工作負載安全

Data Infrastructure Insights

NetApp
January 17, 2025

目錄

工作負載安全

關於儲存工作負載安全性

資料基礎架構洞見儲存工作負載安全性（前身為 Cloud Secure ）可針對內部威脅提供可據以行動的情報、協助保護您的資料。它可集中監控所有企業資料在混合雲環境中的存取、確保達成安全性與法規遵循目標。

可見度

集中可見度並控制使用者對儲存在內部部署或雲端的重要企業資料的存取。

取代無法提供即時且準確的資料存取與控制可見度的工具和手動程序。工作負載安全功能可在雲端和內部部署儲存系統上進行獨特作業、為您提供惡意使用者行為的即時警示。

保護

透過進階的機器學習和異常偵測功能、保護組織資料免遭惡意或遭入侵的使用者濫用。

透過進階機器學習和異常偵測使用者行為、警示您任何異常的資料存取。

法規遵循

稽核使用者資料存取儲存在內部部署或雲端的關鍵企業資料、確保企業符合法規要求。

快速入門

工作負載安全入門

您必須先完成一些組態工作、才能開始使用工作負載安全功能來監控使用者活動。

工作負載安全系統使用代理程式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。

您必須先設定下列項目、才能開始收集資料：

工作	相關資訊
設定代理程式	"代理程式需求" "新增代理程式" "影片：代理程式部署"
設定使用者目錄連接器	"新增使用者目錄連接器" "影片：Active Directory連線"
設定資料收集器	按一下 * 工作負載安全性 > 收集器 * 按一下您要設定的資料收集器。請參閱文件的資料收集器廠商參考資料一節。"影片 ONTAP ：SVM連線"

建立使用者帳戶	"管理使用者帳戶"
疑難排解	"影片：疑難排解"

工作負載安全功能也能與其他工具整合。例如，"請參閱本指南"與 Splunk 整合。

工作負載安全代理程式需求

您必須"安裝代理程式"從資料收集器取得資訊。在安裝代理程式之前、您應確保環境符合作業系統、CPU、記憶體及磁碟空間的需求。

元件	**Linux**需求
作業系統	執行下列其中一項授權版本的電腦： * CentOS 8 Stream （64 位元），CentOS 9 Stream ， SELinux * openSUSE Leap15.3 至 15.5 （64 位元） * Oracle Linux 8.6 至 8.8 ， 9.1 至 9.4 （64 位元） * Red Hat Enterprise Linux 8.6 至 8.8 ， 9.1 至 9.4 （64 位元），SELinux建議使用專屬伺服器。
命令	安裝時需要「解壓縮」。此外、安裝、執行指令碼及解除安裝時、還需要使用「su–」命令。
CPU	4個CPU核心
記憶體	16 GB RAM
可用磁碟空間	磁碟空間應以下列方式分配： NetApp 36 GB （檔案系統建立後至少有 35 GB 可用空間）注意：建議您分配額外的磁碟空間，以便建立檔案系統。確定檔案系統中至少有 35 GB 可用空間。如果 /opt 是 NAS 儲存設備的掛載資料夾、請確定本機使用者可以存取此資料夾。如果本機使用者沒有此資料夾的權限，則代理程式或資料收集器可能無法安裝。如需詳細資訊，請參閱"疑難排解"一節。
網路	100 Mbps至1 Gbps乙太網路連線、靜態IP位址、所有裝置的IP連線、以及工作負載安全性執行個體（80或443）所需的連接埠。

請注意：工作負載安全代理程式可安裝在與 Data Infrastructure Insights 擷取單元和 / 或代理程式相同的機器上。不過、最好將這些安裝在不同的機器上。如果這些安裝在同一部機器上、請如下所示分配磁碟空間：

可用磁碟空間	對於Linux、應以下列方式配置磁碟空間：/opp/netapp 25-30 GB /var/log/netapp 25 GB

其他建議

- 強烈建議ONTAP 您使用*網路時間傳輸協定（NTP）或*簡易網路時間傳輸協定（**SNTP**）、同步化支援系統和代理機器上的時間。

雲端網路存取規則

對於*美國型*工作負載安全環境：

傳輸協定	連接埠	來源	目的地	說明
TCP	443	工作負載安全代理程式	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	存取 Data Infrastructure Insights
TCP	443	工作負載安全代理程式	gateway.C01.cloudinses.com/cloudamse.com.comagentlogin.cs01.cloudinses.cloudinses.com NetApp NetApp	存取驗證服務

對於*歐洲型*工作負載安全環境：

傳輸協定	連接埠	來源	目的地	說明
TCP	443	工作負載安全代理程式	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	存取 Data Infrastructure Insights
TCP	443	工作負載安全代理程式	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	存取驗證服務

對於* APAC型*工作負載安全環境：

傳輸協定	連接埠	來源	目的地	說明
TCP	443	工作負載安全代理程式	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	存取 Data Infrastructure Insights
TCP	443	工作負載安全代理程式	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	存取驗證服務

網路內規則

傳輸協定	連接埠	來源	目的地	說明
TCP	389（LDAP）636（LDAPS / start-TLS）	工作負載安全代理程式	LDAP伺服器URL	連線至LDAP
TCP	443	工作負載安全代理程式	叢集或SVM管理IP位址（視SVM收集器組態而定）	API與ONTAP NetApp通訊
TCP	35000 - 55000	SVM資料LIF IP位址	工作負載安全代理程式	從 ONTAP 到工作負載安全代理程式的 Fpolicy 事件通訊。這些連接埠必須向工作負載安全性代理程式開啟、 ONTAP 才能傳送事件給它、包括工作負載安全性代理程式本身的任何防火牆（若有）。請注意、您不需要保留 * 所有 * 這些連接埠、但您為此保留的連接埠必須在此範圍內。建議您先保留約 100 個連接埠、必要時增加。
TCP	7	工作負載安全代理程式	SVM資料LIF IP位址	從 Agent 回應至 SVM Data 生命
SSH	22	工作負載安全代理程式	叢集管理	CIFS/SMB 使用者封鎖所需。

系統規模調整

請參閱"事件率檢查器"文件以取得有關規模調整的資訊。

工作負載安全代理程式安裝

「工作負載安全性」（前身Cloud Secure 為「功能」）會使用一或多個代理程式來收集使用者活動資料。代理程式會連線至租戶上的裝置，並收集傳送至工作負載安全 SaaS 層的資料以供分析。請參閱"代理程式需求"以設定代理程式 VM 。

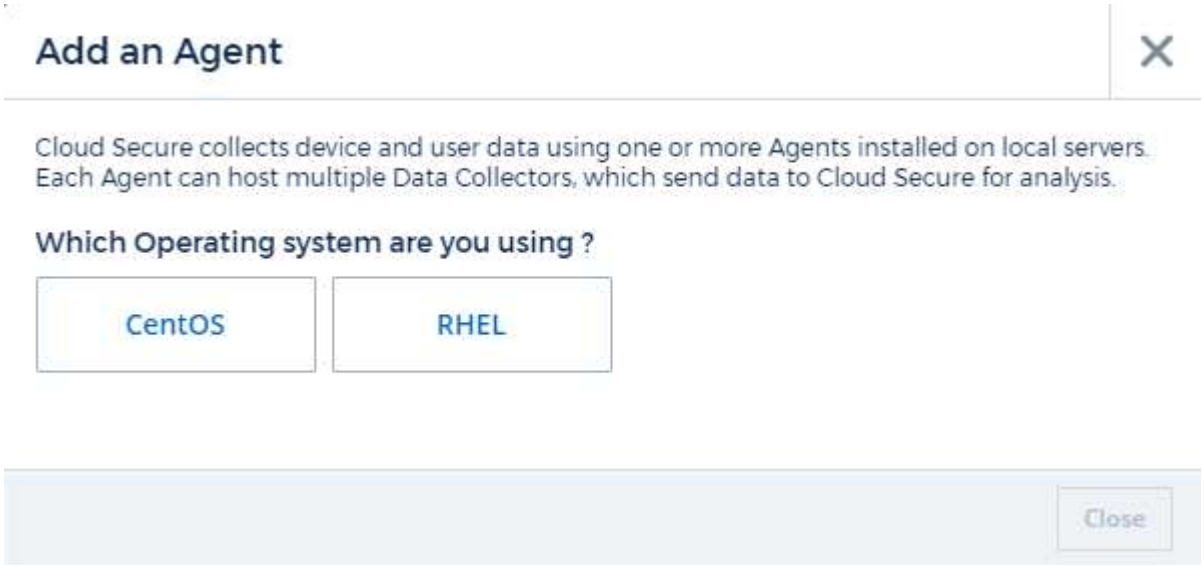
開始之前

- 安裝、執行指令碼及解除安裝時、都需要使用Sudo權限。
- 安裝代理程式時、會在機器上建立本機使用者_cssy和本機群組_*cssy*。如果權限設定不允許建立本機使用者、而需要Active Directory、則必須在Active Directory伺服器中建立使用者名稱為_cssy__的使用者。
- 您可以閱讀 Data Infrastructure Insights 安全性"請按這裡"。

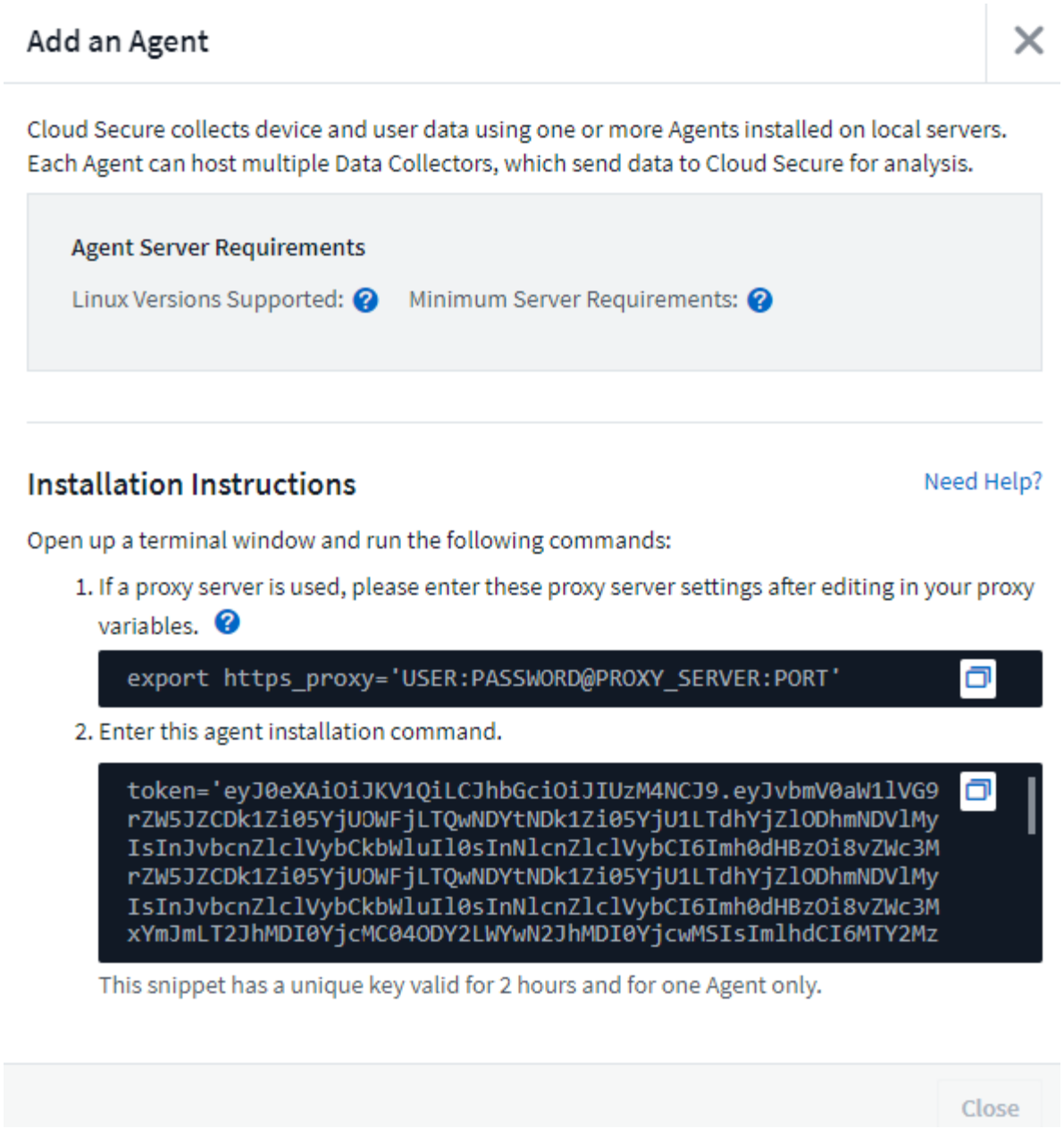
安裝代理程式的步驟

1. 以系統管理員或帳戶擁有者身分登入工作負載安全環境。
2. 選取 * 收集器 > 值機員 > + 值機員 *

   系統會顯示「新增代理程式」頁面：



3. 確認代理伺服器符合最低系統需求。
4. 若要驗證代理伺服器是否執行支援的Linux版本、請按一下_versions Supported（i）_。
5. 如果您的網路使用Proxy伺服器、請依照Proxy一節中的指示來設定Proxy伺服器詳細資料。



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. 安裝成功完成時、系統會顯示下列訊息：

完成後

1. 您需要設定"使用者目錄收集器"。
2. 您需要設定一或多個資料收集器。

網路組態

在本機系統上執行下列命令、以開啟工作負載安全性所使用的連接埠。如果對連接埠範圍有安全顧慮、您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`

