。

{空的}

---

*問題：*選擇 SVM 模式時資料收集器發生錯誤。 *試試看：*在 SVM 模式下連接時，如果使用叢集管理 IP 而不是 SVM 管理 IP 進行連接，則連接將會出錯。確保使用正確的 SVM IP。

{空的}

---

*問題：*啟用「拒絕存取」功能時，資料收集器顯示錯誤訊息：「連接器處於錯誤狀態。服務名稱：審計。失敗原因：無法在 SVM test_svm 上配置 fpolicy。原因：用戶未獲得授權。」 *試試看：*使用者可能缺少「拒絕存取」功能所需的 REST 權限。請按照"本頁"設定權限。

設定權限後重新啟動收集器。

{空的}

問題： 收集器處於錯誤狀態，訊息為：連接器處於錯誤狀態。 失敗原因：無法在 SVM <SVM 名稱> 上配置持久性儲存。 原因：無法在 SVM“<SVM Name>”中找到磁碟區“<volumeName>”的合適聚合。 原因：聚合「<aggregateName>」的效能資訊目前不可用。 請稍等幾分鐘，然後再次嘗試該命令。服務名稱：審計。失敗原因：無法在 SVM <SVM Name> 上設定持久性儲存區。原因：無法在 SVM "<SVM Name>" 中找到適合的集合體以用於磁碟區 "<volumeName>"。原因：目前無法取得集合體 "<aggregateName>" 的效能資訊。請稍候幾分鐘，然後再次嘗試該指令。

*試試這個方法：*等待幾分鐘，然後重新啟動收集器。

{空的}

如果您仍然遇到問題，請聯絡*幫助>支援*頁面中提到的支援連結。

設定Cloud Volumes ONTAP和Amazon FSx for NetApp ONTAP收集器

透過為Cloud Volumes ONTAP和Amazon FSx for NetApp ONTAP設定 Workload Security 資料收集器，監控整個雲端儲存基礎架構中的檔案和使用者存取。本指南提供了在 AWS 中部署代理並將其連接到雲端儲存實例的逐步說明。

Cloud Volumes ONTAP儲存配置

請參閱OnCommand Cloud Volumes ONTAP文檔，以配置單節點/HA AWS 執行個體來託管工作負載安全代理：https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

配置完成後，請按照以下步驟設定您的 SVM：https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

支援的平台

- Cloud Volumes ONTAP，在所有可用的雲端服務供應商處均受支援。例如：Amazon、Azure、Google Cloud。
- ONTAPAmazon FSx

代理機器配置

代理機器必須在雲端服務提供者的各自子網路中配置。在[代理要求]中閱讀有關網路存取的更多資訊。

以下是在 AWS 中安裝代理程式的步驟。可以在 Azure 或 Google Cloud 中依照適用於雲端服務供應商的等效步驟進行安裝。

在 AWS 中，使用下列步驟將機器配置為用作工作負載安全代理：

使用下列步驟將機器配置為工作負載安全代理程式：

步驟

1. 登入 AWS 控制台並導覽至 EC2-Instances 頁面並選擇_啟動執行個體_。
2. 選擇具有此頁面中提到的適當版本的 RHEL 或 CentOS AMI：https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. 選擇 Cloud ONTAP個體所在的 VPC 和子網路。
4. 選擇 *t2.xlarge*（4 vcpus 和 16 GB RAM）作為分配的資源。
    a. 建立 EC2 執行個體。
5. 使用 YUM 套件管理器安裝所需的 Linux 套件：
    a. 安裝 *wget* 和 *unzip* 本機 Linux 套件。

安裝工作負載安全代理

1. 以管理員或帳戶擁有者的身分登入您的Data Infrastructure Insights環境。
2. 導覽至工作負載安全*收集器*並點選*代理*標籤。
3. 點選 **+Agent** 並指定 RHEL 作為目標平台。
4. 複製代理安裝指令。
5. 將代理安裝指令貼到您登入的 RHEL EC2 執行個體中。這將安裝 Workload Security 代理，提供所有"代理先決條件"均已滿足。

有關詳細步驟，請參閱此連結： https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

故障排除

下表描述了已知問題及其解決方法。

問題	解決
資料收集器顯示「工作負載安全：無法確定 Amazon FxSN 資料收集器的ONTAP類型」錯誤。客戶無法將新的 Amazon FSxN 資料收集器新增至 Workload Security 中。從代理程式到連接埠 443 上的 FSxN 叢集的連線逾時。防火牆和 AWS 安全群組已啟用所需規則以允許通訊。代理程式已部署並且也位於同一個 AWS 帳戶中。同一代理用於連接和監控其餘的NetApp設備（並且所有設備都在運行）。	透過將 fsxadmin LIF 網路段新增至代理程式的安全規則來解決此問題。如果您不確定端口，請允許所有端口。

使用者管理

工作負載安全用戶帳戶透過Data Infrastructure Insights進行管理。

Data Infrastructure Insights提供四個使用者帳戶層級：帳戶擁有者、管理員、使用者和訪客。每個帳戶都分配有特定的權限等級。具有管理員權限的使用者帳戶可以建立或修改用戶，並為每個使用者指派以下工作負載安全角色之一：

角色	工作負載安全訪問
行政人員	可執行所有工作負載安全功能，包括警報、取證、資料收集器、自動回應策略和工作負載安全 API。管理員也可以邀請其他用戶，但只能分配工作負載安全角色。
使用者	可以查看和管理警報並查看取證。使用者角色可以更改警報狀態、新增註釋、手動拍攝快照以及限制使用者存取。
客人	可以查看警報和取證。來賓角色不能更改警報狀態、新增註解、手動拍攝快照或限制使用者存取。

步驟

1. 登入工作負載安全
2. 在選單中，按一下“管理”>“使用者管理”

   您將被轉發到資料基礎設施洞察的使用者管理頁面。

3. 為每個使用者選擇所需的角色。

新增使用者時，只需選擇所需的角色（通常是使用者或訪客）。

有關用戶帳戶和角色的更多信息，請參閱Data Infrastructure Insights"使用者角色"文件.

事件速率檢查器：代理程式大小調整指南

在部署資料收集器之前，請透過測量 SVM 產生的 NFS 和 SMB 事件速率來確定最佳 Agent 機器大小。Event Rate Checker 指令碼可協助您了解容量限制（每個 Agent 最多

50 個資料收集器），並確保您的 Agent 基礎架構能夠處理預期的事件量，以實現可靠的威脅偵測。

要求：

- 集群 IP
- 叢集管理員使用者名稱和密碼

執行此腳本時，不應為正在確定事件率的 SVM 執行ONTAP SVM 資料收集器。

步驟：

1. 請依照 CloudSecure 中的說明安裝代理程式。
2. 安裝代理程式後，以 sudo 使用者身分執行 *server_data_rate_checker.sh* 腳本：

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. 該腳本需要在 Linux 機器上安裝 _sshpass_。有兩種安裝方法：
```

   a. 運行以下命令：

```
 linux_prompt> yum install sshpass
.. 如果這不起作用，則從網路下載 _sshpass_ 到 Linux 機器並執行以下命令：
```

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

3. 出現提示時提供正確的值。請參閱下面的範例。
4. 該腳本大約需要 5 分鐘才能運行。
5. 運行完成後，腳本將從 SVM 列印事件率。您可以在控制台輸出中檢查每個 SVM 的事件率：

```
“Svm svm_rate is generating 100 events/sec”.
```

每個 Ontap SVM 資料收集器可以與單一 SVM 關聯，這表示每個資料收集器將能夠接收單一 SVM 產生的事件數量。

請記住以下幾點：

A) 使用此表格作為一般尺寸指南。您可以增加核心和/或記憶體的數量來增加支援的資料收集器的數量，最多可增加 50 個資料收集器：

代理機器配置	SVM 資料收集器的數量	代理機器可以處理的最大事件速率
4核，16GB	10名資料收集員	20K 事件/秒

4核，32GB	20名資料收集員	20K 事件/秒

B) 若要計算總事件數，請將該代理人的所有 SVM 產生的事件數相加。

C) 如果腳本不在高峰時段運行，或者高峰流量難以預測，則保持 30% 的事件率緩衝。

B+C應該小於A，否則Agent機器會監控失敗。

也就是說，單一代理機器上可以新增的資料採集器數量應遵循以下公式：

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
```

查看link:concept_cs_agent_requirements.html["代理要求"]頁面以了解其他先決條件和要求。

例子

假設我們有三個 SVMS，分別每秒產生 100、200 和 300 個事件。

我們應用公式：

```
 (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.
```

控制台輸出在代理機器的目前工作目錄中的檔案名稱 *fpolicy_stat_<SVM Name>.log* 中可用。

在以下情況下，腳本可能會給出錯誤的結果：

- 提供的憑證、IP 或 SVM 名稱不正確。
- 具有相同名稱、序號等的已存在 fpolicy 將會出現錯誤。
- 腳本在運行時突然停止。

範例腳本運行如下所示：

```
[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]#
```

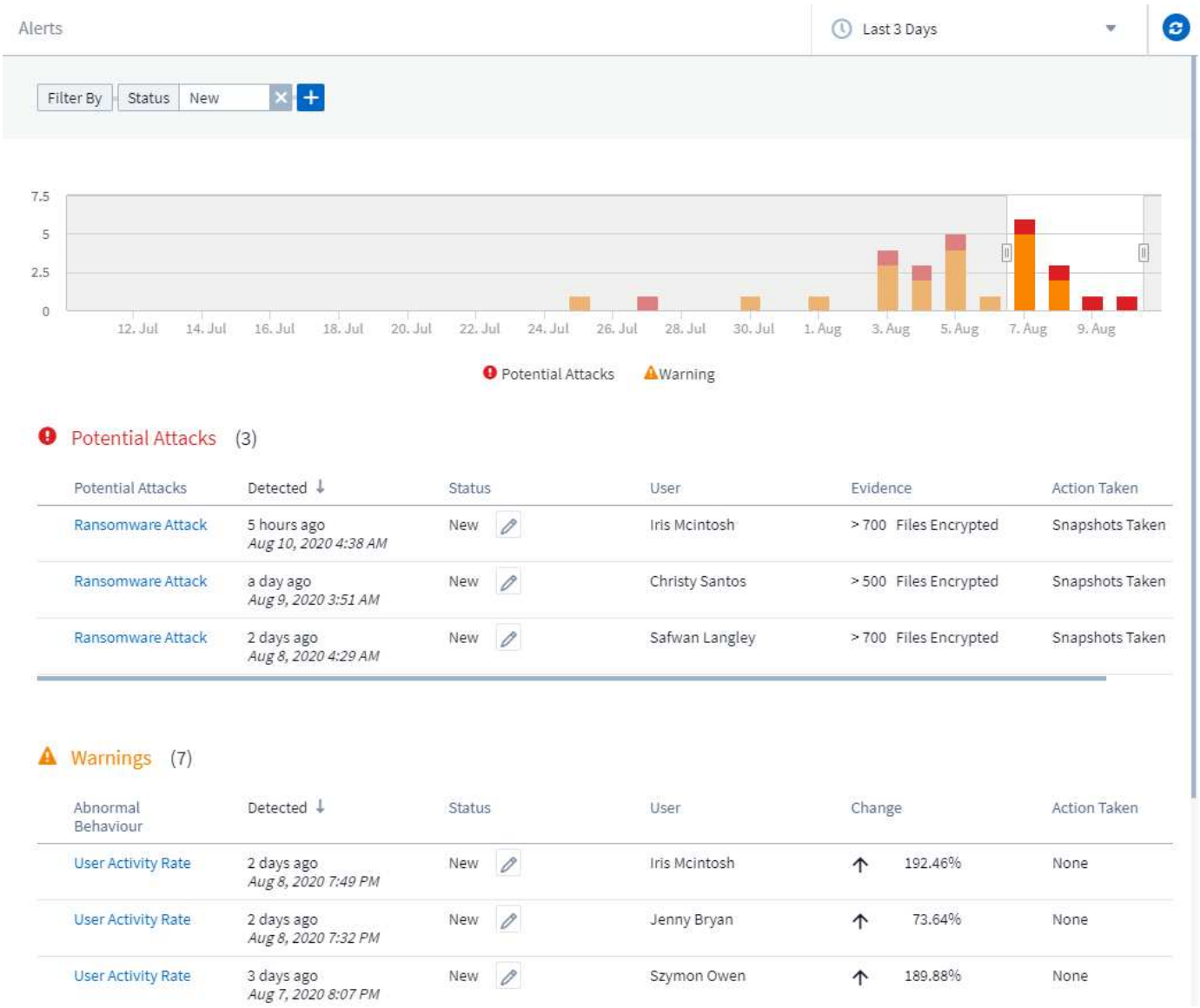
故障排除

問題	回答
如果我在已配置工作負載安全的 SVM 上執行此腳本，它是否僅使用 SVM 上現有的 fpolicy 配置，還是設定臨時配置並執行該過程？	即使對於已經配置了工作負載安全性的 SVM，事件率檢查器也可以正常運作。應該不會有影響。

我可以增加可運行該腳本的 SVM 數量嗎？	是的。只需編輯腳本並將 SVM 的最大數量從 5 更改為任何所需的數量。
如果我增加 SVM 的數量，會增加腳本的運行時間嗎？	不會。即使 SVM 的數量增加，該腳本最多也會運作 5 分鐘。
我可以增加可運行該腳本的 SVM 數量嗎？	是的。您需要編輯腳本並將 SVM 的最大數量從 5 更改為任何所需的數量。
如果我增加 SVM 的數量，會增加腳本的運行時間嗎？	不會。即使 SVM 的數量增加，該腳本最多也會運作 5 分鐘。
如果我使用現有代理程式運行事件率檢查器會發生什麼情況？	針對已存在的代理程式運行事件率檢查器可能會導致 SVM 上的延遲增加。當事件率檢查器運作時，這種增加將是暫時的。

了解和調查警示

工作負載安全警報頁面提供了已偵測到的威脅和警告的完整時間線，以及詳細的調查工具。查看警報詳情、管理狀態更新、按條件篩選、追蹤使用者活動，以便有效率地調查和應對安全事件。



警報

警報清單顯示一個圖表，顯示在選定時間範圍內發生的潛在攻擊和/或警告的總數，後面是該時間範圍內發生的攻擊和/或警告的清單。您可以透過調整圖表中的開始時間和結束時間滑桿來變更時間範圍。

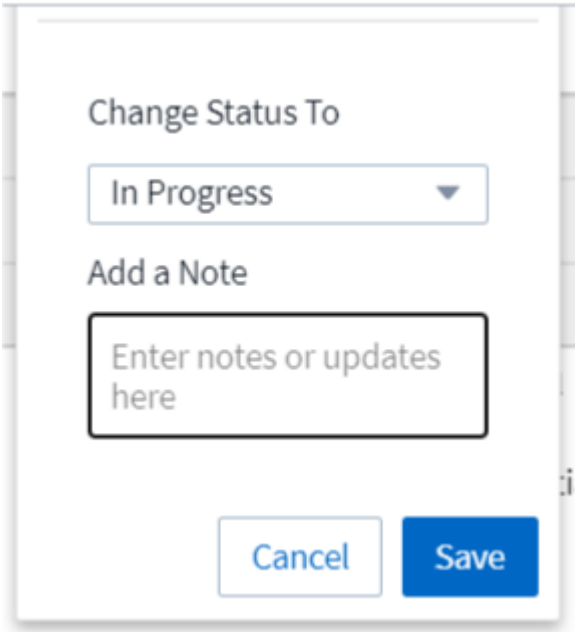
每個警報都會顯示以下內容：

潛在攻擊：

- 潛在攻擊類型（例如，文件篡改或破壞）
- 偵測到潛在攻擊的日期和時間
- 警報的_狀態_：
  - 新：這是新警報的預設設定。
  - 進行中：團隊成員正在調查該警報。
  - 已解決：警報已被團隊成員標記為已解決。

- 已解除：警報已因誤報或預期行為而解除。

  管理員可以更改警報的狀態並新增註釋以協助調查。



- 其行為觸發警報的_用戶_
- 攻擊的證據（例如，大量文件被加密）
- 採取的動作（例如，拍攝快照）

警告：

- 觸發警告的_異常行為_
- 偵測到該行為的日期和時間
- 警報的狀態（新、進行中等）
- 其行為觸發警報的_用戶_
- 對「變更」的描述（例如，檔案存取異常增加）
- 已採取的行動

篩選選項

您可以按以下方式過濾警報：

- 警報的_狀態_
- *Note* 中的具體文本
- _攻擊/警告_的類型
- 其操作觸發警報/警告的_用戶_

警報詳細資訊頁面

您可以點擊警報列表頁面上的警報鏈接，打開該警報的詳細資訊頁面。根據攻擊或警報的類型，警報詳情可能會有所不同。例如，文件竄改攻擊詳情頁面可能顯示以下資訊：

摘要部分：

- 攻擊類型（檔案篡改、破壞）和警報 ID（由工作負載安全分配）
- 偵測到攻擊的日期和時間
- 採取的行動（例如，拍攝了自動快照）。快照時間顯示在摘要部分正下方）
- 狀態（新、進行中等）

