Cloud Secure

Cloud Insights

NetApp
August 16, 2022

目錄

Cloud Secure

關於Cloud Secure 本公司

利用可據以行動的內部威脅情報、協助保護您的資料。Cloud Secure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。獨特的運作方式適用於雲端和內部部署儲存系統、可針對惡意使用者行為提供即時警示。Cloud Secure

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

功能入門Cloud Secure

您必須先完成一些組態工作、才能開始使用Cloud Secure 功能以監控使用者活動。

此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Cloud Secure 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*管理>資料收集器*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"

代理程式需求

您必須 "安裝代理程式" 以便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	執行下列其中一種授權版本的電腦：Red Hat Enterprise Linux 7.x、8.x 64位元CentOS 7.x 64位元CentOS 8 Stream Ubuntu 20至22 64位元本電腦不應執行其他應用程式層級軟體。建議使用專屬伺服器。
命令	安裝、執行指令碼及解除安裝時、必須使用「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：/opp/netapp 35 GB（最小）
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、Cloud Secure 以及連接至該實例所需的連接埠（80或443）。

請注意Cloud Secure ：可以將此Same Agent安裝在Cloud Insights 同一部機器上、做為一個收購單元和/或代理程式。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* Cloud Secure 的*不全環境：

傳輸協定	連接埠	目的地	方向	說明
TCP	443..	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	傳出	存取Cloud Insights功能

傳輸協定	連接埠	目的地	方向	說明
TCP	443..	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	傳出	存取驗證服務

歐洲 Cloud Secure 的*《》《》《*》

傳輸協定	連接埠	目的地	方向	說明
TCP	443..	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	傳出	存取Cloud Insights功能
TCP	443..	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	傳出	存取驗證服務

若為* APAC型* Cloud Secure 的環境：

傳輸協定	連接埠	目的地	方向	說明
TCP	443..	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	傳出	存取Cloud Insights功能
TCP	443..	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	傳出	存取驗證服務

網路內規則

傳輸協定	連接埠	目的地	方向	說明
TCP	389（LDAP）636（LDAPS / start-TLS）	LDAP伺服器URL	傳出	連線至LDAP
TCP	443..	叢集或SVM管理IP位址（視SVM收集器組態而定）	傳出	API與ONTAP NetApp通訊
TCP	35000 - 55000	SVM資料LIF IP位址	傳入/傳出	與ONTAP 適用於Fpolicy活動的功能溝通
TCP	7.	SVM資料LIF IP位址	雙向	在不同時使用的情況下進行雙向。ONTAP Cloud Secure代理程式Ping SVM LIF。

相關：

請參閱 "事件率檢查器" 規模調整的相關資訊文件。

安裝過程Cloud Secure

使用一或多個代理程式收集使用者活動資料。Cloud Secure代理程式會連線至您環境中的裝置、並收集傳送至Cloud Secure 該SaaS層進行分析的資料。請參閱 "代理程式需求" 設定代理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。

安裝代理程式的步驟

1. 以系統管理員或帳戶擁有者身分登入Cloud Secure 您的支援環境。
2. 按一下*管理>資料收集器>代理程式>+agent*

   系統會顯示「新增代理程式」頁面：

   [新增代理程式1] | *Add-agent-1.png*
3. 選取要安裝代理程式的作業系統。
4. 確認代理伺服器符合最低系統需求。
5. 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）_。
6. 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。

   [代理程式安裝附有Proxy附註]

7. 按一下「複製到剪貼簿」圖示以複製安裝命令。
8. 在終端機視窗中執行安裝命令。
9. 安裝成功完成時、系統會顯示下列訊息：

   [新代理程式偵測] | *new-agent-detect.png*

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Cloud Secure 將由資訊系統使用的連接埠。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. 「Udo firewall-cmd --fonary --區域=public-add-port=35000-55000/tcp」
2. 「Udo firewall-cmd --reload」

依照您的平台執行後續步驟：

- CentOS 7.x / RHEL 7.x *：
  1. 「Udo iptater-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. 「Udo firewall-cmd --ZONE =公有-清單連接埠| grep 35000」（適用於CentOS 8）

範例輸出：

```
35000-55000/tcp
```

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。錯誤會重新導向至標準輸出、並使用「journalctl -u cloudsecure-agent.service`」命令顯示在服務記錄中。此命令可用於進一步疑難排解問題。
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」。	支援的平台僅適用於RHEL 7.x / CentOS 7.x Cloud Secure請確定您未在RHEL 6.x或CentOS 6.x系統上安裝代理程式。
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。
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「傳送系統狀態cloudsecure-agent.service`」檢查代理程式服務的狀態。1.檢查記錄是否顯示「無法啟動Cloud Secure 支援服務」訊息。2.檢查代理機器中是否存在cssys使用者。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。《Udo id cssys》（《Udo 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。「Udo useradd cssys」「show group」、「cssys」5。之後執行下列命令重新啟動代理程式服務：「Udo systemctl重新啟動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.向代理機器SSH。2.執行下列命令、在之後重新啟動代理程式服務：「Udo systemctl restart cloudsecure-agent.service` 3.透過「傳送系統狀態cloudsecure-agent.service`」檢查代理程式服務的狀態。4.代理程式應進入連線狀態。
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、Cloud Secure 因此當Zscaler CA簽署時、就會顯示出該驗證憑證、因此代理程式不信任該通訊內容。	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、Cloud Secure 則無法使用。
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「tokent=……」 …・/cloudseced-agent-install.sh」安裝命令、然後按Enter鍵。4.安裝應可繼續進行。

問題：	解決方法：
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Cloud Insights 「不完整」序號以開啟案例、並將記錄附加到案例中、如前所述。	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（cloudseced-agent-症狀。zip）。答/opp/NetApp/cloudsec/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。答ID cssys b.群組cssys c.Cat /etc/os-release

刪除**Cloud Secure** 一個功能不一的代理程式

當您刪除Cloud Secure 某個解決方法時、必須先刪除所有與代理程式相關的資料收集器。

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Cloud Secure 這個入口網站刪除。

   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*管理>資料收集器>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

可設定為從Active Directory伺服器收集使用者屬性。Cloud Secure

開始之前

- 您必須是Cloud 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. 在功能表中、按一下Cloud Secure ：管理>資料收集器>使用者目錄收集器>+使用者目錄收集器、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*
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Cloud Secure 《LDAP使用者權限：