依照您的平台執行後續步驟：

- 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
```

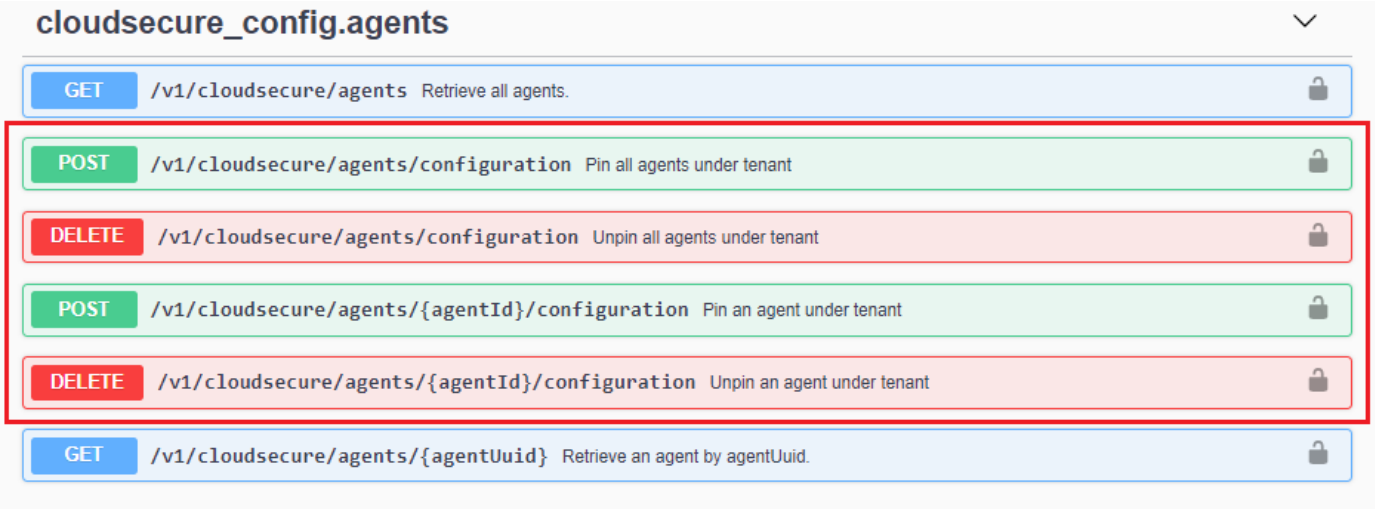
「固定」目前版本的值機員

根據預設、 Data Infrastructure Insights Workload Security 會自動更新代理程式。有些客戶可能想要暫停自動更新、這會讓值機員保持目前版本、直到發生下列其中一種情況：

- 客戶會繼續自動更新值機員。
- 30 天過去了。請注意、 30 天從最新值機員更新的當天開始、而非從值機員暫停的當天開始。

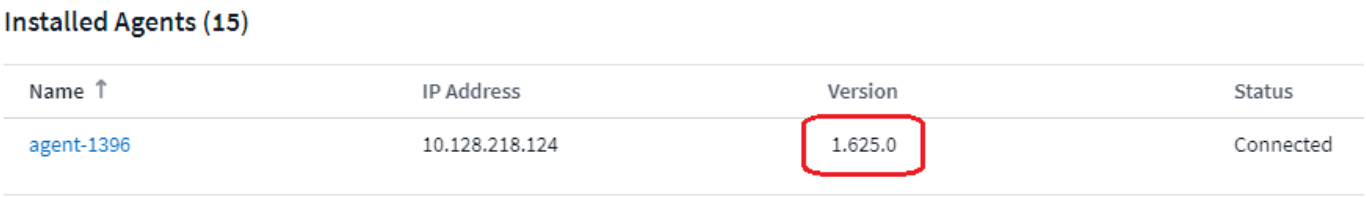
在上述每種情況下、代理程式都會在下次工作負載安全性重新整理時更新。

若要暫停或恢復自動代理程式更新、請使用 *cloudsecure_config.agents* API ：



請注意、暫停或恢復動作可能需要五分鐘才能生效。

您可以在 * 工作負載安全性 > 收集器 * 頁面的 * 代理程式 * 標籤中檢視目前的代理程式版本。



疑難排解代理程式錯誤

下表說明已知問題及其解決方法。

問題：	解決方法：
代理程式安裝無法建立/opp/NetApp/cloudsec/agent/logs/agent.log資料夾、且install.log檔案未提供相關資訊。	此錯誤發生於代理程式的開機期間。錯誤並未記錄在記錄檔中、因為它發生在記錄程式初始化之前。此錯誤會重新導向至標準輸出、並可在服務記錄中使用 `journalctl -u cloudsecure-agent.service`命令查看。此命令可用於進一步疑難排解問題。 EST
代理程式安裝失敗、無法使用「不支援此Linux套裝作業系統。結束安裝」。	當您嘗試在不受支援的系統上安裝代理程式時、就會出現此錯誤。請參閱。 "代理程式需求"
代理程式安裝失敗、並顯示錯誤：「-bash: unZip：command not found"	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unzip軟體。之後、從代理程式安裝UI重新複製命令、然後貼到CLI中、以再次執行安裝。

問題：	解決方法：
代理程式已安裝且正在執行。但代理程式突然停止。	SSH到代理機器。透過檢查代理服務的狀態 `sudo systemctl status cloudsecure-agent.service`。1.檢查日誌是否顯示消息“ Failed to start Workload Security daemon service ”（無法啓動工作負載安全守護程序服務）。2.檢查是否有 cssys 使用者存在於 Agent 機器中。以root權限逐一執行下列命令、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、則集中化監控原則可能已刪除`cssys`使用者。4.執行下列命令，手動建立 `cssys` 使用者和群組。 `sudo useradd cssys` `sudo groupadd cssys`5.執行下列命令之後重新啟動代理程式服務： `sudo systemctl restart cloudsecure-agent.service` 6.如果仍未執行、請檢查其他疑難排解選項。
無法將超過50個資料收集器新增至代理程式。	只能將50個資料收集器新增至代理程式。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「未連線」狀態。	重新啟動代理程式的步驟。1.SSH到代理機器。2.執行下列命令之後重新啟動代理程式服務： `sudo systemctl restart cloudsecure-agent.service` 3.透過檢查代理服務的狀態 `sudo systemctl status cloudsecure-agent.service`。4.值機員應進入「已連線」狀態。
代理VM位於Zscaler Proxy之後、代理程式安裝失敗。由於Zscaler Proxy的SSL檢查、工作負載安全性憑證會在Zscaler CA簽署時顯示、因此代理程式不信任通訊。	在Zscaler Proxy中停用*.cloudinsights.netapp.com URL的SSL檢查。如果Zscaler執行SSL檢查並取代憑證、則工作負載安全性將無法運作。
安裝代理程式時、解壓縮後安裝會暫停。	「chmod 755 -RF」命令失敗。當代理程式安裝命令是由工作目錄中有檔案、屬於其他使用者、且這些檔案的權限無法變更的非root Sudo使用者執行時、命令就會失敗。由於chmod命令失敗、安裝的其餘部分將不會執行。1.建立名為「 cloudsecure 」的新目錄。2.移至該目錄。3.複製並貼上完整的「 token = …… . /cloudsecure-agent-install.sh 」安裝命令，然後按 Enter 鍵。4.安裝應該能夠繼續進行。
如果代理程式仍無法連線至SaaS、請透過NetApp支援開啟案例。提供 Data Infrastructure Insights 序號以開啟案例、並依所述將記錄附加至案例。	若要將記錄附加至案例：1.以 root 權限執行下列指令碼，並共用輸出檔案（ cloudsecure-agent-appeds.zip ）。 a. NetApp /opt/oracle/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2 。以 root 權限逐一執行下列命令，並共用輸出。 a. id cssys b. 群組 cssys c. cat /etc/os-release

問題：	解決方法：
cloudsecure-agent-symptom-collector.sh指令碼失敗、並出現下列錯誤。[root@machine tmp]#/opt/NetApp/cloudecure/agent/bin/cloudsecure-agent-symptom-collector.sh收集服務記錄收集應用程式記錄收集代理程式組態擷取服務狀態快照擷取代理程式目錄結構快照…… 。…… 。/opt/NetApp/cloudecure/agent/bin/cloudecure-agent-症狀 收集器.sh：第52行：郵遞區號：找不到命令錯誤：無法建立/tmp/cloudsecure-agent-symptoms.zip	未安裝Zip工具…執行命令「yum install zip」來安裝壓縮工具。然後再次執行cloudsecure-agent-symptom-collector.sh。
使用useradd安裝代理程式失敗：無法建立目錄/home/cssys	如果因為缺乏權限而無法在/home下建立使用者的登入目錄、就可能發生此錯誤。因應措施是建立cssys使用者、然後使用下列命令手動新增其登入目錄：*Sudo useradd usern_name -m -d home_DIR*-m：如果使用者的主目錄不存在、請建立該使用者的主目錄。d：使用home_DIR建立新使用者、做為使用者登入目錄的值。例如、*Sudo useradd cssys -m -d /cssys_*會新增使用者*_cssys*、並在root下建立其登入目錄。
代理程式在安裝後未執行。*Systemctl* 狀態 *cloudsecure-agent.service* NetApp cloudsecure-agent.service: 顯示下列資訊： [root@demo ~]# systemctl 狀態 cloudsecure-agent.service agent.service cloudsecure-agent.service –工作負載安全代理程式精靈服務已載入（ /usr/lib/systemd/system/cloudsecure-agent.service; 已啟用；廠商預設值：已停用）作用：啟動（自動重新啟動）（結果：結束代碼）自星期二 2021-08 月 03 21 日 12:2603 年 8 月 21 日： 12 ： 26 示範系統 d[1] ： cloudsecure-agent.service 失敗。	這可能是因為_cssys_使用者可能沒有安裝權限而失敗。如果/opp/netapp是NFS掛載、而且_cssy使用者無法存取此資料夾、安裝將會失敗。*_cssy*是由工作負載安全性安裝程式所建立的本機使用者、可能沒有存取掛載共用的權限。您可以嘗試使用_cssys_使用者來存取/opp/NetApp/cloudsec/agent/in/cloudseced-Agent來檢查此問題。如果傳回「權限遭拒」、表示安裝權限不存在。安裝在機器本機的目錄上、而非掛載的資料夾。
代理程式一開始是透過Proxy伺服器連線、並在代理程式安裝期間設定代理。現在Proxy伺服器已經變更。如何變更代理程式的Proxy組態？	您可以編輯agent.properties以新增Proxy詳細資料。請遵循下列步驟：1.變更至內含內容檔案的資料夾：CD /opp/netapp/cloudsec/conf2。使用您最愛的文字編輯器、開啟_agent.properties_檔案進行編輯。3.新增或修改下列行：agent_proxy_host=scspa1950329001.vm.vm.com NetApp agent_proxy_port=80 agent_proxy_user=pXuser agent_proxy_password=pass1234 。儲存檔案。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程式

刪除工作負載安全代理程式時、必須先刪除與代理程式相關的所有資料收集器。

刪除代理程式

刪除值機員會刪除所有與值機員相關的資料收集器。如果您打算使用不同的代理程式來設定資料收集器、則應先建立資料收集器組態的備份、然後再刪除代理程式。

開始之前

1. 請確定所有與代理程式相關的資料收集器都已從工作負載安全入口網站刪除。

   附註：如果所有相關的收集器都處於「已停止」狀態、請忽略此步驟。

刪除代理程式的步驟：

1. 在代理VM中執行SSH、然後執行下列命令。出現提示時、請輸入「y」繼續。

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

2. 按一下 * 工作負載安全性 > 收集器 > 代理程式 *

   系統會顯示已設定的值機員清單。

3. 按一下您要刪除之代理程式的選項功能表。
4. 按一下*刪除*。

   系統將顯示「刪除代理」頁面。

5. 按一下*刪除*以確認刪除。

設定Active Directory（AD）使用者目錄收集器

工作負載安全性可設定為從Active Directory伺服器收集使用者屬性。

開始之前

- 您必須是 Data Infrastructure Insights 管理員或帳戶擁有者、才能執行此工作。
- 您必須擁有裝載Active Directory伺服器的伺服器IP位址。
- 在設定使用者目錄連接器之前、必須先設定代理程式。

設定使用者目錄收集器的步驟

1. 在 Workload Security 功能表中，按一下： * Collectors > User Directory Collectors > + User Directory Collector* ，然後選取 * Active Directory*

   系統會顯示Add User Directory（新增使用者目錄）畫面。

在下列表格中輸入所需的資料、以設定使用者目錄收集器：

名稱	說明
名稱	使用者目錄的唯一名稱。例如_GlobalADCollector_
代理程式	從清單中選取已設定的代理程式
伺服器IP/網域名稱	裝載作用中目錄之伺服器的IP位址或完整網域名稱（FQDN）
樹系名稱	目錄結構的樹系層級。樹系名稱允許使用下列兩種格式：*x.y.z*⇒直接網域名稱、如同您在SVM上的名稱一樣。*DC=x*、*DC=y*、*DC=z*⇒相對辨別名稱[範例：DC=HQ、DC=公司名稱、DC=com]、您也可以指定下列項目： *OU=Engineering*、*DC=HQ*、*DC*=公司名稱、*DC=com*[依特定OU工程篩選]*CN=UserName*、*OU=Engineering*、*DC=companyname*、*DC=NetApp*、*DC=com*[僅從OU <Engineering取得特定使用者]_CN=acrooms使用者、CN=Users、DC=HQ、DC=companyname、DC=useals=公司名稱、DC=com、DC、DC、DC =公司名稱、DC =公司名稱、DC =公司名稱、DC =公司名稱、DC =、DC =、DC =公司名稱、DC =、DC =、DC、DC =、DC =公司名稱、DC =、DC =、
連結DN	允許使用者搜尋目錄。例如：*username@companyname.com* 或 *username@domainname.com* 此外，還需要網域唯讀權限。使用者必須是安全性群組 _ 唯讀網域控制站 _ 的成員。
連結密碼	目錄伺服器密碼（即用於Bind DN的使用者名稱密碼）
傳輸協定	LDAP、LDAPS、LDAP-start-TLS
連接埠	選取連接埠

如果Active Directory中已修改預設屬性名稱、請輸入下列Directory Server必要屬性。在Active Directory中、這些屬性名稱通常是「_not」修改、在這種情況下、您只需繼續使用預設屬性名稱即可。

屬性	目錄伺服器中的屬性名稱
顯示名稱	名稱
SID	objectSid
使用者名稱	SamAccountName

按一下「包含選用屬性」以新增下列任何屬性：

屬性	目錄伺服器中的屬性名稱
電子郵件地址	郵件
電話號碼	電話號碼
角色	標題
國家/地區	合作夥伴

州/省	州/省
部門	部門
相片	thumbnailPhoto
ManagerDN	經理
群組	成員

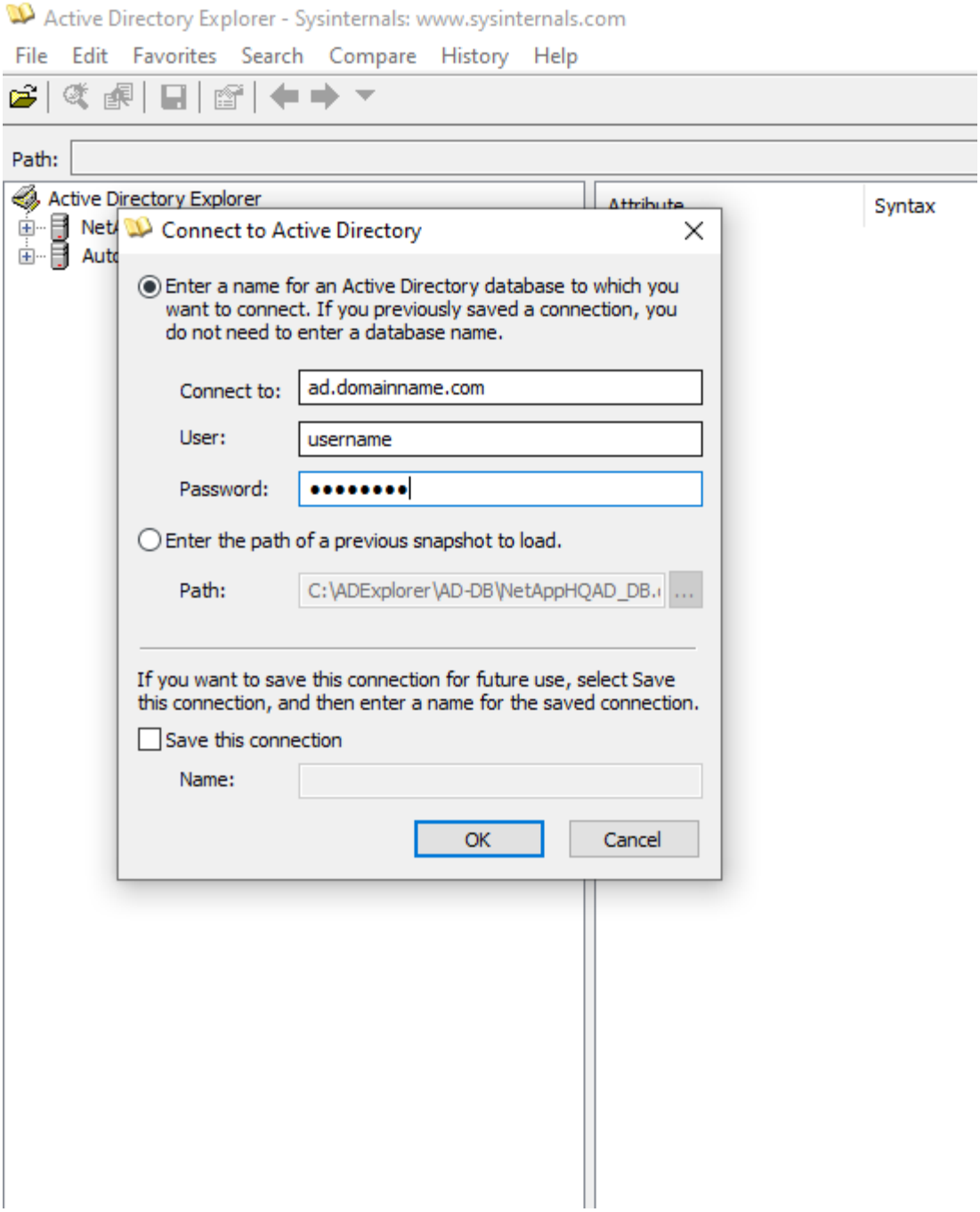
測試使用者目錄收集器組態

您可以使用下列程序來驗證LDAP使用者權限和屬性定義：

- 使用下列命令來驗證工作負載安全性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檔案總管瀏覽AD資料庫、檢視物件內容和屬性、檢視權限、檢視物件架構、執行精密的搜尋、您可以儲存並重新執行。
  - 安裝"廣告資源管理器"在任何可連線到 AD 伺服器的 Windows 機器上。
  - 使用AD目錄伺服器的使用者名稱/密碼連線至AD伺服器。



疑難排解使用者目錄收集器組態錯誤

下表說明收集器組態期間可能發生的已知問題和解決方法：

問題：	解決方法：
新增使用者目錄連接器會導致「錯誤」狀態。錯誤顯示「LDAP伺服器提供的認證無效」。	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。錯誤顯示：「無法取得對應於DN=DC=HQ、DC=domainname、DC=com的物件做為樹系名稱。」	提供的樹系名稱不正確。編輯並提供正確的樹系名稱。

問題：	解決方法：
「工作負載安全性使用者設定檔」頁面不會顯示網域使用者的選用屬性。	這可能是因為CloudSecure中新增的選用屬性名稱與Active Directory中的實際屬性名稱不相符。編輯並提供正確的選用屬性名稱。
資料收集器處於錯誤狀態、並顯示「無法擷取LDAP使用者。故障原因：無法連線至伺服器、連線為null	按一下「*Restart*」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。	請確定您已提供必要欄位（伺服器、樹系名稱、綁定DN、綁定密碼）的有效值。確保始終以「Administrator @」（系統管理員@）的形式提供Bind-DN輸入、或以具有網域管理員權限的使用者帳戶提供。
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、TCP命令[Connect(localhost:35012,None,List(),sents(,seconds,true)]失敗、因為java.net.ConnectionException:Connection拒絕。」	提供給AD伺服器的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。錯誤顯示「無法建立LDAP連線」。	提供給AD伺服器的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。錯誤顯示：「無法載入設定。原因：資料來源組態發生錯誤。具體原因：/connector / conf/application.conf：70：LDAP.LDAP連接埠具有類型字串而非數字」	提供的連接埠值不正確。請嘗試使用AD伺服器的預設連接埠值或正確的連接埠號碼。
我從必備屬性開始著手、就能順利運作。新增選用的屬性之後、就無法從AD擷取選用的屬性資料。	這可能是因為CloudSecure中新增的選用屬性與Active Directory中的實際屬性名稱不相符。編輯並提供正確的必要或選用屬性名稱。
重新啟動收集器之後、AD同步何時會發生？	收集器重新啟動後、廣告同步將立即進行。擷取使用者資料約30萬名使用者約需15分鐘、每12小時自動重新整理一次。
使用者資料會從AD同步至CloudSecure。資料何時會刪除？	如果沒有更新、使用者資料會保留13個月。如果刪除租戶、資料將會刪除。
使用者目錄連接器會導致「錯誤」狀態。"連接器處於錯誤狀態。服務名稱：usersLdap。失敗原因：無法擷取LDAP使用者。失敗原因：80090308: LdapErr：DSID-0C90453、註解：AcceptSecurityConttext錯誤、資料52e、v3839	提供的樹系名稱不正確。請參閱上述內容、瞭解如何提供正確的樹系名稱。

問題：	解決方法：
電話號碼未填入使用者設定檔頁面。	這很可能是因為Active Directory的屬性對應問題所致。1.編輯從 Active Directory 擷取使用者資訊的特定 Active Directory 收集器。2.請注意，在選用屬性下，會有一個欄位名稱「電話號碼」對應至 Active Directory 屬性「 telephonenumber 」。4.現在，請使用上述 Active Directory 檔案總管工具來瀏覽 Active Directory ，並查看正確的屬性名稱。3.請確定 Active Directory 中有一個名為「 telephonenumber 」的屬性，該屬性確實具有使用者的電話號碼。5.我們在 Active Directory 中說，它已被修改為「電話編號」。6.然後編輯 CloudSecure 使用者目錄收集器。在選用屬性區段中、將「電話號碼」取代為「電話號碼」。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，並在使用者設定檔頁面中顯示相同的電話號碼。
如果Active Directory（AD）伺服器上已啟用加密憑證（SSL）、則工作負載安全性使用者目錄收集器將無法連線至AD伺服器。	在設定使用者目錄收集器之前、請先停用AD伺服器加密。擷取使用者詳細資料後、將會保留13個月。如果擷取使用者詳細資料後AD伺服器中斷連線、則不會擷取AD中新增的使用者。若要再次擷取、使用者目錄收集器必須連線至AD。
CloudInsights Security中有來自Active Directory的資料。想要刪除CloudInsights中的所有使用者資訊。	不可能只從CloudInsights Security刪除Active Directory使用者資訊。若要刪除使用者、必須刪除完整的租戶。

設定**LDAP**目錄伺服器收集器

您可以設定工作負載安全性、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 管理員或帳戶擁有者、才能執行此工作。
- 您必須擁有裝載LDAP目錄伺服器的伺服器IP位址。
- 在設定LDAP目錄連接器之前、必須先設定代理程式。

設定使用者目錄收集器的步驟

1. 在 Workload Security 功能表中，按一下： * Collectors > User Directory Collectors > + User Directory Collector* ，然後選取 * LDAP Directory Server*

   系統會顯示Add User Directory（新增使用者目錄）畫面。

在下列表格中輸入所需的資料、以設定使用者目錄收集器：

名稱	說明
名稱	使用者目錄的唯一名稱。例如_GlobalLDAPCollector
代理程式	從清單中選取已設定的代理程式
伺服器IP/網域名稱	裝載LDAP目錄伺服器之伺服器的IP位址或完整網域名稱（FQDN）

搜尋基礎	LDAP伺服器搜尋庫的搜尋庫可同時使用下列兩種格式：*x.y.z*=您在SVM上擁有的直接網域名稱。*DC=x*、*DC=y*、*DC=z*⇒相對辨別名稱[範例：DC=HQ、DC=公司名稱、DC=com]、您也可以指定下列項目：*OU=Engineering*、*DC=HQ*、*DC*=公司名稱、*DC=com*[依特定OU工程篩選]*CN=UserName*、*OU=Engineering*、*DC=companyname*、*DC=NetApp*、*DC=com*[僅從OU <Engineering取得特定使用者]_CN=acrooms使用者、CN=Users、DC=HQ、DC=companyname、DC=useals=公司名稱、DC=acrokams=公司名稱、DC、DC、DC =公司名稱、DC =公司名稱、DC =公司名稱、DC =公司名稱、DC =、DC =、DC =、DC、DC =公司名稱、DC =
連結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 john@dorp.company.com 。 dorp.company.com
-帳戶	使用者
-John	-Anna
連結密碼	目錄伺服器密碼（即用於Bind DN的使用者名稱密碼）
傳輸協定	LDAP、LDAPS、LDAP-start-TLS
連接埠	選取連接埠

如果LDAP Directory Server中的預設屬性名稱已修改、請輸入下列Directory Server必要屬性。在LDAP目錄伺服器中、這些屬性名稱通常是「_not」修改、在這種情況下、您只需繼續使用預設屬性名稱即可。

屬性	目錄伺服器中的屬性名稱
顯示名稱	名稱
UNIX ID	uidNumber
使用者名稱	UID

按一下「包含選用屬性」以新增下列任何屬性：

屬性	目錄伺服器中的屬性名稱
電子郵件地址	郵件
電話號碼	電話號碼
角色	標題
國家/地區	合作夥伴
州/省	州/省
部門	部門編號
相片	相片

ManagerDN	經理
群組	成員

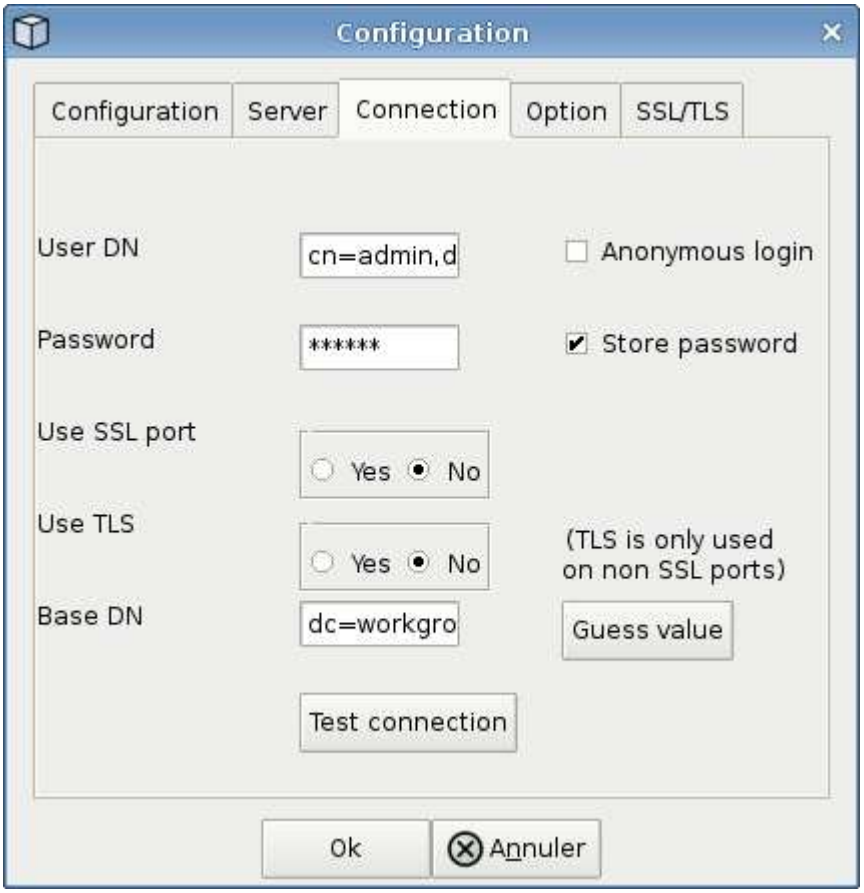
測試使用者目錄收集器組態

您可以使用下列程序來驗證LDAP使用者權限和屬性定義：

- 使用下列命令來驗證工作負載安全性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檔案總管瀏覽
LDAP資料庫、檢視物件內容和屬性、檢視權限、檢視物件架構、執行精密的搜尋、您可以儲存並
重新執行。
```

