



快速入門

Data Infrastructure Insights

NetApp
October 08, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/data-infrastructure-insights/task_cs_getting_started.html on October 08, 2025. Always check docs.netapp.com for the latest.

目錄

快速入門	1
工作負載安全入門	1
工作負載安全代理程式需求	1
其他建議	2
雲端網路存取規則	2
網路內規則	3
系統規模調整	4
工作負載安全代理程式安裝	4
開始之前	5
安裝代理程式的步驟	5
網路組態	7
「固定」目前版本的值機員	7
疑難排解代理程式錯誤	8
刪除工作負載安全代理程式	10
刪除代理程式	11
設定Active Directory (AD) 使用者目錄收集器	11
測試使用者目錄收集器組態	13
疑難排解使用者目錄收集器組態錯誤	14
設定LDAP目錄伺服器收集器	16
測試使用者目錄收集器組態	18
疑難排解LDAP目錄收集器組態錯誤	19
設定ONTAP SVM Data Collector	20
開始之前	20
測試資料收集器的連線能力	22
使用者存取封鎖的先決條件	23
權限相關注意事項	23
設定資料收集器	26
MetroCluster 的建議組態	27
服務原則	27
Play-Pause Data Collector	27
持續儲存區	28
移轉收集器	29
疑難排解	29
ONTAP SVM 資料收集器疑難排解	30
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	35
儲存組態Cloud Volumes ONTAP	35
支援的平台	36
代理機器組態	36
安裝工作負載安全代理程式	36

疑難排解	37
使用者管理	37
SVM事件率檢查器（代理程式規模調整指南）	38
所學專業：電子	38
範例	39
疑難排解	40

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

你必須"[安裝工作負載安全代理](#)"以便從資料收集者那裡獲取資訊。在安裝代理之前，請確保您的環境符合作業系統、CPU、記憶體和磁碟空間要求。

元件	Linux需求
作業系統	執行下列任一授權版本的電腦：* AlmaLinux 9.4（64 位元）至 9.5（64 位元）、10（64 位元），包括 SELinux* CentOS Stream 9（64 位元）* Debian 11（64 位元）、12（64 位元），包括 SEL 8.10（64 位元）、9.1（64 位元）至 9.6（64 位元），包括 SELinux* Red Hat Enterprise Linux 8.10（64 位元）、9.1（64 位元）至 9.6（64 位元）、10（64 位元），包括 SELinux* Rock 15 SP4（64 位元）至 15 SP6（64 位元），包括 SELinux * Ubuntu 20.04 LTS（64 位元）、22.04 LTS（64 位元）、24.04 LTS（64 位元）此電腦不應執行其他應用程式級軟體。建議使用專用伺服器。
命令	安裝時需要「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

元件	Linux需求
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	agentlogin.cs01.cloudinsights.netapp.com	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	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	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

傳輸協定	連接埠	來源	目的地	說明
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	35000-55000	叢集管理IP	工作負載安全代理程式	從 ONTAP 叢集管理 IP 到工作負載安全代理程式的通信，用於處理 EMS 事件。必須向工作負載安全代理程式開啟這些端口，以便 ONTAP 向其發送 EMS 事件，包括工作負載安全代理本身上的任何防火牆（如果存在）。請注意、您不需要保留 * 所有 * 這些連接埠、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。
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](#)。



全域變化可能會對您的ONTAP系統產生潛在影響。強烈建議在非尖峰時段進行影響大量資料收集器的變更。

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：

Add an Agent

Cloud Secure collects device and user data using one or more Agents installed on local servers. Each Agent can host multiple Data Collectors, which send data to Cloud Secure for analysis.

Which Operating system are you using ?