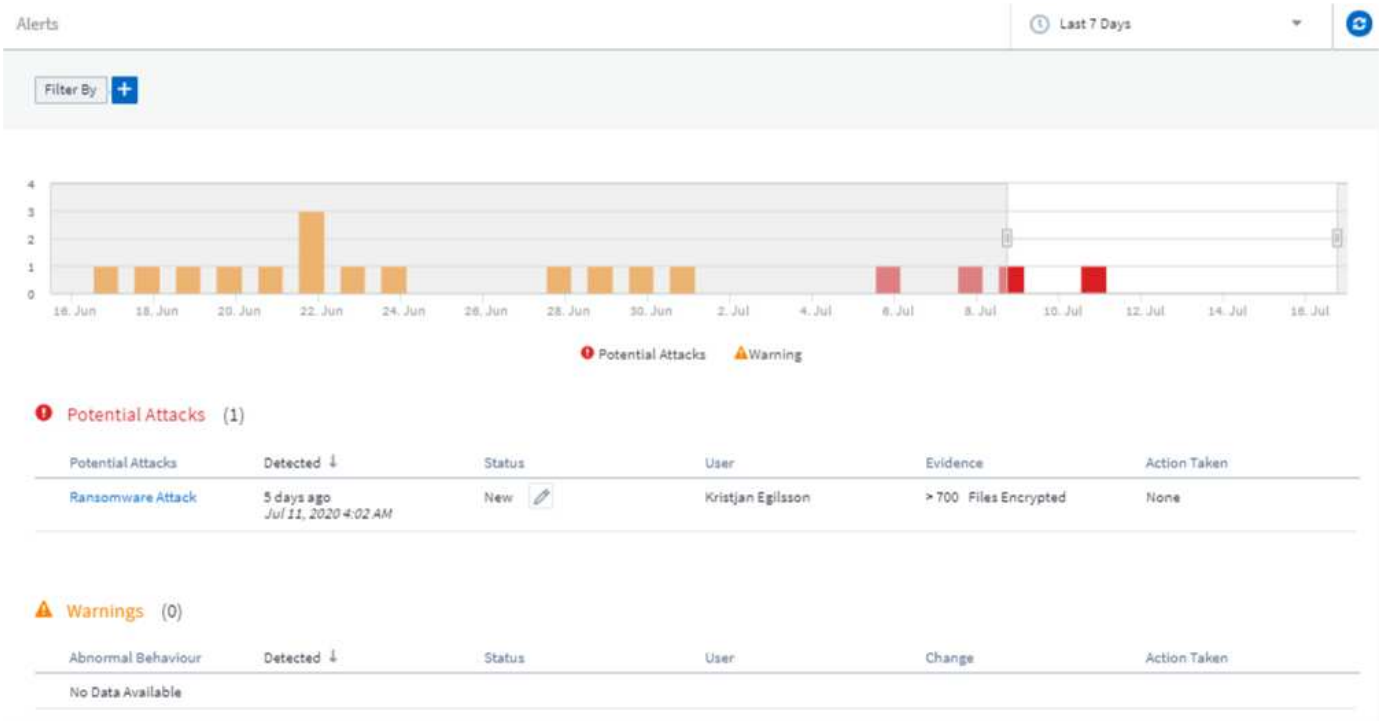
攻擊結果部分：

- 受影響捲和文件的數量
- 檢測結果摘要
- 顯示攻擊期間文件活動的圖表

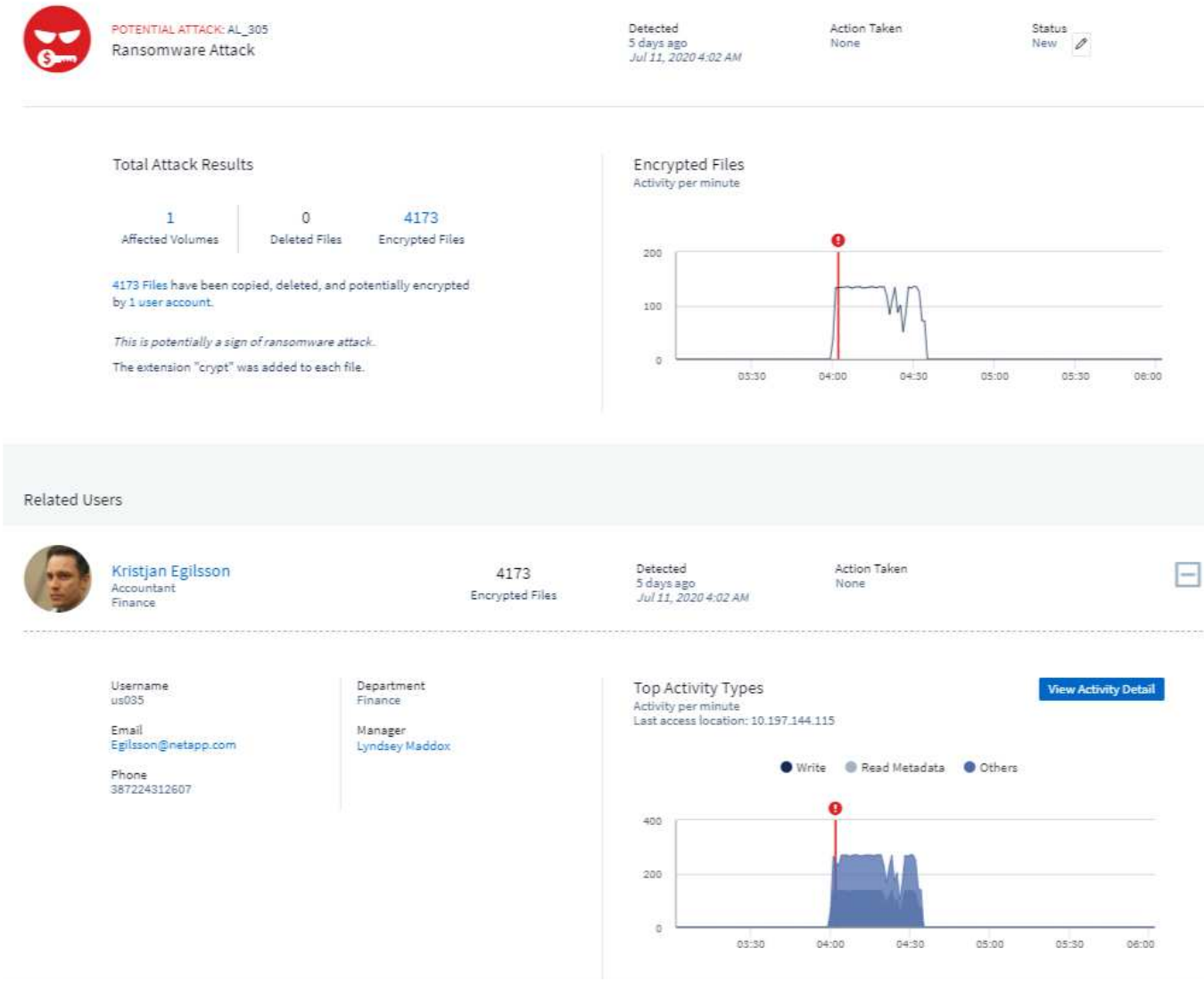
相關使用者部分：

此部分顯示有關參與潛在攻擊的用戶的詳細信息，包括用戶的熱門活動圖表。

警報頁面（此範例顯示了潛在的文件篡改攻擊）：



詳情頁面（此範例展示了潛在的文件篡改攻擊）：

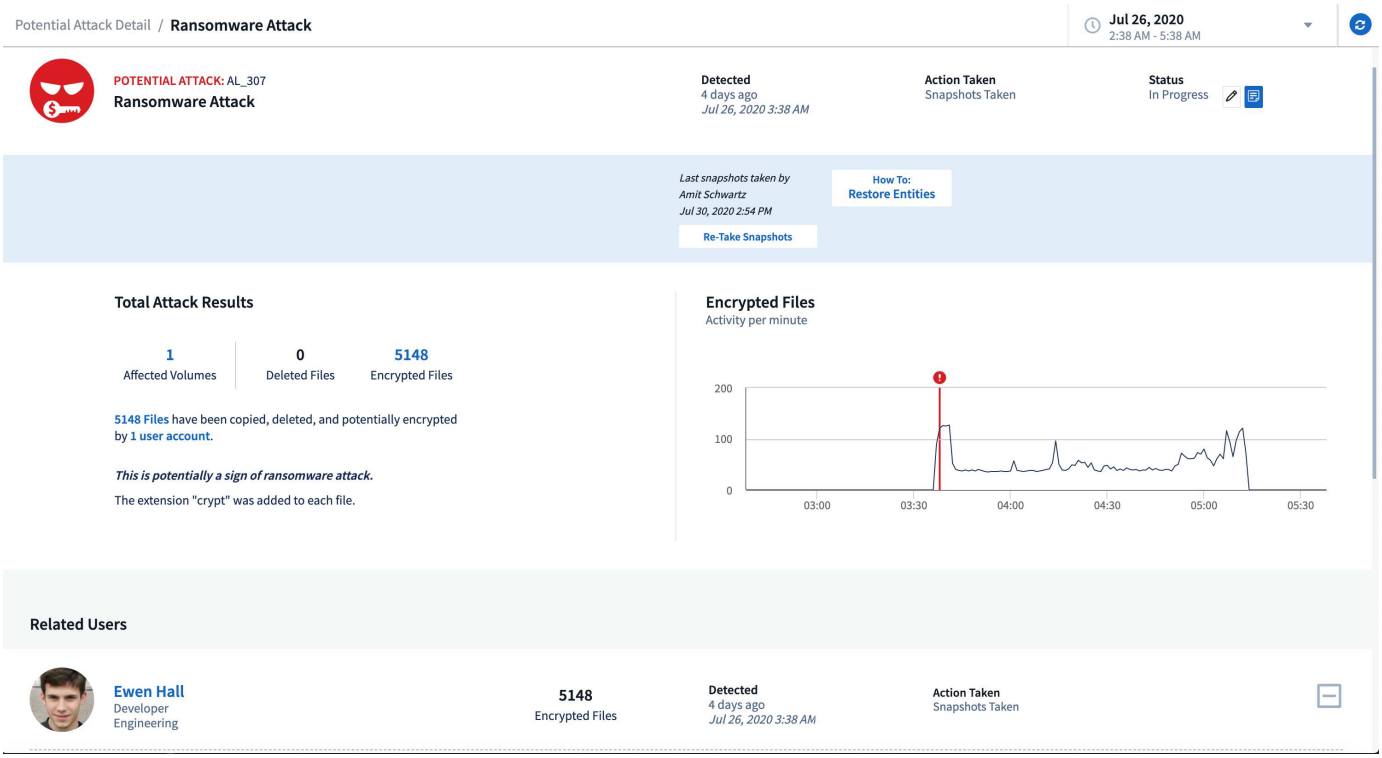


_拍攝快照_動作

工作負載安全性會在偵測到惡意活動時自動拍攝快照來保護您的數據，確保您的資料已安全備份。

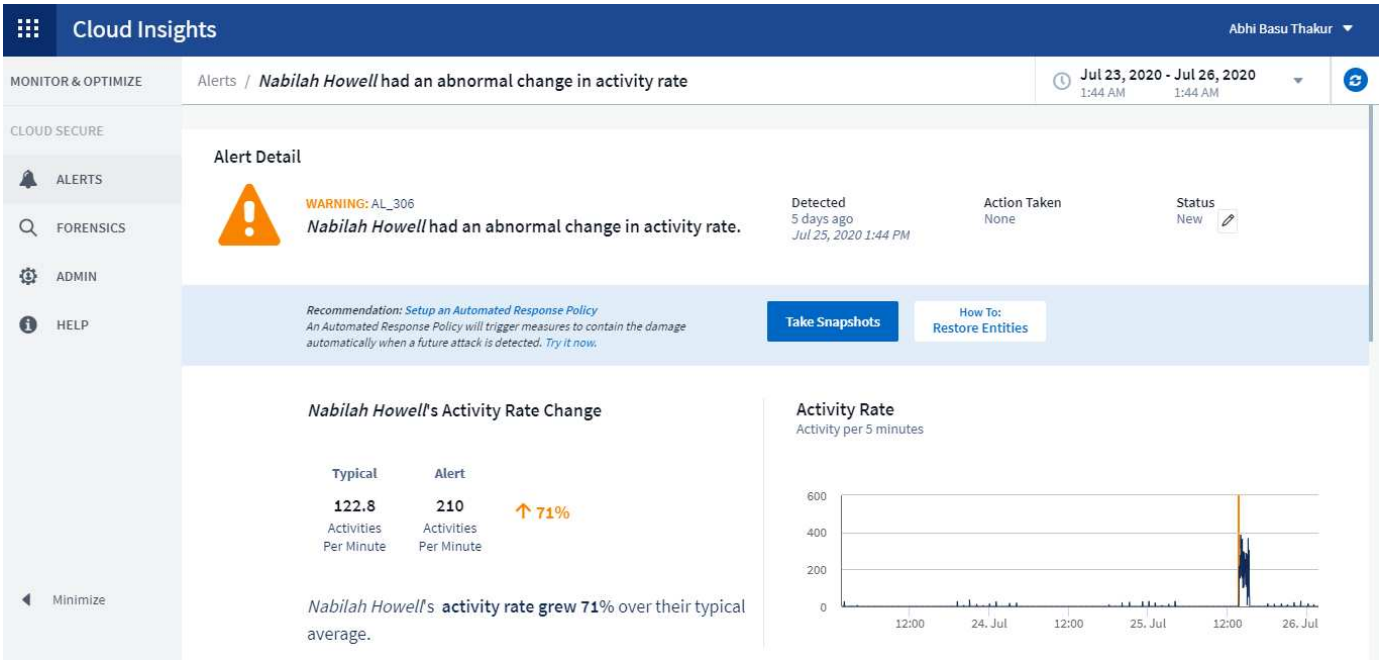
你可以定義 "自動回應策略" 當偵測到檔案竄改攻擊或其他異常使用者活動時，會拍攝快照。您也可以從警報頁面手動截取快照。

自動拍攝快照
：



手動快照

：



警報通知

對於針對警報採取的每個操作，都會向警報收件者清單發送警報的電子郵件通知。若要設定警報收件人，請按一下*管理>通知*並輸入每個收件人的電子郵件地址。

保留政策

警報和警告保留 13 個月。超過 13 個月的警報和警告將被刪除。如果刪除了工作負載安全環境，則與該環境相

關的所有資料也將被刪除。

故障排除

問題：	試試一下：
有一種情況是， ONTAP每天每小時拍攝一次快照。工作負載安全性 (WS) 快照會影響它嗎？ WS 快照會取代每小時快照嗎？預設每小時快照會停止嗎？	工作負載安全快照不會影響每小時快照。 WS 快照不會佔用每小時快照空間，並且應該像以前一樣繼續。預設每小時快照不會停止。
如果ONTAP中達到最大快照數，會發生什麼事？	如果達到最大快照數，後續快照拍攝將會失敗，且工作負載安全性將顯示錯誤訊息，指出快照已滿。使用者需要定義快照策略來刪除最舊的快照，否則將不會拍攝快照。在ONTAP 9.3 及更早版本中，一個磁碟區最多可以包含 255 個 Snapshot 副本。在ONTAP 9.4 及更高版本中，一個磁碟區最多可以包含 1023 個 Snapshot 副本。有關以下信息，請參閱ONTAP文檔"設定快照刪除策略"。
工作負載安全根本無法拍攝快照。	確保用於建立快照的角色具有連結： https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions [已指派適當的權限]。確保已建立的 *csrole* 具有拍攝快照所需的適當存取權限：security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
對於從工作負載安全性中刪除並隨後重新新增的 SVM ，快照對於較舊的警報失敗。對於再次新增 SVM 後出現的新警報，將拍攝快照。	這是一種罕見的情況。如果您遇到這種情況，請登入ONTAP並手動為舊警報拍攝快照。
在「警報詳情」頁面中，「拍攝快照」按鈕下方顯示「上次嘗試失敗」錯誤訊息。將滑鼠懸停在錯誤上會顯示「對於具有 id 的資料收集器，呼叫 API 命令已逾時」。	如果 SVM 的 LIF 在ONTAP中處於 *disabled* 狀態，則當透過 SVM 管理 IP 將資料收集器新增至工作負載安全性時，可能會發生這種情況。在ONTAP中啟用特定的 LIF，並從工作負載安全觸發_手動拍攝快照_。快照操作將會成功。

法醫

取證 - 所有活動

「所有活動」頁面可協助您了解在工作負載安全環境中對實體執行的操作。

檢查所有活動數據

按一下“取證 > 活動取證”，然後按一下“所有活動”標籤以存取“所有活動”頁面。此頁面概述了租戶上的活動，重點介紹了以下資訊：

- 顯示「活動歷史」的圖表（基於選定的全域時間範圍）

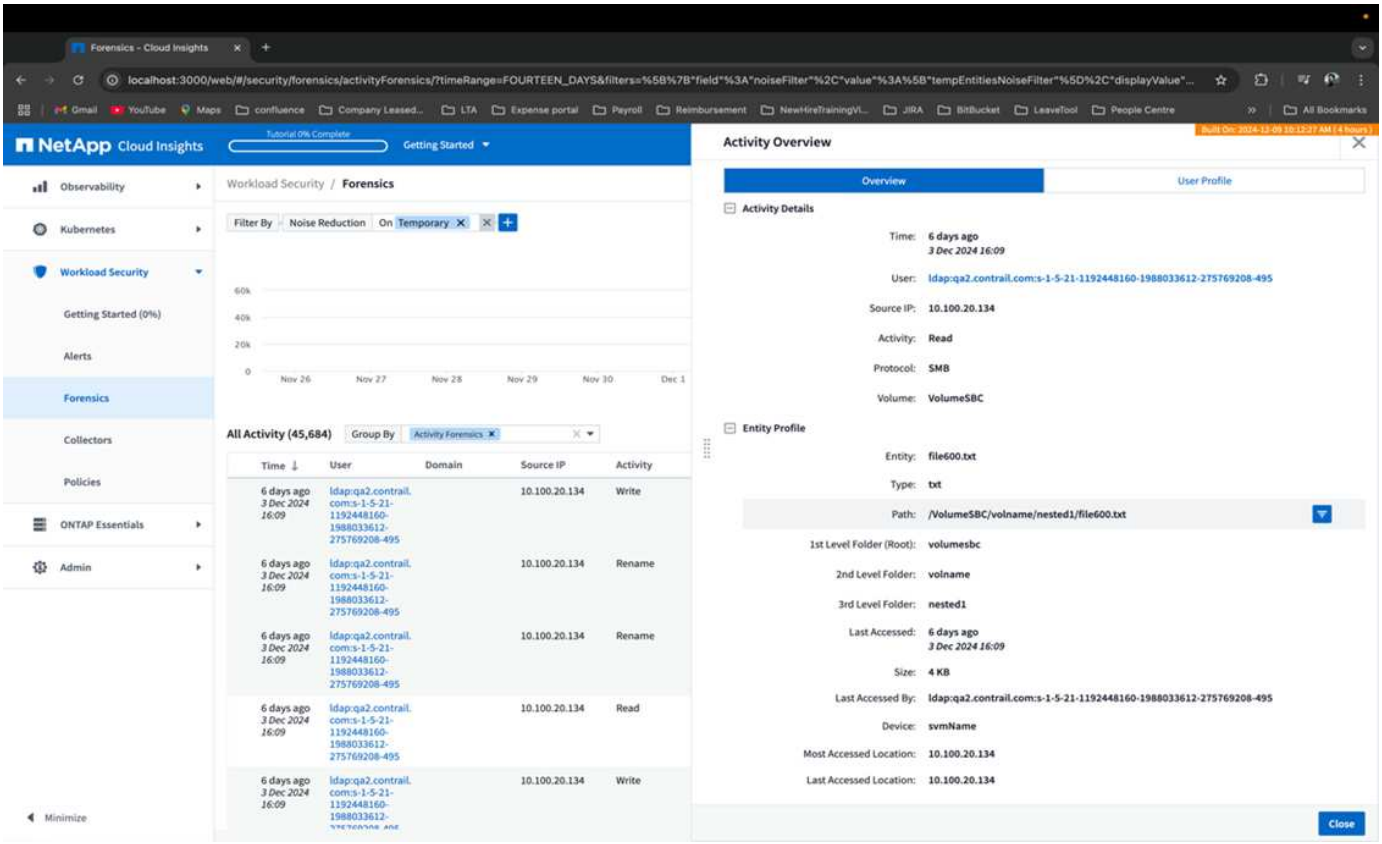
  您可以透過在圖形中拖出一個矩形來縮放圖形。將載入整個頁面以顯示縮放的時間範圍。放大時，會顯示按鈕讓使用者縮小。

- _所有活動_資料的清單。
- 分組下拉式選單將提供按使用者、資料夾、實體類型等對活動進行分組的選項。
- 表格上方將出現一個常用路徑按鈕，點擊該按鈕我們可以獲得帶有實體路徑詳細資訊的滑出面板。

*所有活動*表格顯示以下資訊。請注意，預設並非所有這些列都會顯示。您可以透過點擊“齒輪”圖示來選擇要顯示的列。

- 存取實體的*時間*，包括上次造訪的年、月、日和時間。
- 透過連結存取實體的*使用者*"使用者資訊"作為滑出面板。
- 使用者執行的*活動*。支援的類型有：
  - 變更群組所有權 - 檔案或資料夾的群組所有權已變更。有關團體所有權的更多詳細信息，請參閱"此連結。"
  - 更改擁有者 - 文件或資料夾的所有權更改為另一個使用者。
  - 變更權限 - 檔案或資料夾權限已變更。
  - 建立 - 建立檔案或資料夾。
  - 刪除－刪除檔案或資料夾。如果刪除了一個資料夾，則會取得該資料夾及其子資料夾中所有檔案的_delete_事件。
  - 讀取-檔案已讀取。
  - 讀取元資料 - 僅在啟用資料夾監控選項時。將在 Windows 上開啟資料夾或在 Linux 中的資料夾內執行「ls」時產生。
  - 重新命名－重新命名檔案或資料夾。
  - 寫入 - 資料寫入檔案。
  - 寫入元數據 - 寫入文件元數據，例如，權限變更。
  - 其他變更 - 任何其他未在上面描述的事件。所有未對應的事件都對應到「其他變更」活動類型。適用於文件和資料夾。
- **Path** 是_entity_路徑。這應該是精確的實體路徑（例如，「*/home/userX/nested1/nested2/abc.txt*」）或遞歸搜尋路徑的目錄部分（例如，「*/home/userX/nested1/nested2/*」）。注意：這裡不允許使用正規表示式路徑模式（例如，*nested*）。或者，也可以為路徑過濾指定如下所述的單獨路徑資料夾層級篩選器。
- **1st Level Folder (Root)** 是小寫的實體路徑的根目錄。
- **2nd Level Folder** 是小寫的實體路徑的二級目錄。
- **3rd Level Folder** 是小寫的實體路徑的第三級目錄。
- **4th Level Folder** 是小寫的實體路徑的第四級目錄。
- 實體類型，包含實體（即檔案）副檔名（.doc、.docx、.tmp 等）。
- 實體所在的*設備*。
- 用於取得事件的*協定*。
- 原始檔案重命名時用於重命名事件的*原始路徑*。預設情況下，此列在表中不可見。使用列選擇器將此列新增至表中。
- 實體所在的*卷*。預設情況下，此列在表中不可見。使用列選擇器將此列新增至表中。
- *實體名稱*是實體路徑的最後一個組成部分；對於檔案類型的實體，它是檔案名稱。

選擇表格行將開啟一個滑出面板，其中一個標籤中顯示使用者設定文件，另一個標籤中顯示活動和實體概覽。



預設的_Group by_方法是_Activity forensics_。如果您選擇不同的「分組依據」方法（例如，實體類型），則會顯示實體「分組依據」表。如果沒有做出選擇，則顯示_Group By_ **all**。

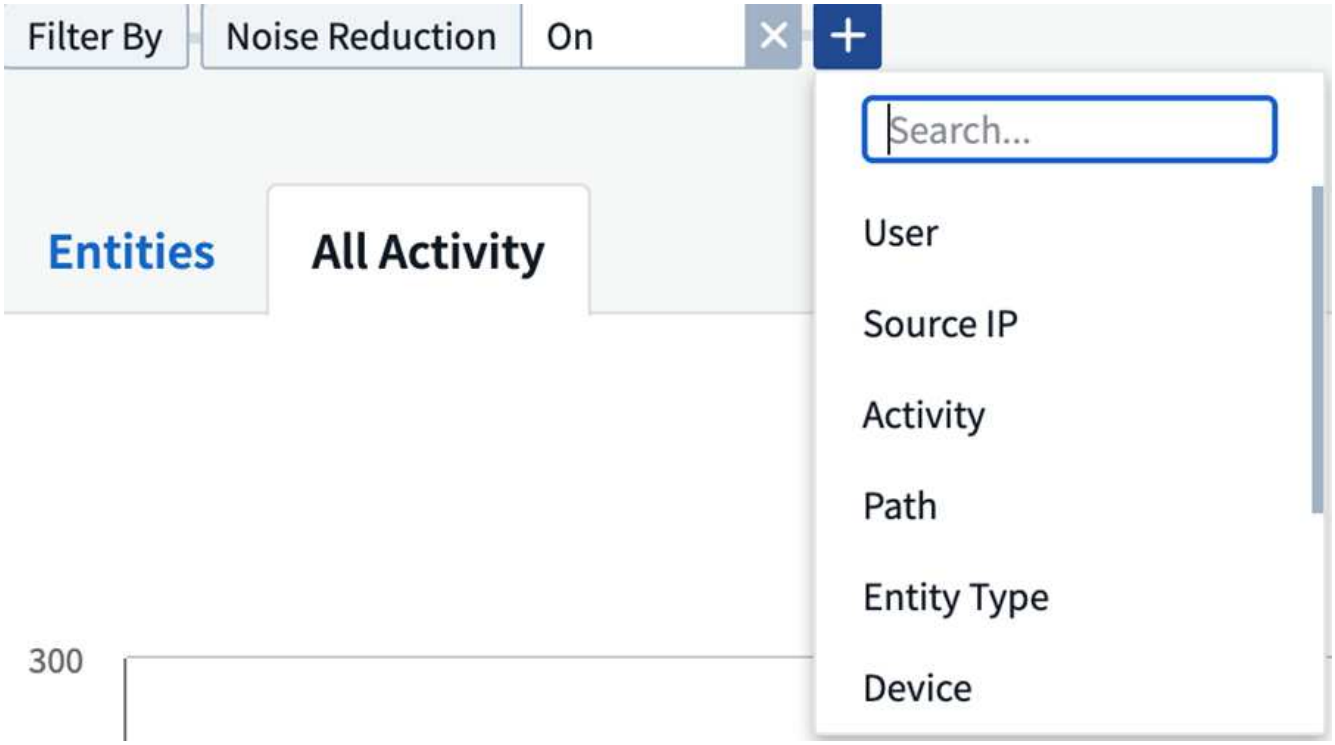
- 活動計數顯示為超連結；選擇此項目將新增選定的分組作為篩選器。活動表將根據該篩選器進行更新。
- 請注意，如果您更改過濾器、改變時間範圍或刷新螢幕，則必須再次設定過濾器才能返回過濾結果。
- 請注意，當選擇實體名稱作為篩選器時，分組依據下拉選單將被停用；此外，當使用者已經在分組依據畫面上時，實體名稱作為篩選器將會被停用。

過濾取證活動歷史數據

您可以使用兩種方法來過濾資料。

- 可以從滑出面板添加過濾器。該值被加到頂部「過濾依據」清單中的相應過濾器中。
- 透過在「篩選依據」欄位中輸入以下內容來篩選資料：

  點擊 **[+]** 按鈕，從頂部的“按條件過濾”小部件中選擇適當的過濾器：



輸入搜尋文字

按 Enter 鍵或按一下篩選器方塊外部即可套用篩選器。

您可以按以下欄位過濾取證活動資料：

- *活動*類型。
- 協議 用於獲取特定於協議的活動。
- 執行活動的使用者的*使用者名稱*。您需要提供準確的用戶名來過濾。使用部分使用者名稱或以「*」為前綴或後綴的部分使用者名稱進行搜尋將無法運作。
- 降噪 過濾使用者在過去 2 小時內建立的檔案。它也用於過濾使用者存取的臨時檔案（例如 .tmp 檔案）。
- 執行活動的使用者的*網域*。您需要提供*精確的域*來進行過濾。搜尋部分域名，或以通配符（'*'）作為前綴或後綴的部分域名將無法運作。可以指定_None_來搜尋缺少的域。

以下欄位需遵守特殊過濾規則：

- 實體類型，使用實體（檔案）副檔名 - 最好在引號內指定確切的實體類型。例如“txt”。
- 實體的*路徑* - 這應該是精確的實體路徑（例如，「*/home/userX/nested1/nested2/abc.txt*」）或遞歸搜尋的路徑的目錄部分（例如，「*/home/userX/nested1/nested2/*」）。注意：這裡不允許使用正規表示式路徑模式（例如，*nested*）。為了更快地獲得結果，建議使用最多 4 個目錄深度的目錄路徑過濾器（以 / 結尾的路徑字串）。例如，「*/home/userX/nested1/nested2/*」。請參閱下表以了解更多詳細資訊。
- 第一層資料夾（根） - 作為篩選器的實體路徑的根目錄。例如，如果實體路徑是 /home/userX/nested1/nested2/，那麼可以使用 home 或「home」。
- 第二層資料夾 - 實體路徑過濾器的第二級目錄。例如，如果實體路徑是 /home/userX/nested1/nested2/，則可以使用 userX 或「userX」。
- 第三層資料夾 – 實體路徑過濾器的第三級目錄。

- 例如，如果實體路徑是 /home/userX/nested1/nested2/，則可以使用 nested1 或“nested1”。
- 第四級資料夾 - 實體路徑過濾器的第四級目錄。例如，如果實體路徑是 /home/userX/nested1/nested2/，則可以使用 nested2 或“nested2”。
- *使用者*執行活動 - 最好在引號內指定確切的使用者。例如，“管理員”。
- 實體所在的*設備*（SVM）
- 實體所在的*體積*
- 原始檔案重命名時用於重命名事件的*原始路徑*。
- 存取實體的*來源 IP*。
  - 您可以使用通配符 * 和 ?。例如：10.0.0.、**10.0.0.10**、**10.10**
  - 如果需要完全匹配，則必須提供雙引號中有效的來源 IP 位址，例如「10.1.1.1。」。帶有雙引號的不完整 IP（例如“10.1.1。”，“10.1..*”等）將不起作用。
- 實體名稱 - 作為篩選器的實體路徑的檔案名稱。例如，如果實體路徑是 /home/userX/nested1/testfile.txt，那麼實體名稱就是 testfile.txt。請注意，建議在引號內指定確切的檔案名稱；盡量避免使用萬用字元搜尋。例如“testfile.txt”。另請注意，建議在較短的時間範圍內（最多 3 天）使用此實體名稱過濾器。

以上欄位在過濾時需要遵循以下原則：

- 確切值應放在引號內：例如：“searchtext”
- 通配符字串不能包含引號：範例：searchtext，*searchtext*，將過濾任何包含「searchtext」的字串。
- 帶有前綴的字串，例如：searchtext*，將搜尋以“searchtext”開頭的任何字串。