  - 將 LDAP Explorer (http://ldaptool.sourceforge.net/（ LDAP 資源管理器(http://jxplorer.org/）或 Java LDAP Explorer （ Java LDAP 資源管理器）安裝在任何可連接到 LDAP 服務器的 Windows 計算機上。
  - 使用LDAP目錄伺服器的使用者名稱/密碼連線至LDAP伺服器。



疑難排解**LDAP**目錄收集器組態錯誤

下表說明收集器組態期間可能發生的已知問題和解決方法：

問題：	解決方法：
新增LDAP目錄連接器會導致「錯誤」狀態。錯誤顯示「LDAP伺服器提供的認證無效」。	提供的綁定DN或綁定密碼或搜尋庫不正確。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。錯誤顯示：「無法取得對應於DN=DC=HQ、DC=domainname、DC=com的物件做為樹系名稱。」	提供的搜尋基礎不正確。編輯並提供正確的樹系名稱。
「工作負載安全性使用者設定檔」頁面不會顯示網域使用者的選用屬性。	這可能是因為CloudSecure中新增的選用屬性名稱與Active Directory中的實際屬性名稱不相符。欄位區分大小寫。編輯並提供正確的選用屬性名稱。
資料收集器處於錯誤狀態、並顯示「無法擷取LDAP使用者。故障原因：無法連線至伺服器、連線為null	按一下「*Restart*」按鈕、重新啟動收集器。
新增LDAP目錄連接器會導致「錯誤」狀態。	請確定您已提供必要欄位（伺服器、樹系名稱、綁定DN、綁定密碼）的有效值。確保始終以uid=LDAPUser,CN=user,CN=accounts,DC=domain,DC=companyname,DC=com的形式提供Bind-DN輸入。
新增LDAP目錄連接器會導致「重試」狀態。顯示錯誤「無法判斷收集器的健全狀況、因此請重新嘗試」	確保提供正確的伺服器 IP 和搜尋基礎 ///
在新增LDAP目錄時、會顯示下列錯誤：「無法在2次重試中判斷收集器的健全狀況、請再次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和搜尋基礎
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、TCP命令[Connect(localhost:35012,None,List(),sents(,seconds,true)]失敗、因為java.net.ConnectionException:Connection拒絕。」	提供給AD伺服器的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。錯誤顯示「無法建立LDAP連線」。	提供給LDAP伺服器的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。請嘗試使用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。錯誤顯示：「無法載入設定。原因：資料來源組態發生錯誤。具體原因：/connector / conf/application.conf：70：LDAP.LDAP連接埠具有類型字串而非數字」	提供的連接埠值不正確。請嘗試使用AD伺服器的預設連接埠值或正確的連接埠號碼。
我從必備屬性開始著手、就能順利運作。新增選用的屬性之後、就無法從AD擷取選用的屬性資料。	這可能是因為CloudSecure中新增的選用屬性與Active Directory中的實際屬性名稱不相符。編輯並提供正確的必要或選用屬性名稱。
重新啟動收集器之後、LDAP同步何時會發生？	LDAP同步會在收集器重新啟動後立即進行。擷取使用者資料約30萬名使用者約需15分鐘、每12小時自動重新整理一次。
使用者資料會從LDAP同步至CloudSecure。資料何時會刪除？	如果沒有更新、使用者資料會保留13個月。如果刪除租戶、資料將會刪除。

問題：	解決方法：
LDAP目錄連接器會導致「錯誤」狀態。"連接器處於錯誤狀態。服務名稱：usersLdap。失敗原因：無法擷取LDAP使用者。失敗原因：80090308: LdapErr：DSID-0C90453、註解：AcceptSecurityConttext錯誤、資料52e、v3839	提供的樹系名稱不正確。請參閱上述內容、瞭解如何提供正確的樹系名稱。
電話號碼未填入使用者設定檔頁面。	這很可能是因為Active Directory的屬性對應問題所致。1.編輯從 Active Directory 擷取使用者資訊的特定 Active Directory 收集器。2.請注意，在選用屬性下，會有一個欄位名稱「電話號碼」對應至 Active Directory 屬性「 telephonenumber 」。4.現在，請使用上述 Active Directory 檔案總管工具來瀏覽 LDAP 目錄伺服器，並查看正確的屬性名稱。3.請確定 LDAP 目錄中有一個名為「 telephonenumber 」的屬性，該屬性確實具有使用者的電話號碼。5.讓我們說，在 LDAP 目錄中，它已被修改為「電話編號」。6.然後編輯 CloudSecure 使用者目錄收集器。在選用屬性區段中、將「電話號碼」取代為「電話號碼」。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，並在使用者設定檔頁面中顯示相同的電話號碼。
如果Active Directory（AD）伺服器上已啟用加密憑證（SSL）、則工作負載安全性使用者目錄收集器將無法連線至AD伺服器。	在設定使用者目錄收集器之前、請先停用AD伺服器加密。擷取使用者詳細資料後、將會保留13個月。如果擷取使用者詳細資料後AD伺服器中斷連線、則不會擷取AD中新增的使用者。若要再次擷取、使用者目錄收集器必須連線至AD。

設定ONTAP SVM Data Collector

「工作負載安全性」使用資料收集器從裝置收集檔案和使用者存取資料。

開始之前

- 下列項目支援此資料收集器：
  - 更新版本。Data ONTAP為獲得最佳效能、請使用高於 9.13.1 的 Data ONTAP 版本。
  - SMB傳輸協定3.1版及更早版本。
  - ONTAP 9.15.1 或更新版本的 NFS 4.1 版本、包括 NFS 4.1 。
  - 支援從支援的更新版本為支援FlexGroup ONTAP
  - 支援的支援ONTAP Select
- 僅支援資料類型SVM。不支援具有無限磁碟區的SVM。
- SVM有多種子類型。其中僅支援_default_、*sync*來源_和_*sync*目的地。
- Agent "必須設定" ，然後再設定資料收集器。
- 請確定您已正確設定使用者目錄連接器、否則事件會在「活動鑑識」頁面中顯示編碼的使用者名稱、而非使用者的實際名稱（儲存在Active Directory中）。
- • ONTAP Persistent Store 可從 9.14.1 獲得支援。

- 為獲得最佳效能、您應將FPolicy伺服器設定為與儲存系統位於同一子網路上。
- 您必須使用下列兩種方法之一來新增SVM：
  - 使用叢集IP、SVM名稱及叢集管理使用者名稱與密碼。這是建議的方法。_
    - SVM名稱必須完全如ONTAP 圖所示、且區分大小寫。
  - 使用SVM Vserver Management IP、使用者名稱和密碼
  - 如果您無法或不願意使用完整的系統管理員叢集 / SVM 管理使用者名稱和密碼，您可以依照下列章節所述，使用較少的 Privileges 建立自訂使用者「權限注意事項」。您可以為SVM或叢集存取建立此自訂使用者。
    - o您也可以使用具有至少具有csrole權限的AD使用者、如以下「權限注意事項」一節所述。另請參閱"ONTAP 文件"。
- 執行下列命令、確保已針對SVM設定正確的應用程式：

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

輸出範例

```
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 已設定 CIFS 伺服器： clusterShell ：：> `vserver cifs show`

  系統會傳回Vserver名稱、CIFS伺服器名稱及其他欄位。

- 設定SVM vsadmin使用者的密碼。如果使用自訂使用者或叢集管理使用者，請略過此步驟。 clusterShell ：：> `security login password -username vsadmin -vserver svmname`
- 解除鎖定SVM vsadmin使用者以進行外部存取。如果使用自訂使用者或叢集管理使用者，請略過此步驟。 clusterShell ：：> `security login unlock -username vsadmin -vserver svmname`
- 確保資料LIF的防火牆原則設定為「mGMT」（而非「dATA」）。如果使用專用管理 lif 來新增 SVM ，clusterShell ：：> ，請略過此步驟 `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- 啟用防火牆時、您必須定義例外狀況、才能使用Data ONTAP 「Data Collector」允許連接埠的TCP流量。

  如需組態資訊，請參閱"代理程式需求"。這適用於安裝在雲端的內部部署代理程式和代理程式。

- 當代理程式安裝在AWS EC2執行個體中以監控Cloud ONTAP SVM時、代理程式和儲存設備必須位於同一個VPC中。如果它們位於獨立的VPC中、則VPC之間必須有有效的路由。

使用者存取封鎖的先決條件

請記住下列事項"使用者存取封鎖"：

此功能需要叢集層級認證、才能正常運作。

如果您使用叢集管理認證、則不需要新的權限。

如果您使用的自訂使用者（例如、*CsUser*）具有授予使用者的權限、請依照下列步驟授予工作負載安全性權限、以封鎖使用者。

對於具有叢集認證的CsUser、請從ONTAP 下列功能執行：

```
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
```

權限相關注意事項

透過*叢集管理**IP***新增權限：

如果您無法使用叢集管理管理員使用者來允許工作負載安全性存取ONTAP 《SVM資料收集器》、您可以建立一個名為「CsUser」的新使用者、其角色如下所示。將工作負載安全資料收集器設定為使用叢集管理IP時、請使用「CsUser」的使用者名稱和密碼。

若要建立新的使用者、ONTAP 請使用叢集管理管理員使用者名稱/密碼登入到功能表、然後在ONTAP 功能表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 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***新增權限：

如果您無法使用叢集管理管理員使用者來允許工作負載安全性存取ONTAP 《SVM資料收集器》、您可以建立一個名為「CsUser」的新使用者、其角色如下所示。將工作負載安全資料收集器設定為使用Vserver Management IP時、請使用「CsUser」的使用者名稱和密碼。

若要建立新的使用者、ONTAP 請使用叢集管理管理員使用者名稱/密碼登入到位、然後在ONTAP 伺服器上執行下列命令。為了方便起見、請先將這些命令複製到文字編輯器、並在ONTAP 執行下列命令之前、以Vserver名稱取代<vservername>：

```
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>
```

原型模式

在收集器的 *Advanced Configuration* 設定中啟用此選項時，工作負載安全性會將 FPolicy 引擎設定為原型模式。ONTAP 9.15 版及更新版本均支援原型模式。

如需此功能的詳細資訊"ONTAP 文件"，請參閱。

protobuf 需要特定權限（其中部分或全部可能已經存在）：

叢集模式：

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

Vserver 模式：

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

ONTAP 自主勒索軟體保護和 **ONTAP** 存取權限遭拒

如果您使用叢集管理認證、則不需要新的權限。

如果您使用的自訂使用者（例如、*CsUser*）具有授予使用者的權限、請依照下列步驟授予工作負載安全性權限、以便從ONTAP Sfor收集與Arp相關的資訊。

如需詳細資訊，請參閱"與 ONTAP 存取整合遭拒"

和 "整合ONTAP 了功能完善的勒索軟體保護功能"

設定資料收集器

組態步驟

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

   系統會顯示可用的資料收集器。

3. 將游標暫留在* NetApp SVM區塊上、然後按一下*+監控*。

   系統會顯示ONTAP 「SVM組態」頁面。輸入每個欄位的必要資料。

欄位	說明
名稱	資料收集器的唯一名稱
代理程式	從清單中選取已設定的代理程式。
透過管理IP連線：	選取叢集IP或SVM管理IP
叢集/ SVM管理IP位址	叢集或SVM的IP位址、取決於您在上方的選擇。
SVM 名稱	SVM名稱（透過叢集IP連線時、此欄位為必填欄位）
使用者名稱	透過叢集IP新增SVM/叢集時、存取SVM/叢集的使用者名稱選項為：1.叢集管理2.「CsUser」3.扮演類似CsUser角色的AD使用者。透過 SVM IP 新增時，選項為： 4. vsadmin 5.「CsUser」6.與CsUser角色相似的AD使用者名稱。
密碼	上述使用者名稱的密碼
篩選共用/磁碟區	選擇是否要在事件集合中包含或排除共用/磁碟區
輸入要排除/包含的完整共用名稱	要從事件集合中排除或包含（視情況而定）的共用清單（以英文分隔）
輸入要排除/包含的完整Volume名稱	要從事件集合中排除或包含（視情況而定）的磁碟區清單（以英文分隔）
監控資料夾存取	核取此選項時、會啟用資料夾存取監控的事件。請注意、即使未選取此選項、仍會監控資料夾的建立/重新命名與刪除。啟用此功能將會增加監控的事件數目。

設定ONTAP 「發送緩衝區大小」	設定ONTAP 不規則傳送緩衝區大小。如果ONTAP 使用9.8p7之前的版本且發現效能問題、ONTAP 則可變更此版本的更新緩衝區大小、以改善ONTAP 效能。如果您沒有看到此選項、並且想要探索、請聯絡NetApp支援部門。

完成後

- 在「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組態屬性。

MetroCluster 的建議組態

MetroCluster 建議使用下列項目：

1. 將兩個資料收集器連接至來源SVM、另一個連接至目的地SVM。
2. 資料收集器應由_叢集IP_連線。
3. 在任何時候、一個資料收集器都應該在執行中、另一個則會發生錯誤。

   目前「執行中」的SVM資料收集器會顯示為_Running。目前的「最新」SVM資料收集器會顯示為_Error_。
4. 每當有切換時、資料收集器的狀態會從「執行中」變更為「錯誤」、反之亦然。
5. 資料收集器從「錯誤」狀態移至「執行中」狀態最多需要兩分鐘的時間。

服務原則

如果將服務原則搭配 ONTAP * 9.9.1 版或更新版本 * 使用、則為了連線至資料來源收集器、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9.9.1之前的ONTAP 版本中、不需要設定_data-fpolice-client_。

Play-Pause Data Collector

2 個新作業現在顯示在收集器的 kebab 功能表上（暫停和繼續）。

如果資料收集器處於 _Running 狀態、您可以暫停收集。開啟收集器的「三點」功能表、然後選取暫停。當收集器暫停時、不會從 ONTAP 收集任何資料、也不會將資料從收集器傳送至 ONTAP 。這表示任何 Fpolicy 事件都不會從 ONTAP 流向資料收集器、也不會從資料基礎架構深入分析。

請注意、如果在 ONTAP 上建立任何新的磁碟區等、而收集器處於暫停狀態、工作負載安全性就不會收集資料、這些磁碟區等資料也不會反映在儀表板或表格中。

請謹記下列事項：

- 根據暫停收集器上設定的設定、不會執行快照清除。
- EMS 事件（例如 ONTAP ARP ）不會在暫停的收集器上處理。這表示如果 ONTAP 發現勒索軟體攻擊、資料基礎架構洞見工作負載安全性將無法取得該事件。
- 系統不會傳送已暫停收集器的健全狀況通知電子郵件。
- 暫停的收集器不支援手動或自動動作（例如 Snapshot 或使用者封鎖）。
- 在代理程式或收集器升級、代理程式 VM 重新啟動 / 重新開機、或代理程式服務重新啟動時、暫停的收集器會保持在 _Paused 狀態。
- 如果資料收集器處於 _ 錯誤 _ 狀態、則無法將收集器變更為 _ 已暫停 _ 狀態。只有在收集器的狀態為 _Running 時、才會啟用「暫停」按鈕。
- 如果代理程式中斷連線、則無法將收集器變更為 _ 已暫停 _ 狀態。收集器將進入 *Stopped* 狀態、並停用暫停按鈕。

持續儲存區

ONTAP 9.14.1 及更新版本支援持續儲存區。請注意、 Volume 名稱指示會因 ONTAP 9.14 至 9.15 而異。

您可以選取收集器編輯 / 新增頁面中的核取方塊來啟用持續儲存區。選取此核取方塊後、會顯示文字欄位以接受 Volume 名稱。Volume 名稱是啟用持續儲存區的必填欄位。

- 對於 ONTAP 9.14.1 、您必須先建立磁碟區才能啟用此功能、並在 _ Volume Name_ 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 、收集器會使用 _ Volume Name_ 欄位中提供的名稱、自動以 16GB 大小建立 Volume 。

持續儲存區需要特定權限（其中部分或全部可能已經存在）：

叢集模式：

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

Vserver 模式：

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

疑難排解

如需疑難排解秘訣、請參閱"SVM 收集器疑難排解"頁面。

設定**Cloud Volumes ONTAP** 適用於**NetApp ONTAP** 的支援**NetApp**的支援功能、包括支援功能

「工作負載安全性」使用資料收集器從裝置收集檔案和使用者存取資料。

儲存組態**Cloud Volumes ONTAP**

請參閱 OnCommand Cloud Volumes ONTAP 說明文件，以設定單一節點 / HA AWS 執行個體來主控工作負載安全性代理程式：https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

完成組態設定後，請依照下列步驟設定 SVM ：https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

支援的平台

- 支援所有雲端服務供應商（無論有何種情況）Cloud Volumes ONTAP 。例如：Amazon、Azure、Google Cloud。
- Amazon FSX ONTAP

代理機器組態

代理機器必須在雲端服務供應商各自的子網路中進行設定。如需網路存取的詳細資訊、請參閱[Agent Requirements（代理程式需求）]。

以下是AWS中的代理程式安裝步驟。您可在Azure或Google Cloud中遵循適用於雲端服務供應商的同等步驟進行安裝。

在AWS中、請使用下列步驟設定要用作工作負載安全代理程式的機器：

請使用下列步驟、將機器設定為工作負載安全代理程式：

步驟

1. 登入AWS主控台並瀏覽至EC2-instances頁面、然後選取_Launch instance_。
2. 請依照本頁所述，選擇適當版本的 RHEL 或 CentOS AMI ：https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. 選取Cloud ONTAP 實例所在的VPC和子網路。
4. 選取「_t2.xlarge」（4個vCPU和16 GB RAM）作為配置資源。
    a. 建立EC2執行個體。
5. 使用YUM套件管理程式安裝所需的Linux套件：
    a. 安裝_wGet_和_unzip _原生Linux套件。

安裝工作負載安全代理程式

1. 以管理員或帳戶擁有者身分登入您的 Data Infrastructure Insights 環境。
2. 瀏覽至 Workload Security * Collector* 、然後按一下 * Agents* 標籤。
3. 按一下「**+**代理程式」、並將RHEL指定為目標平台。

4. 複製代理程式安裝命令。
5. 將「代理程式安裝」命令貼到您登入的RHEL EC2執行個體中。這會安裝工作負載安全代理程式，只要符合所有"代理程式先決條件"要求即可。

如需詳細步驟，請參閱此連結： https://docs 。 NetApp 。 com/us-en/cloudimses/task_cs_add_agent.html#Steps to 安裝代理程式

疑難排解

下表說明已知問題及其解決方法。

問題	解決方案
Data Collector會顯示「工作負載安全性：無法判斷ONTAP Amazon FxSN資料收集器的支援類型」錯誤。客戶無法將新的Amazon FSxN資料收集器新增至工作負載安全性。從代理程式連接埠443連線至FSxN叢集的連線逾時。防火牆和AWS安全性群組已啟用必要的規則、以允許通訊。代理程式已經部署、而且也位於相同的AWS帳戶中。此相同的代理程式可用來連接及監控其餘的NetApp裝置（且所有裝置均正常運作）。	將fsxadmin LIF網路區段新增至代理程式的安全性規則、即可解決此問題。如果您不確定連接埠、則允許所有連接埠。

使用者管理

工作負載安全性使用者帳戶是透過 Data Infrastructure Insights 來管理。

Data Infrastructure Insights 提供四種使用者帳戶層級：帳戶擁有者、系統管理員、使用者和訪客。每個帳戶都會被指派特定的權限等級。擁有系統管理員權限的使用者帳戶可以建立或修改使用者、並將下列其中一個工作負載安全角色指派給每位使用者：

角色	工作負載安全存取
系統管理員	可執行所有工作負載安全功能、包括警示、鑑識、資料收集器、自動回應原則、以及工作負載安全API等功能。管理員也可以邀請其他使用者、但只能指派工作負載安全性角色。
使用者	可檢視及管理警示、以及檢視鑑識。使用者角色可以變更警示狀態、新增附註、手動擷取快照及限制使用者存取。
訪客	可檢視警示和鑑識。來賓角色無法變更警示狀態、新增附註、手動擷取快照或限制使用者存取。

步驟

1. 登入工作負載安全性
2. 在功能表中、按一下*管理>使用者管理*

   您將被轉寄至 Data Infrastructure Insights 的「使用者管理」頁面。

3. 為每位使用者選取所需的角色。

新增使用者時、只要選擇所需的角色（通常是使用者或訪客）即可。

如需使用者帳戶和角色的詳細資訊、請參閱 Data Infrastructure Insights "使用者角色" 文件。

SVM事件率檢查器（代理程式規模調整指南）

「事件率檢查器」用於檢查SVM中的NFS/SMB組合事件率、然後再安裝ONTAP 一套SVM資料收集器、以查看一部代理機器能夠監控的SVM數量。使用「事件率檢查器」做為規模調整指南、協助您規劃安全環境。

Agent 最多可支援 50 個資料收集器。

所學專業：電子

- 叢集 IP
- 叢集管理使用者名稱和密碼

執行此指令碼時ONTAP 、不應針對正在判斷事件率的SVM執行任何SVM Data Collector。

步驟：

1. 依照CloudSecure中的指示安裝代理程式。
2. 安裝代理程式後、以Sudo使用者身分執行_server_data_rate_checker.sh_指令碼：