CentOS RHEL

Close

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。

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：

cloudsecure_config.agents

**GET**`/v1/cloudsecure/agents` Retrieve all agents.**POST**`/v1/cloudsecure/agents/configuration` Pin all agents under tenant**DELETE**`/v1/cloudsecure/agents/configuration` Unpin all agents under tenant**POST**`/v1/cloudsecure/agents/{agentId}/configuration` Pin an agent under tenant**DELETE**`/v1/cloudsecure/agents/{agentId}/configuration` Unpin an agent under tenant**GET**`/v1/cloudsecure/agents/{agentUuid}` Retrieve an agent by agentUuid.

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。

Installed Agents (15)

Name ↑	IP Address	Version	Status
agent-1396	10.128.218.124	1.625.0	Connected

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 <code>sudo systemctl status cloudsecure-agent.service</code> 。1.檢查日誌是否顯示消息“Failed to start Workload Security daemon service”（無法啟動工作負載安全守護程序服務）。2.檢查是否有 <code>cssys</code> 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 <code>cssys</code> 使用者和群組是否存在。 <code>sudo id cssys</code> <code>sudo groups cssys`</code> 3.如果不存在、則集中化監控原則可能已刪除 <code>cssys</code> 使用者。4.執行下列命令，手動建立 <code>cssys</code> 使用者和群組。 <code>`sudo useradd cssys</code> <code>sudo groupadd cssys`</code> 5.執行下列命令之後重新啟動代理程式服務： <code>`sudo systemctl restart cloudsecure-agent.service</code> 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： <code>sudo systemctl restart cloudsecure-agent.service</code> 3.透過檢查代理服務的狀態 <code>sudo systemctl status cloudsecure-agent.service</code> 。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。	「 <code>chmod 755 -RF</code> 」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 <code>chmod</code> 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「 <code>token = /cloudsecure-agent-install.sh</code> 」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（ <code>cloudsecure-agent-appeds.zip</code> ）。a. NetApp <code>/opt/oracle/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh</code> 2。以 root 權限逐一執行下列命令，並共用輸出。a. <code>id cssys</code> b. 群組 <code>cssys</code> c. <code>cat /etc/os-release</code>

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 =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