請注意，所有過濾欄位都是區分大小寫的搜尋。例如：如果套用的篩選器是實體類型，值為“searchtext”，它將傳回實體類型為“searchtext”、“SearchText”、“SEARCHTEXT”的結果

活動取證過濾器範例：

使用者應用的過濾表達式	預期結果	績效評估	評論
路徑 = “/home/userX/nested1/nested2/”	遞歸查找給定目錄下的所有檔案和資料夾	快速地	最多 4 個目錄的目錄搜尋將會很快。
路徑 = “/home/userX/nested1/”	遞歸查找給定目錄下的所有檔案和資料夾	快速地	最多 4 個目錄的目錄搜尋將會很快。
路徑 = “/home/userX/nested1/test”	路徑值與 /home/userX/nested1/test 完全匹配	慢點	與目錄搜尋相比，精確搜尋的速度較慢。
路徑 = “/home/userX/nested1/nested2/nested3/”	遞歸查找給定目錄下的所有檔案和資料夾	慢點	超過 4 個目錄的搜尋速度較慢。
任何其他非基於路徑的過濾器。建議將使用者和實體類型過濾器放在引號中，例如，使用者=“管理員”實體類型=“txt”		快速地	

使用者應用的過濾表達式	預期結果	績效評估	評論
實體名稱 = “test.log”	檔案名為 test.log 的精確匹配	快速地	因為它是完全匹配
實體名稱 = *test.log	檔案名稱以 test.log 結尾	慢的	由於通配符，它可能會很慢。
實體名稱 = test*.log	檔案名稱以 test 開頭，以 .log 結尾	慢的	由於通配符，它可能會很慢。
實體名稱 = test.lo	檔案名稱以 test.lo 開頭 例如：它將符合 test.log 、test.log.1、test.log1	慢點	由於最後有通配符，所以速度可能會很慢。
實體名稱 = 測試	以 test 開頭的檔名	最慢	由於末尾有通配符並且使用了更多通用值，因此速度可能最慢。

筆記：

1. 當選定的時間範圍跨越 3 天以上時，「所有活動」圖示旁顯示的活動計數將四捨五入為 30 分鐘。例如，時間範圍「9 月 1 日上午 10:15 至 9 月 7 日上午 10:15」將顯示從 9 月 1 日上午 10:00 到 9 月 7 日上午 10:30 的活動計數。
2. 同樣，當選定的時間範圍跨越 3 天以上時，活動歷史記錄圖表中顯示的計數指標將四捨五入為 30 分鐘。

將取證活動歷史資料排序

您可以按時間、使用者、來源 IP、活動、實體類型、第一級資料夾（根）、第二級資料夾、第三層資料夾和第四級資料夾對活動歷史資料進行排序。預設情況下，表格按時間降序排列，這表示最新的數據將首先顯示。 *Device* 和 *Protocol* 欄位的排序已停用。

非同步匯出使用者指南

概況

儲存工作負載安全性中的非同步導出功能旨在處理大量資料導出。

逐步指南：使用非同步匯出匯出數據

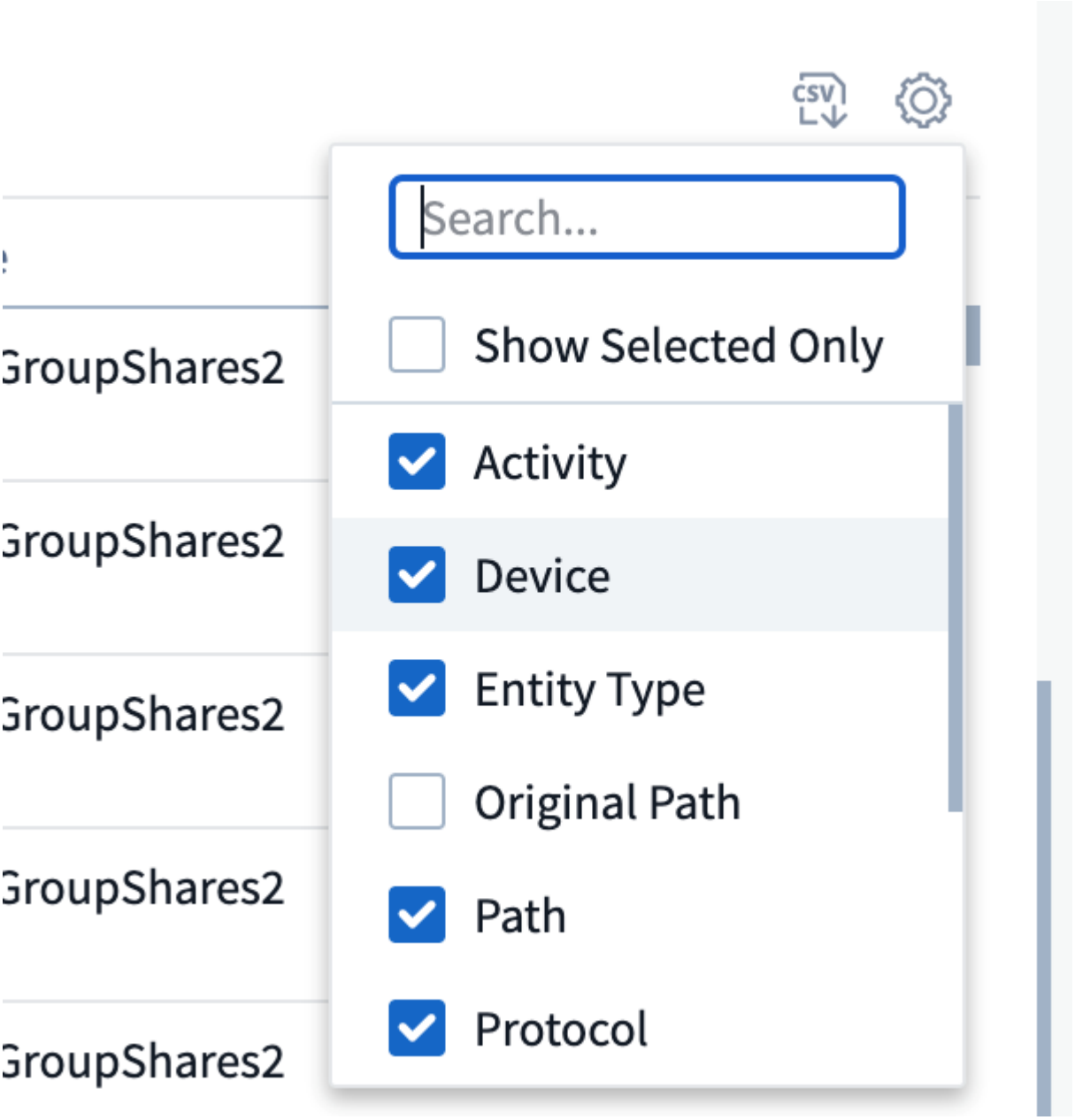
1. 啟動匯出：選擇所需的匯出時間長度和篩選器，然後按一下匯出按鈕。
2. 等待匯出完成：處理時間可能從幾分鐘到幾個小時不等。您可能需要重新整理取證頁面幾次。匯出作業完成後，「下載最後匯出的 CSV 檔案」按鈕將會啟用。
3. 下載：點擊「下載最後建立的匯出檔案」按鈕以取得.zip格式的匯出資料。這些資料將可供下載，直到使用者啟動另一個非同步匯出或 3 天過去（以先發生者為準）。該按鈕將保持啟用狀態，直到啟動另一個非同步匯出。
4. 限制：
   - 目前，每位使用者每個活動和活動分析表的非同步下載次數限制為 1 次，每位租用戶的非同步下載次數限制為 3 次。
   - 對於活動表，匯出的資料限制為最多 100 萬筆記錄；而對於分組，限制為 50 萬筆記錄。

代理程式上的 */opt/netapp/cloudsecure/agent/export-script/* 處有一個透過 API 提取取證資料的範例腳本。有關

該腳本的更多詳細信息，請參閱此處的自述文件。

所有活動的列選擇

_所有活動_表預設顯示選定列。若要新增、刪除或變更列，請按一下表格右側的齒輪圖標，然後從可用列清單中進行選擇。



活動歷史記錄保留

對於活躍的工作負載安全環境，活動記錄將保留 13 個月。

取證頁面中過濾器的適用性

篩選	它的作用	例子	適用於這些過濾器	不適用於這些過濾器	結果
*（星號）	讓您搜尋一切	Auto*03172022 如果搜尋文字包含連字號或底線，請在括號中給出表達式。例如，(svm*) 用於搜尋 svm-123	使用者、實體類型、裝置、磁碟區、原始路徑、第一層資料夾、第二層資料夾、第三層資料夾、第四層資料夾、實體名稱、來源 IP		傳回所有以「Auto」開頭並以「03172022」結尾的資源
？（問號）	使您能夠搜尋特定數量的字符	AutoSabotageUser1_03172022？	使用者、實體類型、裝置、磁碟區、第一層資料夾、第二層資料夾、第三層資料夾、第四層資料夾、實體名稱、來源 IP		返回 AutoSabotageUser1_03172022A、AutoSabotageUser1_03172022B、AutoSabotageUser1_03172022 5 等等
或者	使您能夠指定多個實體	AutoSabotageUser1_03172022 或 AutoRansomUser4_03162022	使用者、網域、實體類型、原始路徑、實體名稱、來源 IP		傳回 AutoSabotageUser1_03172022 或 AutoRansomUser4_03162022 中的任一個
不是	允許您從搜尋結果中排除文本	NOT AutoRansomUser4_03162022	使用者、網域、實體類型、原始路徑、一級資料夾、二級資料夾、三級資料夾、四級資料夾、實體名稱、來源 IP	裝置	傳回所有不以「AutoRansomUser4_03162022」開頭的內容
沒有任何	在所有欄位中搜尋 NULL 值	沒有任何	領域		傳回目標欄位為空的結果

路徑搜尋

有和沒有 / 的搜尋結果會有所不同

“/AutoDir1/AutoFile03242022”	僅精確搜尋有效；傳回所有具有精確路徑為 /AutoDir1/AutoFile03242022 的活動（不區分大小寫）
“/AutoDir1/”	有效；傳回與 AutoDir1 相符的第一級目錄的所有活動（不區分大小寫）
“/AutoDir1/AutoFile03242022/”	有效；傳回與 AutoDir1 相符的第一級目錄和與 AutoFile03242022 相符的第二層目錄的所有活動（不區分大小寫）

/AutoDir1/AutoFile03242022 或 /AutoDir1/AutoFile03242022	不起作用
不是/AutoDir1/AutoFile03242022	不起作用
不是/AutoDir1	不起作用
不是/AutoFile03242022	不起作用
*	不起作用

本機根 **SVM** 使用者活動變化

如果本機根 SVM 使用者正在執行任何活動，現在將在使用者名稱中考慮安裝 NFS 共用的用戶端的 IP，該 IP 將在取證活動和使用者活動頁面中顯示為 root@<ip-address-of-the-client>。

例如：

- 如果 SVM-1 由 Workload Security 監控，且該 SVM 的根使用者在 IP 位址為 10.197.12.40 的用戶端上掛載共用，則取證活動頁面中顯示的使用者名稱將為 *root@10.197.12.40*。
- 如果將同一個 SVM-1 安裝到 IP 位址為 10.197.12.41 的另一個用戶端，則取證活動頁面中顯示的使用者名稱將為 *root@10.197.12.41*。

*• 這樣做是為了透過 IP 位址隔離 NFS 根使用者活動。以前，所有活動都被認為僅由_root_用戶完成，沒有IP區別。

故障排除

問題	嘗試一下
在「所有活動」表中的「使用者」欄位下，使用者名稱顯示為：「ldap：HQ.COMPANYNAME.COM：S-1-5-21-3577637-1906459482-1437260136-1831817」或「ldap：default：80038	可能的原因有：1.尚未配置使用者目錄收集器。若要新增一個，請前往*工作負載安全性>收集器>使用者目錄收集器*，然後按一下*+使用者目錄收集器*。選擇“Active Directory”或“LDAP 目錄伺服器”。2.已配置使用者目錄收集器，但它已停止或處於錯誤狀態。請前往*收集器>使用者目錄收集器*並檢查狀態。請參閱"使用者目錄收集器故障排除"請參閱文件中的故障排除提示部分。正確配置後，名稱將在 24 小時內自動解析。如果仍然沒有解決，請檢查您是否已新增了正確的使用者資料收集器。確保該使用者確實是所新增的 Active Directory/LDAP 目錄伺服器的一部分。
某些 NFS 事件在 UI 中看不到。	檢查以下內容：1.應執行設定了 POSIX 屬性的 AD 伺服器的使用者目錄收集器，並從 UI 啟用 unixid 屬性。2.從 UI 3 在使用者頁面中搜尋時，應該可以看到任何進行 NFS 存取的使用者。 NFS 4 不支援原始事件（尚未發現使用者的事件）。對 NFS 導出的匿名存取將不會受到監控。5.確保使用的 NFS 版本為 4.1 或更低版本。 （請注意， ONTAP 9.15 或更高版本支援 NFS 4.1。）

在取證_所有活動_或_實體_頁面的篩選器中輸入一些包含萬用字元（如星號 (*)）的字母後，頁面載入速度非常慢。	搜尋字串中的星號 (*) 可搜尋所有內容。但是，以 *<*searchTerm*> 或 *<*searchTerm*>* 等為首的通配符字串將導致查詢速度變慢。為了獲得更好的效能，請改用前綴字串，格式為 <*searchTerm*>*（換句話說，在搜尋字詞後面附加星號 (*)）。範例：使用字串 *testvolume**，而不是 **testvolume* 或 **test*volume*。使用目錄搜尋以遞歸方式查看給定資料夾下的所有活動（分層搜尋）。例如，「/path1/path2/path3/」將以遞歸方式列出 /path1/path2/path3 下的所有活動。或使用「所有活動」標籤下的「新增至篩選器」選項。 」
使用路徑過濾器時遇到「請求失敗，狀態代碼 500/503」錯誤。	嘗試使用較小的日期範圍來篩選記錄。
使用 *path* 過濾器時，Forensic UI 載入資料的速度很慢。	目錄路徑過濾器（以 / 結尾的路徑字串）建議深度最多為 4 個目錄，以便更快獲得結果。例如，如果目錄路徑是 /Aaa/Bbb/Ccc/Ddd，請嘗試搜尋“/Aaa/Bbb/Ccc/Ddd/”以更快地載入資料。
使用實體名稱過濾器時，Forensics UI 載入資料緩慢且故障。	請嘗試使用較小的時間範圍並使用雙引號進行精確值搜尋。例如，如果 entityPath 是“/home/userX/nested1/nested2/nested3/testfile.txt”，則嘗試使用“testfile.txt”作為實體名稱過濾器。

法醫用戶概述

使用者概覽中提供了每個使用者的資訊。使用這些視圖來了解使用者特徵、關聯實體和最近的活動。

使用者設定檔

用戶資料資訊包括用戶的聯絡資訊和位置。此設定檔提供以下資訊：

- 用戶姓名
- 使用者的電子郵件地址
- 使用者管理員
- 用戶的電話聯絡方式
- 使用者位置

使用者行為

使用者行為資訊識別使用者最近的活動和執行的操作。這些資訊包括：

- 近期活動
  - 最後訪問位置
  - 活動圖
  - 警報
- 過去七天的營運狀況

- 操作次數

刷新間隔

使用者清單每 12 小時刷新一次。

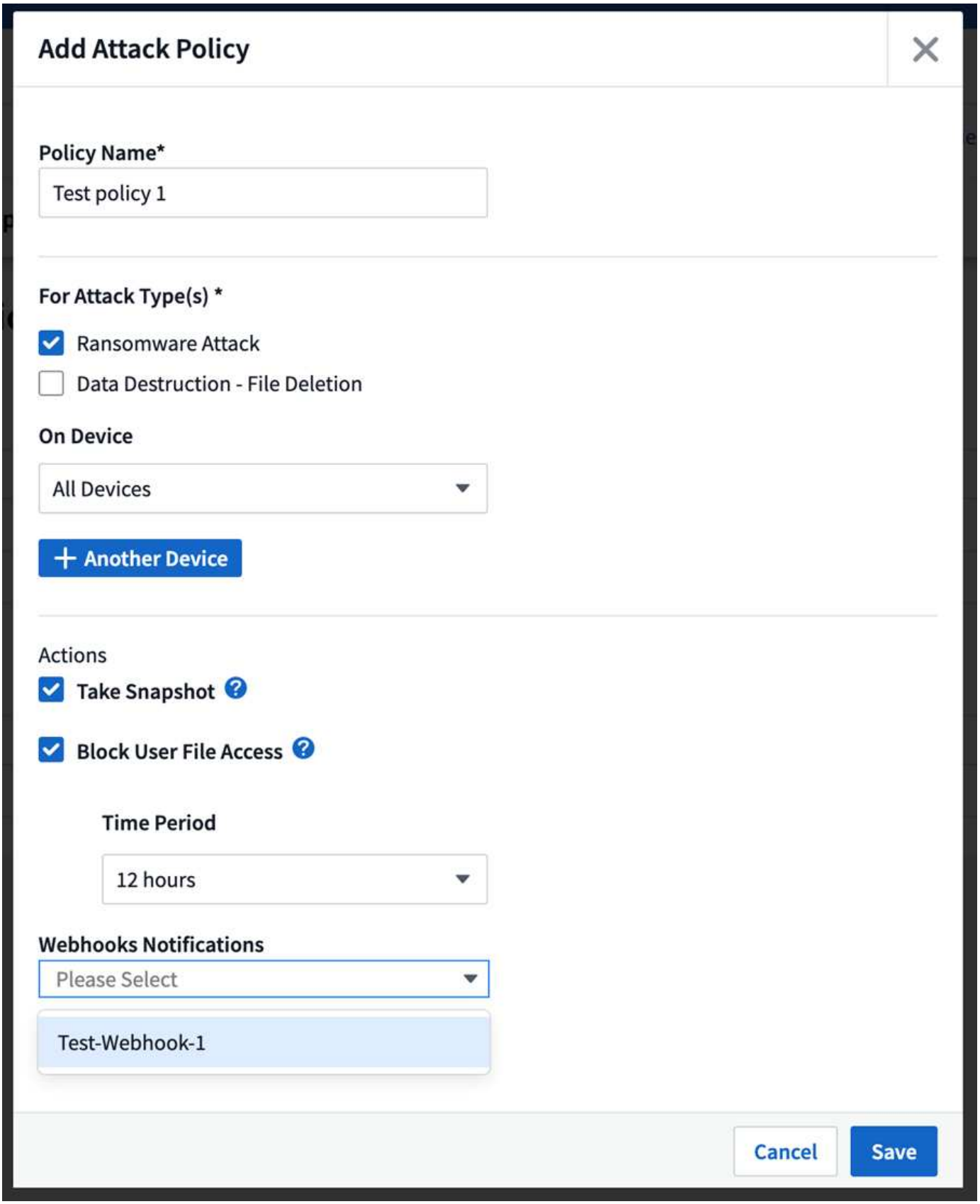
保留政策

如果沒有再次刷新，用戶清單將保留 13 個月。 13個月後，數據將被刪除。如果您的工作負載安全環境已刪除，則與該環境相關的所有資料也將被刪除。

自動回應策略

回應策略會在發生攻擊或異常使用者行為時觸發諸如拍攝快照或限制使用者存取等操作。

您可以針對特定裝置或所有裝置設定策略。若要設定回應策略，請選擇*管理 > 自動回應策略*，然後按一下對應的*+策略*按鈕。您可以建立針對攻擊或警告的策略。



您必須使用唯一的名稱儲存該策略。

若要停用自動回應操作（例如，拍攝快照），只需取消選取該動作並儲存策略。

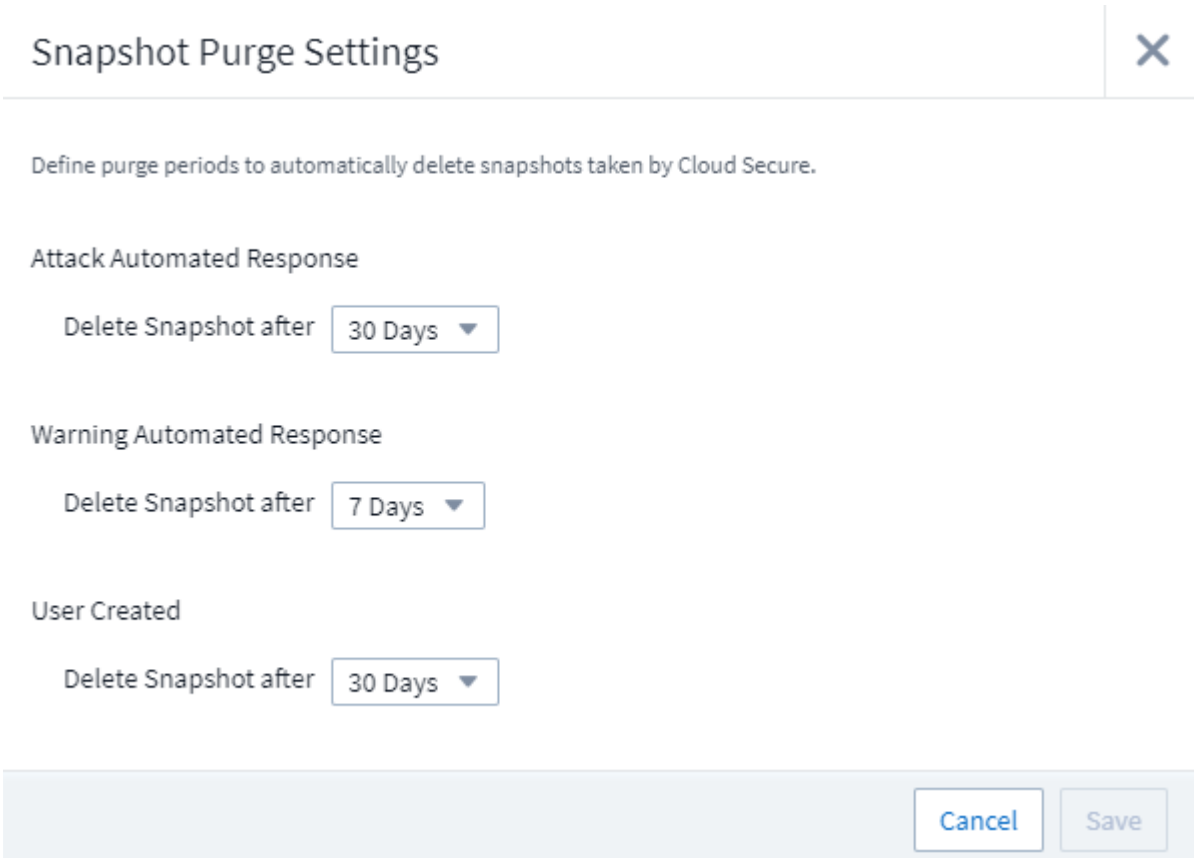
當針對指定設備（或所有設備，如果選擇）觸發警報時，自動回應策略會對您的資料進行快照。您可以在"警報詳細資訊頁面"。

查看"限制用戶訪問"頁面以了解有關透過 IP 限制使用者存取的更多詳細資訊。

您可以將一個或多個 webhook 附加到策略，以便在建立警報和採取行動時收到通知。建議向策略添加不超過 10 個 webhook。請記住，如果策略暫停，則不會觸發 webhook 通知。