```
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

. 此指令碼需要在Linux機器上安裝_sshpass_。安裝方法有兩種：

a. 執行下列命令：

```
linux_prompt> yum install sshpass
```

.. 如果這不管用、請從網路下載_sshpass_到Linux機器、然後執行下列命令：

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

3. 出現提示時、請提供正確的值。請參閱以下範例。
4. 執行指令碼大約需要5分鐘。
5. 執行完成後、指令碼會從SVM列印事件速率。您可以在主控台輸出中檢查每個SVM的事件率：

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

每ONTAP 個SVM資料收集器都可與單一SVM建立關聯、這表示每個資料收集器都能接收單一SVM產生的事件

數。

請謹記下列事項：

a ）使用此表格做為一般尺寸指南。您可以增加核心和 / 或記憶體的數量、以增加支援的資料收集器數量、最多可增加 50 個資料收集器：

代理機器組態	SVM資料收集器數量	代理機器可處理的最大事件速率
4核心、16GB	10個資料收集器	20K個事件/秒
4核心、32GB	20個資料收集器	20K個事件/秒

b）若要計算事件總數、請新增為該代理程式的所有SVM所產生的事件。

c）如果指令碼未在尖峰時間執行、或尖峰流量難以預測、則事件速率緩衝區應保持30%。

B + C應小於A、否則值機員機器將無法監控。

換句話說、可新增至單一代理機器的資料收集器數量應符合下列公式：

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

請參閱link:concept_cs_agent_requirements.html["代理程式需求"]**頁面以取得其他先決條件和要求。**

範例

假設我們有三種SVMS、每秒產生100、200和300個事件的事件率。

我們採用以下公式：

```
 (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.
```

在代理機器中、主控台輸出位於目前工作目錄的檔案名稱為_fpolicy_stat_<SVM Name>.log__。

指令碼可能會在下列情況下產生錯誤結果：

- 提供的認證資料、IP或SVM名稱不正確。
- 已存在且名稱、順序編號等相同的fpolicy將會產生錯誤。
- 指令碼在執行時突然停止。

執行指令碼的範例如下所示：

```
[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
```

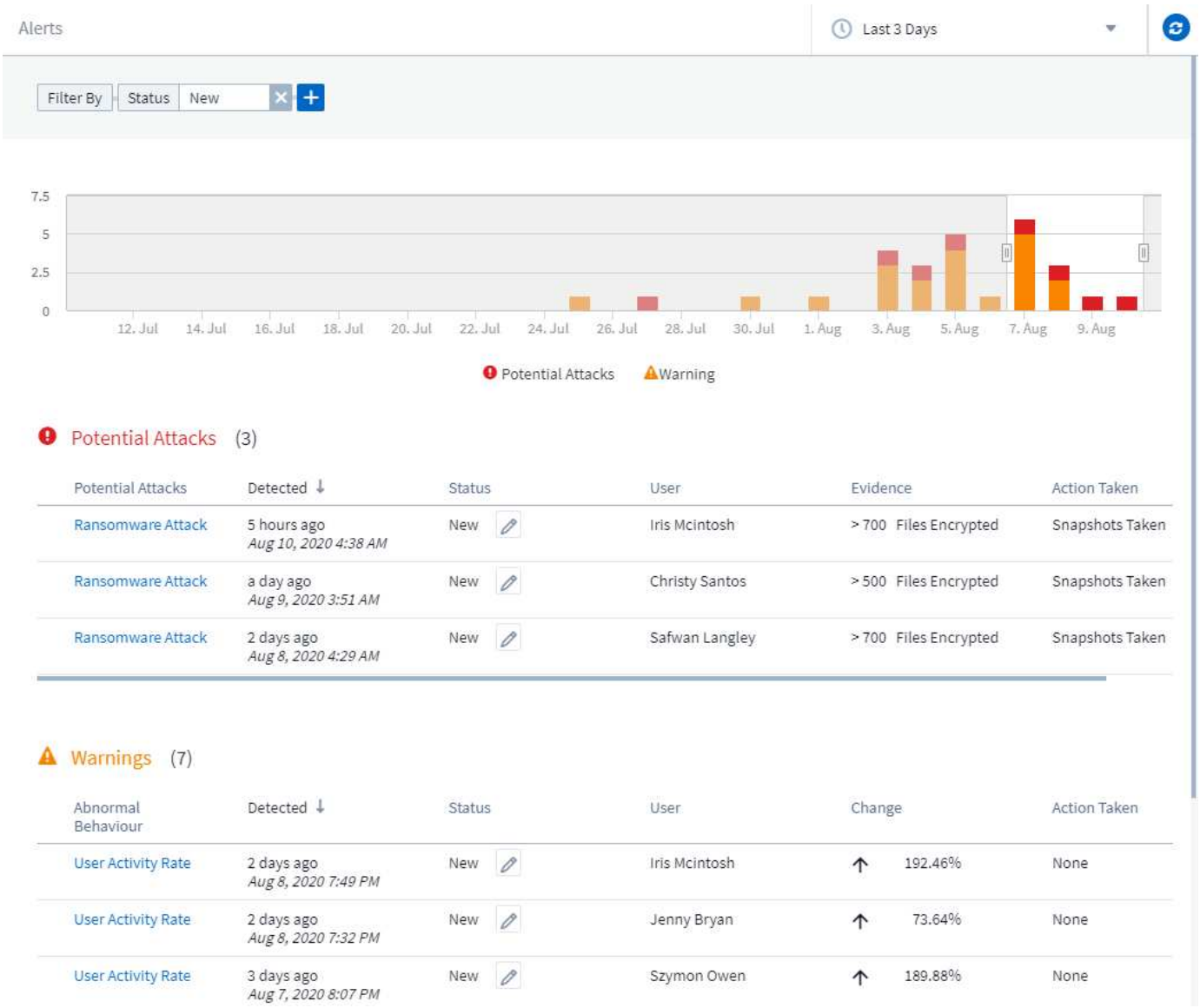
```
------------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press 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]#
```

問題	答
如果我在已設定為工作負載安全性的SVM上執行此指令碼、它是否只使用SVM上現有的fpolicy組態、或是設定暫用的組態並執行程序？	即使已設定為工作負載安全性的SVM、事件率檢查器仍可正常執行。應該沒有影響。
我可以增加執行指令碼的SVM數量嗎？	是的。只要編輯指令碼、並將SVM的最大數量從5變更為任何所需的數量即可。
如果增加SVM數量、是否會增加指令碼的執行時間？	否。即使 SVM 數量增加，指令碼也會執行最多 5 分鐘。
我可以增加執行指令碼的SVM數量嗎？	是的。您需要編輯指令碼、並將SVM的最大數量從5變更為任何所需的數量。
如果增加SVM數量、是否會增加指令碼的執行時間？	否。即使 SVM 數量增加，指令碼也會執行最多 5 分鐘。
如果我使用現有的代理程式執行「事件率檢查器」、會發生什麼事？	針對已存在的代理程式執行「事件率檢查器」、可能會增加SVM的延遲。這種增加是在事件率檢查器執行期間的暫時性增加。

警示

工作負載安全警示頁面會顯示最近攻擊和/或警告的時間表、並可讓您檢視每個問題的詳細資料。



警示

警示清單會顯示圖表、顯示在所選時間範圍內提出的潛在攻擊和/或警告總數、然後顯示該時間範圍內發生的攻擊和/或警告清單。您可以調整圖表中的開始時間和結束時間滑桿、以變更時間範圍。

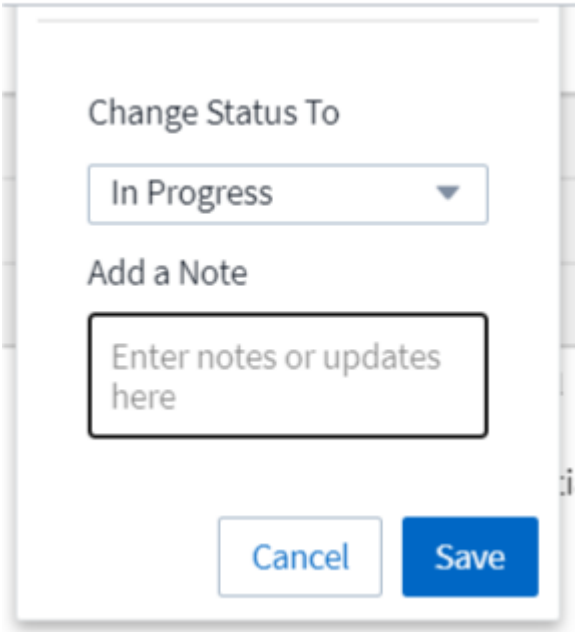
每個警示都會顯示下列項目：

潛在攻擊：

- _Potential攻擊_類型（例如勒索軟體或破壞）
- 可能遭受攻擊的日期和時間_偵測_
- 警示的_Status：
  - 新增：這是新警示的預設值。
  - 進行中：警示正在由團隊成員或成員進行調查。
  - 已解決：警示已由團隊成員標記為「已解決」。

- 已遭解僱：警示已遭解僱為誤判或預期行為。

  系統管理員可以變更警示狀態、並新增附註以協助調查。



- 行為觸發警示的_User_
- _證據_攻擊（例如、大量檔案已加密）
- 採取的動作_（例如、已建立快照）

警告：

- 觸發警告的_異常行為_
- 偵測到行為的日期和時間_
- 警示的_Status（新增、進行中等）
- 行為觸發警示的_User_
- _Chang__的說明（例如檔案存取異常增加）
- 採取的行動_

篩選選項

您可以依下列項目篩選警示：

- 警示的_Status
- 註釋_中的特定文字
- _攻擊/警告_的類型
- 動作觸發警示/警告的_User_

「警示詳細資料」頁面

您可以按一下警示清單頁面上的警示連結、開啟警示的詳細資料頁面。警示詳細資料可能會因攻擊類型或警示而異。例如、勒索軟體攻擊詳細資料頁面可能會顯示下列資訊：

摘要區段：

- 攻擊類型（勒索軟體、破壞）和警示ID（由工作負載安全指派）
- 偵測到攻擊的日期和時間
- 已採取的行動（例如、已執行自動快照。快照時間會立即顯示在摘要區段下方）
- 狀態（新增、進行中等）