  "ldapsearch -o ldim-wap=no -ll -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、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" 可連線至AD伺服器的任何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。

[AD連線]

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。
網域使用者的選用屬性不會出現在Cloud Secure 「無法使用者設定檔」頁面上。	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。

問題：	解決方法：
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。」	針對AD伺服器提供不正確的IP或FQDN。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」。	針對AD伺服器提供不正確的IP或FQDN。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、何時會進行AD同步？	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。
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.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「電話號碼」。4.現在、請依照上述說明使用Active Directory Explorer工具來瀏覽Active Directory、並查看正確的屬性名稱。3.確定Active Directory中有一個名為「電話號碼」的屬性、其中確實有使用者的電話號碼。5、讓我們在Active Directory中說、它已改為「電話網路電話」。6.然後編輯CloudSecure User Directory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、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號碼。

問題：	解決方法：
如果Active Directory（AD）伺服器上已啟用加密憑證（SSL）、Cloud Secure 則無法連接到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**LDAP**目錄伺服器收集器

您可以設定Cloud Secure 使用此功能、從LDAP目錄伺服器收集使用者屬性。

開始之前

- 您必須是Cloud 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「支援」功能表中、按一下Cloud Secure ：管理**>**資料收集器**>**使用者目錄收集器**>+**使用者目錄收集器、然後選取* LDAP目錄伺服器*

   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=user,CN=accounts,DC=domain,DC=companyname,DC=com uid=john,CN=user,CN=accounts,DC=dorp,DC=company,DC=com（適用於使用者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Cloud Secure 《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。

- 安裝LDAP檔案總管 (http://ldaptool.sourceforge.net/) 或Java LDAP Explorer (http://jxplorer.org/) 可連線至LDAP伺服器的任何Windows機器上。
- 使用LDAP目錄伺服器的使用者名稱/密碼連線至LDAP伺服器。

[LDAP連線]

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。
網域使用者的選用屬性不會出現在Cloud Secure 「無法使用者設定檔」頁面上。	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。」	針對AD伺服器提供不正確的IP或FQDN。編輯並提供正確的IP位址或FQDN。///

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「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。
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.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「電話號碼」。4.現在、請依照上述說明使用Active Directory Explorer工具來瀏覽LDAP目錄伺服器、並查看正確的屬性名稱。3.確保在LDAP目錄中有一個名爲「電話號碼」的屬性、該屬性確實具有使用者的電話號碼。5、讓我們在LDAP目錄中說、它已改為「電話網路電話」。6.然後編輯CloudSecure User Directory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、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號碼。
如果Active Directory（AD）伺服器上已啟用加密憑證（SSL）、Cloud Secure 則無法連接到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。

Amazon FSX for NetApp ONTAP 的「架構組態」

此資料收集器可收集Amazon FSX for NetApp ONTAP 的檔案與使用者存取資料。此資料收集器將逐步提供給Cloud Insights 整個「穩定」服務區域。如果Cloud Insights 您在自己的《不景》中沒有看到此收藏器的圖示、請聯絡您的銷售人員。

代理機器組態

請使用下列步驟來設定機器以做Cloud Secure 為一個物件代理程式：

1. 登入AWS主控台並瀏覽至EC2-instances頁面、然後選取Launch instance。
2. 選取RHEL或CentOS AMI的適當版本、如中所述 "需求"。
3. 在Amazon FSX for NetApp ONTAP 的VPC和子網路中建立「代理程式」方塊、此方塊與Amazon FSX for NetApp的執行個體位於相同的VPC和子網路中。

   或是Agent Box應位於VPC中、可連線至Amazon FSX for NetApp ONTAP VPC。

   請確定代理程式與Amazon FSX for NetApp ONTAP 之間存在雙向通訊。
4. 選取T2.xLarge（4個vCPU和16 GB RAM）作為已配置資源。
   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並解壓縮原生Linux套件。

安裝**Cloud Secure** 此功能

1. 以系統管理員或帳戶擁有者身分登入Cloud Insights 您的支援環境。
2. 瀏覽Cloud Secure 至「資料收集器」>「資料收集器」、然後按一下「值機員」索引標籤。
3. 按一下「+Agent」、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。

   只Cloud Secure 要符合所有的代理程式先決條件、即可安裝此程式。

如需詳細步驟、請參閱Cloud Secure 《》 "代理程式安裝" 第頁、

設定ONTAP SVM Data Collector

使用資料收集器從裝置收集檔案和使用者存取資料。Cloud Secure

開始之前

- 下列項目支援此資料收集器：
  - 更新版本。Data ONTAP若要獲得最佳效能、請在Data ONTAP 何處使用VMware版本 "此問題" 已修正。
  - SMB傳輸協定3.1版及更早版本
  - NFS傳輸協定4.0版及更早版本
  - 支援從支援的更新版本為支援FlexGroup ONTAP
- 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。其中只支援_default_和_sync來源_。
- 代理程式 "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）。
- 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管理員叢集/ SVM管理使用者名稱和密碼、您可以建立具有較低權限的自訂使用者、如中所述 "「權限注意事項」" 部分。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 "本文檔 ONTAP"。
- 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：[SVM命令輸出範例]

- 確認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、請跳過此步驟。clusterShell：：>「安全登入密碼-使用者名稱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、請跳過此步驟。clusterShell：：>「安全登入解除鎖定-使用者名稱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、請跳過此步驟。clusterShell：：>「網路介面修改-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。

  請參閱 "代理程式需求" 以取得組態資訊。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。

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Cloud Secure Sfuse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。設定Cloud Secure 使用叢集管理IP的資料收集器時、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 none
security login role create -role csrole -cmddirname "network interface"
-access readonly
security login role create -role csrole -cmddirname version -access
readonly
security login role create -role csrole -cmddirname volume -access
readonly
security login role create -role csrole -cmddirname vserver -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 role create -role csrole -cmddirname "vserver export-policy
rule" -access all -query "-policyname cloudsecure_*"
```

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Cloud Secure Sfuse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Cloud Secure 使用者名稱「CsUser」和密碼設定為使用Vserver Management IP時、請使用「CsUser」。

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 role create -vserver <vservername> -role csrole -cmddirname
"vserver export-policy rule" -access all -query "-policyname
cloudsecure_*"
```