您可以透過選擇策略下拉式選單中的選項來修改或暫停自動回應策略。

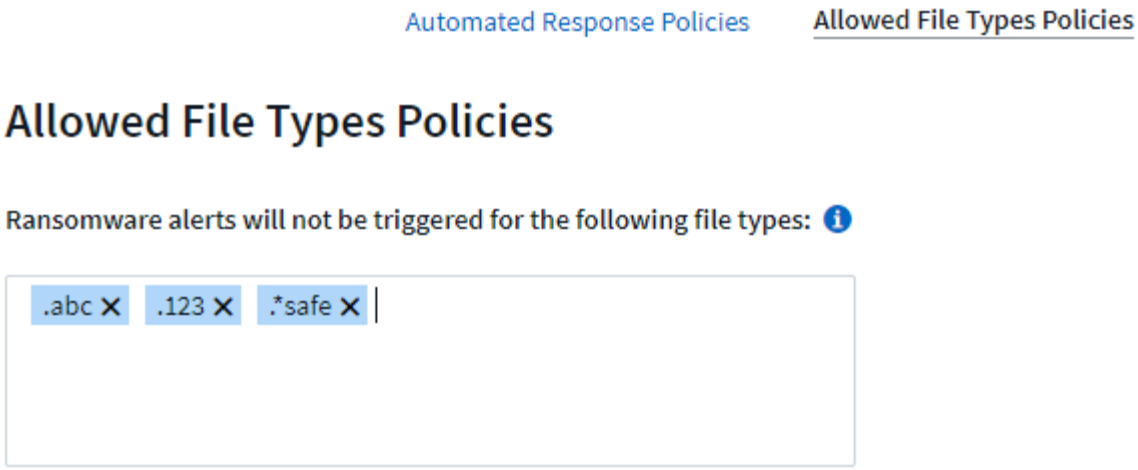
工作負載安全性將根據快照清除設定每天自動刪除一次快照。



允許的文件類型策略

如果偵測到已知檔案副檔名的檔案竄改攻擊，並且在「警報」畫面上產生警報，則可以將該檔案副檔名新增至_允許的檔案類型_清單中，以防止不必要的警報。

導覽至*工作負載安全性>策略*並前往_允許的檔案類型原則_標籤。



一旦新增到_允許的檔案類型_清單中，就不會針對該允許的檔案類型產生檔案篡改攻擊警報。請注意，_允許的檔案類型_策略僅適用於檔案篡改偵測。

例如，如果將名為 *test.txt* 的檔案重新命名為 *test.txt.abc*，且工作負載安全系統因 *.abc* 副檔名而偵測到檔案篡改攻擊，則可以將 *.abc* 副檔名新增至 允許的檔案類型 清單中。新增至清單後，將不再針對副檔名為 *.abc* 的檔案產生檔案篡改攻擊。

允許的檔案類型可以是完全符合（例如“ .abc”）或表達式（例如“ **.type”**、**“ .type**”或“ **type**”）。不支援「.a*c」、「.p*f」類型的表達式。

與ONTAP自主勒索軟體防護集成

ONTAP自主保護功能利用 NAS（NFS 和 SMB）環境中的工作負載分析，主動偵測並警告可能表明惡意攻擊或未經授權的資料修改的異常檔案內活動。

關於 ARP 的更多詳細資訊和許可要求可以找到"這裡"。

工作負載安全性與ONTAP整合以接收 ARP 事件並提供額外的分析和自動回應層。

工作負載安全性從ONTAP接收 ARP 事件並執行下列操作：

1. 將捲加密事件與使用者活動關聯起來，以識別造成損害的人。
2. 實施自動回應策略（如果定義）
3. 提供取證能力：
   - 允許客戶進行資料外洩調查。
   - 確定哪些文件受到了影響，幫助更快地恢復並進行資料外洩調查。

先決條件

1. 最低ONTAP版本：9.11.1
2. ARP 啟用磁碟區。關於啟用 ARP 的詳細資訊可以找到"這裡"。必須透過OnCommand System Manager啟用 ARP。工作負載安全性無法啟用 ARP。

3. 應透過叢集 IP 新增工作負載安全收集器。
4. 此功能需要集群級憑證才能運作。換句話說，新增 SVM 時必須使用叢集等級憑證。

需要使用者權限

如果您使用叢集管理憑證，則不需要新的權限。

如果您使用具有指定權限的自訂使用者（例如 *csuser*），請依照下列步驟授予 Workload Security 從ONTAP收集 ARP 相關資訊的權限。

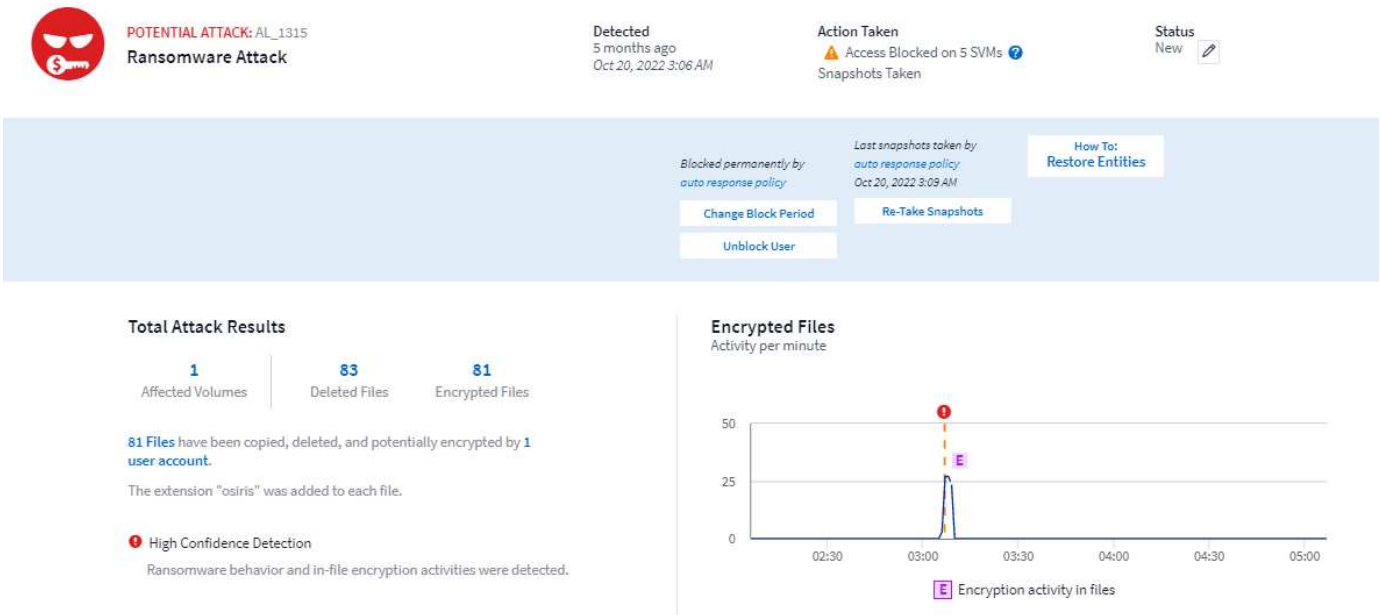
對於具有叢集憑證的 *csuser*，從ONTAP命令列執行下列操作：

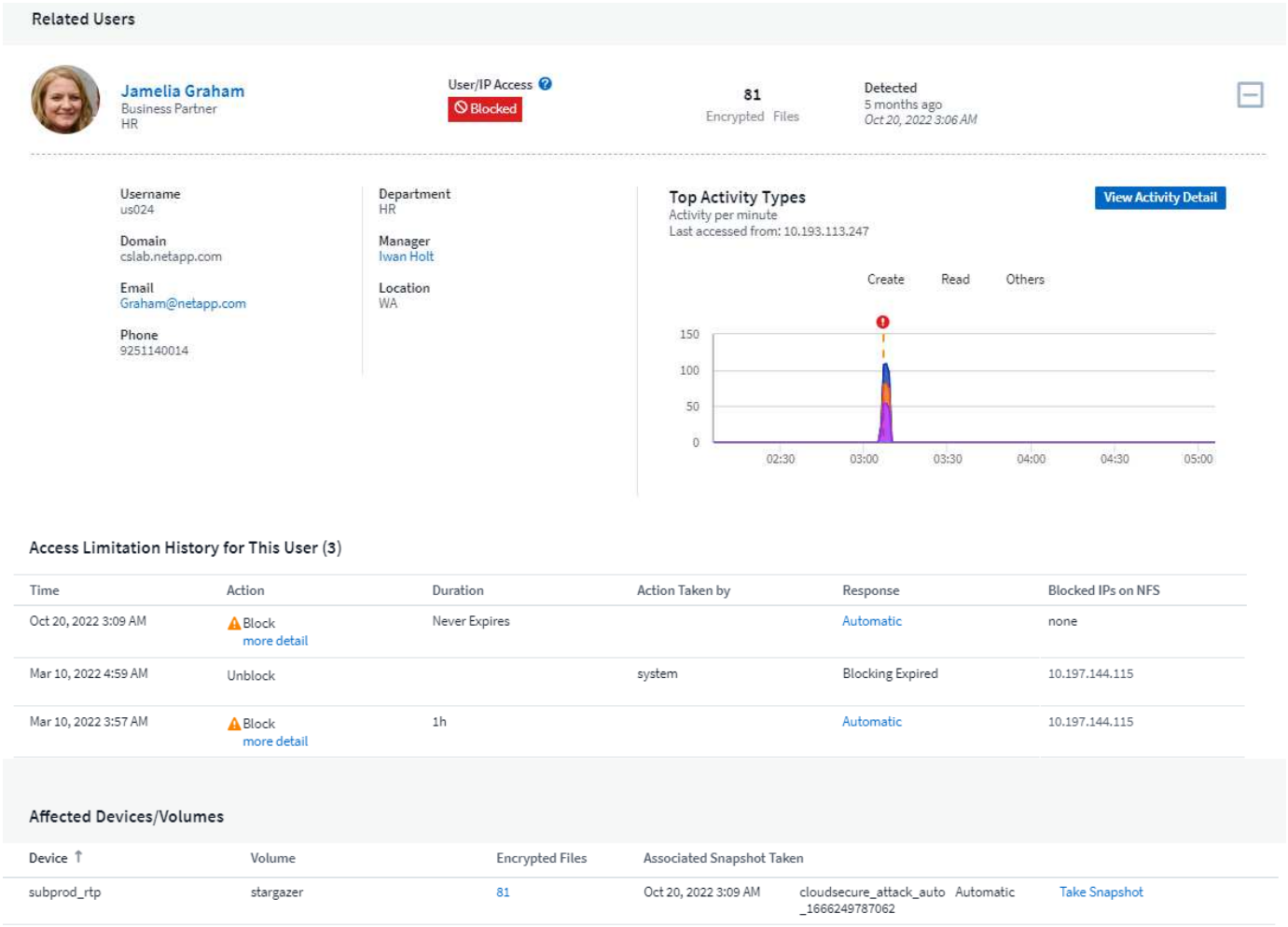
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

閱讀有關配置其他內容的更多信息"ONTAP 權限"。

樣本警報

由於 ARP 事件產生的警報示例如下所示：





高置信度橫幅表示攻擊已顯示文件篡改行為以及文件加密活動。加密檔案圖表顯示了 ARP 解決方案偵測到磁碟區加密活動的時間戳記。

限制

如果 SVM 未受到 Workload Security 監控，但ONTAP產生了 ARP 事件，則 Workload Security 仍會接收並顯示這些事件。但是，與警報相關的取證資訊以及使用者映射將不會被捕獲或顯示。

故障排除

下表描述了已知問題及其解決方法。

問題：	解決：
偵測到攻擊後 24 小時會收到電子郵件警報。在 UI 中，警報會在Data Infrastructure Insights工作負載安全收到電子郵件之前 24 小時顯示。	當ONTAP將「偵測到勒索軟體」事件傳送到Data Infrastructure Insights工作負載安全（即工作負載安全）時，就會發送電子郵件。此事件包含攻擊清單及其時間戳記。工作負載安全 UI 顯示第一個受到攻擊的檔案的警報時間戳。當一定數量的文件被編碼時， ONTAP 會將「偵測到勒索軟體」事件傳送到Data Infrastructure Insights。因此，警報在 UI 中顯示的時間與電子郵件發送的時間之間可能會有差異。

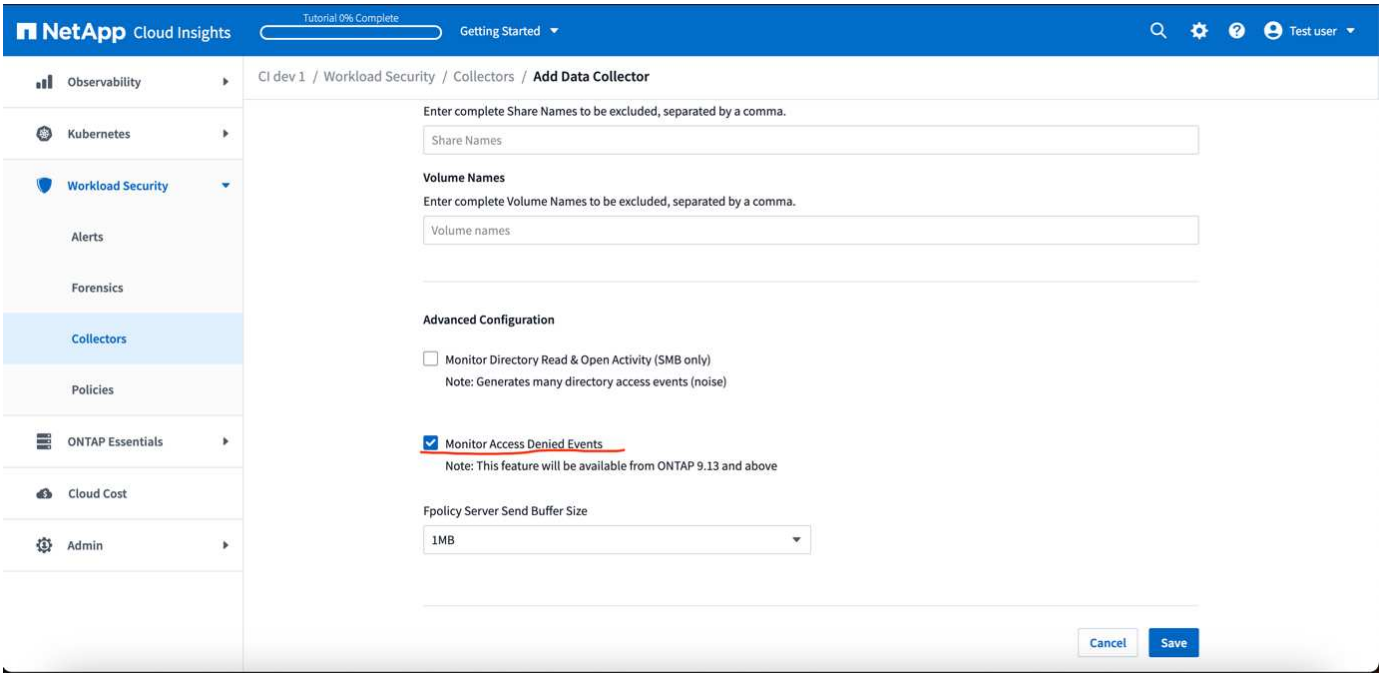
與ONTAP整合存取被拒絕

ONTAP存取被拒絕功能使用 NAS 環境（NFS 和 SMB）中的工作負載分析來主動偵測並警告失敗的檔案操作（即使用者嘗試執行他們沒有權限的操作）。這些失敗的文件操作通知——特別是在發生與安全相關的故障的情況下——將進一步有助於在早期階段阻止內部攻擊。

Data Infrastructure Insights工作負載安全性與ONTAP整合以接收存取被拒絕事件並提供額外的分析和自動回應層。

先決條件

- 最低ONTAP版本：9.13.0。
- 工作負載安全性管理員必須在新增收集器或編輯現有收集器時啟用「拒絕存取」功能，方法是選取「進階配置」下的「監控拒絕存取事件」複選框。



需要使用者權限

如果使用叢集管理憑證新增資料收集器，則不需要新的權限。

如果使用自訂使用者（例如 *csuser*）新增收集器並向該使用者授予權限，請依照下列步驟為工作負載安全性提供必要的權限，以便使用ONTAP註冊存取被拒絕事件。

對於具有 *cluster* 憑證的 csuser，從ONTAP命令列執行下列命令。請注意，此權限可能已經存在。

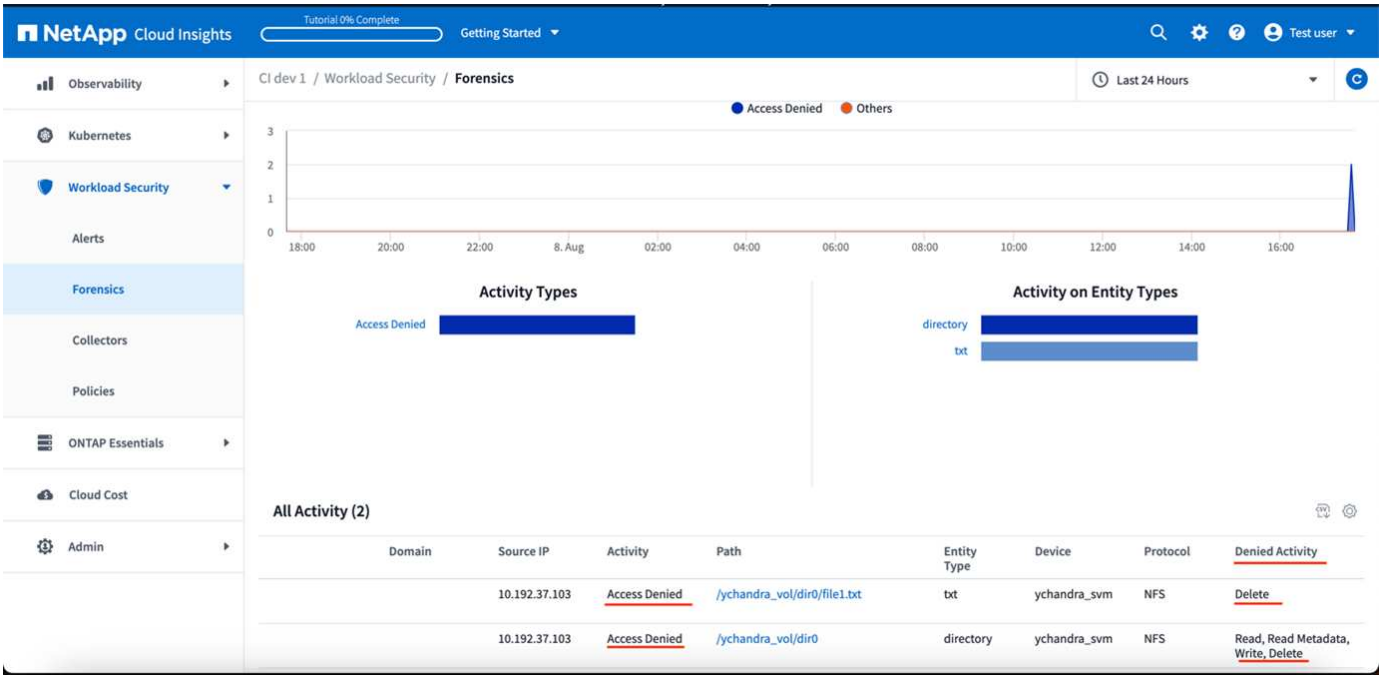
```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
```

對於具有 `_SVM_` 憑證的 `csuser`，從ONTAP命令列執行下列命令。請注意，此權限可能已經存在。

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
```
閱讀有關配置其他內容的更多信息link:task_add_collector_svm.html["ONTAP 權限"]。

訪問被拒絕事件

從ONTAP系統取得事件後，「工作負載安全取證」頁面將顯示「存取被拒絕」事件。除了顯示的資訊之外，您還可以透過從齒輪圖示新增「所需活動」欄位來查看特定操作缺少的使用者權限。



阻止用戶訪問以阻止攻擊

立即阻止偵測到的攻擊，阻止受感染用戶的訪問，以防止進一步的資料損壞或外洩。工作負載安全功能既可以透過自動回應策略實現自動阻止，也可以透過警報或使用者詳細資訊頁面進行手動幹預，從而讓您靈活控制安全回應。存取限制會自動套用於所有受監控的儲存卷，並且有時間限制，以便自動復原。

使用者的 SMB 存取將直接被阻止，而引發攻擊的主機的 IP 位址的 NFS 存取將被阻止。這些機器 IP 位址將被阻止存取由工作負載安全監控的任何儲存虛擬機器 (SVM)。

例如，假設工作負載安全管理 10 個 SVM，並且為其中 4 個 SVM 配置了自動回應策略。如果攻擊源自四個 SVM 中的一個，則使用者的存取將在所有 10 個 SVM 中被封鎖。仍在原始 SVM 上拍攝快照。

如果有四個 SVM，其中一個 SVM 配置為 SMB，一個 SVM 配置為 NFS，其餘兩個 SVM 同時配置為 NFS 和 SMB，則如果攻擊源自四個 SVM 中的任何一個，則所有 SVM 都會被阻止。

使用者存取阻止的先決條件

此功能需要集群級憑證才能運作。

如果您使用叢集管理憑證，則不需要新的權限。

如果您正在使用具有指定權限的自訂使用者（例如，*csuser*），請依照下列步驟向 Workload Security 授予封鎖使用者的權限。

對於具有叢集憑證的 csuser，請從ONTAP命令列執行下列操作：

```
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
```

請務必查看"配置ONTAP SVM 資料收集器"頁面也是如此。

如何啟用該功能？

- 在工作負載安全性中，導覽至*工作負載安全性>策略>自動回應策略*。選擇*+攻擊策略*。
- 選擇（選取）阻止使用者檔案存取。

如何設定自動用戶存取阻止？

- 建立新的攻擊策略或編輯現有的攻擊策略。
- 選擇應監控攻擊策略的 SVM。
- 點選複選框「阻止使用者檔案存取」。選擇此項目後，該功能將會啟用。
- 在「時間段」下選擇套用封鎖的時間。
- 若要測試自動用戶阻止，您可以透過以下方式模擬攻擊"類比腳本"。

如何知道系統中是否有被封鎖的使用者？

- 在警報清單頁面中，如果有任何使用者被封鎖，螢幕頂部將顯示橫幅。
- 點擊橫幅將帶您進入「使用者」頁面，您可以在此查看被封鎖使用者的清單。
- 在「使用者」頁面中，有一個名為「使用者/IP存取」的欄位。在該欄位中將顯示使用者封鎖的目前狀態。

手動限制和管理用戶訪問

- 您可以轉到警報詳細資訊或使用者詳細資料螢幕，然後從這些螢幕手動封鎖或還原使用者。

使用者存取限制歷史記錄

在警報詳細資訊和使用者詳細資料頁面的使用者面板中，您可以查看使用者存取限制歷史記錄的審核：時間、操作（封鎖、解除封鎖）、持續時間、採取的操作、手動/自動以及受影響的 NFS IP。

如何停用該功能？

您可以隨時停用該功能。如果系統中有受限用戶，則必須先恢復他們的存取權限。

- 在工作負載安全性中，導覽至*工作負載安全性>策略>自動回應策略*。選擇*+攻擊策略*。
- 取消選擇（取消選取）阻止使用者檔案存取。

該功能將在所有頁面中隱藏。

手動恢復 **NFS** 的 **IP**

如果您的 Workload Security 試用版已過期，或代理程式/收集器已關閉，請依照下列步驟從ONTAP手動復原任何 IP。

1. 列出 SVM 上的所有匯出策略。

```
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. 透過指定對應的 RuleIndex，刪除 SVM 上所有將「cloudsecure_rule」作為客戶端相符的策略中的規則。工作負載安全規則通常為 1。

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
```

. 確保工作負載安全規則已被刪除（選用步驟確認）。

```
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.
```

手動恢復 **SMB** 用戶

如果您的 Workload Security 試用版已過期，或代理程式/收集器已關閉，請依照下列步驟從ONTAP手動恢復任何使用者。

您可以從使用者清單頁面取得工作負載安全性中被封鎖的使用者清單。

1. 使用群集_admin_憑證登入ONTAP叢集（您想要解除使用者封鎖的位置）。（對於Amazon FSx，使用 FSx 憑證登入）。
2. 執行下列命令列出所有 SVM 中被 Workload Security for SMB 封鎖的所有使用者：

```
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.
```

在上面的輸出中，有 2 個使用者（US030、US040）被域 CSLAB 封鎖。

1. 一旦我們從上面的輸出中識別出位置，請執行以下命令來解除對使用者的封鎖：