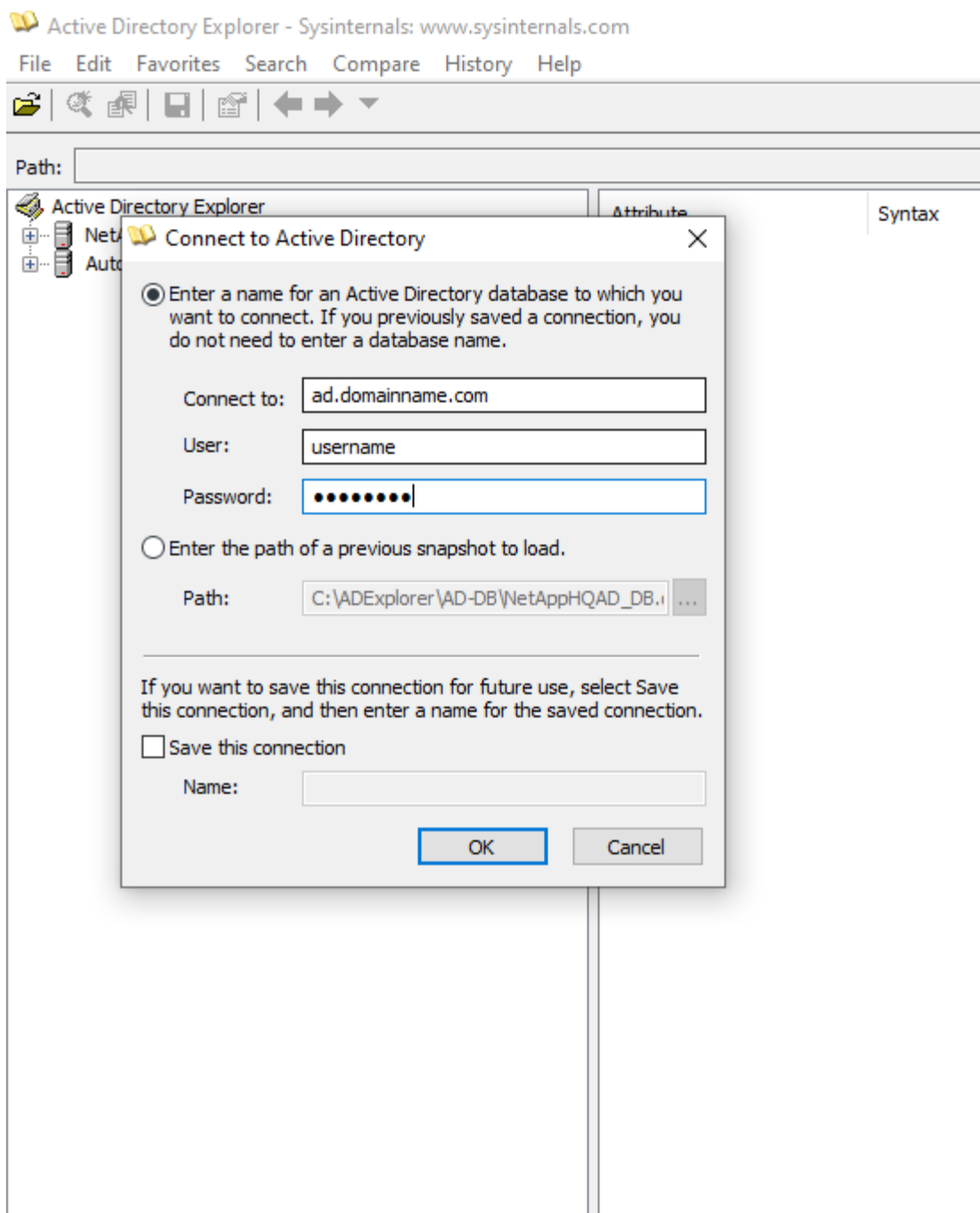
測試使用者目錄收集器組態

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：AcceptSecurityContext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://daptool.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。

The screenshot shows a 'Configuration' dialog box with the 'Option' tab selected. The 'User DN' field contains 'cn=admin,d'. The 'Password' field is masked with asterisks. The 'Use SSL port' section has radio buttons for 'Yes' and 'No', with 'No' selected. The 'Use TLS' section also has radio buttons for 'Yes' and 'No', with 'No' selected. The 'Base DN' field contains 'dc=workgro'. There is a 'Test connection' button. Checkboxes for 'Anonymous login' and 'Store password' are present, with 'Store password' checked. A note indicates '(TLS is only used on non SSL ports)'. The bottom of the dialog has 'Ok' and 'Annuler' buttons.

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：AcceptSecurityContext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

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



全域變化可能會對您的ONTAP系統產生潛在影響。強烈建議在非尖峰時段進行影響大量資料收集器的變更。

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。
 - NFS 版本（包括 NFS 4.1）（請注意，ONTAP 9.15 或更新版本支援 NFS 4.1）。
 - 支援從支援的更新版本為支援FlexGroup ONTAP
 - ONTAP 9.7 及更高版本的 NFS 支援FlexCache。
 - ONTAP 9.14.1 及更高版本的 SMB 支援FlexCache。

- 支援的支援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。
 - 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 <vservename> -user-or-group
-name <username>
```

輸出範例

```
Vserver: svmname
User/Group      Application  Authentication  Role Name  Acct Locked  Second Authentication Method
Name            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「GMT」（非「ATA」）。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。如果它們位於不同的 VPC 中，則 VPC 之間必須有有效的路由。

測試資料收集器的連線能力

測試連線功能（於 2025 年 3 月推出）旨在協助終端使用者在 Data Infrastructure Insights （DII）工作負載安全性中設定資料收集器時，找出故障的特定原因。這可讓使用者自行修正與網路通訊或遺失角色相關的問題。