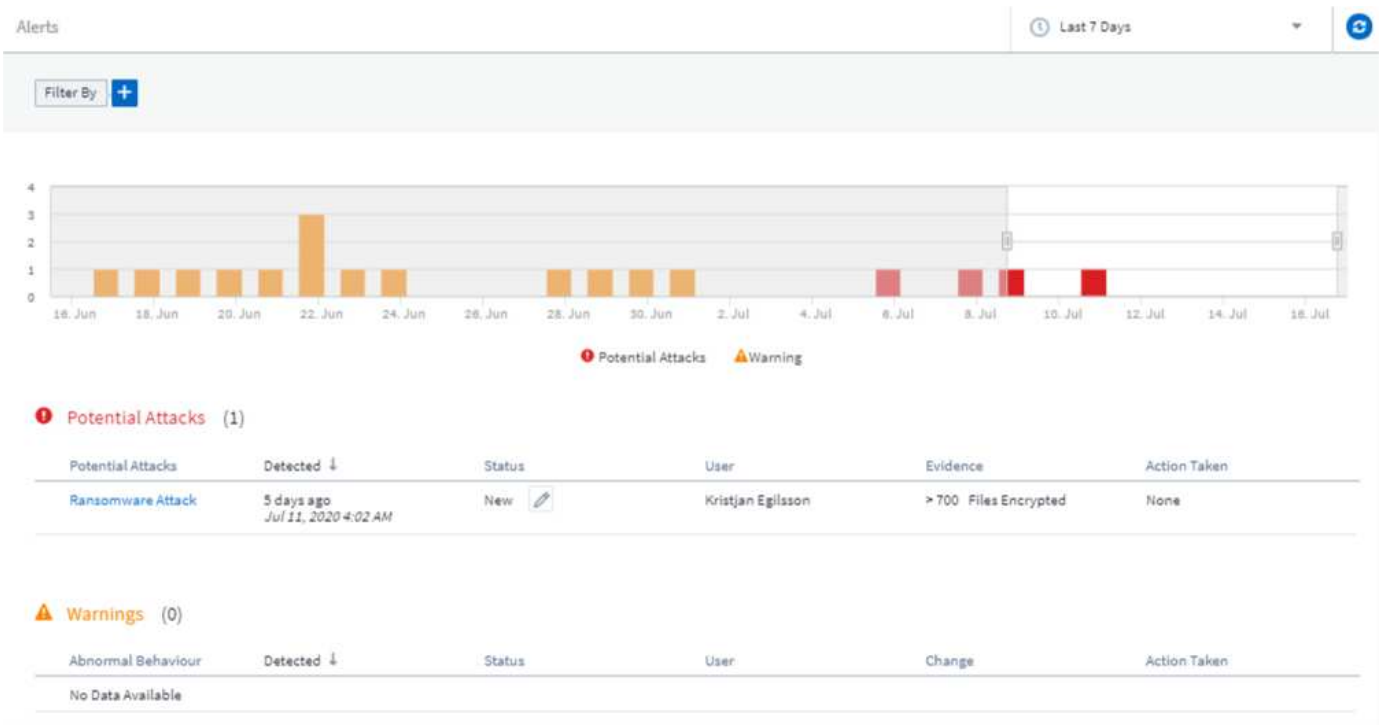
攻擊結果區段：

- 受影響的磁碟區和檔案計數
- 偵測的隨附摘要
- 顯示攻擊期間檔案活動的圖表

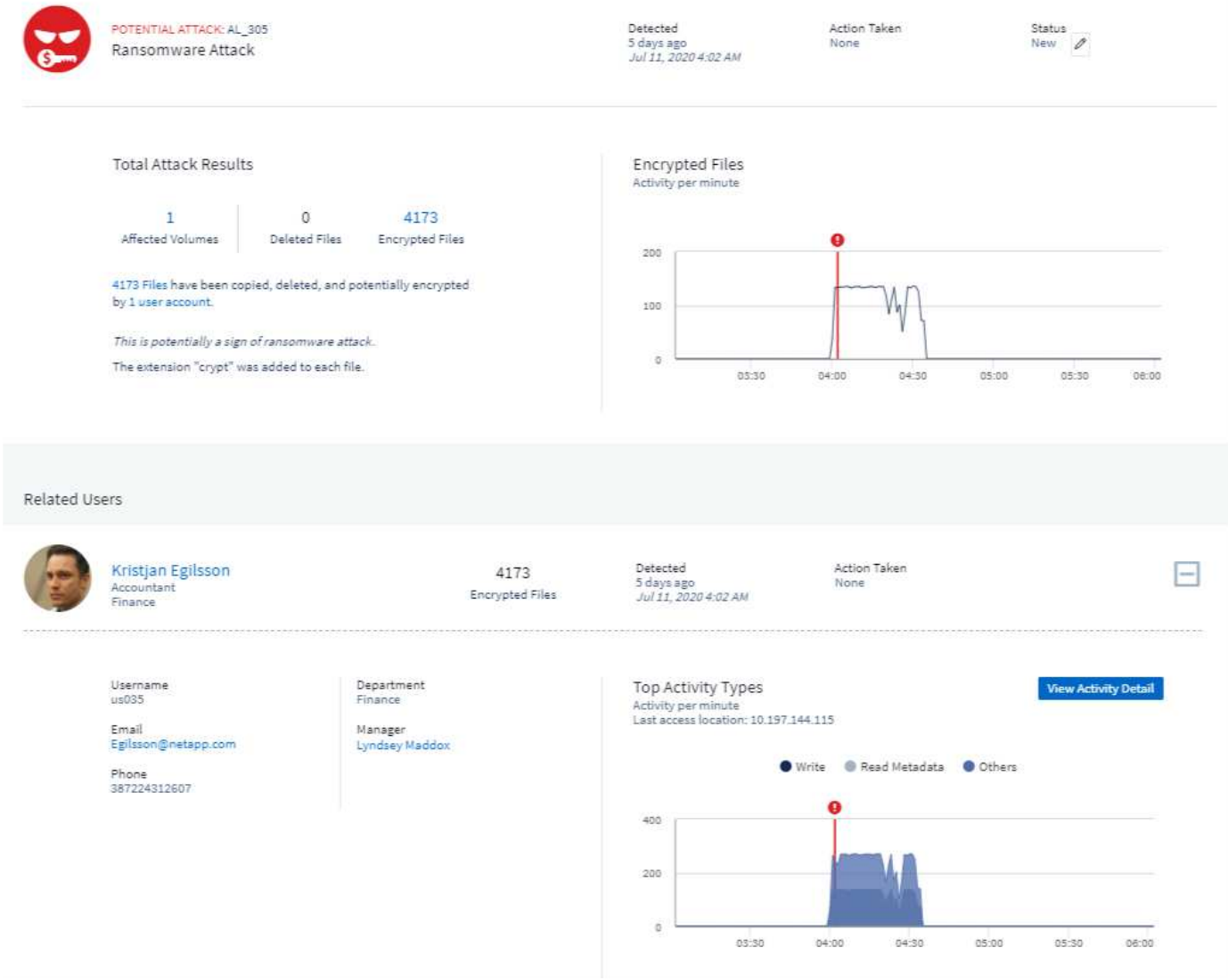
相關使用者區段：

本節將詳細說明可能遭受攻擊的使用者、包括使用者的熱門活動圖表。

警示頁面（此範例顯示可能的勒索軟體攻擊）：



詳細資料頁面（此範例顯示可能的勒索軟體攻擊）：

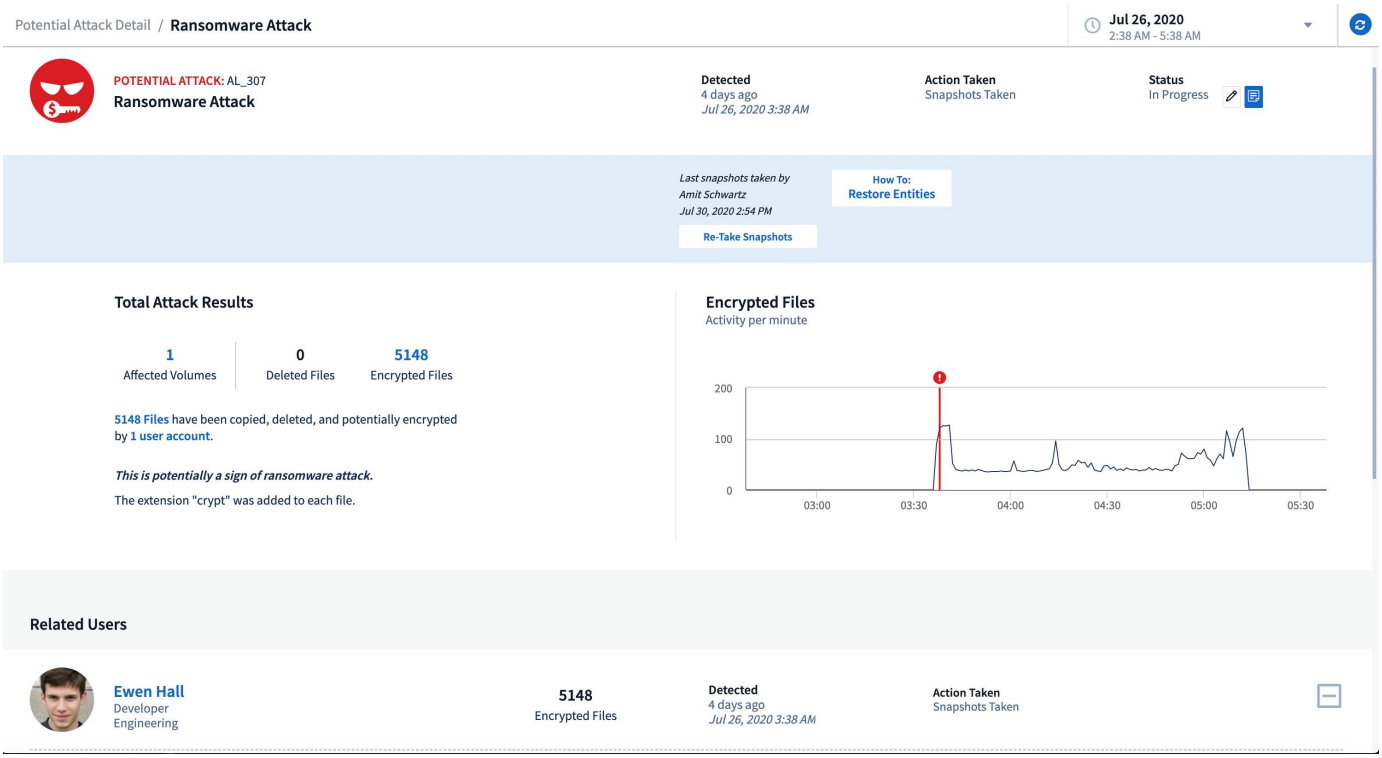


_執行Snapshot動作

工作負載安全功能可在偵測到惡意活動時自動擷取快照、確保資料安全備份、進而保護資料安全。

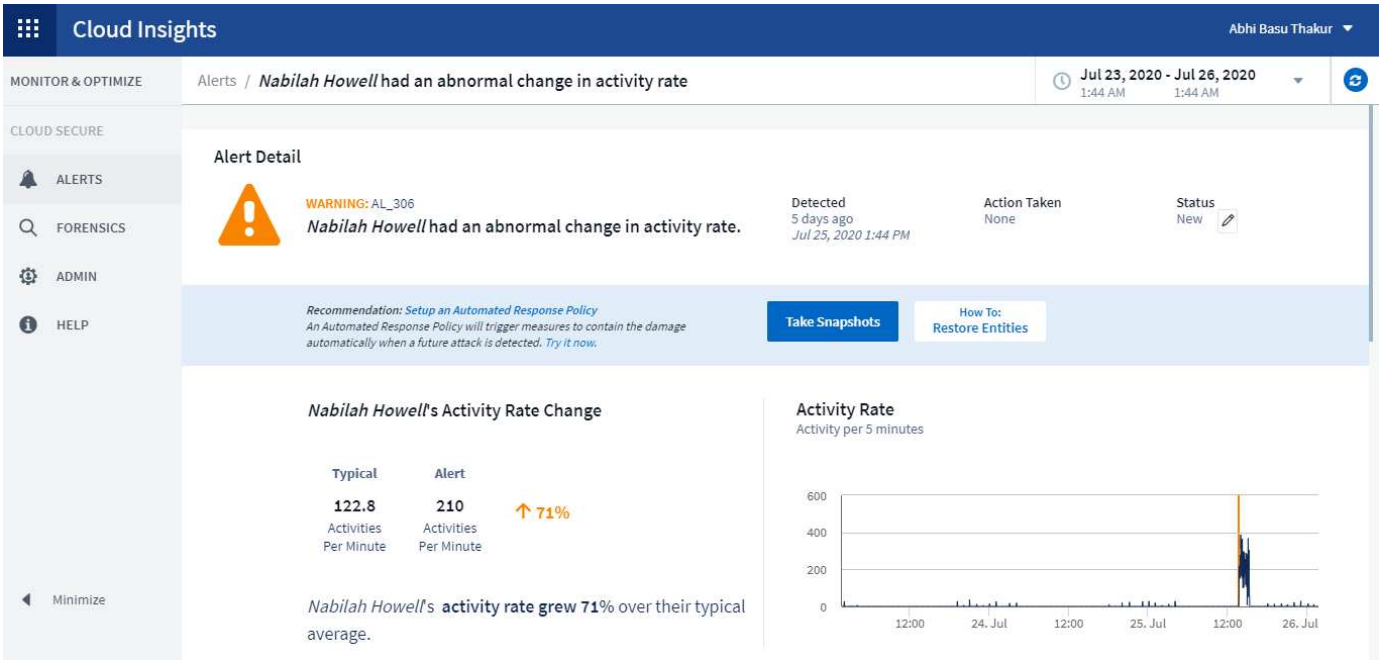
您可以定義"自動化回應原則"在偵測到勒索軟體攻擊或其他異常使用者活動時，拍攝快照。您也可以從警示頁面手動擷取快照。

自動拍攝快照
：



手動快照

:



警示通知

警示的電子郵件通知會針對警示上的每個動作傳送至警示收件者清單。若要設定警示收件者、請按一下*管理>通知*、然後輸入每個收件者的電子郵件地址。

保留政策

警示與警告會保留13個月。超過13個月的警示和警告將會刪除。如果刪除工作負載安全環境、則與環境相關的

所有資料也會一併刪除。

疑難排解

問題：	試用：
在這種情況ONTAP 下、每小時執行一次快照。工作負載安全性（ WS ）快照是否會影響它？WS 快照是否會採用每小時快照的位置？預設的每小時快照是否會停止？	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的快照空間、因此應該像以前一樣繼續。預設的每小時快照不會停止。
如果在不確定的情況下達到最大快照數、會發生什麼情況ONTAP ？	如果快照數量達到上限、後續的快照拍攝將會失敗、而工作負載安全性會顯示錯誤訊息、指出快照已滿。使用者需要定義Snapshot原則來刪除最舊的快照、否則將無法擷取快照。在不含更新版本的版本中、Volume最多可包含255個Snapshot複本。ONTAP在NetApp 9.4及更新版本中、Volume最多可包含1023個Snapshot複本。ONTAP有關的信息，請參閱 ONTAP 文檔"設定Snapshot刪除原則"。
工作負載安全功能完全無法擷取快照。	請確定用於建立快照的角色具有下列連結：https://docs 。 NetApp 。 com/us-en/cloudimses/task_add_collector 。 svm.html#a-note about 權限 [已指派適當權限] 。請確定已建立具有適當存取權限的_csrole_、以供拍攝快照：安全登入角色create -vserver <vservername>-role csrole -cmd dirname "volume snapshot"-access all
在SVM上的舊警示（從工作負載安全性中移除後又重新新增）、快照失敗。對於再次新增SVM之後發生的新警示、會擷取快照。	這是罕見的情況。如果您遇到這種情況、請登入ONTAP 到「介紹」、然後手動擷取舊警示的快照。
在_警示詳細資料_頁面中、「上次嘗試失敗」錯誤訊息會顯示在_「拍攝Snapshot」按鈕下方。將游標停留在錯誤上會顯示「Invoke API command has timed out for the data collector with id」。	如果SVM的LIF處於_disabled_狀態ONTAP 、則透過SVM管理IP將資料收集器新增至工作負載安全性時、就可能發生這種情況。啟用ONTAP 支援功能中的特定LIF、並從工作負載安全性觸發_手動拍攝Snapshot _。然後Snapshot行動就會成功。

鑑識

鑑識-所有活動

「所有活動」頁面可協助您瞭解在工作負載安全性環境中、對實體所執行的行動。

檢查所有活動資料

按一下「鑑識」>「活動鑑識」、然後按一下「所有活動」索引標籤以存取「所有活動」頁面。本頁提供租戶活動的概觀，並強調下列資訊：

- 顯示 _ 活動歷程記錄 _ 的圖表（根據所選的整體時間範圍）

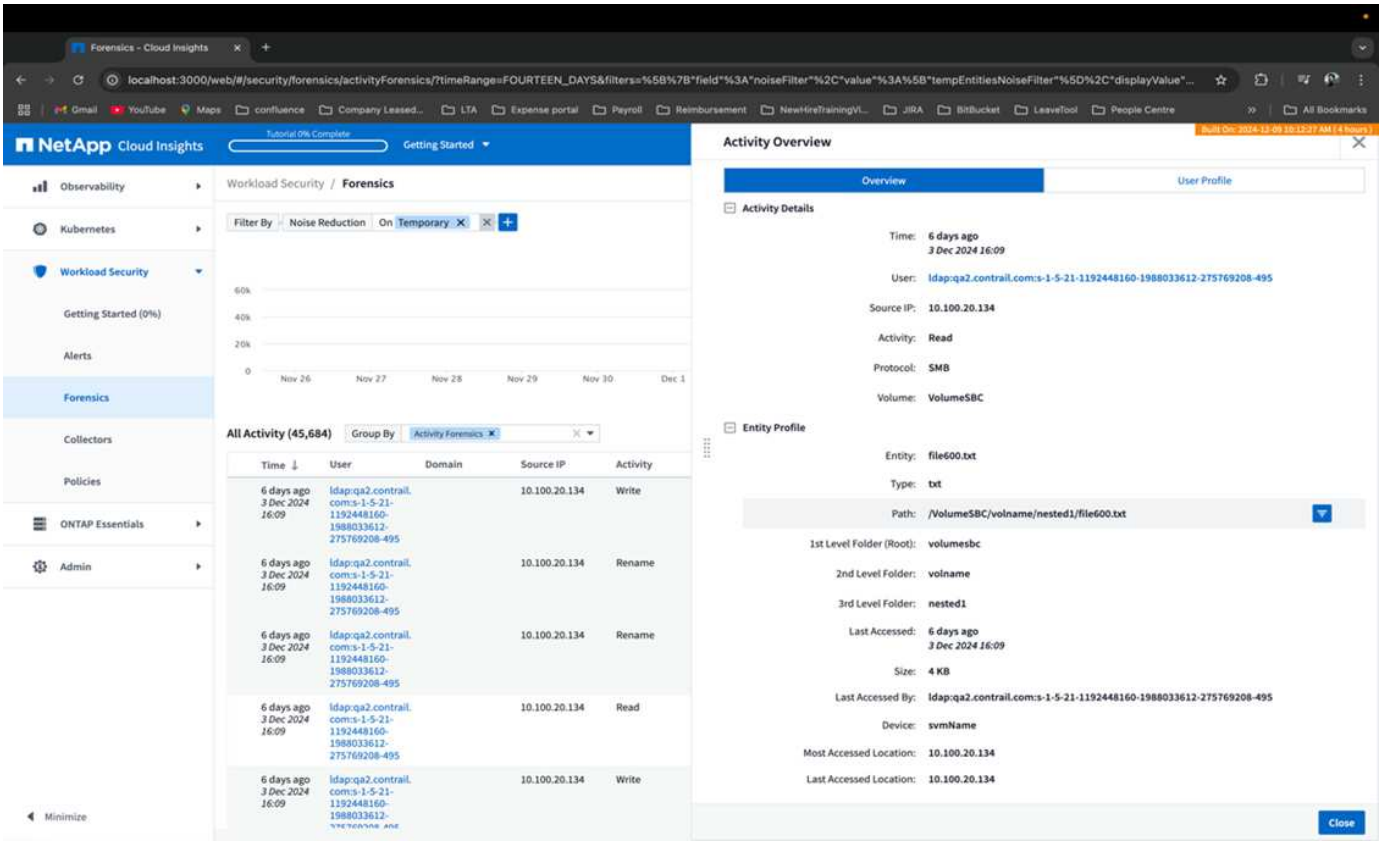
  您可以在圖表中拖曳矩形來縮放圖表。將載入整個頁面以顯示縮放時間範圍。放大時、會顯示可讓使用者縮小的按鈕。

- _ 所有活動 _ 資料的清單。
- 群組依據下拉式清單將提供選項，可依使用者，路徑，實體類型等來分組活動
- 在表格上方會出現一個通用路徑按鈕，我們可以在表格上方取得內含實體路徑詳細資料的滑出面板。

「_*所有活動*」表格顯示下列資訊。請注意、並非所有這些欄都會預設顯示。您可以按一下「齒輪」圖示來選取要顯示的欄。

- 存取實體的*時間*、包括上次存取的年、月、日和時間。
- 以滑出式面板連結存取實體的 * 使用者 * "使用者資訊"。
- 使用者執行的*活動*。支援的類型包括：
  - 變更群組擁有權：群組擁有權屬於檔案或資料夾。如需群組擁有權的詳細資訊，請參閱"此連結。"
  - 變更擁有者：檔案或資料夾的擁有權變更為其他使用者。
  - 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。如果刪除資料夾、則會針對該資料夾和子資料夾中的所有檔案取得_DELETE _事件。
  - 讀取-檔案已讀取。
  - 讀取中繼資料：僅適用於啟用資料夾監控選項。將在Windows上開啟資料夾或在Linux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。
  - 寫入中繼資料-寫入檔案中繼資料、例如權限已變更。
  - 其他變更：上述未提及的任何其他事件。所有未對應的事件都會對應至「其他變更」活動類型。適用於檔案和資料夾。
- **Path** 是 *entity* 路徑。這應該是確切的實體路徑（例如「 */home/userX/nested1/nested2/abc.txt* 」），或是遞迴搜尋路徑的目錄部分（例如「 */home/userX/nested1/nested2/* 」）。注意：此處不允許 regex 路徑模式（例如 *userX* ）。或者，也可以指定如下所述的個別路徑資料夾層級篩選器來進行路徑篩選。
- * 第一層資料夾（根目錄） * 是實體路徑的根目錄（小寫）。
- * 第二層資料夾 * 是實體路徑的第二層目錄（以較低的大小寫表示）。
- * 第三層資料夾 * 是實體路徑的第三層目錄（以較低的大小寫表示）。
- * 第四層資料夾 * 是實體路徑的第四層目錄（以較低的大小寫表示）。
- * 實體類型 * ，包括實體（例如檔案）副檔名（ .doc ， .docx ， .tmp 等）。
- 實體所在的 * 裝置 * 。
- 用於擷取事件的*傳輸協定*。
- 當原始檔案重新命名時、用於重新命名事件的*原始路徑*。根據預設、此欄在表格中不可見。使用欄選取器將此欄新增至表格。
- 實體所在的* Volume *。根據預設、此欄在表格中不可見。使用欄選取器將此欄新增至表格。

選取表格列會開啟滑出面板，其中一個索引標籤中會顯示使用者設定檔，另一個索引標籤則會顯示活動和實體總覽。



預設 _ 群組依據 _ 方法為 _ 活動鑑識 _ 。如果您選取不同的 _ 群組依據 _ 方法（例如，實體類型），則會顯示實體 _ 群組依據 _ 表格。如果沒有選擇，則會顯示 _Group by * all* 。

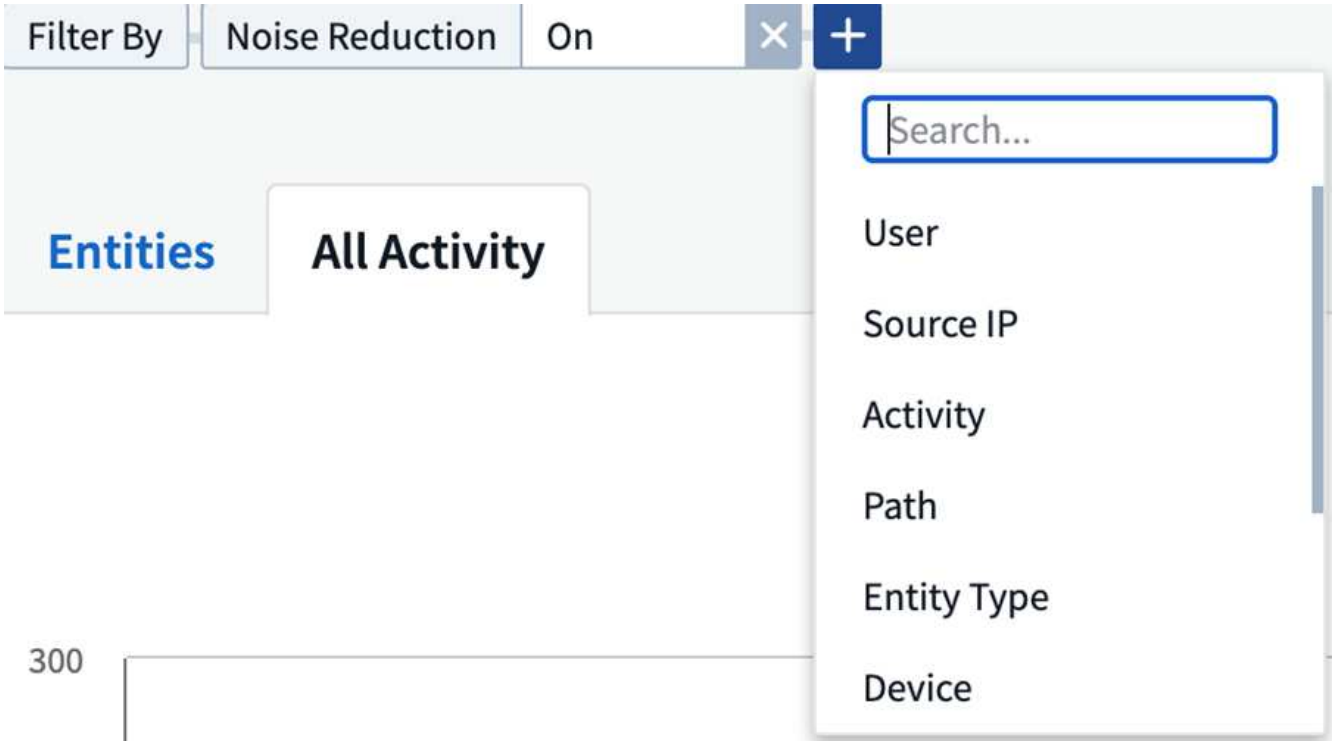
- 活動計數會顯示為超連結；選取此選項會將選取的群組新增為篩選。活動表會根據該篩選條件更新。
- 請注意，如果您變更篩選條件，變更時間範圍或重新整理畫面，則必須重新設定篩選條件，才能返回篩選結果。