設定資料收集器

組態步驟

1. 以系統管理員或帳戶擁有者身分登入Cloud Insights 您的支援環境。
2. 按一下*管理>資料收集器>+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、選項如下：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。

疑難排解

下表說明已知問題及其解決方法。

發生錯誤時、請按一下「_Status」（狀態）欄中的「_Mor詳細 資料」、以取得錯誤的詳細資料。

[]

問題：	解決方法：
資料收集器會執行一段時間、並在隨機時間後停止、失敗時顯示：「錯誤訊息：連接器處於錯誤狀態。服務名稱：稽核。故障原因：外部fpolicy伺服器過載。"	來自於此的事件率ONTAP 遠高於值機員方塊所能處理的事件率。因此連線終止。當中斷連線時、請檢查CloudSecure中的尖峰流量。您可以從* CloudSecure >活動鑑識> All Activ練習*頁面查看。如果尖峰彙總流量高於值機員方塊所能處理的流量、請參閱「事件率檢查器」頁面、瞭解如何在值機員方塊中調整收集器部署的規模。如果代理程式安裝於2021年3月4日之前的Agent方塊中、請在Agent方塊中執行下列命令：回應「net.core。rmem_max = 8388608」>>/etc/syscl.conf回應「net.ipve.tcp_rmem = 40962097152 8388608'>>/etc/syscntl.conf syscl.conf syscp from the collector重新啟動後、重新啟動。

問題：	解決方法：
Collector會報告錯誤訊息：「在連接器上找不到可連線至SVM資料介面的本機IP位址」。	這很可能是ONTAP 因為位在邊上的網路問題。請遵循下列步驟：1.請確定SVM資料LIF或管理LIF上沒有防火牆、無法與SVM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可從代理VM進行Ping。發生問題時、請檢查閘道、網路遮罩和路由以取得LIF。您也可以嘗試使用叢集管理IP透過ssh登入叢集、然後ping代理IP。請確定代理程式IP可調校：*network ping -vserver <vserver name>-destination <Agent IP>-lIF <LIF Name>-show-detail* _如果無法調校、請確定*ONTAP* 位於的網路設定正確無誤、以便代理程式機器可調校。*3.*如果您嘗試透過叢集*IP*進行連線但無法運作、請嘗試直接透過*SVM IP*進行連線。請參閱上述步驟、瞭解透過*SVM IP*進行連線的步驟。*4.*透過*SVM IP*和*vsadmin*認證新增收集器時、請檢查*SVM LIF*是否已啟用*Data plus Mgmt*角色。在這種情況下、*ping SVM LIF*會正常運作、但*SSH*到*SVM LIF*則無法運作。如果是、請建立僅限*SVM*管理*LIF*、並嘗試透過此*SVM*管理僅*LIF*進行連線。*5.*如果仍無法運作、請建立新的*SVM LIF*、然後嘗試透過該*LIF*進行連線。確定子網路遮罩設定正確。*6.*進階除錯：*a*）在*ONTAP* 不執行*b*）嘗試從*CloudSecure UI*將資料收集器連接至*SVM*。*c*）等待錯誤出現。停止*ONTAP* 封包追蹤。*d*）從*ONTAP* 資訊系統開啟封包追蹤。可在此位置查看：https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/_ e）確認存在從ONTAP Setc到Agent Box的同步。f）ONTAP 如果不存在來自不支援的Syn、ONTAP 則這是指在資訊系統中存在防火牆問題。g）在ONTAP 支援的地方開啟防火牆、ONTAP 以便讓支援鏈接代理程式方塊。7.如果仍無法運作、請洽詢網路團隊、確定沒有外部防火牆封鎖ONTAP從「VMware連線至代理程式」方塊的連線。8.如果以上皆無法解決問題、請使用開啟案例 "NetApp支援" 以取得進一步協助。
訊息：「無法判斷ONTAP [hostname:<IP Address>的資訊類型。原因：連線錯誤至儲存系統<IP位址>：主機無法連線（主機無法連線）"	1.確認已提供正確的SVM IP管理位址或叢集管理IP。2.SSH連線至您要連線的SVM或叢集。連線後、請確認SVM或叢集名稱正確無誤。
錯誤訊息：「連接器處於錯誤狀態。service.name：稽核。故障原因：外部fpolicy伺服器已終止。"	1.防火牆很可能會封鎖代理程式機器中的必要連接埠。確認已開啟連接埠範圍35000-55000/TCP、讓代理機器從SVM連線。此外、請確保ONTAP 沒有啟用任何防火牆、從「邊」封鎖與代理機器的通訊。2.在「代理程式」方塊中輸入下列命令、並確定連接埠範圍已開啟。_Sudo iptarts-SAVE