```
 vserver name-mapping delete -direction win-unix -position <position>
```

. 透過執行以下命令確認用戶已解除封鎖：

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

對於先前被封鎖的用戶，不應顯示任何條目。

故障排除

問題	嘗試一下
儘管發生了攻擊，但一些用戶並未受到限制。	1.確保 SVM 的資料收集器和代理程式處於_正在運行_狀態。如果資料收集器和代理停止，工作負載安全性將無法發送命令。2.這是因為用戶可能從具有以前未使用過的新 IP 的機器存取了儲存。限制是透過使用者存取儲存的主機的 IP 位址進行的。在 UI（警報詳細資訊 > 此使用者的存取限制歷史記錄 > 受影響的 IP）中檢查受限制的 IP 位址清單。如果使用者從具有不同於受限 IP 的 IP 的主機存取存儲，則使用者仍然能夠透過非受限 IP 存取存儲。如果使用者嘗試從 IP 受限的主機進行訪問，則儲存將無法存取。
手動點選「限制存取」會出現「此使用者的 IP 位址已被限制」的情況。	需要限制的 IP 已被其他使用者限制。
無法修改策略。原因：未授權執行該指令。	檢查是否使用 csuser，是否如上所述授予使用者權限。
NFS 的使用者（IP 位址）阻止有效，但對於 SMB/CIFS，我看到一條錯誤訊息：「SID 到網域轉換失敗。原因超時：套接字未建立”	如果 *csuser* 沒有執行 ssh 的權限，則可能會發生這種情況。 （確保叢集層級的連接，然後確保使用者可以執行 ssh）。 *csuser* 角色需要這些權限。 https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking對於具有群集憑證的 *csuser*，請從ONTAP命令列執行以下操作： security login role create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role cole -cmcm firname - vi^cm none kkd -cmFiial f55 -cmi fir fFald -cmFirname -vvi nv "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 -cmirname"vserver_cmirname "vserver_cmircc -Fat_cmircoat_Flu_cmirname"vserver_cmirname"vserver_cmircc -Fat_cmirname s fat_cmirFvserver_cmdirFvserver_cmirc -Fat_cmirc -Fat_cmirname n_vv.並且使用叢集層級的管理員用戶，請確保管理員用戶具有ONTAP的 ssh 權限。

問題	嘗試一下
我收到錯誤訊息 *SID* 轉換失敗。 _ _原因：*255*：錯誤：命令失敗：未授權執行該命令錯誤：「*access-check*」不是可識別的命令，而使用者應該被阻止。	當 *csuser* 沒有正確的權限時，就會發生這種情況。看"使用者存取阻止的先決條件"了解更多。應用權限後，建議重新啟動ONTAP資料收集器和使用者目錄資料收集器。所需的權限命令如下圖所示。 ---- 安全登入角色建立 -role csrole -cmddirname「vserver export-policy rule」-access all 安全登入角色建立 -role csrole -cmddirname 設定 -access all 安全登入角色建立 -role csrole -cmddirname「vserver accvsession 」服務安全登入角色建立 -role csrole -cmddirname「vserver accvsession)」服務-安全登入角色 - 安全性」authentication translate”-access all 安全登入角色建立 -role csrole -cmddirname“vserver name-mapping”-access all ----

工作負載安全：模擬文件篡改

您可以按照本頁上的說明，使用隨附的文件篡改模擬腳本來模擬文件篡改，以測試或演示工作負載安全性。

開始前需要注意的事項

- 此檔案篡改模擬腳本僅適用於 Linux 系統。如果使用者已將ONTAP ARP 與工作負載安全性集成，則模擬腳本也應產生高置信度警報。
- 只有當ONTAP版本為 9.15 或更高版本時，工作負載安全才會偵測使用 NFS 4.1 產生的事件和警報。
- 此腳本隨工作負載安全代理安裝檔一起提供。它可以在安裝了工作負載安全代理程式的任何機器上使用。
- 您可以在工作負載安全代理機器本身上執行該腳本；無需準備另一台 Linux 機器。但是，如果您希望在另一個系統上運行該腳本，只需複製該腳本並在那裡運行即可。
- 使用者可以根據自己的喜好和系統需求選擇 Python 或 shell 腳本。
- Python 腳本具有先決條件安裝。如果不想使用python，就使用shell腳本。

指南：

該腳本應在包含大量需要加密的檔案（理想情況下為 100 個或更多，包括子資料夾中的檔案）的資料夾的 SVM 上執行。確保文件不為空。

若要產生警報，請在建立測試資料之前暫時暫停收集器。一旦產生範例文件，恢復收集器並啟動加密過程。

步驟：

準備系統：

首先，將目標磁碟區安裝到機器上。您可以掛載 NFS 或 CIFS 匯出。

要在 **Linux** 中掛載 **NFS** 導出：

```
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
```

請勿掛載 NFS 版本 4.1；Fpolicy 不支援它。

要在 **Linux** 中掛載 **CIFS**：

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

啟用 **ONTAP** 自主勒索軟體防護（選用）：

如果您的ONTAP叢集版本是 9.11.1 或更高版本，您可以透過在ONTAP命令控制台上執行以下命令來啟用ONTAP勒索軟體防護服務。

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
```

接下來，設定資料收集器：

1. 如果尚未完成，請設定工作負載安全代理程式。
2. 如果尚未完成，請設定 SVM 資料收集器。
3. 確保在配置資料收集器時選擇了安裝協定。

以程式設計方式產生範例文件：

在建立文件之前，您必須先停止或"暫停資料收集器"加工。

在運行模擬之前，您必須先新增要加密的檔案。您可以手動將要加密的檔案複製到目標資料夾中，也可以使用其中的腳本以程式設計方式建立檔案。無論使用哪種方法，請確保至少有 100 個檔案需要加密。

如果您選擇以程式設計方式建立文件，則可以使用 Shell 或 Python：

殼：

1. 登入代理箱。
2. 將 NFS 或 CIFS 共用從檔案管理器的 SVM 掛載到代理電腦。轉到該資料夾。
3. 將腳本從代理安裝目錄（%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh）複製到目標安裝位置。
4. 使用掛載目錄（例如 /root/demo）中的腳本執行以下命令來建立測試資料集資料夾和檔案：

```
'./create_dataset.sh'
```
. 這將在名為「test_dataset」的目錄下的掛載資料夾內建立 100 個具有各種副檔名的非空檔案。

Python：

Python 腳本先決條件：

- 安裝 Python（如果尚未安裝）。
  - 從下列位置下載 Python 3.5.2 或更高版本 https://www.python.org/。
  - 若要檢查 Python 安裝，請執行 `python --version`。
  - 該 Python 腳本已在最早 3.5.2 版本上進行測試。
- 如果尚未安裝 pip，請安裝：
  - 從以下位置下載 get-pip.py 腳本 https://bootstrap.pypa.io/。
  - 使用以下方式安裝 pip `python get-pip.py` 。
  - 使用以下命令驗證 pip 安裝 `pip --version`。
- PyCryptodome 庫：
  - 該腳本使用 PyCryptodome 庫。
  - 使用以下方式安裝 PyCryptodome `pip install pycryptodome` 。
  - 透過運行確認 PyCryptodome 安裝 `pip show pycryptodome`。

Python建立檔案腳本：

1. 登入代理箱。
2. 將 NFS 或 CIFS 共用從檔案管理器的 SVM 掛載到代理電腦。轉到該資料夾。
3. 將腳本從代理安裝目錄（%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py）複製到目標安裝位置。
4. 使用已安裝目錄（例如 /root/demo）中的腳本執行以下命令來建立測試資料集資料夾和檔案：

```
'python create_dataset.py'
```
. 這將在名為"test_dataset"的目錄下的掛載資料夾中建立 100 個具有各種副檔名的非空文件

恢復收集器

如果您在執行這些步驟之前暫停了收集器，請確保在建立範例檔案後恢復收集器。

以程式設計方式產生範例文件：

在建立文件之前，您必須先停止或"暫停資料收集器"加工。

若要產生檔案篡改警報，您可以執行隨附的腳本，該腳本將在工作負載安全中模擬檔案篡改警報。

殼：

1. 將腳本從代理安裝目錄（%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh）複製到目標安裝位置。
2. 使用掛載目錄（例如 /root/demo）中的腳本執行以下命令來加密測試資料集：

```
'./simulate_attack.sh'
```

. 這將加密在"test_dataset"目錄下建立的範例檔案。

Python：

1. 將腳本從代理安裝目錄（%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py）複製到目標安裝位置。
2. 請注意，python 先決條件是按照 Python 腳本先決條件部分安裝的
3. 使用掛載目錄（例如 /root/demo）中的腳本執行以下命令來加密測試資料集：

```
'python simulate_attack.py'
```

. 這將加密在"test_dataset"目錄下建立的範例檔案。

在工作負載安全性中產生警報

模擬器腳本執行完成後，幾分鐘內就會在 Web UI 上看到警報。

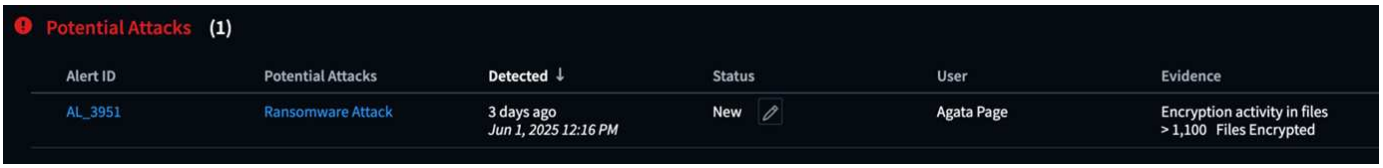
注意：如果滿足以下所有條件，則會產生高置信度警報。

1. 監控的 SVM 的ONTAP版本高於 9.11.1
2. ONTAP自主勒索軟體防護已配置
3. 在叢集模式下新增了工作負載安全資料收集器。

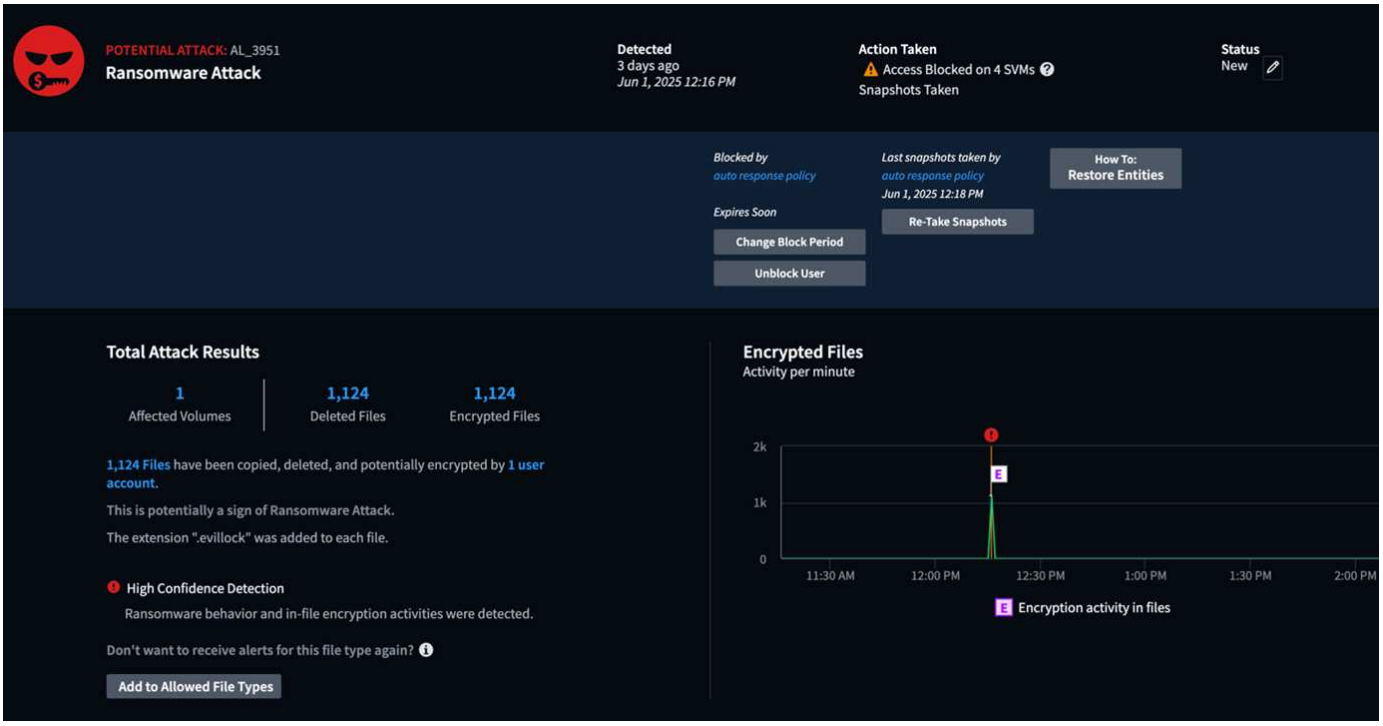
Workload Security 根據使用者行為偵測檔案竄改模式，而ONTAP ARP 則會根據檔案中的加密活動偵測檔案竄改活動。

如果滿足條件，Workload Security 會將警報標記為高可信度警報。

警報清單頁面上的高可信度警報範例：



高可信度警報詳細資訊範例：



多次觸發警報

工作負載安全功能會學習使用者行為，對於同一使用者在 24 小時內重複發生的檔案竄改攻擊，不會發出警報。

若要使用不同的使用者產生新的警報，請再次執行相同的步驟（建立測試數據，然後加密測試數據）。

配置警報、警告和代理/資料來源收集器健康狀況的電子郵件通知

電子郵件通知使您能夠及時了解潛在攻擊、安全警告和基礎設施健康狀況問題。在「管理 > 通知」設定中設定收件人電子郵件地址，以接收根據每個收件人的職責量身定制的即時警報。

潛在攻擊警報和警告

若要傳送_潛在攻擊_警報通知，請在_傳送潛在攻擊警報_部分輸入收件者的電子郵件地址。對於警報上的每個操作，都會向警報收件者清單發送電子郵件通知。

若要傳送_警告_通知，請在_傳送警告警報_部分輸入收件者的電子郵件地址。

代理商和數據收集器健康監控

您可以透過通知監控代理程式和資料來源的健康狀況。

為了在代理程式或資料來源收集器無法運作時接收通知，請在「資料收集健康警報」部分輸入收件人的電子郵件地址。

請記住以下幾點：

- 僅當代理商/收集者停止報告至少一小時後才會發送健康警報。
- 即使代理程式或資料收集器長時間斷開連接，在給定的 24 小時內也只會向預期收件者發送一封電子郵件通知。
- 如果代理程式發生故障，則會發送警報（而不是每個收集器發送警報）。該電子郵件將包含所有受影響的 SVM 的清單。
- Active Directory 資料收集失敗會被報告為警告；它不會影響威脅偵測。
- 入門設定清單現在包括一個新的「設定電子郵件通知」階段。

接收代理程式和資料收集器升級通知

- 在「資料收集健康警報」中輸入電子郵件 ID。
- “啟用升級通知”複選框變為啟用狀態。
- 代理程式和資料收集器升級電子郵件通知將在計劃升級前一天發送到電子郵件 ID。

故障排除

問題：	試試這個：
電子郵件 ID 出現在「資料收集器健康警報」中，但我沒有收到通知。	通知電子郵件從NetApp Data Infrastructure Insights網域發送，即從 *accounts@service.cloudinsights.netapp.com* 發送。有些公司會封鎖來自外部網域的來電電子郵件。確保來自NetApp Data Infrastructure Insights網域的外部通知已列入白名單。

Webhook 通知

使用 **webhook** 的工作負載安全通知

Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送關鍵或警告警報通知。

許多商業應用程式支援 webhook 作為標準輸入接口，例如：Slack、PagerDuty、Teams 和 Discord。透過支援通用、可自訂的 webhook 通道，Workload Security 可以支援許多這樣的交付通道。有關配置 webhook 的資訊可以在相應應用程式的網站上找到。例如，Slack 提供"這個有用的指南"。

您可以建立多個 webhook 通道，每個通道針對不同的目的、單獨的應用程式、不同的收件者等。

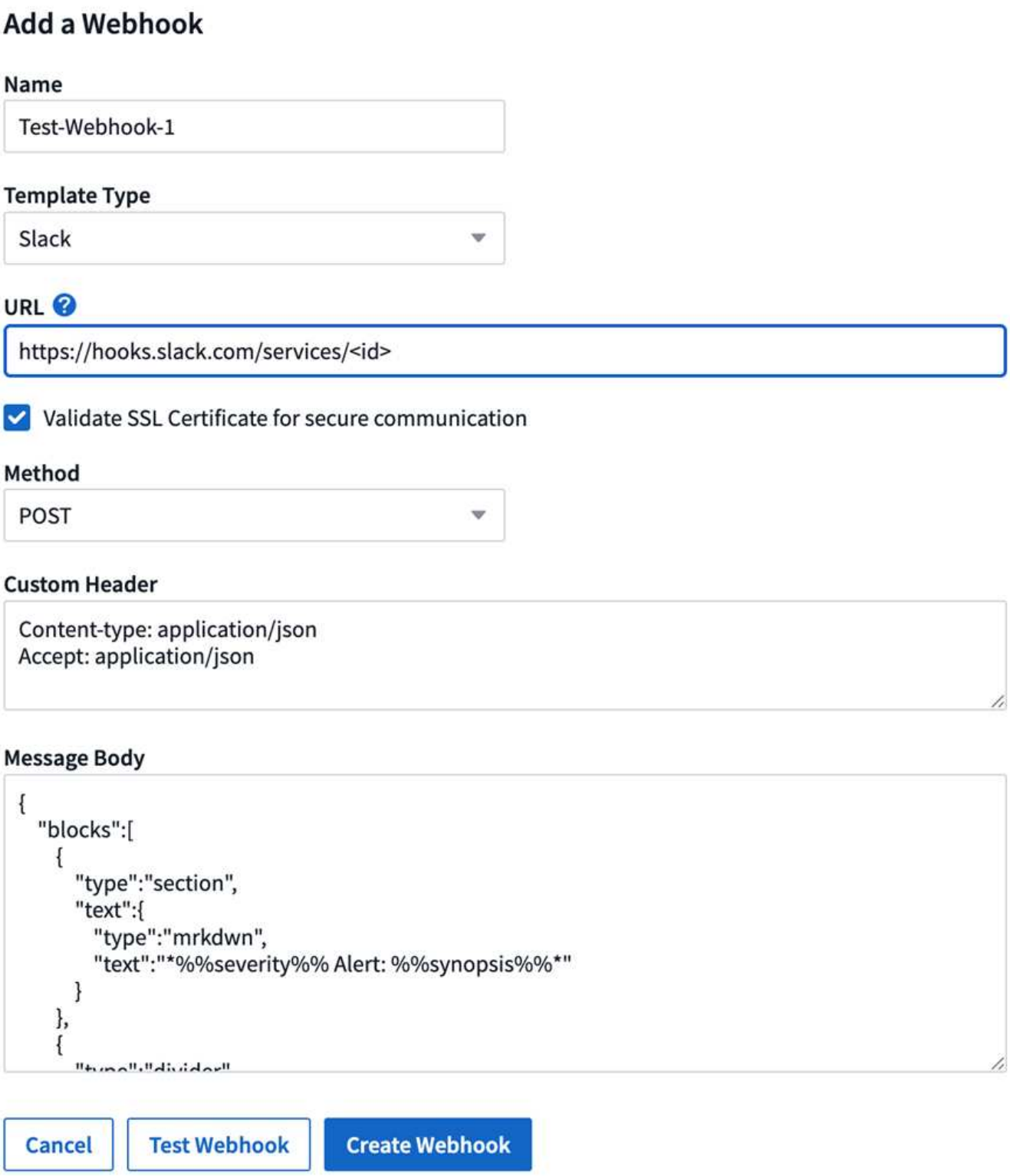
Webhook 通道實例由下列元素組成

Name	描述
網址	Webhook 目標 URL，包括 http:// 或 https:// 前綴以及 URL 參數
方法	GET/POST - 預設為 POST
自訂標題	在此處指定任何自訂標題
訊息正文	在此處填寫您的郵件正文
預設警報參數	列出 webhook 的預設參數
自訂參數和機密	自訂參數和秘密可讓您新增唯一參數和安全元素，例如密碼

創建 **webhook**

若要建立工作負載安全性 Webhook，請前往管理 > 通知並選擇「工作負載安全性 Webhook」標籤。下圖顯示了 Slack webhook 建立畫面的範例。

注意：使用者必須是工作負載安全性_管理員_才能建立和管理工作負載安全性 Webhook。



- 在每個欄位中輸入適當的信息，然後按一下「儲存」。
- 您也可以點擊「測試 Webhook」按鈕來測試連線。請注意，這將根據所選方法將「訊息正文」（不含替換）傳送到定義的 URL。
- SWS webhook 包含許多預設參數。此外，您還可以建立自己的自訂參數或秘密。

參數：它們是什麼以及如何使用它們？

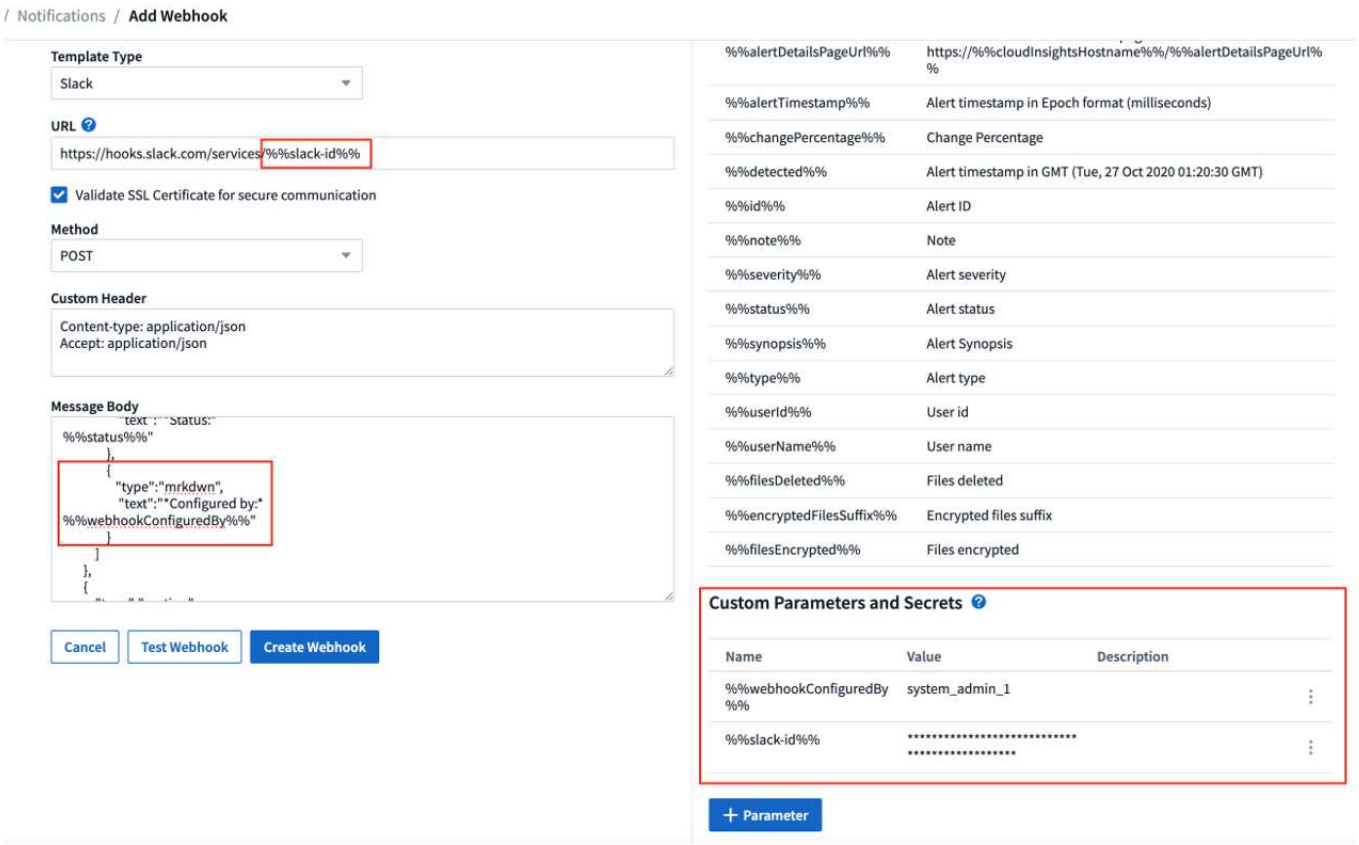
警報參數是每個警報填充的動態值。例如，*%%severity%%* 參數將被替換為警報的嚴重性類型。