篩選取證活動歷程記錄資料

您可以使用兩種方法來篩選資料。

- 可以從滑出面板新增篩選器。此值會新增至頂端_Filter by（篩選條件）清單中的適當篩選條件。
- 輸入「篩選條件」欄位以篩選資料：

  按一下「+」按鈕、從頂端的「篩選條件」小工具中選取適當的篩選條件：



輸入搜尋文字

按Enter或按一下篩選方塊外側以套用篩選條件。

您可以依下列欄位篩選取證活動資料：

- *活動*類型。
- 存取實體的來源**IP**。您必須以雙引號提供有效的來源IP位址、例如「10.1.1.1」。不完整的IP（例如"10.1.1. "、**"10.1.**.*"等）將無法運作。
- *傳輸協定*以擷取特定傳輸協定的活動。
- 執行活動的使用者名稱。您需要提供確切的使用者名稱以進行篩選。無法使用部分使用者名稱進行搜尋、或是以「*」為前置或後置的部分使用者名稱進行搜尋。
- *雜訊抑制*可篩選使用者在過去2小時內建立的檔案。它也可用來篩選使用者存取的暫存檔（例如、.tmp檔案）。
- * 執行活動之使用者的網域 * 。您需要提供 * 精確的網域 * 來進行篩選。搜尋部分網域、或以萬用字元（「 * 」）為前置或後置的部分網域將無法運作。_ 無 _ 可以指定來搜尋遺失的網域。

下列欄位必須遵守特殊篩選規則：

- * 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 Path* ：這應該是確切的實體路徑（例如「 */home/userX/nested1/nested2/abc.txt* 」），或是遞歸搜尋路徑的目錄部分（例如「 *_/home/userX/nested1/nested2/* 」）。注意：此處不允許 regex 路徑模式（例如 * 使用者 X* ）。建議目錄路徑篩選器（以 / 結尾的路徑字串）最多 4 個目錄深，以獲得更快的結果。例如， *"/home/userX/nested1/nested2/"* 。如需詳細資訊、請參閱下表。
- 第一層資料夾（根目錄） - 實體路徑的根目錄作為篩選器。例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 Home 或 Home 。

- 第二層資料夾 - 實體路徑篩選器的第二層目錄。例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 userX 或「 userX 」。
- 第三層資料夾–實體路徑篩選器的第三層目錄。
- 例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 nested1 或「 nested1 」。
- 第四層資料夾 - 實體路徑篩選器的目錄第四層目錄。例如，如果實體路徑為 /home/userX/nested1/nested2/ ，則可使用 nested2 或「 nested2 」。
- * 執行活動的使用者 * ：最好在報價中指定確切的使用者。例如、 _ 「管理員」 _ 。
- 實體所在的設備（SVM）
- *實體所在的Volume *
- 當原始檔案重新命名時、用於重新命名事件的*原始路徑*。

篩選時、上述欄位必須符合下列條件：

- 確切值應在引號內：範例：「searchtext」
- 萬用字元字串不得包含引號：範例：searchtext、*searchtext*會篩選任何包含「searchtext」的字串。
- 字串加上字首、例如：searchtext*、會搜尋以「searchtext」開頭的任何字串。

活動鑑識篩選器範例：

使用者套用的篩選運算式	預期成果	績效評估	留言
路徑 = "/home/userX/nested1/nested2/"	遞迴查詢指定目錄下的所有檔案和資料夾	快速	目錄搜尋最多 4 個目錄的速度很快。
路徑 = "/home/userX/nested1/"	遞迴查詢指定目錄下的所有檔案和資料夾	快速	目錄搜尋最多 4 個目錄的速度很快。
路徑 = 「 /home/userX/nested1/test 」	路徑值與 /home/userX/nested1/test 完全相符	慢一點	與目錄搜尋相比，搜尋的確切搜尋速度較慢。
路徑 = 「 /home/userX/nested1/nested2/nested3/"	遞迴查詢指定目錄下的所有檔案和資料夾	慢一點	搜尋超過 4 個目錄的速度較慢。
任何其他非路徑型篩選器。建議使用報價的使用者和實體類型篩選條件、例如、 User="Administrator" Entity Type ="txt"		快速	

附註：

1. 當所選時間範圍超過 3 天時，「所有活動」圖示旁顯示的「活動」計數會四捨五入至 30 分鐘。例如， 9 月 1 日上午 10 ： 15 至 9 月 7 日上午 10 ： 15 的時間範圍將顯示 9 月 1 日上午 10 ： 00 至 9 月 7 日上午 10 ： 30 的活動計數。
2. 同樣地，當所選時間範圍超過 3 天時，「活動歷程記錄」圖表中顯示的計數度量會四捨五入至 30 分鐘。

排序取證活動記錄資料

您可以依 _ 時間，使用者，來源 IP ，活動， _ ， _ 實體類型 _ ，第一層資料夾（根目錄），第二層資料夾，第三層資料夾和第四層資料夾來排序活動記錄資料。根據預設、表格會依遞減的_Timed_順序排序、表示最新的資料會先顯示。「_Device」和「_Protocol」欄位的排序功能已停用。

非同步匯出使用者指南

總覽

儲存工作負載安全性中的非同步匯出功能是專為處理大型資料匯出而設計。

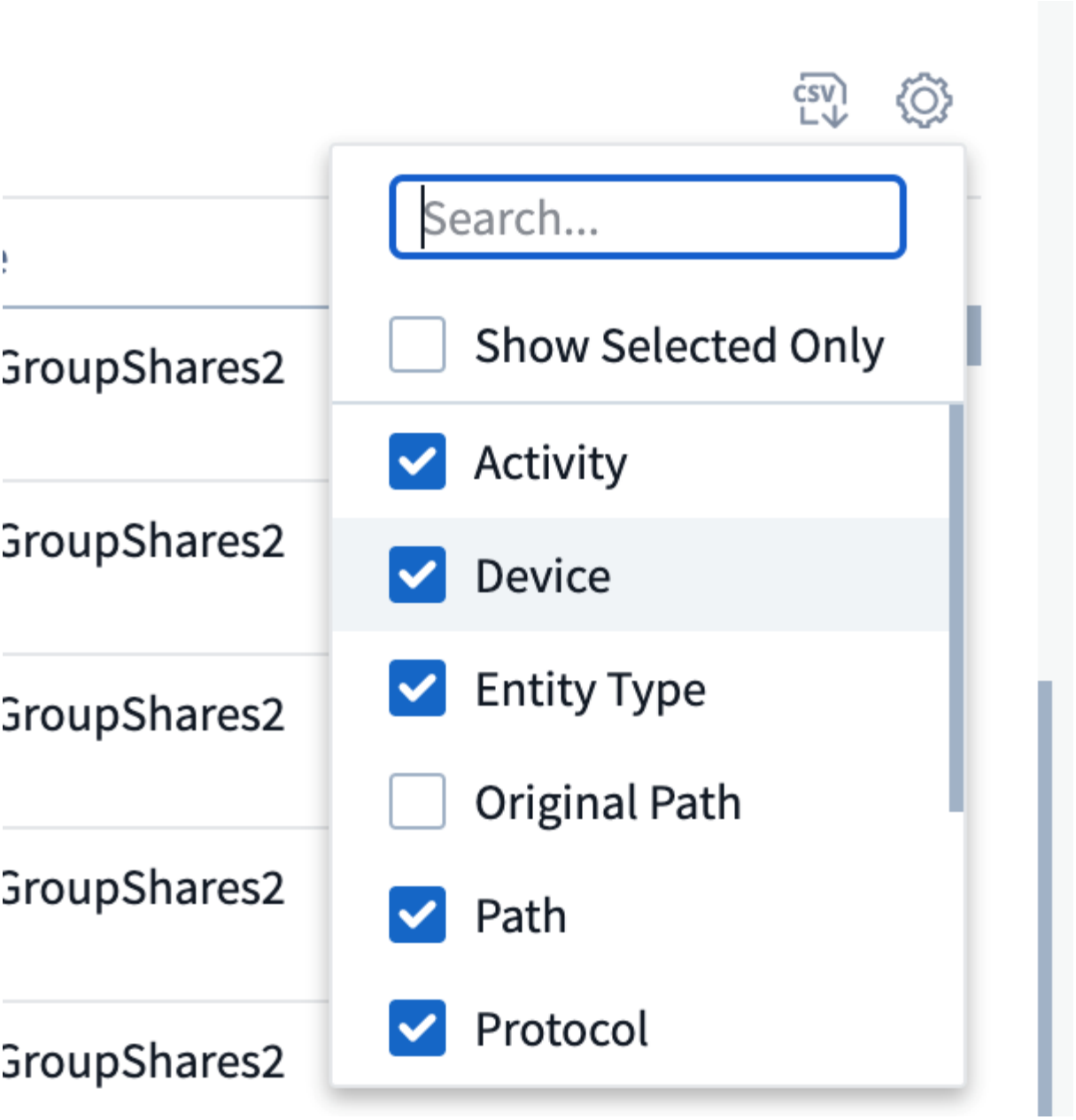
逐步指南：使用非同步匯出匯出資料

1. * 啟動匯出 * ：選取所需的匯出時間長度和篩選條件、然後按一下匯出按鈕。
2. * 等待匯出完成 * ：處理時間可從數分鐘到數小時不等。您可能需要重新整理鑑識頁面數次。匯出工作完成後、將會啟用「下載上次匯出 CSV 檔案」按鈕。
3. * 下載 * ：按一下「下載上次建立的匯出檔案」按鈕、以 .zip 格式取得匯出的資料。此資料將可供下載、直到使用者啟動另一個「非同步匯出」或已過 3 天（以先發生者為準）為止。此按鈕將保持啟用狀態、直到啟動另一個「非同步匯出」為止。
4. * 限制 * ：
    - 非同步下載的數量目前限制為每位使用者 1 次、每位租戶 3 次。
    - 匯出的資料上限為 100 萬筆記錄。

透過 API 擷取取鑑識資料的範例指令碼位於 NetApp 代理程式上的 /opt/oracle/cloudsecure/agent/Export 指令碼 // 。如需指令碼的詳細資訊、請參閱此位置的讀我檔案。

所有活動的欄選擇

「_All activity」（全部活動）表格預設會顯示選取欄。若要新增、移除或變更欄、請按一下表格右側的齒輪圖示、然後從可用欄清單中選取。



活動記錄保留

活動歷程記錄會保留13個月、適用於作用中的工作負載安全環境。

Forensics頁面中篩選器的適用性

篩選器	它的作用	範例	適用於這些篩選器	不適用於這些篩選器	結果
*（星號）	可讓您搜尋所有內容	Auto*03172022 如果搜尋文字包含連字號或底線、請在方括號中提供運算式、例如（ SVM* ）用於搜尋 SVM-123	使用者，實體類型，裝置， Volume ，原始路徑， 1stLevel 資料夾， 2ndLevel 資料夾， 3rdLevel 資料夾， 4thLevel 資料夾		傳回以「 Auto 」開頭並以「 03172022 」結尾的所有資源
？（問號）	可讓您搜尋特定字元數	AutoSabotageUser1_03172022？	使用者，實體類型，裝置， Volume ， 1stLevel 資料夾， 2ndLevel 資料夾， 3rdLevel 資料夾， 4thLevel 資料夾		傳回AutoSabotageUser1_03172022A、AutoSabotageUser1_031720222B、AutoSabotageUser1_031720225等
或	可讓您指定多個實體	AutoSabotageUser1_03172022 或AutoRansomUser4_03162022	使用者，網域，實體類型，原始路徑		傳回任何AutoSabotageUser1_03172022或AutoRansomUser4_03162022
不是	可讓您從搜尋結果中排除文字	非AutoRansomUser4_03162022	使用者，網域，實體類型，原始路徑， 1stLevel 資料夾， 2ndLevel 資料夾， 3rdLevel 資料夾， 4thLevel 資料夾	裝置	傳回所有開頭為「AutoRansomUser4_03162022」的項目
無	在所有欄位中搜尋空值	無	網域		傳回目標欄位為空白的結果

路徑搜尋

包含/不含/的搜尋結果會有所不同

"/AutoDir1/AutoFile03242022"	只能使用精確搜尋；會傳回所有具有正確路徑的活動，例如 /AutoDir1/AutoFile03242022 （不敏感的案例）
" / 自動直接 1/ "	有效；傳回與 AutoDir1 相符之第一層目錄的所有活動（案例不敏感）
"/AutoDir1/AutoFile03242022"	有效；傳回與 AutoDir1 相符的第一層目錄，以及與 AutoFile03242022 相符的第二層目錄的所有活動（案例不敏感）
/AutoDir1/AutoFile03242022 或/AutoDir1/AutoFile03242022	無法運作

不是/AutoDir1/AutoFile03242022	無法運作
不是/AutoDir1	無法運作
不是/AutoFile03242022	無法運作
*	無法運作

本機根 **SVM** 使用者活動變更

如果本機根 SVM 使用者正在執行任何活動、則安裝 NFS 共用的用戶端 IP 現在會納入使用者名稱中、在鑑識活動和使用者活動頁面中會顯示為 <ip-address-of-the-client> 。

例如：

- 如果 SVM-1 受到工作負載安全性的監控、且 SVM 的根使用者將共用裝載於 IP 位址為 10.197.12.40 的用戶端上、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 裝載到另一個 IP 位址為 10.197.12.41 的用戶端、取證活動頁面中顯示的使用者名稱將為 *root@10.197.12.41* 。
- •這是為了依照 IP 位址來分隔 NFS 根使用者活動。以前、所有活動都只由 *root* 使用者執行、沒有 IP 區分。

疑難排解

問題	試試看
在「All Activities」（所有活動）表格的「User」（使用者）欄下、使用者名稱顯示為：「LDAP:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817”」或「LDAP:Default：80038003」。	可能的原因可能是：1.尚未設定使用者目錄收集器。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 Directory Server_。2.已設定使用者目錄收集器，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。如需疑難排解秘訣，請參閱"使用者目錄收集器疑難排解"文件的一節。正確設定後、名稱將在24小時內自動解析。如果仍無法解決、請檢查是否已新增正確的使用者資料收集器。確定使用者確實是新增Active Directory / LDAP目錄伺服器的一部分。
UI中未顯示某些NFS事件。	請檢查下列項目：1.具有POSIX屬性集的AD伺服器之使用者目錄收集器應以從UI啟用的unixid屬性執行。2.從 UI 3 在使用者頁面中搜尋時，應該會看到任何執行 NFS 存取的使用者。NFS不支援原始事件（尚未探索使用者的事件）4。不會監控匿名存取NFS匯出。5.請確定 NFS4.1 版本低於 NFS4.1 。

在 Forensics *All Activity* 或 *Entity* 頁面的篩選器中輸入一些包含如星號（ * ）等萬用字元的字母後，頁面載入速度會非常緩慢。	搜尋字串中的星號（ * ）會搜尋所有項目。但是，諸如 <searchTerm> 或 <searchTerm> 等領先的通配符字符串將導致查詢速度緩慢。若要獲得更好的效能、請改用字首字串、格式為 <searchTerm> * （換句話說、在搜尋詞彙後加上星號（ * ）。範例：使用字串 _testvolume * 、而非 _*testvolume 或 _*test* Volume 。使用目錄搜尋，以遞歸方式查看指定資料夾下的所有活動（階層式搜尋）。例如，「 /path1/path2/path3// 」會在 /path1/path2/path3 下以遞歸方式列出所有活動。或者、也可以使用「 All Activity) 標籤下的「 Add to Filter 」（新增至篩選器）選項。
使用路徑篩選器時、我遇到「要求失敗、狀態碼 500/503 」錯誤。	請嘗試使用較小的日期範圍來篩選記錄。
取證使用者介面使用 *path* 篩選器時，資料載入速度緩慢。	目錄路徑篩選器（以 / 結尾的路徑字串）建議使用最多 4 個目錄深度，以獲得更快的結果。例如，如果目錄路徑為 /aaa/BBB/CCC/DDD ，請嘗試搜尋「 /AAA/BBB/CCC/DDD/」 ，以更快載入資料。

鑑識使用者總覽

每位使用者的資訊都會在「使用者總覽」中提供。使用這些檢視來瞭解使用者特性、相關實體及最近的活動。

使用者設定檔

使用者設定檔資訊包括聯絡資訊和使用者位置。設定檔提供下列資訊：

- 使用者名稱
- 使用者的電子郵件地址
- 使用者管理程式
- 使用者的電話聯絡人
- 使用者位置

使用者行為

使用者行為資訊可識別使用者最近執行的活動和作業。這些資訊包括：

- 最近的活動
  - 上次存取位置
  - 活動圖表
  - 警示
- 過去七天的營運
  - 作業數量

重新整理時間間隔

使用者清單每12小時重新整理一次。

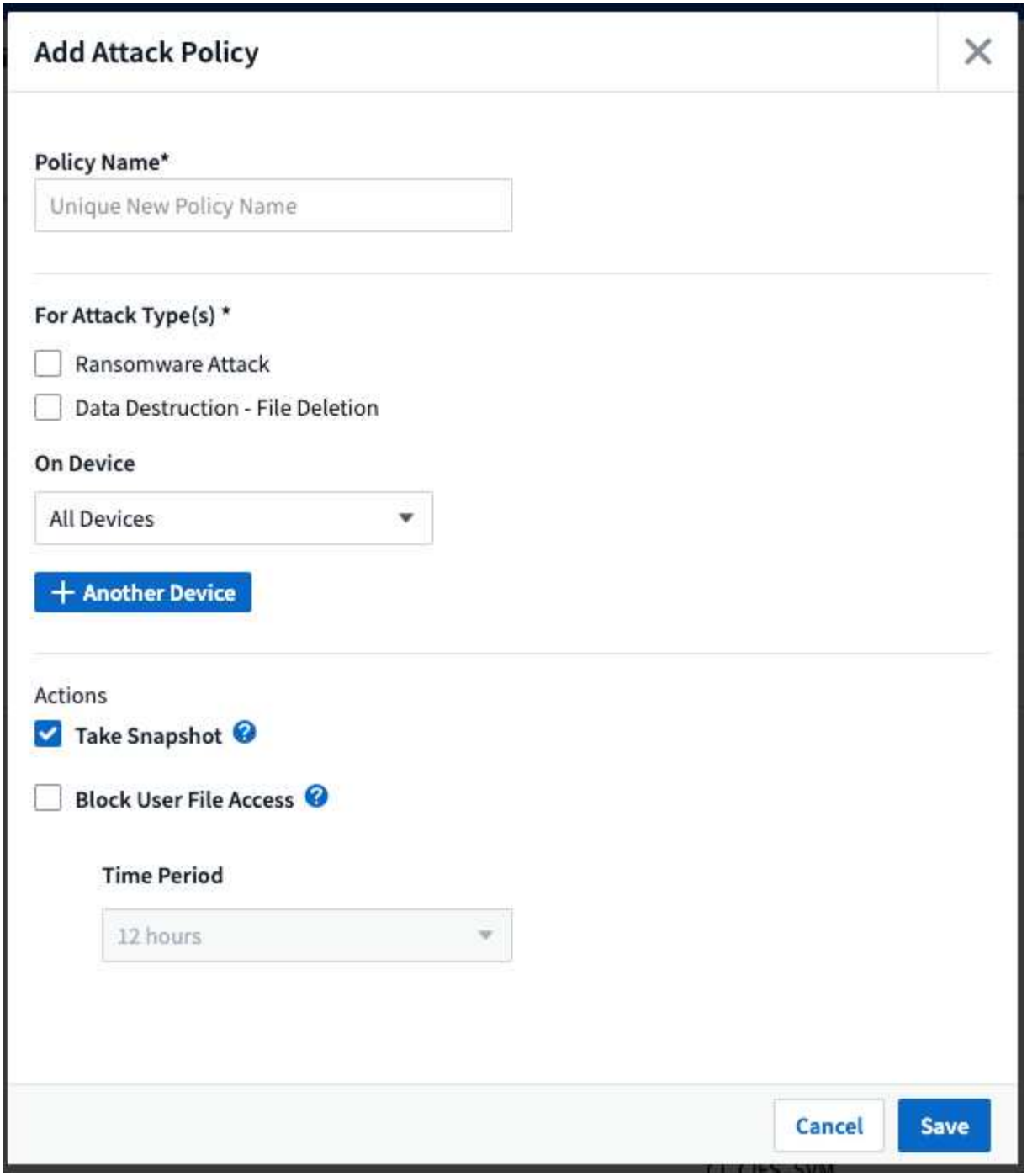
保留政策

如果不再重新整理、使用者清單會保留13個月。13個月後、資料將會刪除。如果您的工作負載安全環境已刪除、則會刪除與環境相關的所有資料。

自動化回應原則

回應原則會觸發動作、例如在發生攻擊或異常使用者行為時、拍攝快照或限制使用者存取。

您可以在特定裝置或所有裝置上設定原則。若要設定回應原則、請選取 * 管理 > 自動回應原則 * 、然後按一下適當的 **+Policy** 按鈕。您可以建立攻擊或警告的原則。