問題：	解決方法：
Grep 3500*範例輸出應如下所示：_A in_public_allow -p tcp -m tcp -dport 35000 -m conntrack -ctst態new -j Accept_3。登入SVM、輸入下列命令、並檢查是否未設定任何防火牆來封鎖與ONTAP 之通訊。_系統服務防火牆show __系統服務防火牆原則show_"檢查防火牆命令" 就在邊上。ONTAP4. SSH至您要監控的SVM/叢集。從SVM資料LIF Ping Agent Box（支援CIFS、NFS傳輸協定）、並確保ping正常運作： _network ping -vserver <vserver name>-destination <Agent ip>-lIF <LIF Name>-show-detect_如果無法ping通、請確定ONTAP 支援更新的網路設定正確、以便代理機器能夠ping通。如果透過2個資料收集器將單一SVM新增兩次至租戶、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。然後資料收集器會顯示「執行中」狀態、並開始接收來自SVM的事件。基本上、在租戶中、只能透過1個資料收集器新增1個SVM。1 SVM不應透過2個資料收集器新增兩次。6.在兩Cloud Secure 個不同的版本環境（租戶）中新增相同SVM的情況下、最後一個將永遠成功。第二個收集器會使用自己的IP位址來設定fpolicy、然後啟動第一個。因此第一個收集器將停止接收事件、其「稽核」服務將進入錯誤狀態。若要避免這種情況發生、請在單一環境中設定每個SVM。	活動頁面未顯示任何事件。
1.檢查ONTAP 收集器是否處於「執行中」狀態。如果是、請開啟部分檔案、確保CIFS用戶端VM上產生部分CIFS事件。2.如果未看到任何活動、請登入SVM並輸入下列命令。*<SVM>EVENT log show -SOURSfpolicy_Please ensure that are no errors related to fpolicy*（事件日誌顯示-*SOURSfpolicy*_請 確保沒有與*fpolicy*相關的錯誤）。*3.*如果未看到任何活動、請登入*SVM*。輸入下列命令：<SVM>fpolicy show_檢查是否已設定名為「clouded_」的fpolicy原則、且狀態為「on」。如果未設定、則代理程式很可能無法在SVM中執行命令。請確認已遵循頁面開頭所述的所有先決條件。	SVM Data Collector處於錯誤狀態、錯誤訊息為「代理程式無法連線至收集器」
1.代理程式可能過載、無法連線至資料來源收集器。2.檢查有多少資料來源收集器連接至代理程式。3.也請在UI的「All Active"（所有活動）頁面中檢查資料流率。4、如果每秒活動數量大幅增加、請安裝另一個代理程式、並將部分資料來源收集器移至新的代理程式。	SVM Data Collector會顯示錯誤訊息「fpolicy.server.connectError: Node失敗、無法與FPolicy伺服器建立連線：12.195.15.146」（原因：「Select Timed Out」（選擇逾時））
在SVM/叢集中啟用防火牆。因此fpolicy引擎無法連線至fpolicy伺服器。可用於取得更多資訊的CLI包括：事件記錄檔show -SOUR叢fpolicy、其中顯示錯誤事件記錄檔show -source fpolicy -功能 變數事件、行動、說明、其中顯示更多詳細資料。ONTAP"檢查防火牆命令" 就在邊上。ONTAP	錯誤訊息：「Connector處於錯誤狀態。服務名稱：稽核。故障原因：SVM上找不到有效的資料介面（角色：資料、資料傳輸協定：NFS或CIFS或兩者、狀態：UP）。」
確保有作業介面（做為CIFS/NFS的資料和資料傳輸協定角色）。	資料收集器會進入「錯誤」狀態、然後在一段時間後進入「執行中」狀態、然後再次返回「錯誤」。此週期會重複。

問題：	解決方法：
這通常發生在下列案例中：1.新增多個資料收集器。2.顯示這類行為的資料收集器、將會在這些資料收集器中新增1個SVM。表示2個以上的資料收集器連接至1個SVM。3.確保1個資料收集器只連接1個SVM。4.刪除其他連線至相同SVM的資料收集器。	連接器處於錯誤狀態。服務名稱：稽核。失敗原因：無法設定（SVM svmname上的原則。原因：在'fpolicy.policy.scoe-modify:"felf"中為「res-to -include'元素指定的值無效
共用名稱必須在沒有任何報價的情況下提供。編輯ONTAP 「SVM DSC」組態以修正共用名稱。_包括和排除共享_不適用於長清單的共享區名稱。如果您要納入或排除大量共用、請改用依磁碟區篩選。	叢集中有未使用的現有fPolicies。安裝Cloud Secure 完不安裝的不知道該怎麼做？
建議刪除所有現有未使用的fpolicy設定、即使它們處於中斷連線狀態。以「cloudseced_」開頭的字元建立fpolicy。Cloud Secure可以刪除所有其他未使用的fpolicy組態。用於顯示fpolicy清單的CLI命令：_fpolicy show_刪除fpolicy組態的步驟：_fpolicy disable-vserver <svmname>-police-name <policy_name>_fpolicy刪除-vserver <svmname>-policy_name>-policy_name <policy_name_vpolicy <vmname -policy -vms_delete policy -policy <vpolicy -name_external policy -name>	啟用Cloud Secure 了不穩定功能之後ONTAP 、效能受到影響：延遲偶爾會變得很高、IOP偶爾會變得很低。
確保您使用Data ONTAP 的是版本不一致的版本 "此問題" 已修正。推薦使用的最低版本為9.8P7。ONTAP如果ONTAP 使用的是9.8p7之前的版本、而且發現此效能問題、ONTAP 則可以變更此版本的更新緩衝區大小、以改善ONTAP 不實的效能。如果您想要瀏覽此選項、但在新增新的資料收集器或編輯現有的資料收集器時卻看不到此設定、請聯絡NetApp支援部門。	資料收集器發生錯誤、顯示此錯誤訊息。「錯誤：連接器處於錯誤狀態。服務名稱：稽核。失敗原因：無法在SVM SVM_TEST上設定原則。原因：缺少ZAPI欄位值：事件。「
從只設定NFS服務的新SVM開始著手。在ONTAP 功能不均的情況下新增一個功能不整的SVM資料收集器Cloud Secure 。CIFS被設定為SVM允許的傳輸協定、同時將ONTAP SVM Data Collector加入Cloud Secure 到等到Cloud Secure 資訊收集器顯示錯誤為止。由於未在SVM上設定CIFS伺服器、Cloud Secure所以如左側所示的錯誤會由SIRSH.顯示。編輯ONTAP 《SVM資料收集器》、並視允許的傳輸協定取消CIFS檢查。儲存資料收集器。它會在僅啟用NFS傳輸協定的情況下開始執行。	資料收集器會顯示錯誤訊息：「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）」。

如果您仍遇到問題、請聯絡*「說明」>「支援*」頁面中提及的支援連結。

設定Cloud Volumes ONTAP 《The Data Collector

使用資料收集器從裝置收集檔案和使用者存取資料。Cloud Secure

儲存組態Cloud Volumes ONTAP

請參閱OnCommand 《VMware Cloud Manager文件》、以設定單一節點/ HA AWS執行個體來裝載Cloud Secure 此支援程式：https://docs.netapp.com/us-en/occm/index.html[]

組態完成後、請依照下列步驟設定SVM：https://docs.netapp.com/us-

en/cloudinsights/task_add_collector_svm.html[]

代理機器組態

請使用下列步驟來設定機器以做Cloud Secure 為一個物件代理程式：

步驟

1. 登入AWS主控台並瀏覽至EC2-instances頁面、然後選取_Launch instance_。
2. 請選擇本頁所述版本適當的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**Cloud Secure** 此功能

1. 以系統管理員或帳戶擁有者身分登入Cloud Insights 您的支援環境。
2. 瀏覽Cloud Secure 至「支援資料」>「資料收集器」、然後按一下「*代理程式」索引標籤。
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Cloud Secure 包含所有項目的資訊代理程式 "代理程式先決條件" 達成。