請注意，按一下「測試 Webhook」按鈕時不會執行替換；測試會傳送有效負載，顯示參數的佔位符（*%%<param-name>%%*），但不會用資料取代它們。

自訂參數和機密

在本節中，您可以新增任何您想要的自訂參數和/或秘密。自訂參數或秘密可以位於 URL 或訊息正文中。秘密允許使用者配置安全的自訂參數，如密碼、apiKey 等。

下面的範例圖展示如何在 webhook 建立中使用自訂參數。



工作負載安全 **Webhook** 清單頁面

Webhooks 清單頁面顯示名稱、建立者、建立日期、狀態、安全性和上次報告欄位。注意：'status' 欄位的值會根據最後一個 webhook 觸發結果不斷變化。以下是狀態結果的範例。

地位	描述
好的	通知已成功發送。
403	禁止。
404	未找到 URL。

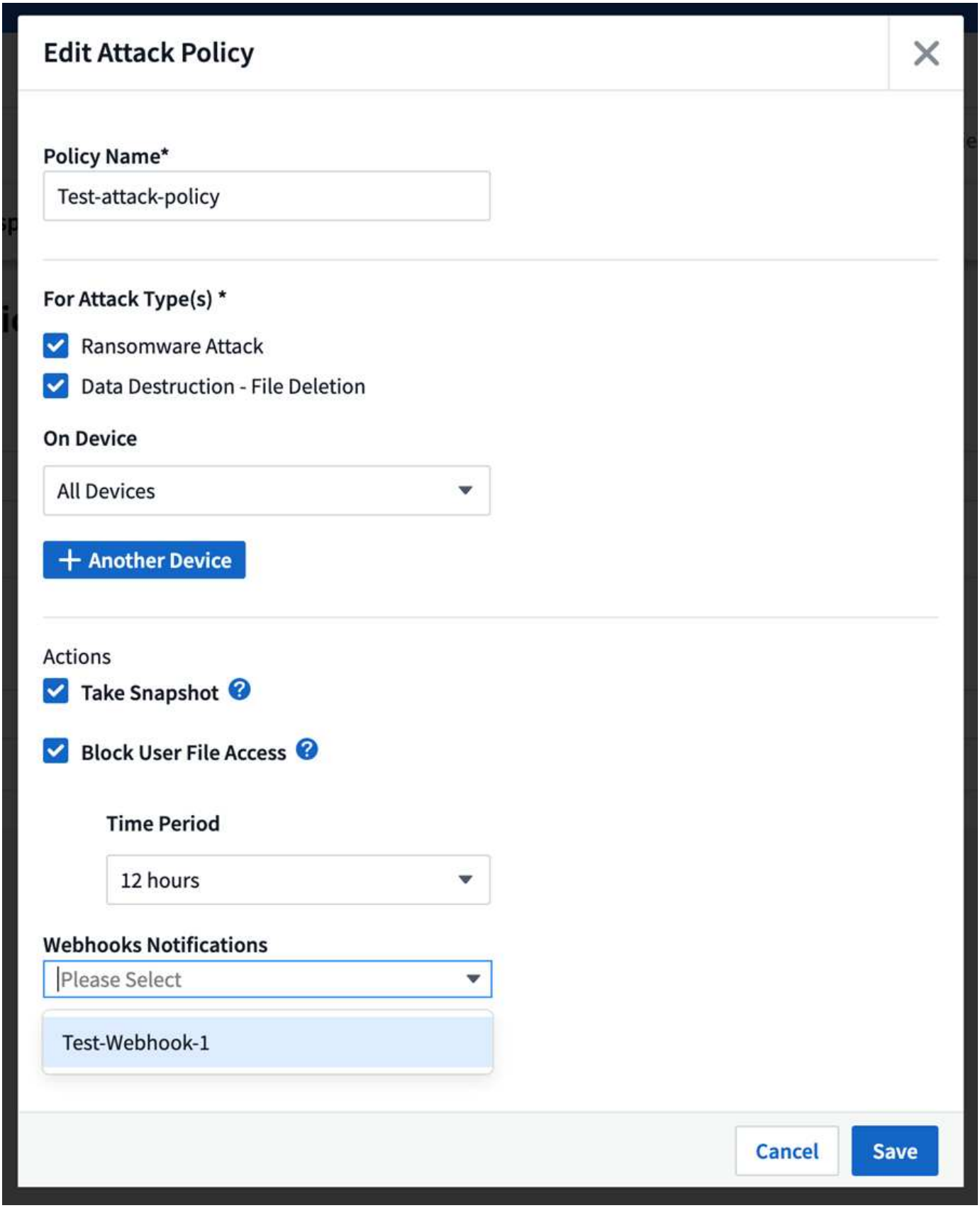
400	錯誤的請求。如果訊息正文中存在任何錯誤，您可能會看到此狀態，例如： • json 格式錯誤。 • 為保留鍵提供無效值。例如，PagerDuty 僅接受“嚴重性”為嚴重/警告/錯誤/訊息。任何其他結果都可能產生 400 狀態。 • 應用程式特定的驗證錯誤。例如，Slack 允許一個部分內最多有 10 個欄位。包含超過 10 個可能會導致 400 狀態。
410	資源不再可用

「上次報告」欄位表示 webhook 上次觸發的時間。

從 webhook 清單頁面，使用者還可以編輯/複製/刪除 webhook。

在警報策略中設定 **Webhook** 通知

若要將 webhook 通知新增至警報策略，請前往“工作負載安全性”>“策略”，然後選擇現有策略或新增策略。在「動作」部分 > “Webhook 通知」下拉式功能表中，選擇所需的 webhook。



Webhook 通知與策略相關。當攻擊（RW/DD/WARN）發生時，將採取配置的操作（拍攝快照/使用者封鎖），然後觸發相關的 webhook 通知。

注意：電子郵件通知與策略無關，它們將照常觸發。

- 如果策略暫停，則不會觸發 webhook 通知。
- 可以將多個 webhook 附加到單一策略，但建議將不超過 5 個 webhook 附加到策略。

工作負載安全性 **Webhook** 範例

Webhook 適用於"鬆弛"

Webhook 適用於"PagerDuty"Webhook 適用於"團隊"Webhook 適用於"不和諧"

Discord 的工作負載安全性 Webhook 範例

Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁提供了為 Discord 設定 webhook 的範例。

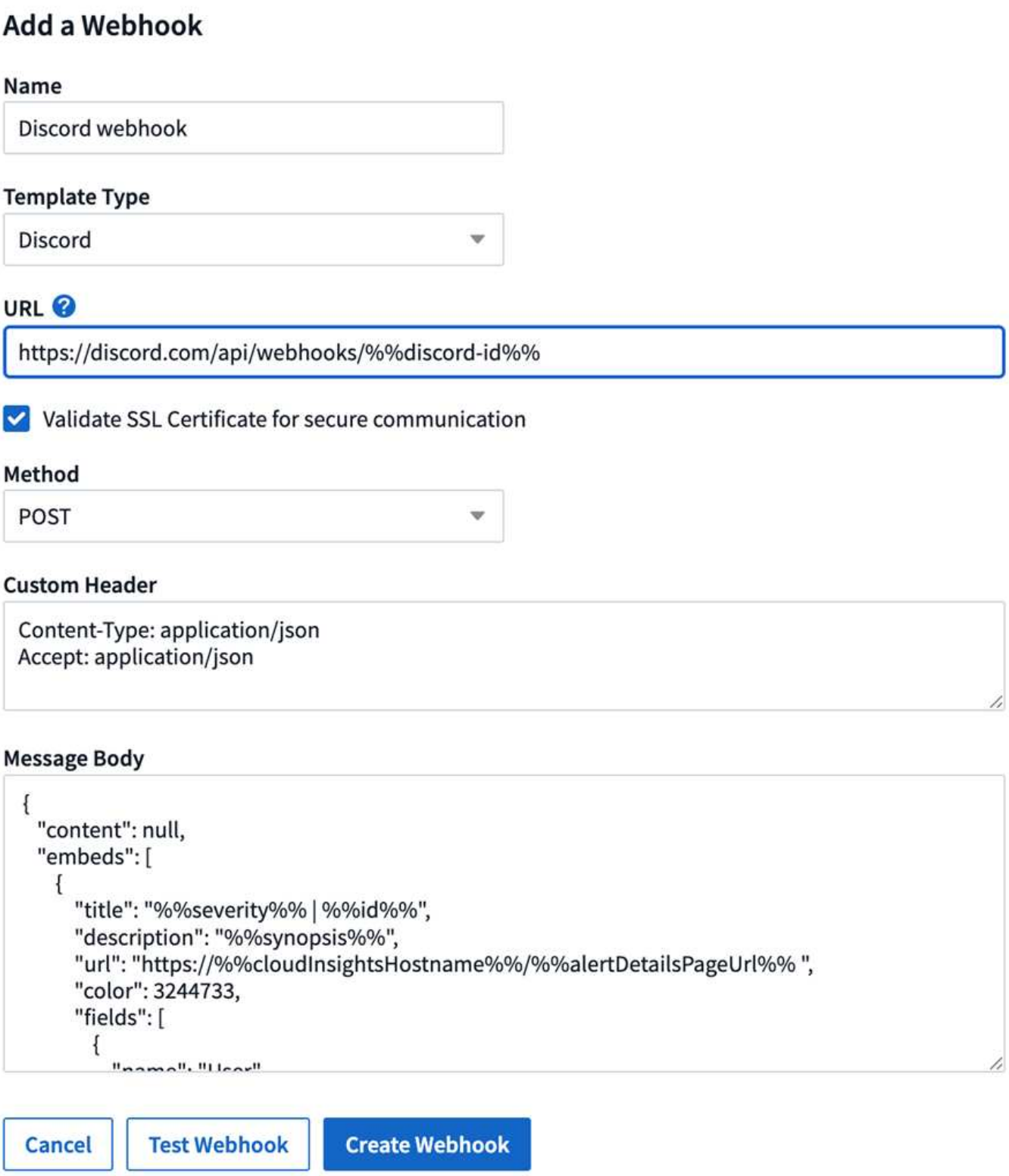
本頁引用第三方說明，這些說明可能會有所變更。請參閱"Discord 文件"以獲取最新資訊。

Discord 設定：

- 在 Discord 中，選擇伺服器，在文字頻道下，選擇編輯頻道（齒輪圖示）
- 選擇“整合”>“查看 Webhook”，然後按一下“新 Webhook”
- 複製 Webhook URL。您需要將其貼上到 Workload Security webhook 設定中。

建立工作負載安全性 **Webhook**：

1. 導覽至“管理”>“通知”，然後選擇“*Workload Security Webhooks*”標籤。點擊“+ Webhook”以建立一個新的 webhook。
2. 為 webhook 賦予一個有意義的名稱。
3. 在“模板類型”下拉式選單中，選擇“Discord”。
4. 將上面的 Discord URL 貼到 *URL* 欄位中。



為了測試 webhook，請暫時將訊息正文中的 URL 值替換為任何有效的 URL（例如 *https://netapp.com*），然後按一下 測試 *Webhook* 按鈕。 Discord 要求提供有效的 URL 才能讓測試 Webhook 功能正常運作。

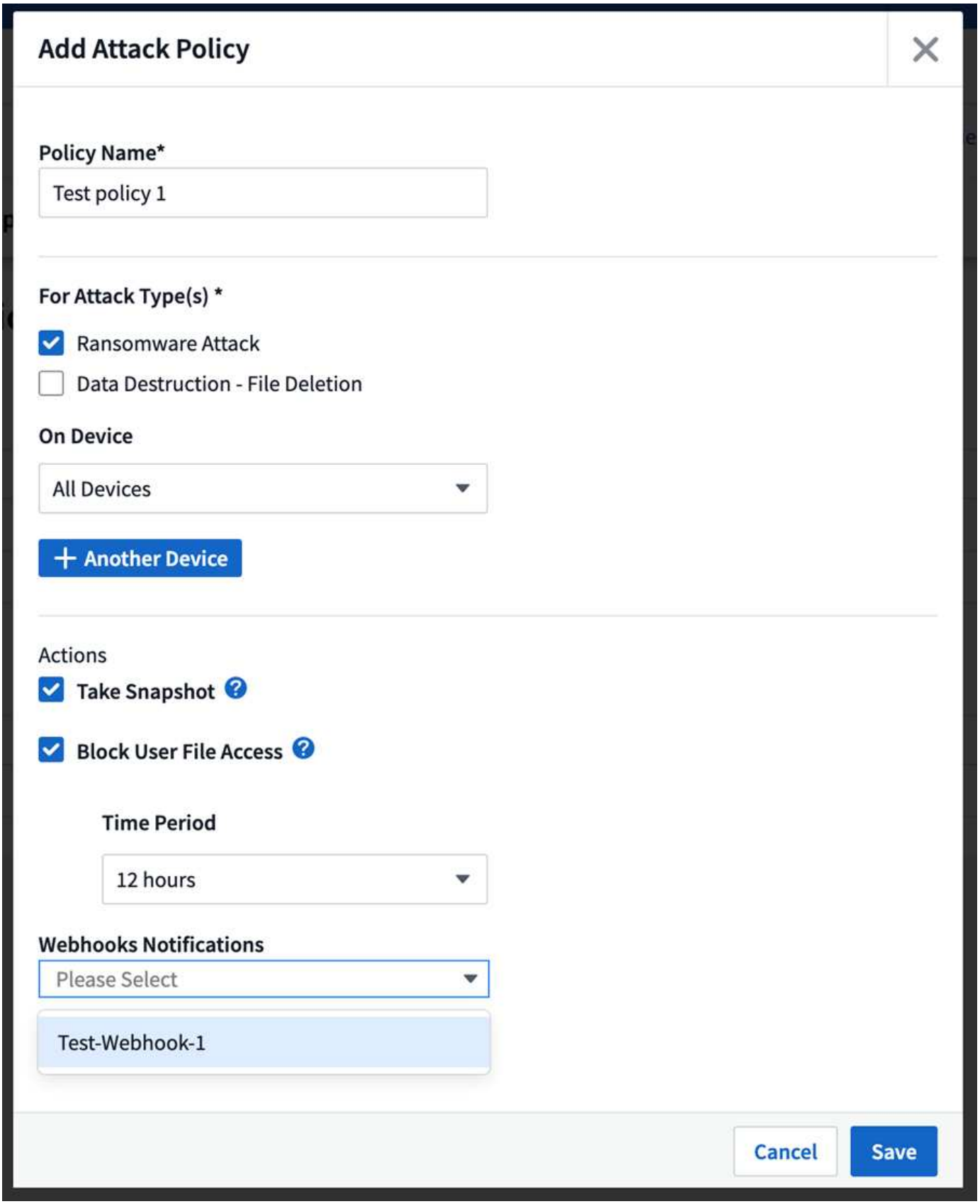
測試完成後，請務必將訊息正文重新設定。

透過 **Webhook** 發送通知

若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。按一下“+攻擊策略”或“+警告策略”。

- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。
- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 Discord webhook 並儲存。

注意：也可以透過編輯將 Webhook 附加到現有策略。



PagerDuty 的工作負載安全性 **Webhook** 範例

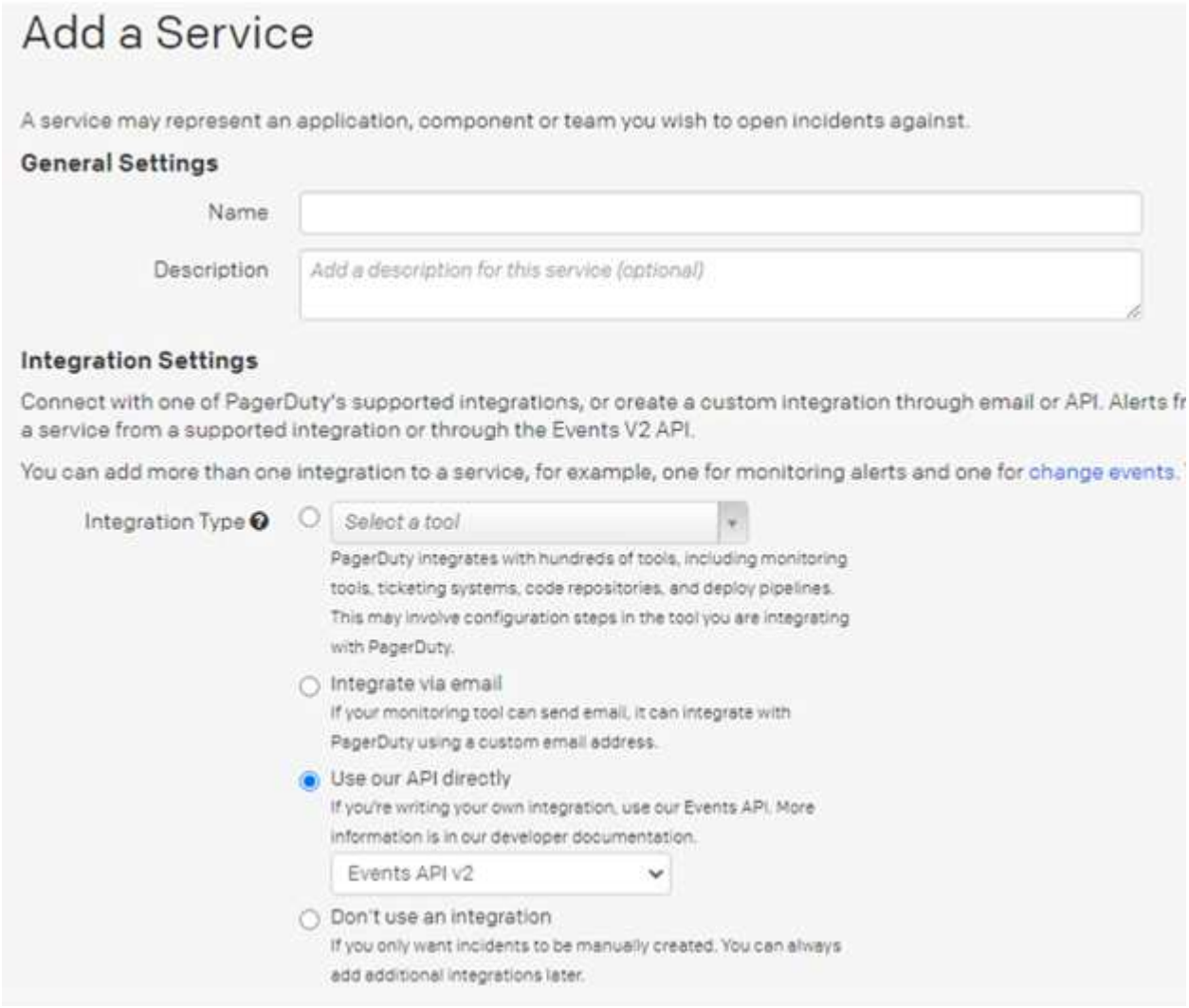
Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁面提

供了為 PagerDuty 設定 webhook 的範例。

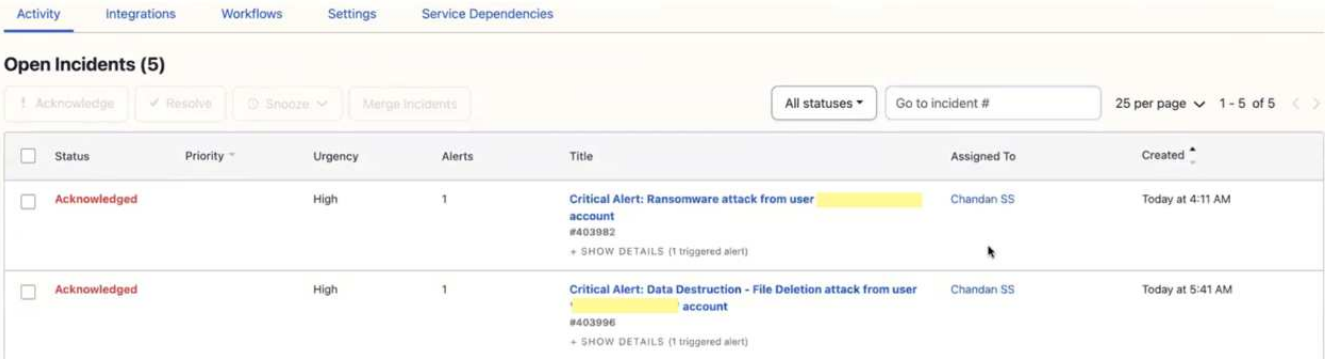
本頁引用第三方說明，可能會有變更。請參閱"PagerDuty 文檔"以獲取最新資訊。

PagerDuty 設定：

1. 在 PagerDuty 中，導覽至 服務 **>** 服務目錄 並點選 **+**新服務 按鈕。
2. 輸入_名稱_並選擇_直接使用我們的 API_。選擇“新增服務”。