您必須以唯一名稱儲存原則。

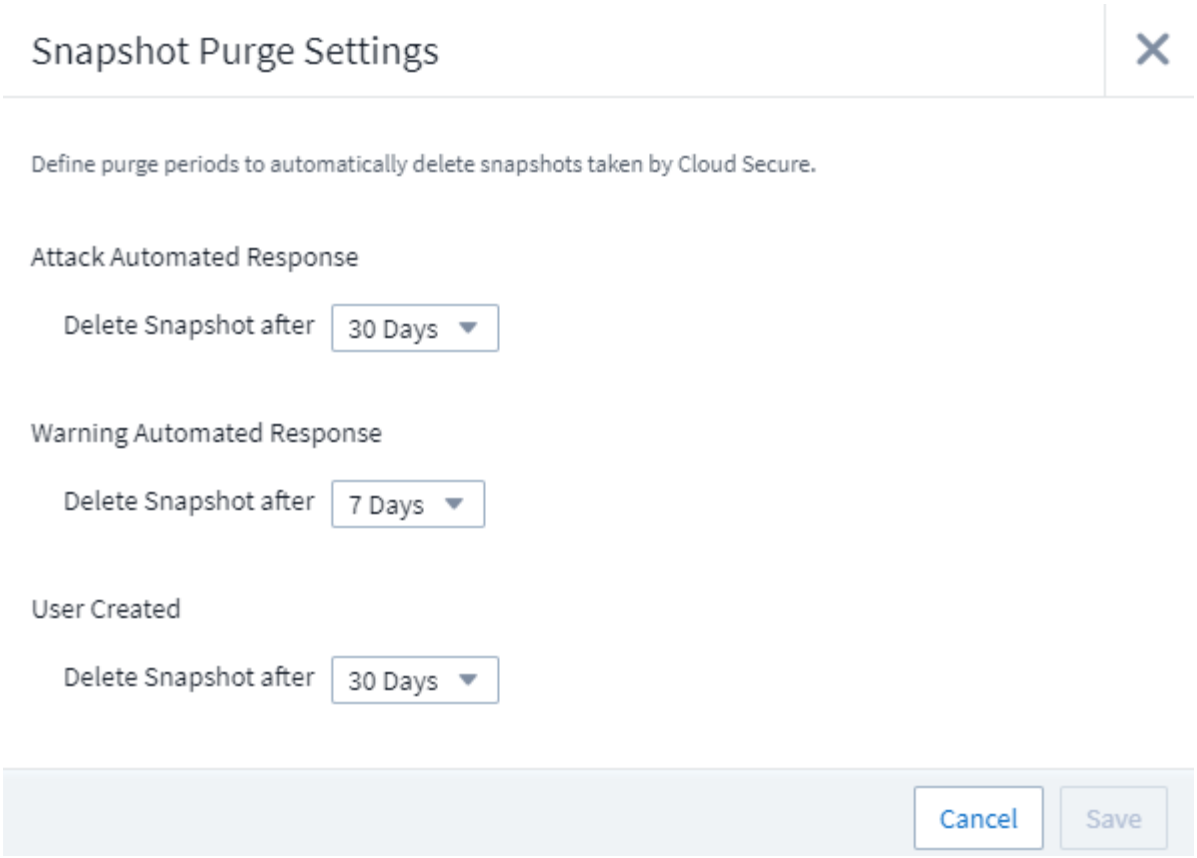
若要停用自動回應動作（例如「拍攝Snapshot」）、只要取消檢查動作並儲存原則即可。

當針對指定的裝置（或所有裝置、如果已選取）觸發警示時、自動回應原則會擷取資料的快照。您可以在上看到快照狀態"警示詳細資料頁面"。

如需限制使用者存取 IP 的詳細資訊，請參閱"限制使用者存取"頁面。

您可以在原則的下拉式功能表中選擇選項、以修改或暫停「自動回應原則」。

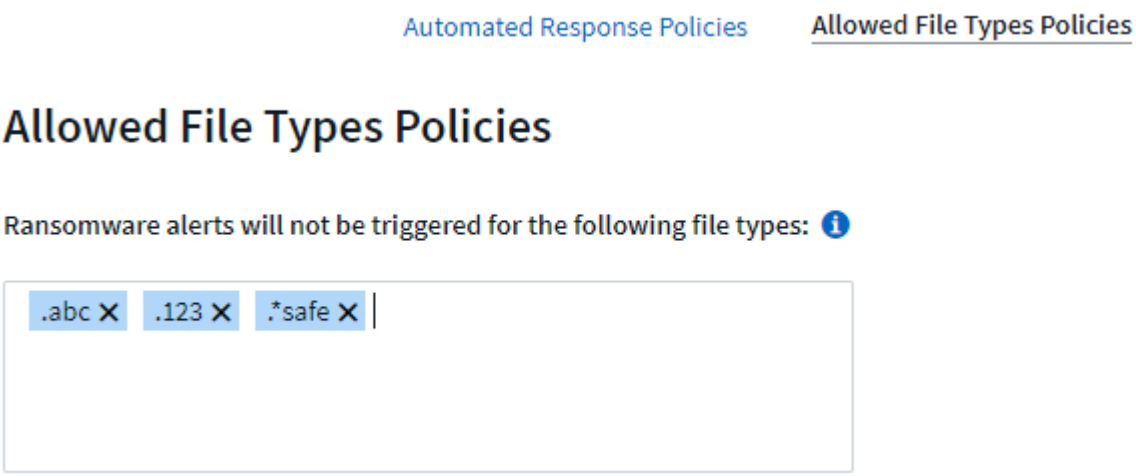
「工作負載安全性」會根據「Snapshot清除」設定、每天自動刪除快照一次。



允許的檔案類型原則

如果偵測到已知副檔名的勒索軟體攻擊、並在警示畫面上產生警示、則可將該副檔名新增至 _ 允許的檔案類型 _ 清單、以避免不必要的警示。

瀏覽至 * 工作負載安全性 > 原則 * 、然後前往 _ 允許的檔案類型原則 _ 索引標籤。



一旦新增至 _ 允許的檔案類型 _ 清單、就不會針對該允許的檔案類型產生勒索軟體攻擊警示。請注意、 _ 允許的檔案類型 _ 原則僅適用於勒索軟體偵測。

例如、如果名為 *test · txt* 的檔案重新命名為 *test · txt · abc* 、且工作負載安全性偵測到勒索軟體攻擊、因為

副檔名是 _ ・ abc_ 、則可以將 _ ・ abc_ 副檔名新增至 _ 允許的檔案類型 _ 清單。將勒索軟體新增至清單後、將不再針對副檔名為 *.abc* 的檔案進行勒索軟體攻擊。

允許的檔案類型可以是完全相符的檔案類型（例如、 ".abc" ）或運算式（例如、 "**.type"** 、 **".type**" 或 "*type" ）。不支援「 .a*c 」、「 .p*f 」類型的運算式。

整合ONTAP 了功能完善的勒索軟體保護功能

此功能使用NAS（NFS和SMB）環境中的工作負載分析功能ONTAP 、主動偵測及警告可能表示勒索軟體攻擊的異常檔案內活動。

有關 ARP "請按這裡"的其他詳細信息和許可證要求，請參閱。

工作負載安全功能與ONTAP VMware整合、可接收ARP事件、並提供額外的分析和自動回應層。

工作負載安全性會接收ONTAP 來自於Arp的事件、並採取下列行動：

1. 將磁碟區加密事件與使用者活動建立關聯、以識別造成損害的原因。
2. 實作自動回應原則（若已定義）
3. 提供鑑識功能：
    - 允許客戶進行資料外洩調查。
    - 找出哪些檔案受到影響、有助於更快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. 啟用了ARP的磁碟區。有關啓用 ARP 的詳細信息"請按這裡"，請參閱。必須透過OnCommand 「支援系統管理程式」來啟用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. 此功能需要叢集層級認證、才能正常運作。換句話說、新增SVM時必須使用叢集層級認證。

需要使用者權限

如果您使用叢集管理認證、則不需要新的權限。

如果您使用的自訂使用者（例如、*CsUser*）具有授予使用者的權限、請依照下列步驟授予工作負載安全性權限、以便從ONTAP Sfor收集與Arp相關的資訊。

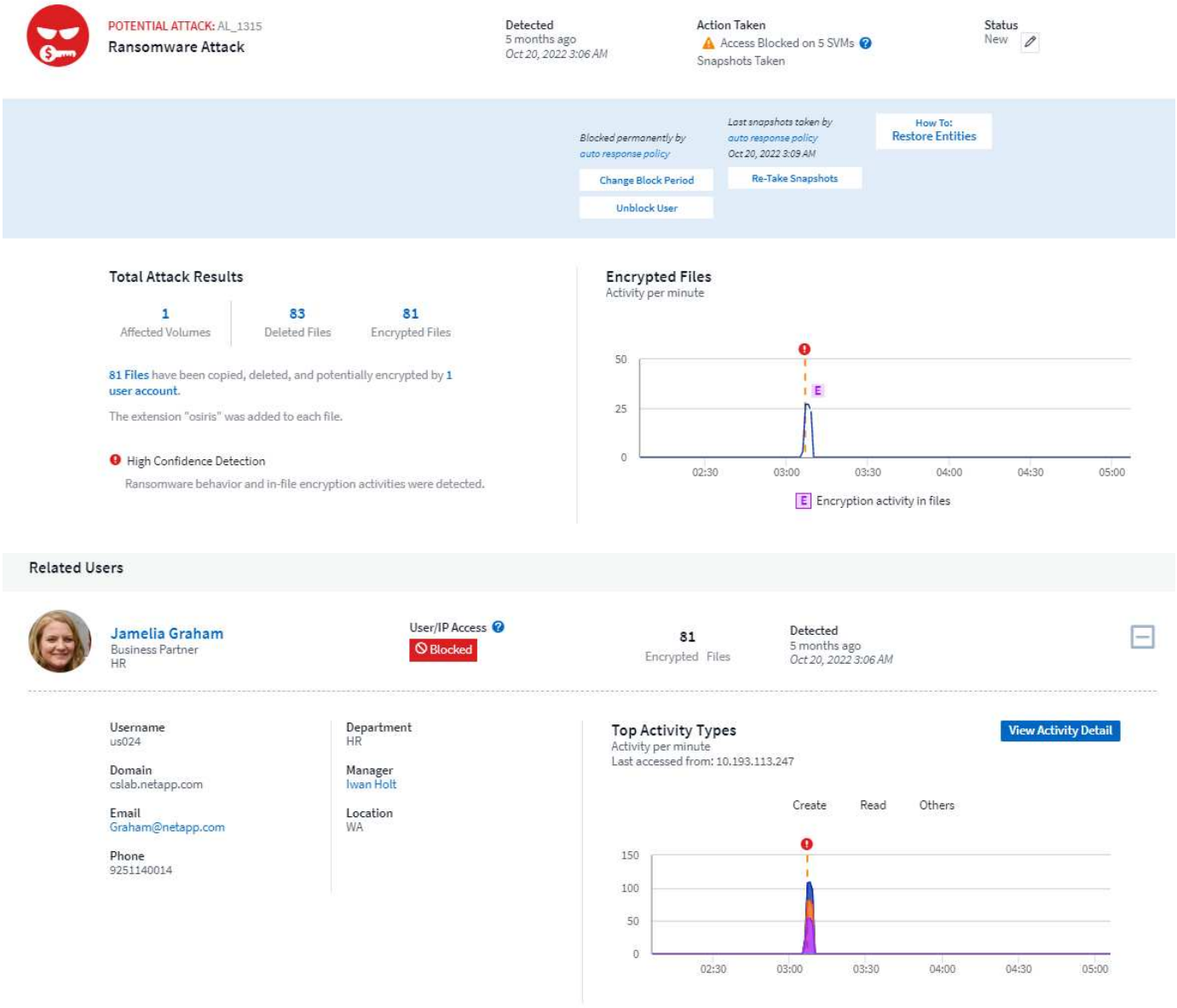
對於具有叢集認證的_CsUser_、請從ONTAP 下列指令行執行下列動作：

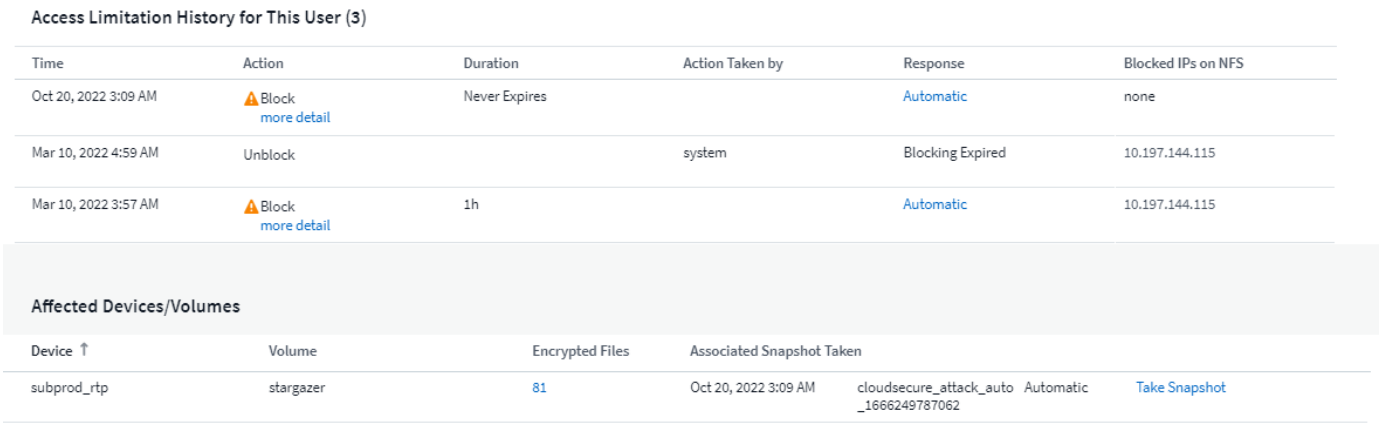
```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application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

瞭解有關配置其他"權限ONTAP"的更多信息。

警示範例

下列為因ARP事件而產生的警示範例：





高可信度橫幅表示攻擊顯示勒索軟體行為及檔案加密活動。加密檔案圖表會指出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未受工作負載安全性監控、但ONTAP 有由效益管理系統產生的ARP事件、則工作負載安全系統仍會接收並顯示這些事件。但是、與警示相關的鑑識資訊以及使用者對應將不會被擷取或顯示。

疑難排解

下表說明已知問題及其解決方法。

問題：	解決方法：
偵測到攻擊後24小時內收到電子郵件警示。在 UI 中、警示會在 Data Infrastructure Insights Workload Security 收到電子郵件之前 24 小時顯示。	當 ONTAP 將 *r*勒索 軟體 *Detected* 事件傳送至資料基礎架構洞見工作負載安全性（即工作負載安全性）時、就會傳送電子郵件。此活動包含攻擊清單及其時間戳記。工作負載安全性UI會顯示第一個受攻擊檔案的警示時間戳記。ONTAP 會在編碼特定數量的檔案時、將「偵測到的勒索軟體」事件傳送至「資料基礎架構洞見」。因此、在UI中顯示警示的時間與電子郵件傳送的時間可能有所不同。

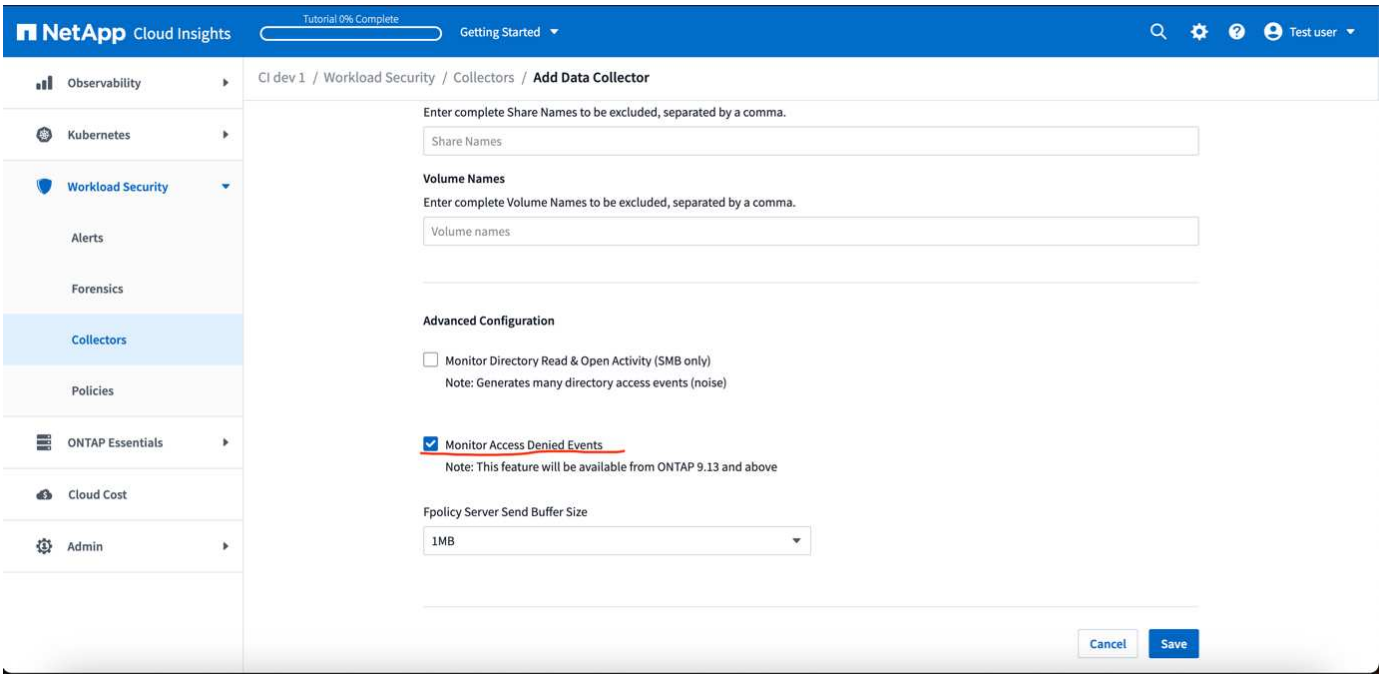
與 ONTAP 存取整合遭拒

ONTAP 存取遭拒功能會在 NAS 環境（ NFS 和 SMB ）中使用工作負載分析、主動偵測並警告檔案作業失敗的情況（例如、使用者嘗試執行他們沒有權限的作業）。這些失敗的檔案作業通知（特別是在安全性相關失敗的情況下）將有助於在早期階段進一步封鎖內部攻擊。

資料基礎架構洞見工作負載安全性與 ONTAP 整合、可接收拒絕存取的事件、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 。
- 工作負載安全管理員在新增收集器或編輯現有收集器時、必須選取「進階組態」下的「監控存取遭拒事件」核取方塊、以啟用「拒絕存取」功能。



需要使用者權限

如果使用叢集管理認證新增 Data Collector 、則不需要新的權限。

如果是使用已授予使用者權限的自訂使用者（例如、 *CsUser* ）來新增收集器、請依照下列步驟、將必要權限授予工作負載安全性、以便向 ONTAP 註冊存取遭拒事件。

若為具有 *CLERY* 認證的 CsUser 、請從 ONTAP 命令列執行下列命令。請注意、 *csrestrole* 是自訂角色、而 *csUser* 是 ONTAP 自訂使用者。

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

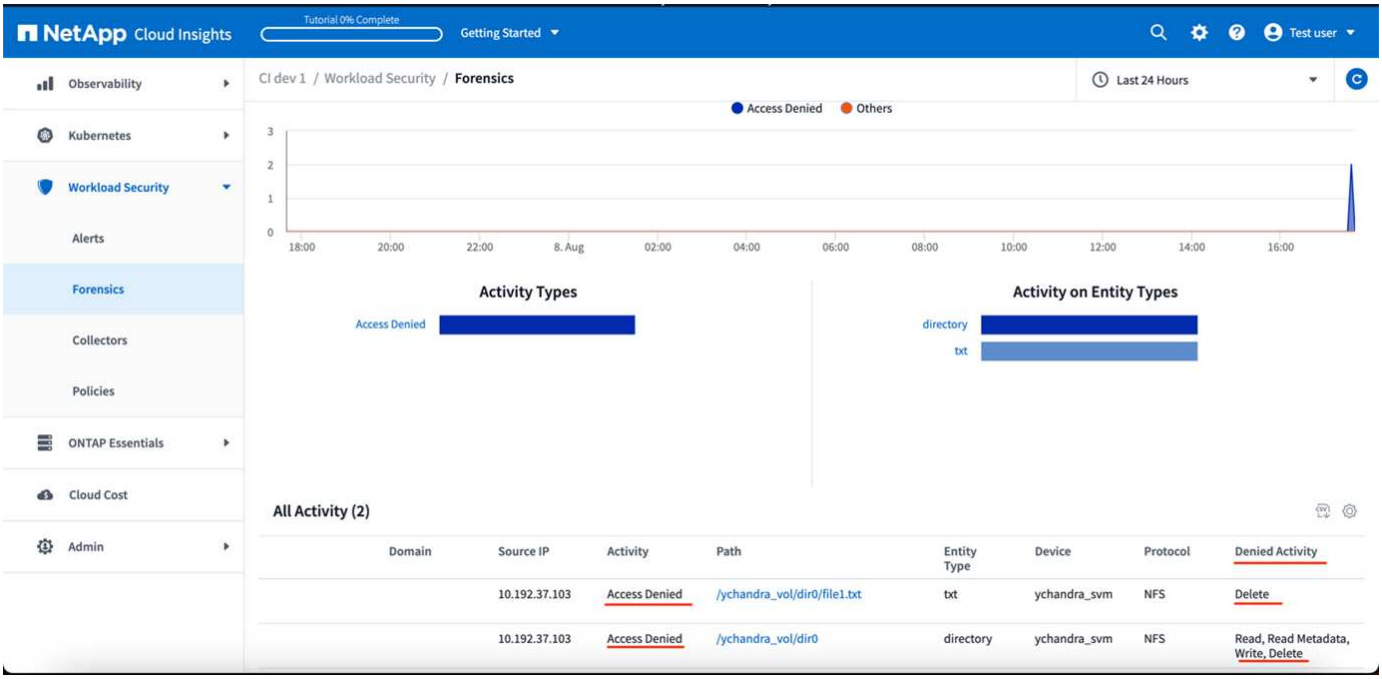
對於具有 *SVM* 認證的 CsUser 、請從 ONTAP 命令列執行下列命令：

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

瞭解有關配置其他"權限ONTAP"的更多信息。

存取遭拒事件

從 ONTAP 系統擷取事件後、工作負載安全性鑑識頁面會顯示存取遭拒事件。除了顯示的資訊外、您也可以從齒輪圖示將 _ 所需活動 _ 欄新增至表格、以檢視特定作業的遺失使用者權限。



封鎖使用者存取

一旦偵測到攻擊、工作負載安全功能就能封鎖使用者存取檔案系統、藉此阻止攻擊。您可以使用自動回應原則、或從警示或使用者詳細資料頁面手動封鎖存取。

當封鎖使用者存取時、您應該定義封鎖時間段。在所選期間結束後、使用者存取權會自動還原。SMB和NFS傳輸協定均支援存取封鎖。

直接封鎖使用者的SMB位址、導致NFS封鎖攻擊的主機機器IP位址。這些機器IP位址將會遭到封鎖、無法存取工作負載安全性所監控的任何儲存虛擬機器（SVM）。

例如、假設工作負載安全性管理10個SVM、而自動回應原則則是針對其中四個SVM進行設定。如果攻擊源自四個SVM之一、則使用者的存取將會在所有10個SVM中遭到封鎖。仍會在原始SVM上執行Snapshot。

如果有四個SVM、其中一個SVM設定為SMB、一個設定為NFS、其餘兩個設定為NFS和SMB、則如果攻擊源自四個SVM中的任一VM、則所有SVM都會遭到封鎖。

使用者存取封鎖的先決條件

此功能需要叢集層級認證、才能正常運作。

如果您使用叢集管理認證、則不需要新的權限。

如果您使用的自訂使用者（例如、*CsUser*）具有授予使用者的權限、請依照下列步驟授予工作負載安全性權限、以封鎖使用者。

對於具有叢集認證的CsUser、請從ONTAP 下列功能執行：