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

使用者管理

使用者帳戶可透過不受資料管理的功能進行管理。Cloud Secure Cloud Insights

提供四種使用者帳戶層級：帳戶擁有者、系統管理員、使用者及來賓。Cloud Insights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Cloud Secure 其中一個功能指派給每位使用者：

角色	存取Cloud Secure
系統管理員	可執行所有Cloud Secure 的功能、包括警示、鑑識、資料收集器、自動回應原則和API等Cloud Secure 功能。管理員也可以邀請其他使用者、但只能指派Cloud Secure 功能不二的角色。
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Cloud Secure 入即可
2. 在功能表中、按一下*管理>使用者管理*

   您將會轉寄至Cloud Insights的User Management（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Cloud Insights 《關於使用者帳戶和角色的資訊 "使用者角色" 文件。

SVM事件率檢查器

「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。代理程式最多可支援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fillowing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”.
```

6. 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規模調整指南：

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
```

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]#
```

疑難排解

問：如果我在已設定Cloud Secure 為使用效益的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此程序？
答：事件率檢查器即使已設定Cloud Secure 為供使用的SVM、也能正常運作。應該沒有影響。
問：我可以增加執行指令碼的SVM數量嗎？
答：可以。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。
問：如果增加SVM數量、是否會增加指令碼的執行時間？
答：不可以指令碼最多可執行5分鐘、即使SVM數量增加也沒問題。
問：我可以增加執行指令碼的SVM數量嗎？
答：可以。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。
問：如果增加SVM數量、是否會增加指令碼的執行時間？
答：不可以指令碼最多可執行5分鐘、即使SVM數量增加也沒問題。

警示

「更新警示」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。Cloud Secure

[警示清單]

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。

[變更警示狀態]

- 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（Cloud Secure 由VMware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（此範例顯示潛在的勒索軟體攻擊）：[勒索軟體警示範例]

詳細資料頁面（此範例顯示潛在的勒索軟體攻擊）：[勒索軟體詳細資料頁面範例]

執行Snapshot動作

當偵測到惡意活動時、利用自動擷取快照功能來保護資料、確保資料安全備份。Cloud Secure

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

自動拍攝的快照：[警示行動畫面、1000]

手動快照：[警示行動畫面、1000]

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。如果刪除了此功能、則與環境相關的所有資料也會一併刪除。Cloud Secure

疑難排解