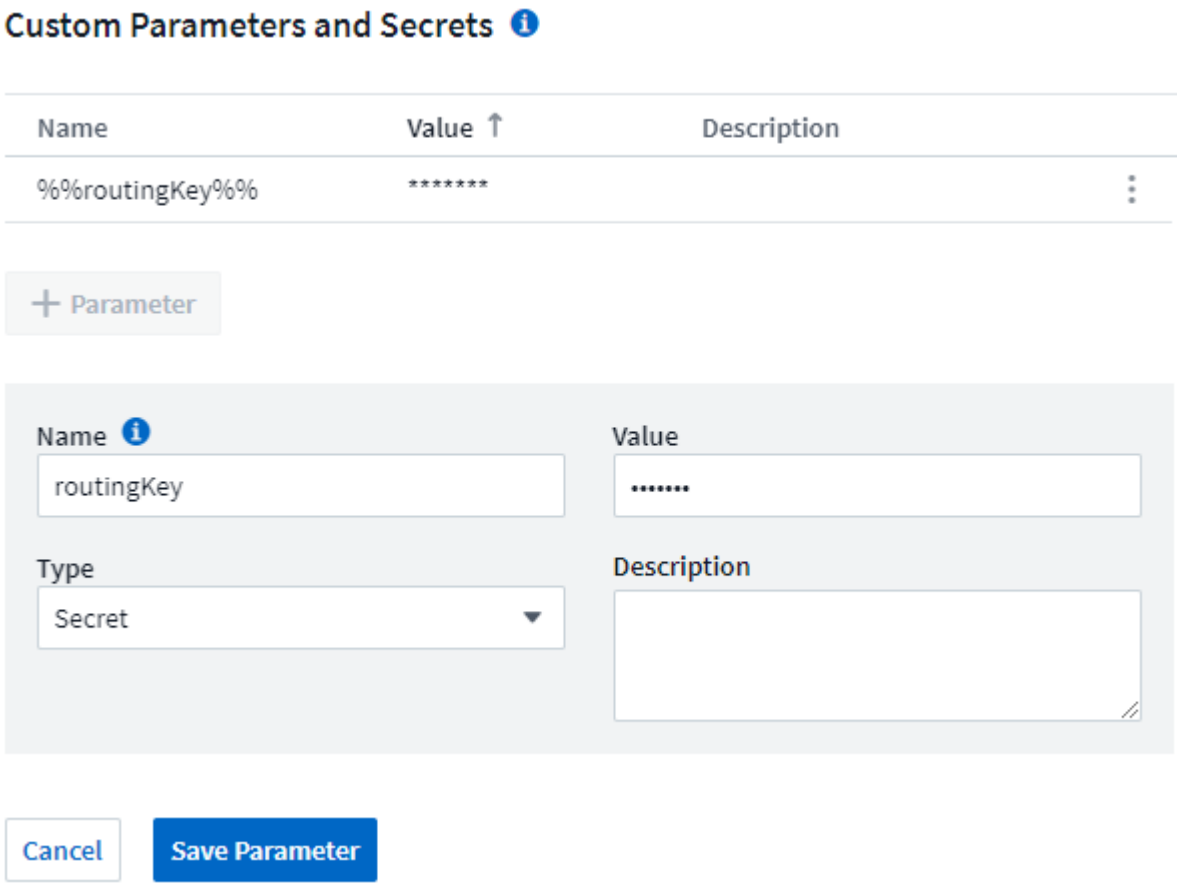


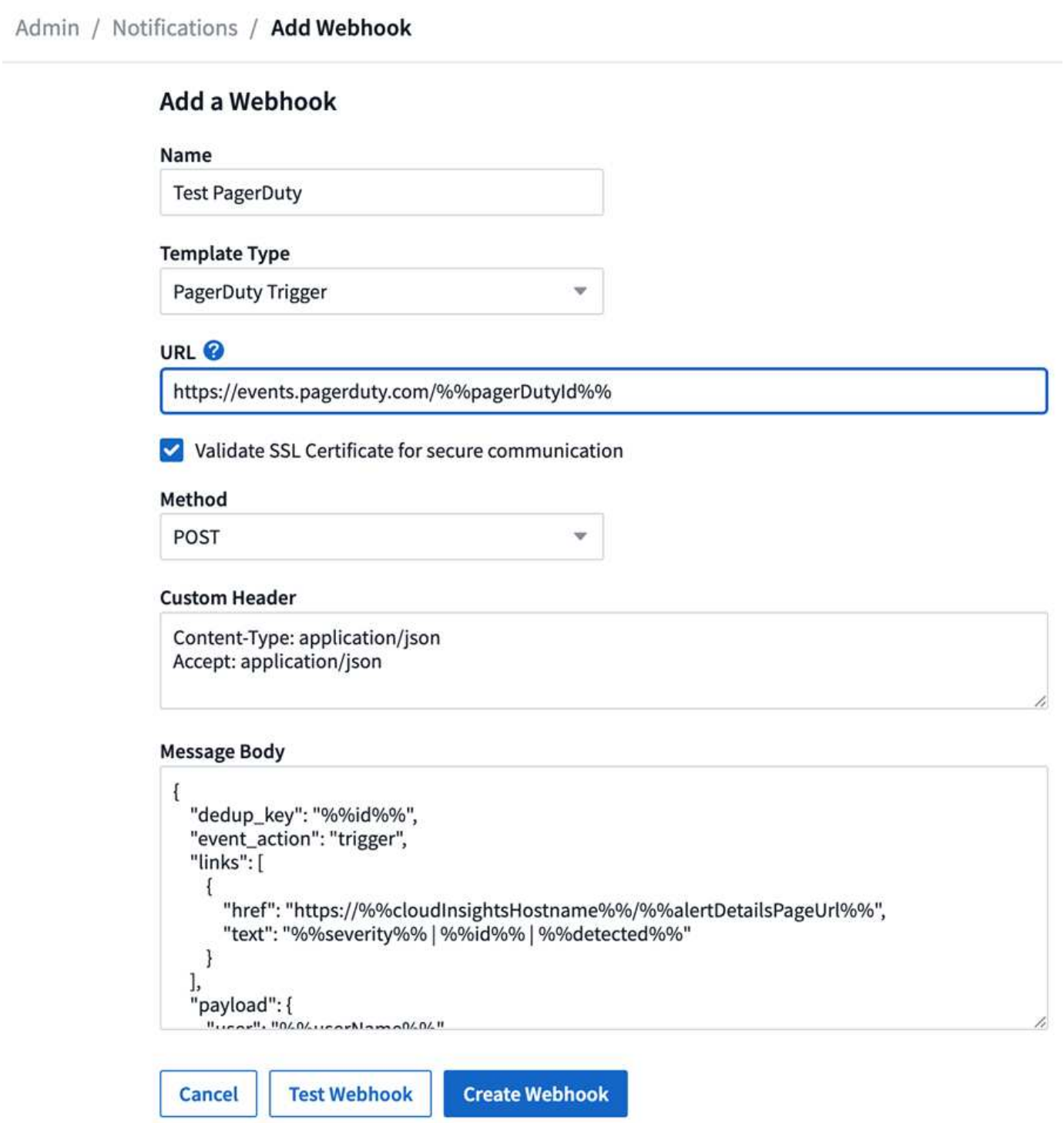
3. 選擇“Integrations”標籤來查看“Integration Key”。當您建立下面的工作負載安全 webhook 時，您將需要此金鑰。
4. 前往*事件*或*服務*查看警報。



建立工作負載安全性 **PagerDuty Webhook**：

- 導覽至“管理”>“通知”，然後選擇“*Workload Security Webhooks*”標籤。選擇“+ Webhook”來建立一個新的webhook。
- 為 webhook 賦予一個有意義的名稱。
- 在「範本類型」下拉式功能表中，選擇「PagerDuty 觸發器」。
- 建立一個名為_routingKey_的自訂參數金鑰，並將其值設為上面建立的PagerDuty_Integration Key_。

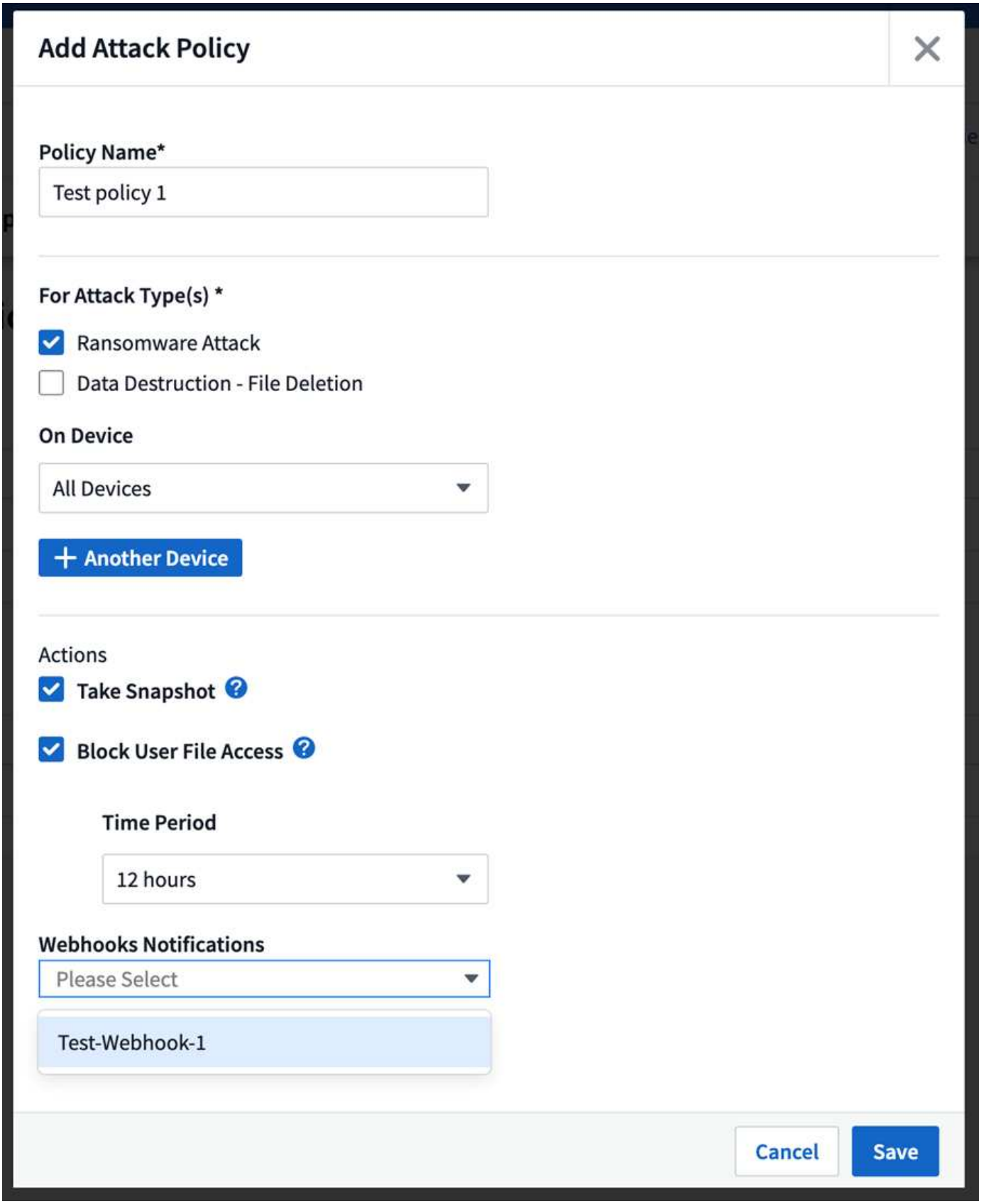




透過 **Webhook** 發送通知

- 若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。選擇“+攻擊策略”或“+警告策略”。
- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。
- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 PagerDuty webhook。保存策略。

注意：也可以透過編輯將 Webhook 附加到現有策略。



Slack 的工作負載安全性 **Webhook** 範例

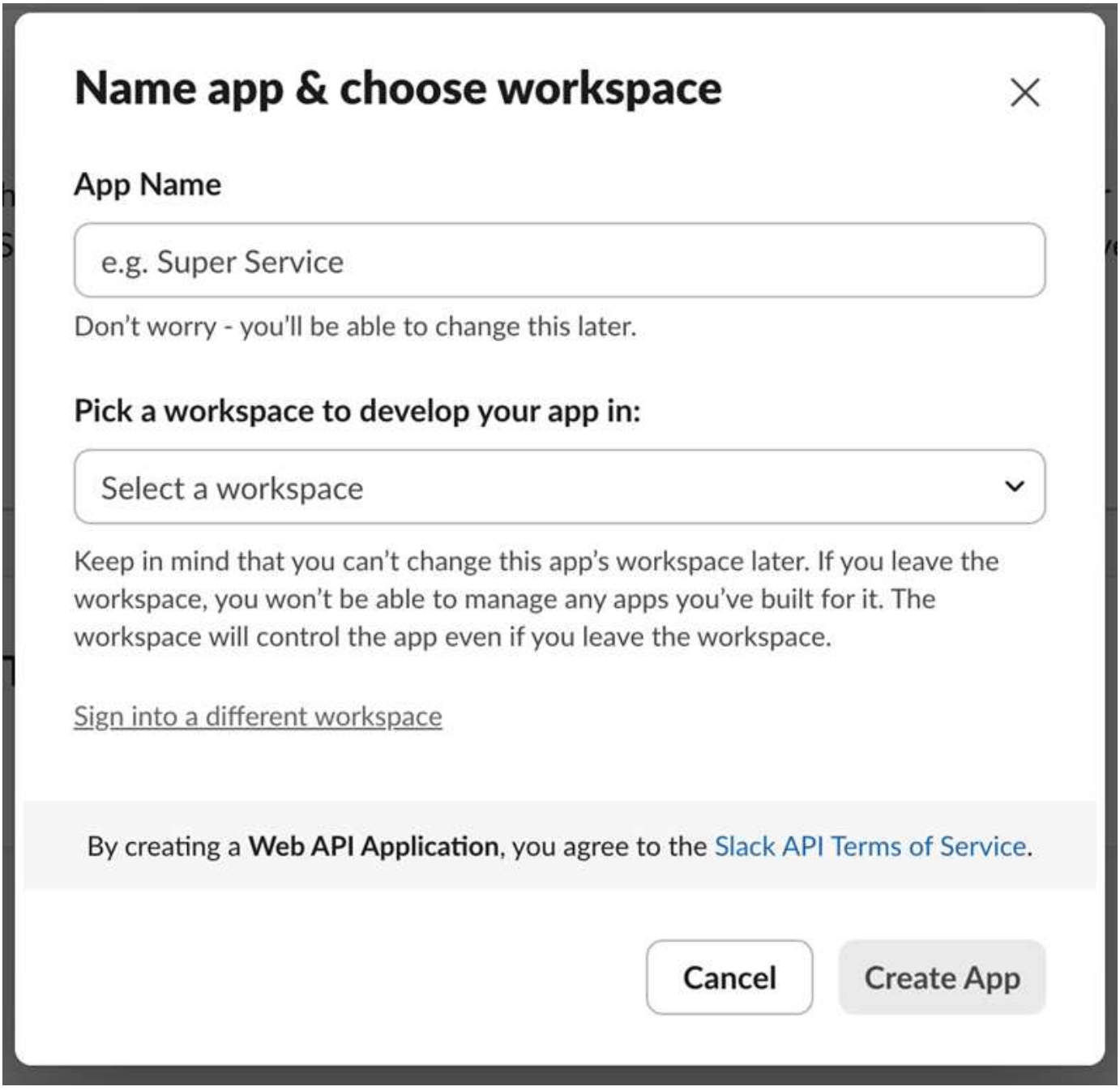
Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁提供

了為 Slack 設定 webhook 的範例。

本頁引用第三方說明，可能會有變更。請參閱 Slack 文件以獲取最新資訊。

Slack 範例

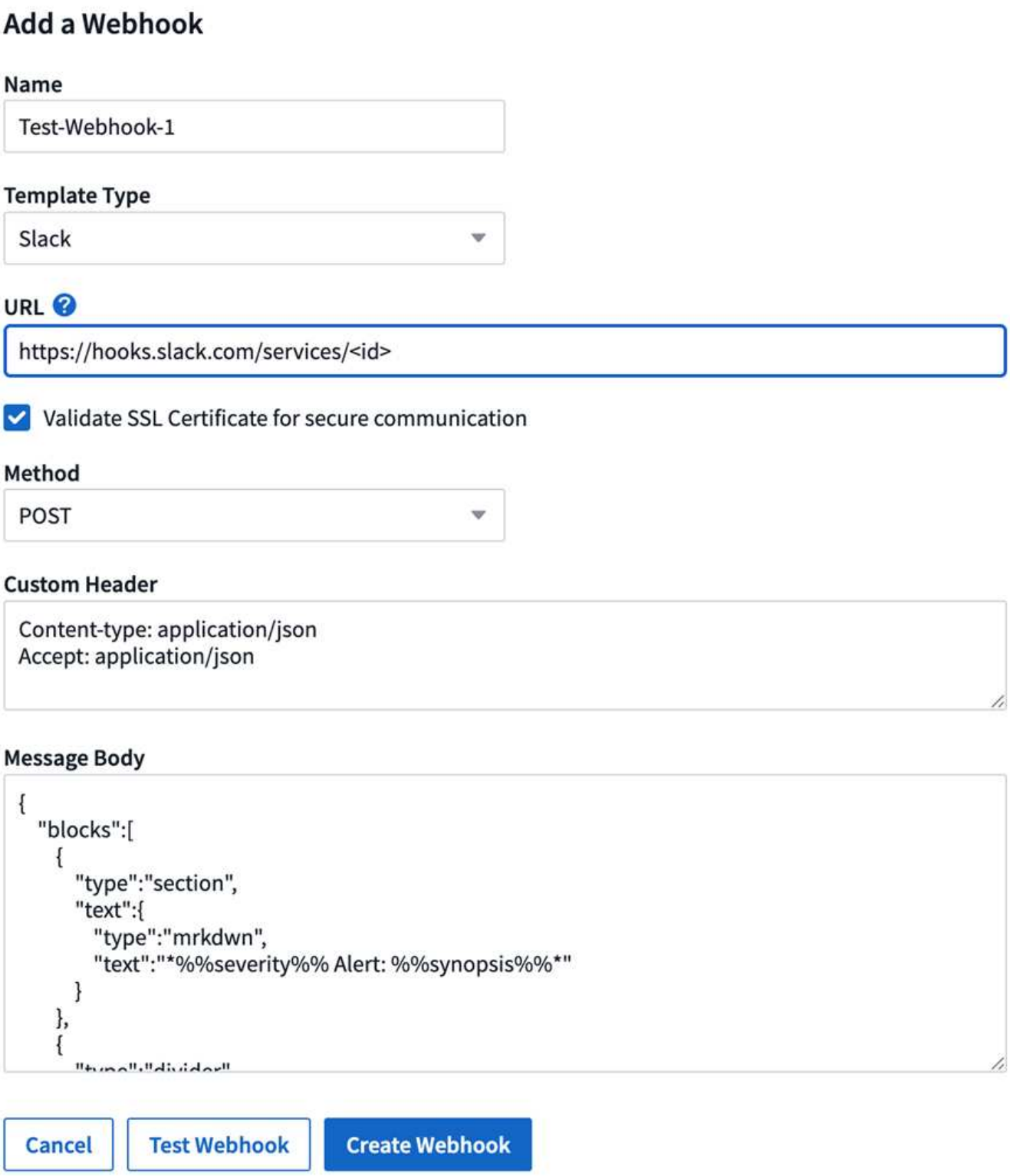
- 前往 https://api.slack.com/apps並創建一個新的應用程式。給它一個有意義的名字並選擇一個工作區。



- 前往傳入 Webhook，按一下_啟動傳入 Webhook_，選擇_新增 Webhook_，然後選擇要發佈的頻道。
- 複製 Webhook URL。建立工作負載安全性 webhook 時將提供此 URL。

建立工作負載安全性 **Slack Webhook**

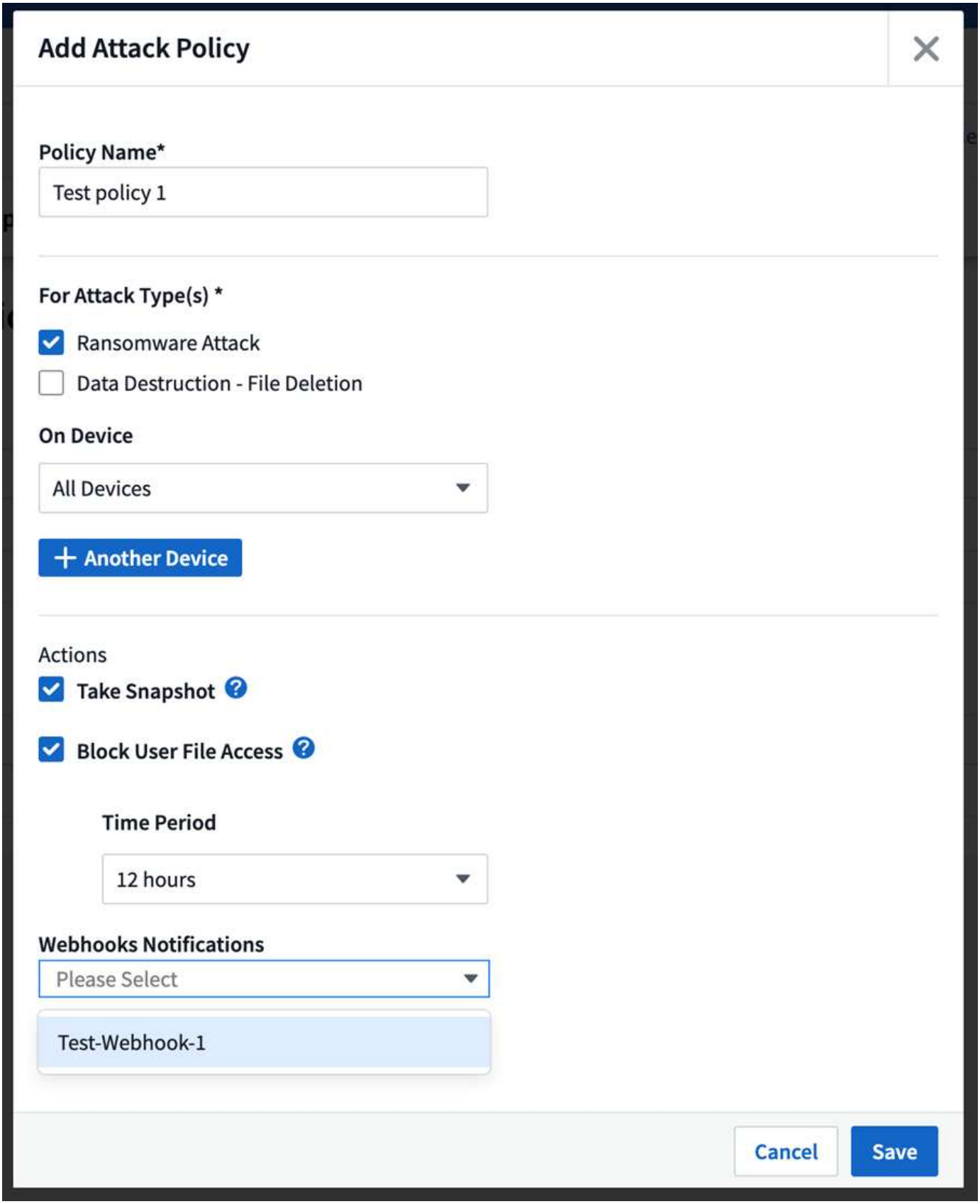
1. 導覽至“管理”>“通知”，然後選擇“*Workload Security Webhooks*”標籤。選擇 + *Webhook* 來建立一個新的 webhook。
2. 為 webhook 賦予一個有意義的名稱。
3. 在“模板類型”下拉式選單中，選擇“Slack”。
4. 貼上從上面複製的 URL。



透過 **webhook** 發送通知

- 若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。按一下“+攻擊策略”或“+警告策略”。
- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。
- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 webhook。保存策略。

注意：也可以透過編輯將 Webhook 附加到現有策略。



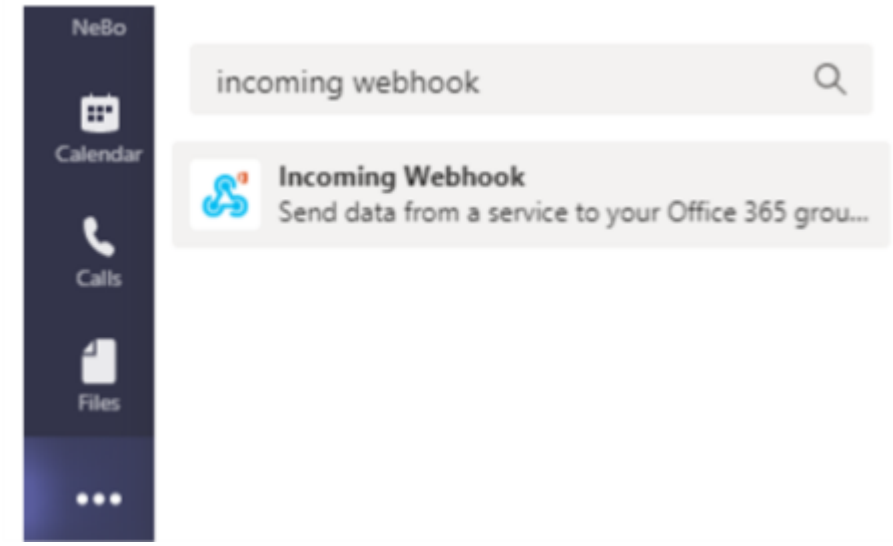
Microsoft Teams 的工作負載安全性 Webhook 範例

Webhook 允許使用者使用自訂的 webhook 通道向各種應用程式發送警報通知。本頁提供了為 Teams 設定 webhook 的範例。

本頁引用第三方說明，可能會有變更。請參閱"團隊文件"以獲取最新資訊。

團隊設定：

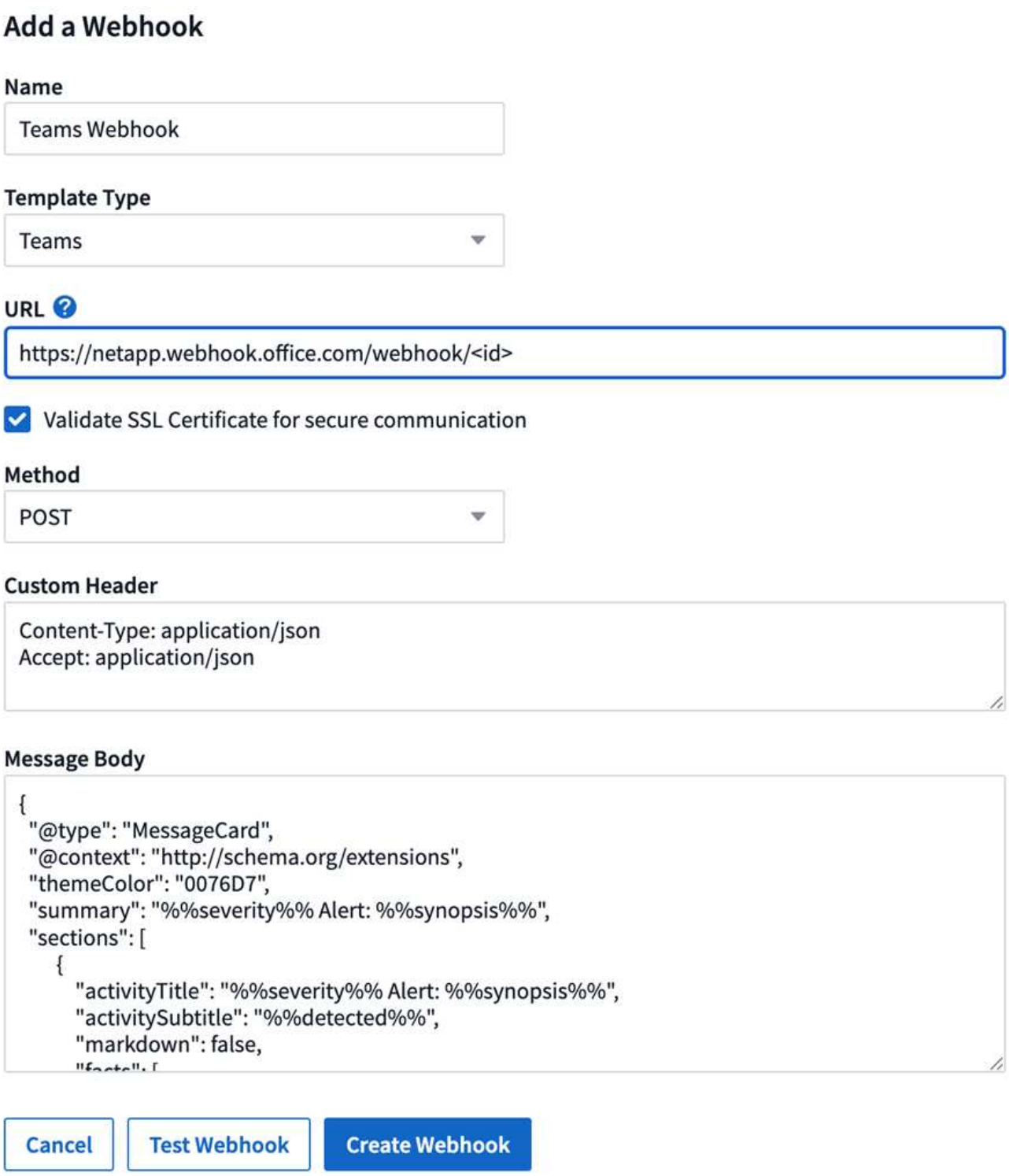
1. 在 Teams 中，選擇 kebab，然後搜尋 Incoming Webhook。