```
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
```

請務必同時檢閱頁面的「權限」區段"設定ONTAP SVM Data Collector"。

如何啟用此功能？

- 在工作負載安全性中、瀏覽至 * 工作負載安全性 > 原則 > 自動回應原則 * 。選擇 *+ 攻擊政策 * 。
- 選取（勾選） _ 封鎖使用者檔案存取 _ 。

如何設定自動使用者存取封鎖？

- 建立新的攻擊原則或編輯現有的攻擊原則。
- 選取應監控攻擊原則的SVM。
- 按一下「封鎖使用者檔案存取」核取方塊。此功能會在選取時啟用。
- 在「Time Period」（時間期間）下、選取應套用封鎖的時間。
- 若要測試自動封鎖使用者，您可以透過模擬攻擊"模擬指令碼"。

如何知道系統中是否有封鎖的使用者？

- 在警示清單頁面中、如果任何使用者遭到封鎖、畫面頂端會顯示橫幅。
- 按一下橫幅將會帶您前往「使用者」頁面、您可以在頁面上看到封鎖的使用者清單。
- 在「Users」（使用者）頁面中、有一欄名為「User/IP Access」（使用者/IP存取）。在該欄中、會顯示使用者封鎖的目前狀態。

手動限制及管理使用者存取

- 您可以前往警示詳細資料或使用者詳細資料畫面、然後從這些畫面手動封鎖或還原使用者。

使用者存取限制歷程記錄

在警示詳細資料與使用者詳細資料頁面的使用者面板中、您可以檢視使用者存取限制歷程記錄的稽核：時間、動作（區塊、取消區塊）、持續時間、採取的行動、 NFS的手動/自動及受影響IP。

如何停用此功能？

您可以隨時停用此功能。如果系統中有受限的使用者、您必須先還原他們的存取權限。

- 在工作負載安全性中、瀏覽至 * 工作負載安全性 > 原則 > 自動回應原則 * 。選擇 *+ 攻擊政策 * 。
- 取消選取（取消勾選） _ 封鎖使用者檔案存取 _ 。

所有頁面都會隱藏此功能。

手動還原NFS的IP

如果您的工作負載安全性試用期到期、或代理程式/收集器當機、請使用下列步驟手動還原ONTAP 任何來自VMware的IP。

1. 列出SVM上的所有匯出原則。

```
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. 在SVM上、將「cloudsecure_rRule」做為用戶端比對的所有原則中刪除規則、方法是指定其各自的規則索引。工作負載安全性規則通常為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刪除（可選步驟確認）。

```
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.
```

手動還原**SMB**的使用者

如果您的工作負載安全性試用版過期、或代理程式/收集器當機、請使用下列步驟手動還原ONTAP 任何來自VMware的使用者。

您可以從使用者清單頁面取得工作負載安全性中封鎖的使用者清單。

1. 使用ONTAP 叢集_admin_認證登入到32個叢集（您想要解除封鎖使用者的位置）。（若為Amazon FSX、請使用FSX認證登入）。
2. 執行下列命令、列出所有SVM中所有被SMB工作負載安全性封鎖的使用者：

```
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.
```

在上述輸出中、有2位使用者被網域CSLAB封鎖（US030、US040）。

1. 當我們從上述輸出中找出位置後、請執行下列命令以解除封鎖使用者：

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

. 執行下列命令、確認使用者已解除封鎖：

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

不應針對先前封鎖的使用者顯示任何項目。

疑難排解

問題	試試看
有些使用者並未受到限制、但仍有攻擊。	1.確定 SVM 的資料收集器和代理程式處於 _Running 狀態。如果停止資料收集器和代理程式、工作負載安全功能將無法傳送命令。2.這是因為使用者可能已從具有新 IP 的機器存取儲存設備，而此前並未使用過。使用者透過其存取儲存設備的主機IP位址進行限制。請查看UI（警示詳細資料>此使用者的存取限制歷程記錄>受影響的IP）、以取得受限的IP位址清單。如果使用者從IP與受限IP不同的主機存取儲存設備、則使用者仍可透過不受限IP存取儲存設備。如果使用者嘗試從IP受限的主機存取、則儲存設備將無法存取。
手動按一下「限制存取」會顯示「此使用者的IP位址已受到限制」。	要限制的IP已受到其他使用者的限制。
無法修改原則。原因：未授權使用該命令。	請檢查是否使用CsUser、是否會如上所述授予使用者權限。
NFS的使用者（IP位址）封鎖正常運作、但對於SMB / CIFS、我看到錯誤訊息：「從SID到網域名稱的轉換失敗。原因逾時：通訊端未建立」	這種情況可能發生於_CsUser_沒有執行ssh的權限。（請確保叢集層級的連線、然後確定使用者可以執行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*對於具有叢集認證的 _*CsUser* ，請從 ONTAP 命令列執行下列動作：安全性登入角色 create -role csrole -cmddirname "vserver 輸出原則規則 " -access all 安全性登入角色 create -role csrole -cmddirname "vserver cifle -cmddirname -access all 安全性登入角色並非使用者角色 ONTAP 。
我收到錯誤訊息 _SID 轉譯失敗。 _ 原因： 255 ：錯誤：命令失敗：未獲得該命令的授權錯誤：當使用者應該遭到封鎖時、「存取檢查」不是可辨識的命令 _ 。	當 *CsUser* 沒有正確的權限時、可能會發生這種情況。如需詳細資訊、請參閱 "使用者存取封鎖的先決條件" 。套用權限之後、建議您重新啟動 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所列。--- 安全登入角色 create -role csrole -cmddirname "vserver 匯出原則規則 " -access all security 登入角色 create -role csrole -cmddirname set -access all security 登入角色 create -role csrole -cmddirname "vserver CIFS 工作階段 " -access all security 登入 角色 create -role csrole -cmddirname "vserver name-mapping" -access all ---

工作負載安全性：模擬攻擊

您可以使用本頁上的指示、模擬攻擊、以便使用隨附的勒索軟體模擬指令碼來測試或示範

工作負載安全性。

開始之前要注意的事項

- 勒索軟體模擬指令碼僅適用於Linux。
- 此指令碼隨工作負載安全代理程式安裝檔案一起提供。它適用於任何已安裝工作負載安全性代理程式的機器。
- 您可以在工作負載安全代理程式機器上執行指令碼、不需要準備其他Linux機器。不過、如果您偏好在其他系統上執行指令碼、只要複製指令碼並在該處執行即可。

至少有**1**、**000**個範例檔案

此指令碼應在SVM上執行、其中的資料夾含有要加密的檔案。建議在該資料夾和任何子資料夾中至少有1、000個檔案。檔案不可為空白。請勿使用相同的使用者建立檔案並加密。「工作負載安全性」將此視為低風險活動、因此不會產生警示（亦即、相同的使用者會修改剛建立的檔案）。

有關的說明，請參閱以下"以程式設計方式建立非空白檔案"內容。

執行模擬器之前的準則：

1. 請確定加密的檔案不是空白的。
2. 請務必加密超過50個檔案。少數檔案將會被忽略。
3. 請勿多次使用相同的使用者執行攻擊。幾次之後、工作負載安全性會學習這種使用者行為、並假設這是使用者的正常行為。
4. 請勿加密剛建立相同使用者的檔案。變更使用者剛建立的檔案並不視為風險活動。而是使用其他使用者所建立的檔案、或是在建立檔案並加密檔案之間等待數小時。

準備系統

首先、將目標Volume掛載到機器上。您可以掛載NFS掛載或CIFS匯出。

若要在Linux中掛載NFS匯出：

```
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 4.1版、Fpolicy不支援。

若要在Linux中掛載CIFS：

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

接下來、設定資料收集器：

1. 如果尚未設定工作負載安全性代理程式、請加以設定。

2. 如果尚未完成、請設定SVM資料收集器。

執行勒索軟體模擬器指令碼

1. 登入（ssh）工作負載安全代理程式機器。
2. 瀏覽至：*/opt /NetApp/cloudsec/agent/install*
3. 呼叫不含參數的模擬器指令碼、查看使用狀況：

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

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

加密測試檔案

若要加密檔案、請執行下列命令：

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

還原檔案

若要解密、請執行下列命令：

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

多次執行指令碼

為使用者產生勒索軟體攻擊之後、請切換至其他使用者、以產生額外的攻擊。「工作負載安全性」會學習使用者行為、不會在短時間內針對相同使用者的反覆勒索軟體攻擊發出警示。

以程式設計方式建立檔案

建立檔案之前、您必須先停止或暫停資料收集器處理。將資料收集器新增至代理程式之前、請先執行下列步驟。如果您已新增資料收集器、只要編輯資料收集器、輸入無效密碼、然後儲存即可。這會暫時將資料收集器置於錯誤狀態。附註：請務必記下原始密碼！

建議選項是"暫停收集器"在建立檔案之前。]

在執行模擬之前、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、或使用指令碼（請參閱以下範例）以程式設計方式建立檔案。無論使用何種方法、請複製至少1、000個檔案。

如果您選擇以程式設計方式建立檔案、請執行下列動作：

1. 登入值機員方塊。
2. 將NFS匯出從檔案管理器的SVM掛載到代理機器。CD至該資料夾。
3. 在該資料夾中建立一個名為createfiles.sh的檔案
4. 將下列行複製到該檔案。

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

5. 儲存檔案。
6. 確保對檔案執行權限：

```
 chmod 777 ./createfiles.sh
```

. 執行指令碼：

```
./createfiles.sh
```

將在目前資料夾中建立1000個檔案。

7. 重新啟用資料收集器

   如果您在步驟1中停用資料收集器、請編輯資料收集器、輸入正確的密碼並儲存。請確定資料收集器已恢復執行狀態。

8. 如果您在執行這些步驟之前暫停了收集器，請務必"恢復收集器"執行。

設定警示、警告及代理/資料來源收集器健全狀況的電子郵件通知

若要設定工作負載安全警示收件者、請按一下*管理>通知*、然後在每個收件者的適當區段中輸入電子郵件地址。

潛在攻擊警示與警告

若要傳送_潛在攻擊_警示通知、請在_傳送可能的攻擊警示_區段中輸入收件者的電子郵件地址。電子郵件通知會針對警示上的每個動作傳送至警示收件者清單。

若要傳送_警告_通知、請在_傳送警告警報_區段中輸入收件者的電子郵件地址。

代理程式與資料收集器健全狀況監控

您可以透過通知來監控代理程式和資料來源的健全狀況。

若要在代理程式或資料來源收集器無法運作時接收通知、請在「資料收集健全狀況警示」區段中輸入收件者的電子郵件地址。

請謹記下列事項：

- 只有在代理程式/收集器停止報告至少一小時後、才會傳送健全狀況警示。
- 在指定的24小時內、只會傳送一封電子郵件通知給目標收件者、即使代理程式或資料收集器中斷連線的時間較長。
- 如果代理程式發生故障、將會傳送一個警示（而非每個收集器一個警示）。此電子郵件將包含所有受影響SVM的清單。
- Active Directory收集失敗會報告為警告、不會影響勒索軟體偵測。
- 「快速入門」設定清單現在包含一個新的_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「資料收集健全狀況警示」中輸入電子郵件 ID 。
- 「啟用升級通知」核取方塊即會啟用。
- 代理程式和資料收集器升級電子郵件通知會在計畫升級前一天傳送至電子郵件 ID 。

疑難排解

問題：	試用：
電子郵件 ID 出現在「資料收集器健全狀況警示」中，但我沒有收到通知。	通知電子郵件會從 NetApp 資料基礎架構 Insights 網域傳送、例如、來自 NetApp .com 。有些公司會封鎖來自外部網域的傳入電子郵件。確保 NetApp Data Infrastructure Insights 網域的外部通知已列入白名單。

工作負載安全API

工作負載安全性API可讓NetApp客戶和獨立軟體廠商（ISV）將工作負載安全性與其他應用程式（例如CMDB或其他票證系統）整合。

API存取需求：

- API存取權杖模式用於授予存取權。
- API權杖管理是由具有管理員角色的工作負載安全使用者執行。

API文件（Swagger）

登入工作負載安全性並瀏覽至*管理> API存取*、即可找到最新的API資訊。按一下「* API Documentation （API文件*）」連結。API 文件是以 Swagger 為基礎，提供 API 的簡短說明和使用資訊，並可讓您在租戶上試用。

如果呼叫鑑識活動 API 、請使用 cloudsecure_forensics 。 * v2* API 。如果您要對此 API 進行多個呼叫、請確定呼叫是依序進行、而非平行進行。多個平行呼叫可能會導致 API 逾時。

API存取權杖

在使用工作負載安全性API之前、您必須先建立一個或多個* API存取權杖*。存取權杖可授予讀取權限。您也可以設定每個存取權杖的到期日。

若要建立存取權杖：

- 按一下「管理**> API**存取」
- 按一下「**+ API**存取權杖」
- 輸入* Token Name*
- 指定*權杖過期*

您的權杖只能在建立程序期間複製到剪貼簿並儲存。建立權杖之後、就無法擷取這些權杖、因此強烈建議您複製權杖、並將其儲存在安全的位置。系統會提示您按一下「複製API存取權杖」按鈕、然後再關閉權杖建立畫面。

您可以停用、啟用及撤銷權杖。停用的權杖可以啟用。

權杖可從客戶的角度，授予 API 一般用途存取權，並管理其租戶範圍內的 API 存取權。

應用程式會在使用者成功驗證及授權存取後、收到存取權杖、然後在呼叫目標API時、將存取權杖作為認證。傳遞的權杖會通知API、該權杖的承載器已獲授權存取API、並根據授權期間授予的範圍執行特定動作。

傳遞存取權杖的HTTP標頭為* X-CloudInsights：Apikes*

例如、使用下列項目來擷取儲存資產：

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
```

其中、_<API_Access_Token >>是您在API存取金鑰建立期間所儲存的權杖。

如需詳細資訊、請參閱「管理**> API**存取」下的「*API*文件」連結。

透過 API 擷取資料的指令碼

工作負載安全代理程式包含匯出指令碼、可將要求的時間範圍分成較小的批次、以利平行呼叫 v2 API 。

指令碼位於： *_/opt/oracle/cloudsecure/agent/export NetApp -script* 。同一目錄中的 README 檔案提供使用說明。

以下是呼叫指令碼的範例命令：

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

主要參數： - `--iteration_interval 12` ：將所要求的時間範圍分成 12 小時的間隔。- `--num_workers 3` ：使用 3 個執行緒平行擷取這些時間間隔。