問題：	試用：
對於由Snapshot（Cloud Secure CS）所拍攝的快照、CS快照是否有清除/歸檔期間？	不可以CS快照並未設定任何清除/歸檔期間。使用者需要定義CS快照的清除原則。請參閱 "本文檔 ONTAP" 如何設定原則。
在這種情況ONTAP 下、每小時執行一次快照。此功能是否Cloud Secure 會受影響？CS快照是否會在每小時快照的地方執行？預設的每小時快照是否會停止？	不影響每小時快照。Cloud SecureCS快照不會佔用每小時的快照空間、而且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Snapshot拍攝將會失敗、Cloud Secure 而且會顯示錯誤訊息、指出Snapshot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如ONTAP 需相關資訊、請參閱《VMware產品資料》 "設定Snapshot刪除原則"。

問題：	試用：
無法擷取快照。Cloud Secure	請確定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[proper權限已指派]。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
快照失敗、因為SVM上的舊警示已從Cloud Secure 無法執行、隨後又重新新增。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Cloud Secure 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SVM時、就可能發生這種情況。啟用ONTAP 支援功能中的特定LIF、並從Cloud Secure 功能表中觸發_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Cloud Secure 在整個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。本頁概述您環境中的活動、重點說明下列資訊：

- 顯示_ActivityHistory（活動記錄）的圖表（根據所選的整體時間範圍、每分鐘/每5分鐘/每10分鐘存取一次）

  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。

- 活動類型_的圖表。若要依活動類型取得活動記錄資料、請按一下對應的x軸標籤連結。
- 「實體類型」上的「活動」圖表。若要依實體類型取得活動記錄資料、請按一下對應的x軸標籤連結。
- 「所有活動」資料的清單

「_*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 [齒輪圖示]。

- 存取實體的*時間*、包括上次存取的年、月、日和時間。
- 使用連結存取實體的*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。

- 實體的*路徑*、並連結至 "實體詳細資料"
- 實體類型、包括實體（例如檔案）副檔名（.doc,.docx、.tmp,等等）
- 實體所在的*設備*
- 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。

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。

1. 將游標暫留在表格中的欄位上、然後按一下出現的篩選圖示。此值會新增至頂端_Filter by（篩選條件）清單中的適當篩選條件。
2. 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：

   [實體Filer、寬=500]

   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*可篩選使用者所建立的新檔案（即過去2小時內）。它也可用來篩選使用者存取的暫存檔（例如、.tmp檔案）。

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
- 實體路徑
- 執行活動的使用者
- 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。

排序取證活動記錄資料

您可以依時間、使用者、來源IP、活動、路徑_和實體類型_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。