2. 選擇*新增至團隊>選擇團隊>設定連接器*。
3. 複製 Webhook URL。您需要將其貼上到 Workload Security webhook 設定中。

建立工作負載安全團隊 **Webhook**：

1. 導覽至“管理”>“通知”，然後選擇“工作負載安全性 Webhooks”標籤。選擇 *+ Webhook* 來建立一個新的 webhook。
2. 為 webhook 賦予一個有意義的名稱。
3. 在“模板類型”下拉式選單中，選擇“團隊”。



4. 將上面的 URL 貼到 *URL* 欄位中。

使用 **Adaptive Card** 範本建立 **Teams** 通知的步驟

1. 請將郵件內文替換為以下範本：

```
{
"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. 如果您使用的是 Power Automate Flows，URL 中的查詢參數採用編碼格式。您必須先解碼 URL 才能輸入。
3. 點擊「測試 Webhook」以確保沒有錯誤。
4. 儲存 webhook。

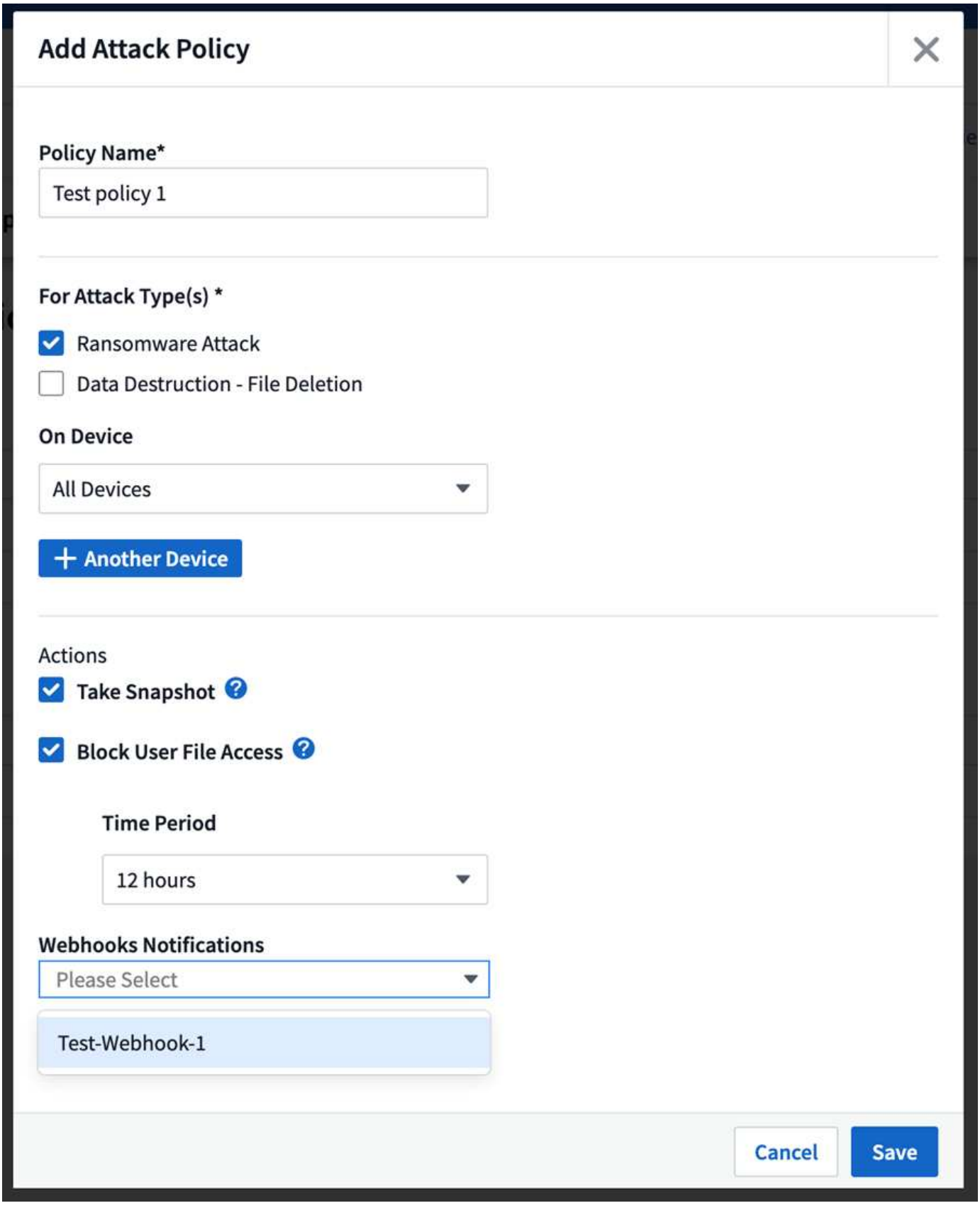
透過 **Webhook** 發送通知

若要透過 webhook 通知事件，請導覽至_工作負載安全性 > 策略_。選擇“+攻擊策略”或“+警告策略”。

- 輸入一個有意義的策略名稱。
- 選擇所需的攻擊類型、應附加策略的設備以及所需的操作。

- 在「Webhooks Notifications」下拉式功能表下，選擇所需的 Teams webhook。保存策略。

注意：也可以透過編輯將 Webhook 附加到現有策略。



工作負載安全 API

利用受安全性令牌認證保護的 REST API，將 Workload Security 整合到您的企業生態系統中。您可以檢索取證活動資料、管理 API 存取令牌，並與 CMDB、工單系統和其他應用程式開發自訂整合。互動式 Swagger 文件提供完整的 API 規範，並允許您直接測試端點。

API 存取要求：

- API 存取令牌模型用於授予存取權限。
- API 令牌管理由具有管理員角色的工作負載安全使用者執行。

API 文件（Swagger）

透過登入 Workload Security 並導覽至 **Admin > API Access** 可以找到最新的 API 資訊。按一下*API 文件*連結。 API 文件基於 Swagger，提供 API 的簡要描述和使用信息，並允許您在租戶上試用。

如果呼叫取證活動 API，請使用 cloudsecure_forensics.activities.**v2** API。如果您要多次呼叫此 API，請確保呼叫按順序進行，而不是並行。多次並行呼叫可能會導致 API 逾時。

API 存取令牌

在使用工作負載安全 API 之前，您必須建立一個或多個 **API** 存取權杖。存取令牌授予讀取權限。您也可以設定每個存取令牌的有效期。

若要建立存取權杖：

- 點選“管理”>“API 存取”
- 點選*+API 存取權令牌*
- 輸入*代幣名稱*
- 指定*令牌到期*

您的令牌僅可在建立過程中複製到剪貼簿並儲存。令牌一旦創建就無法檢索，因此強烈建議複製令牌並將其保存在安全的位置。系統將提示您按一下「複製 API 存取權杖」按鈕，然後才能關閉令牌建立畫面。

您可以停用、啟用和撤銷令牌。已禁用的令牌可以啟用。

令牌從客戶的角度授予對 API 的通用存取權限，管理其自身租用戶範圍內對 API 的存取。

使用者成功驗證並授權存取後，應用程式將收到存取令牌，然後在呼叫目標 API 時將存取令牌作為憑證傳遞。傳遞的令牌通知 API，令牌持有者已被授權存取 API 並根據授權期間授予的範圍執行特定操作。

傳遞存取令牌的 HTTP 標頭是 **X-CloudInsights-ApiKey:**

例如，使用以下命令檢索儲存資產：

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
```
其中 _<API_Access_Token>_ 是您在建立 API 存取金鑰期間所儲存的令牌，而 _<Workload Security Tenant>_ 是您的 Workload Security 環境的租用戶 URL。

詳細資訊可以在*管理 > API 存取*下的_API 文件_連結中找到。

透過 API 提取資料的腳本

工作負載安全代理程式包括一個匯出腳本，透過將請求的時間範圍劃分為更小的批次來促進對 v2 API 的平行呼叫。

該腳本位於 */opt/netapp/cloudsecure/agent/export-script*。同一目錄中的 README 檔案提供了使用說明。

以下是呼叫腳本的範例命令：

```
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
```

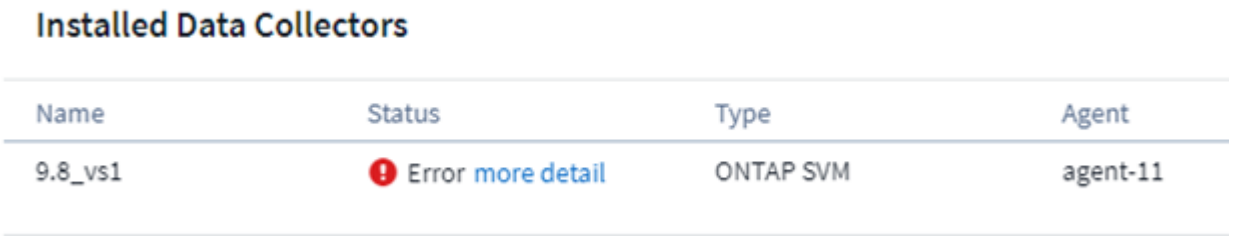
關鍵參數：- `--iteration_interval 12` ：將請求的時間範圍分成 12 小時的間隔。 - `--num_workers 3` ：使用 3 個執行緒並行取得這些間隔。

ONTAP SVM 資料收集器故障排除

工作負載安全使用資料收集器從設備收集文件和使用者存取資料。您可以在這裡找到解決此收集器問題的提示。

查看"配置 SVM 收集器"頁面以取得有關配置此收集器的說明。

如果發生錯誤，您可以按一下「已安裝的資料收集器」頁面的「狀態」列中的「詳細資訊」以了解有關錯誤的詳細資訊。



已知問題及其解決方案如下所述。

問題：*資料收集器運作一段時間後在隨機時間後停止，並發生故障：「錯誤訊息：連接器處於錯誤狀態。服務

名稱：審計。失敗原因：外部 **fpolicy** 伺服器超載。 」*試試看： ONTAP的事件率遠高於代理盒可以處理的事件率。因此連線被終止。

檢查斷開連接時 CloudSecure 中的峰值流量。您可以從 **CloudSecure > Activity Forensics > All Activity** 頁面進行檢查。

如果峰值聚合流量高於代理箱可以處理的流量，請參閱事件速率檢查器頁面，以了解如何確定代理箱中收集器的部署規模。

如果代理程式是在 2021 年 3 月 4 日之前安裝在代理框中的，請在代理框中執行以下命令：

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

調整大小後從 UI 重新啟動收集器。

{空的}

*問題：*收集器報告錯誤訊息：「在連接器上找不到可以到達 SVM 資料介面的本機 IP 位址」。 *試試看：*這很可能是由於ONTAP端的網路問題造成的。請依照以下步驟操作：

1. 確保 SVM 資料生命週期或管理生命週期上沒有防火牆阻止來自 SVM 的連線。
2. 透過叢集管理 IP 新增 SVM 時，請確保 SVM 的資料 lif 和管理 lif 可以從代理 VM ping 通。如果出現問題，請檢查網關、網路遮罩和路由。

   您也可以嘗試使用集群管理 IP 透過 ssh 登入集群，並 ping 代理 IP。確保代理 IP 可 ping 通：

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

   如果無法 ping 通，請確保ONTAP中的網路設定正確，以便 Agent 機器可以 ping 通。
3. 如果您嘗試透過 Cluster IP 連線但不成功，請嘗試直接透過 SVM IP 連線。請參閱上文以了解透過 SVM IP 連線的步驟。
4. 透過 SVM IP 和 vsadmin 憑證新增收集器時，檢查 SVM Lif 是否啟用了資料加管理角色。在這種情況下，ping 到 SVM Lif 將會起作用，但是 SSH 到 SVM Lif 將不起作用。如果是，請建立 SVM Mgmt Only Lif 並嘗試透過此 SVM 管理專用 Lif 進行連線。
5. 如果仍然不起作用，請建立新的 SVM Lif 並嘗試透過該 Lif 進行連線。確保子網路遮罩設定正確。
6. 進階調試：
   a. 在ONTAP中啟動資料包追蹤。
   b. 嘗試從 CloudSecure UI 將資料收集器連接到 SVM。
   c. 等待直到錯誤出現。在ONTAP中停止資料包追蹤。

d. 從ONTAP開啟資料包追蹤。可在此位置取得

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. 確保從ONTAP到代理框有一個 SYN。
.. 如果沒有來自ONTAP的 SYN，那麼這是ONTAP中的防火牆有問題。
.. 在ONTAP中開啟防火牆，以便ONTAP能夠連接代理盒。
```

7. 如果仍然不起作用，請諮詢網路團隊，以確保沒有外部防火牆阻止從ONTAP到代理盒的連線。
8. 如果以上方法都無法解決問題，請提交案例"Netapp 支持"以獲得進一步的幫助。

{空的}

問題：*訊息：「無法確定 [主機名稱：**<IP** 位址**>]** 的**ONTAP**類型。原因：與儲存系統 **<IP** 位址**>** 的連線錯誤：主機無法存取（主機無法存取）」*嘗試此操作：

1. 驗證是否提供了正確的 SVM IP 管理位址或叢集管理 IP。
2. 透過 SSH 連接到您要連接的 SVM 或叢集。連接後，請確保 SVM 或叢集名稱正確。

{空的}

問題：*錯誤訊息：「連接器處於錯誤狀態。服務名稱：審計。失敗原因：外部 **fpolicy** 伺服器終止。」 *試試這個：

1. 最有可能的是防火牆阻止了代理機器中的必要連接埠。驗證連接埠範圍 35000-55000/tcp 是否已打開，以便代理電腦從 SVM 進行連線。也要確保ONTAP端沒有啟用防火牆來阻止與代理機器的通訊。
2. 在代理框中輸入以下命令並確保連接埠範圍是開放的。

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

範例輸出應如下圖所示：

```
 -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
NEW -j ACCEPT
. 登入 SVM，輸入以下命令並檢查是否沒有設定防火牆來阻止與ONTAP 的通訊。
```

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

"檢查防火牆命令"在ONTAP方面。

3. 透過 SSH 連接到您要監控的 SVM/叢集。從 SVM 資料生命週期 (支援 CIFS、NFS 協定) 對代理程式盒執行 ping 操作，並確保 ping 操作正常：

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

如果無法 ping 通，請確保ONTAP中的網路設定正確，以便 Agent 機器可以 ping 通。

4. 如果透過 2 個資料收集器將單一 SVM 兩次新增至租用戶，則會顯示此錯誤。透過 UI 刪除其中一個資料收集器。然後透過 UI 重新啟動其他資料收集器。然後資料收集器將顯示“RUNNING”狀態並開始從 SVM 接收事件。

基本上，在一個租用戶中，應該只透過 1 個資料收集器添加 1 個 SVM 一次。 1 個 SVM 不應透過 2 個資料收集器添加兩次。

5. 如果在兩個不同的工作負載安全環境（租用戶）中新增了相同的 SVM，則最後一個 SVM 總是會成功。第二個收集器將使用自己的 IP 位址配置 fpolicy，並踢出第一個收集器。因此第一個收集器將停止接收事件，並且其「稽核」服務將進入錯誤狀態。為防止這種情況，請在單一環境上配置每個 SVM。
6. 如果服務策略配置不正確，也可能會出現此錯誤。使用ONTAP 9.8 或更高版本時，為了連接到資料來源收集器，需要 data-fpolicy-client 服務以及資料服務 data-nfs 和/或 data-cifs 。此外，data-fpolicy-client 服務必須與受監控 SVM 的資料生命週期相關聯。

{空的}

問題：*活動頁面中未顯示任何事件。 *試試這個：

1. 檢查ONTAP收集器是否處於「正在運作」狀態。如果是，則透過開啟一些檔案確保在 cifs 用戶端虛擬機器上產生一些 cifs 事件。
2. 如果沒有看到任何活動，請登入 SVM 並輸入以下命令。

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

請確保沒有與 fpolicy 相關的錯誤。

3. 如果沒有看到任何活動，請登入 SVM。輸入以下命令：

```
<SVM>fpolicy show
```

檢查以「cloudsecure_」為前綴的 fpolicy 政策是否已設定且狀態為「on」。如果未設置，那麼代理程式很可能無法執行 SVM 中的命令。請確保已遵循頁面開頭所述的所有先決條件。

{空的}

問題： SVM 資料收集器處於錯誤狀態，錯誤訊息為「代理無法連線到收集器」 嘗試下列操作：

1. 最有可能的是代理超載並且無法連接到資料來源收集器。
2. 檢查有多少個資料來源收集器連接到代理程式。
3. 也可以檢查 UI 中「所有活動」頁面的資料流量。
4. 如果每秒的活動數量非常高，請安裝另一個代理並將一些資料來源收集器移至新的代理程式。

{空的}

問題： SVM 資料收集器顯示錯誤訊息為「fpolicy.server.connectError：節點無法與 FPolicy 伺服器「12.195.15.146」建立連線（原因：「選擇逾時」）」 嘗試此操作： SVM/Cluster 中啟用了防火牆。因此 fpolicy 引擎無法連接到 fpolicy 伺服器。 ONTAP中可用於取得更多資訊的 CLI 包括：

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

"檢查防火牆命令"在ONTAP方面。

{空的}

*問題：*錯誤訊息：「連接器處於錯誤狀態。服務名稱：審計。失敗原因：在 SVM 上找不到有效的資料介面（角色：資料、資料協定：NFS 或 CIFS 或兩者、狀態：啟動）。 *試試看：*確保有一個操作介面（具有資料角色和 CIFS/NFS 資料協定）。

{空的}

---

*問題：*資料收集器進入錯誤狀態，一段時間後進入運作狀態，然後再次傳回錯誤狀態。如此循環往復。 *試試看：*這通常發生在以下場景：

1. 新增了多個數據收集器。
2. 表現出這種行為的資料收集器將會有 1 個 SVM 加入這些資料收集器。意思是 2 個或更多資料收集器連接到 1 個 SVM。
3. 確保 1 個資料收集器僅連接到 1 個 SVM。
4. 刪除連接到相同 SVM 的其他資料收集器。

{空的}

問題：*連接器處於錯誤狀態。服務名稱：審計。失敗原因：無法設定（**SVM svmname** 上的策略）。原因：在「**fpolicy.policy.scope-modify: “Federal”**中為**“shares-to-include”**元素指定的值無效*嘗試此操作： *共享名稱需要不帶任何引號。編輯ONTAP SVM DSC 配置以更正共享名稱。

_包括和排除共享_不適用於較長的共享名稱清單。如果您需要包含或排除大量股票，請使用按數量過濾。

{空的}

---

*問題：*集群中存在未使用的現有 fpolicies。在安裝 Workload Security 之前該做什麼？ *試試看：*建議刪除所有現有的未使用的 fpolicy 設置，即使它們處於斷開連接狀態。工作負載安全性將建立帶有前綴“cloudsecure_”的 fpolicy。所有其他未使用的 fpolicy 配置都可以刪除。

顯示 fpolicy 清單的 CLI 指令：

```
 fpolicy show
```

刪除 `fpolicy` 配置的步驟：

```
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>
```

{空的}

---

*問題：*啟用工作負載安全後， ONTAP效能受到影響：延遲偶爾會升高，IOPS 偶爾會降低。 *試試看這個：*在使用ONTAP和工作負載安全時，有時會在ONTAP中看到延遲問題。造成這種情況可能有以下幾個原因："1372994" ， "1415152" ， "1438207" ， "1479704" ， "1354659" 。所有這些問題均已在ONTAP 9.13.1 及更高版本中修復；強烈建議使用其中一個更高版本。

{空的}

問題：*資料收集器顯示錯誤訊息：「錯誤：兩次重試後無法確定收集器的健康狀況，請嘗試重新啟動收集器（錯誤代碼：**AGENT008**）」。 *試試這個：

1. 在資料收集器頁面上，捲動到出現錯誤的資料收集器的右側，然後按一下 3 個點選單。選擇“編輯”。再次輸入資料擷取器的密碼。按下「儲存」按鈕儲存資料收集器。數據收集器將重新啟動並且錯誤應該解決。
2. 代理機器可能沒有足夠的 CPU 或 RAM 空間，這就是 DSC 失敗的原因。請檢查機器中新增到代理程式的資料收集器的數量。如果超過20，請增加Agent機器的CPU和RAM容量。一旦 CPU 和 RAM 增加，DSC 將自動進入初始化狀態，然後進入運作狀態。查看尺寸指南"本頁"。

{空的}

---

*問題：*選擇 SVM 模式時資料收集器發生錯誤。 *試試看：*在 SVM 模式下連接時，如果使用叢集管理 IP 而不

是 SVM 管理 IP 進行連接，則連接將會出錯。確保使用正確的 SVM IP。

{空的}

---

*問題：*啟用「拒絕存取」功能時，資料收集器顯示錯誤訊息：「連接器處於錯誤狀態。服務名稱：審計。失敗原因：無法在 SVM test_svm 上配置 fpolicy。原因：用戶未獲得授權。」 *試試看：*使用者可能缺少「拒絕存取」功能所需的 REST 權限。請按照"本頁"設定權限。

設定權限後重新啟動收集器。

{空的}

問題： 收集器處於錯誤狀態，訊息為：連接器處於錯誤狀態。 失敗原因：無法在 SVM <SVM 名稱> 上配置持久性儲存。 原因：無法在 SVM“<SVM Name>”中找到磁碟區“<volumeName>”的合適聚合。 原因：聚合「<aggregateName>」的效能資訊目前不可用。 請稍等幾分鐘，然後再次嘗試該命令。服務名稱：審計。失敗原因：無法在 SVM <SVM Name> 上設定持久性儲存區。原因：無法在 SVM "<SVM Name>" 中找到適合的集合體以用於磁碟區 "<volumeName>"。原因：目前無法取得集合體 "<aggregateName>" 的效能資訊。請稍候幾分鐘，然後再次嘗試該指令。

*試試這個方法：*等待幾分鐘，然後重新啟動收集器。

{空的}

如果您仍然遇到問題，請聯絡*幫助>支援*頁面中提到的支援連結。