匯出所有活動

您可以按一下「活動記錄」表格上方的「_Export」（匯出）按鈕、將活動記錄匯出至.CSV檔案。請注意、只會匯出前10、000筆記錄。

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。

[活動選擇器、寬=30%]

活動記錄保留

活動記錄保留13個月、以供動態Cloud Secure 的不活躍的地方使用。

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*管理>資料收集器>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。請移至*管理>資料收集器>使用者目錄收集器*、然後檢查狀態。請參閱 "使用者目錄收集器疑難排解" 說明文件中的一節、以取得疑難排解秘訣。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.在UI 3的使用者頁面中搜尋時、應該會看到執行NFS存取的任何使用者。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.確定NFS版本的使用版本低於NFS4.1。

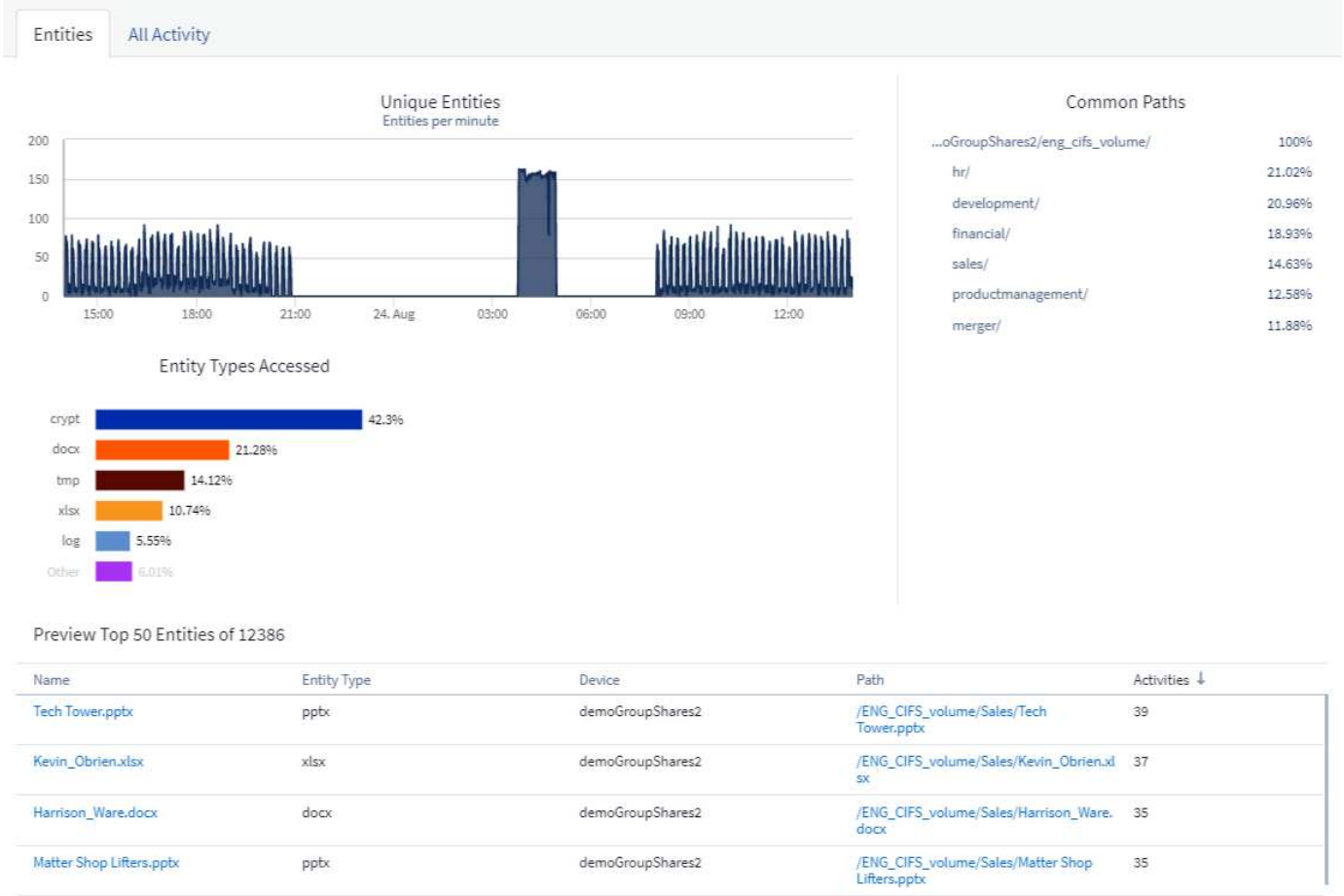
「鑑識實體」頁面

「鑑識實體」頁面提供您環境中實體活動的詳細資訊。

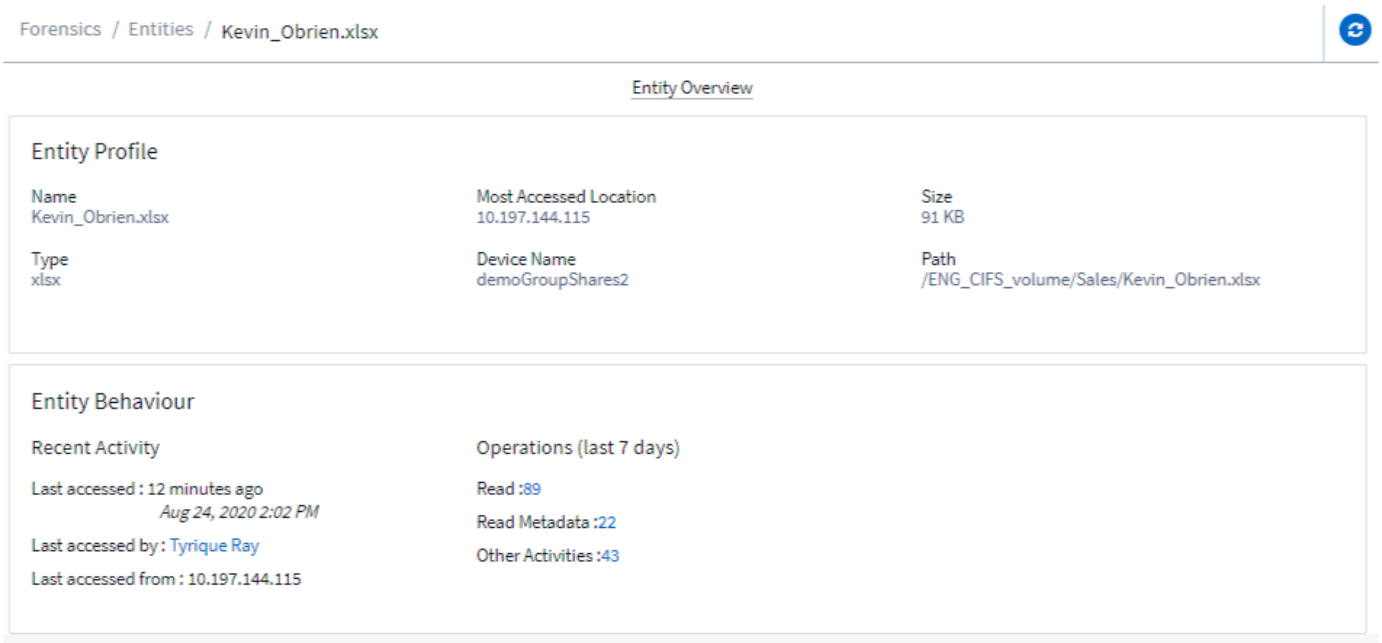
檢查實體資訊

按一下「鑑識」>「活動鑑識」、然後按一下「實體」索引標籤以存取「實體」頁面。

本頁概述您環境中的實體活動、重點說明下列資訊： *每分鐘存取的_獨特實體_圖表*存取的_實體類型_*公用路徑的明細表_*總共50個實體中的_前50個實體_清單



按一下清單中的實體、會開啟該實體的總覽頁面、顯示實體的設定檔、其中包含名稱、類型、裝置名稱、最常存取的位置IP和路徑、以及實體行為、例如使用者、IP、 以及上次存取實體的時間。



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。

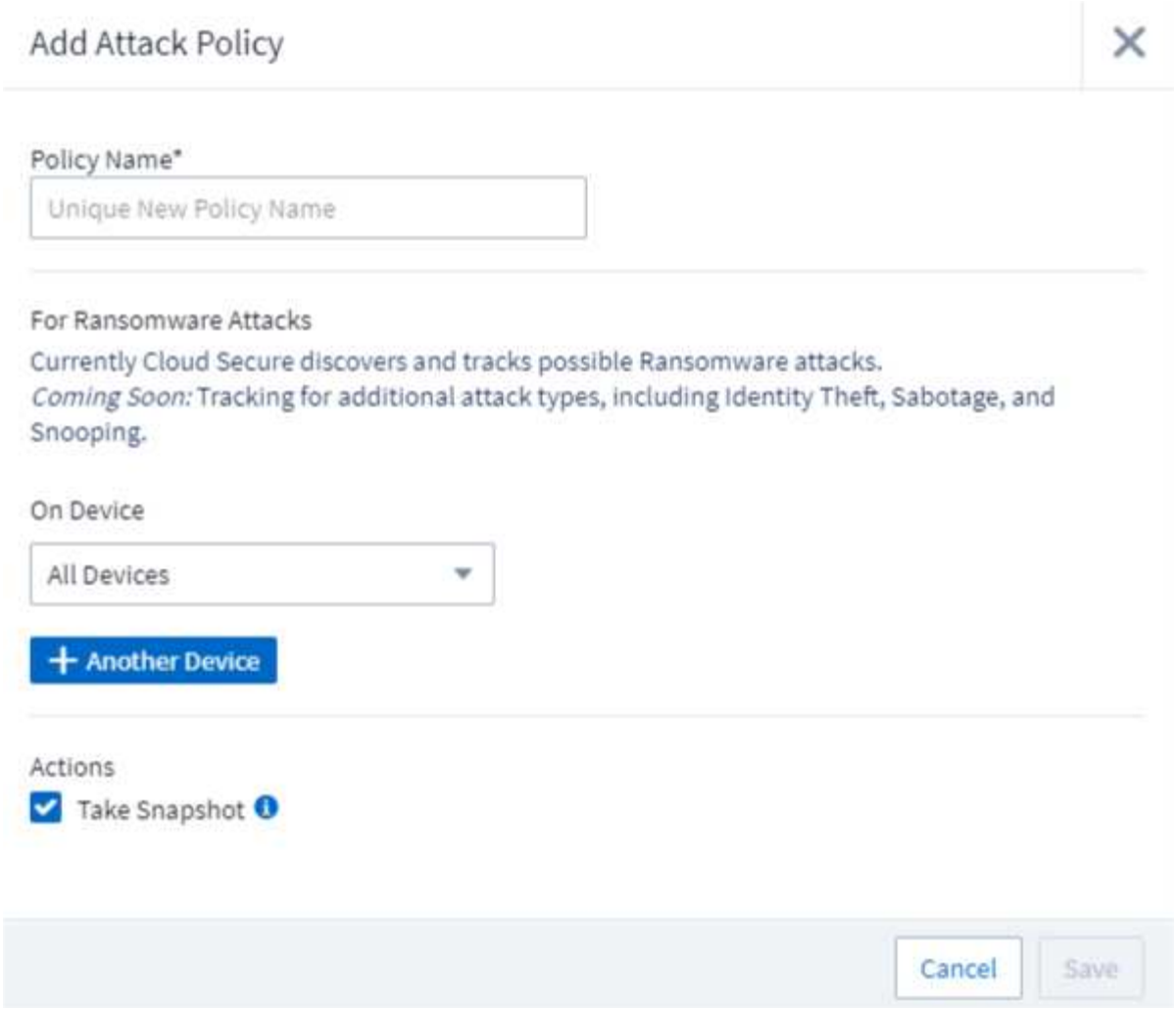
保留政策

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Cloud Secure 刪除您的不完整環境、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*+原則+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。

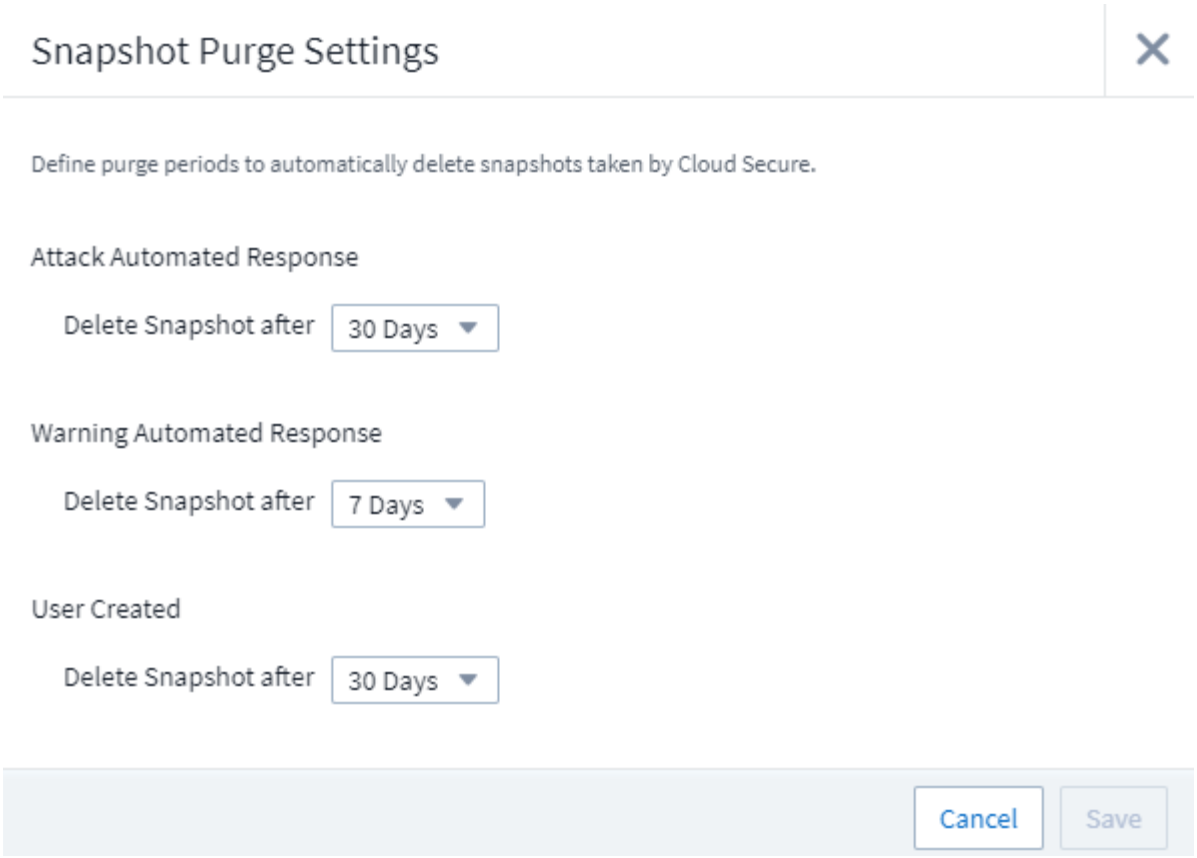
若要停用自動回應動作（例如「拍攝Snapshot」）、只要取消檢查動作並儲存原則即可。

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"。

請參閱 "限制使用者存取" 頁面以取得限制IP使用者存取的詳細資訊。

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」。

根據Snapshot清除設定、系統每天會自動刪除快照一次。Cloud Secure



封鎖使用者存取

一旦偵測到攻擊、Cloud Secure 利用阻止使用者存取檔案系統、即可停止攻擊。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位址將會被封鎖、無法存取Cloud Secure 由VMware監控的任何儲存虛擬機器（SVM）。

舉例Cloud Secure 來說、我們可以說、此功能可管理10個SVM、而其中4個SVM則設定了自動回應原則。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。

使用Amazon FSX資料收集器時、SMB的使用者封鎖功能無法終止目前的使用者工作階段。請參閱 疑難排解 章節以取得更多資訊。

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Cloud Secure 權限、以便封鎖使用者。

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
security login role create -role csrole -cmddirname "cluster show" -access
readonly
```

如何啟用此功能？

- 在「支援」中Cloud Secure 、瀏覽至*管理>自動回應原則>回應原則設定>封鎖使用者存取*。
- 將「Enable Block User Access（啟用區塊使用者存取）」設為_enabled（啟用）。

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「限制使用者存取」下、選取應套用的限制模式。
- 在「Time Period」（時間期間）下、選取應套用封鎖的時間。
- 若要測試自動使用者封鎖、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「支援」中Cloud Secure 、瀏覽至*管理>自動回應原則>回應原則設定>封鎖使用者存取*
- 取消選取「Enable Block User Access（啟用區塊使用者存取）」以停用。

所有頁面都會隱藏此功能。

手動還原**NFS**的**IP**

如果您的VMware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IP Cloud Secure 。

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。通常情況下、這個規則是1。Cloud Secure

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. 確保Cloud Secure 刪除此規則（可選的確認步驟）。
```

```
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.
```

```
== Manually Restore Users for SMB
```

如果您的VMware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Cloud Secure 。

您可以從Cloud Secure 使用者清單頁面取得遭封鎖的使用者清單。

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Cloud Secure 所有SVM中所有被支援Sfor SMB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、則無法傳送命令。Cloud Secure2、這是因為使用者可能使用之前未使用過的新IP、從機器存取儲存設備。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。
我看到錯誤：svm1：使用者網域\user01的現有CIFS工作階段未關閉。此錯誤會顯示在警示詳細資料頁面的「採取行動」區段、以及警示與使用者清單頁面下方的「存取限制歷程記錄」。看到此錯誤時、使用者目前的工作階段不會關閉、但是在連結期間到期之前、使用者將會遭到任何新工作階段的封鎖。	這是Amazon FSX的已知問題。無法關閉現有的SMB工作階段。Cloud Secure目前沒有任何因應措施可封鎖Amazon FSX現有的SMB工作階段。如果收集器類型為CVO或ONTAP 不一致、請務必確認所述的權限正確無誤 先決條件 區段。

產品特色：模擬攻擊Cloud Secure

您可以使用本頁的說明、模擬攻擊、Cloud Secure 使用隨附Cloud Secure 的勒索軟體模擬指令碼來測試或展示VMware。

開始之前要注意的事項

- 勒索軟體模擬指令碼僅適用於Linux。
- 指令碼會隨Cloud Secure 附於介紹代理程式安裝檔案。可在Cloud Secure 任何安裝了下列功能的機器上使用此功能：
- 您可以在Cloud Secure 物件代理機器上執行指令碼、不需要再準備另一台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。此為低風險活動、因此不會產生警示（亦即同一位使用者修改剛建立的檔案）Cloud Secure 。

請參閱以下說明 "以程式設計方式建立非空白檔案"。

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Cloud Secure 尚未設定、請設定該程式。
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）Cloud Secure 到資訊不限代理機器。
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。針對同一位使用者、在短時間內會得知使用者行為、不會針對反覆勒索軟體攻擊發出警示。Cloud Secure

以程式設計方式建立檔案

在建立檔案之前、您必須先停止資料收集器處理。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！

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。

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Cloud Secure 此警示收件者、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。

部分API Cloud Secure

利用此解決方案、NetApp客戶和獨立軟體廠商（ISV）能夠將支援功能與其他應用程式（例如CMDB或其他票務系統）整合。Cloud Secure Cloud Secure

API存取需求：

- API存取權杖模式用於授予存取權。
- API Token管理是Cloud Secure 由具備管理員角色的使用者執行。

API文件（Swagger）

您可以登入Cloud Secure 到「介紹」並瀏覽至「管理**> API**存取」、以找到最新的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的簡短說明與使用資訊、並可讓您在環境中試用。

API存取權杖

在使用Cloud Secure 此功能之前、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。

權杖可從客戶的觀點授予API一般用途存取權限、以管理其本身環境範圍內的API存取。

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。