此功能可協助使用者在設定資料收集器之前，判斷是否已執行所有網路相關檢查。此外，它會根據在 ONTAP 中指派給使用者的 ONTAP 版本，角色和權限，通知使用者他們可以存取的功能。



使用者目錄收集器不支援測試連線

連線測試的先決條件

- 此功能必須具備叢集層級認證，才能完整運作。
- SVM 模式不支援功能存取檢查。
- 如果您使用叢集管理認證、則不需要新的權限。
- 如果您使用的是自訂使用者（例如， *CsUser* ），請針對您要使用的功能，提供必要的權限和特定功能權限。



請務必同時檢閱[權限](#)以下部分。

測試連線

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

Add ONTAP SVM

[Need Help?](#)

An Agent is required to fetch data from the ONTAP SVM in to Storage Workload Security

Network Checks:

Https: Connection successful on port 443 (AGENT -> ONTAP)

Ontap Version: 9.14.1

Data Lifs: Found 1 (10.10.10.10) data interfaces in the SVM which contains service name data-fpolicy-client, admin/oper status as up.

Agent IP: Determined agent IP address to be used (10.10.10.10)

✔ Fpolicy Server: Connection successful on Agent IP (10.10.10.10), ports [35037, 35038, 35039] (ONTAP -> AGENT)

Features (User has permissions):

Snapshot, Ems, Access Denied, Persistent Store, Ontap ARP, User Blocking

Features (User does not have permissions):

Protobuf: Ontap version 9.14.1 is below minimum supported version 9.15.0

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，請遵循中的步驟，"使用者存取封鎖"授予工作負載安全性權限以封鎖使用者。

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。

附註：您可以建立單一角色，用於自訂使用者的所有功能權限。如果有現有使用者，請先使用下列命令刪除現有的使用者和角色：

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

若要建立新的使用者、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 role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole

```

透過* **vserver**管理IP*新增權限：

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。

附註：您可以建立單一角色，用於自訂使用者的所有功能權限。如果有現有使用者，請先使用下列命令刪除現有的使用者和角色：

```

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

```

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<vservename>：

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

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

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

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

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 role create -role csrole -cmddirname "vserver fpolicy"  
-access all  
Vserver 模式：
```

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

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：

- 將兩個資料收集器連接至來源SVM、另一個連接至目的地SVM。
- 資料收集器應由_叢集IP_連線。
- 在任何時間點，目前「正在運行」的 SVM 的資料收集器將顯示為「正在運行」。目前「停止」的 SVM 資料收集器將顯示為「已停止」。
- 每當發生切換時，資料收集器的狀態將從_Running_變為_Stopped，反之亦然。
- 資料收集器從_停止_狀態轉變為_運行_狀態最多需要兩分鐘。

服務原則

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

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，這些磁碟區等也不會反映在儀表板或表格中。



如果收集器已限制使用者，則無法暫停。在暫停收集器之前還原使用者存取權。

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

Vserver 模式：

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

移轉收集器

您可以輕鬆地將工作負載安全收集器從一個代理程式移轉到另一個代理程式，以便在代理程式之間有效地平衡收集器的負載。

先決條件

- 來源代理必須處於 `_Connected` 狀態。
- 要移轉的收集器必須處於 `_Running` 狀態。

附註：

- Data 和 User Directory 收集器都支援移轉。
- 不支援手動託管租戶移轉收集器。

移轉收集器

若要移轉收集器，請遵循下列步驟：

1. 前往「編輯收集器」頁面。
2. 從值機員下拉式清單中選取目的地代理。
3. 按一下「儲存收集器」按鈕。

工作負載安全性將會處理要求。成功移轉後，使用者將重新導向至收集器清單頁面。若發生故障，編輯頁面上會顯示適當的訊息。

附註：當收集器成功移轉至目的地代理程式時，先前在「編輯收集器」頁面上所做的任何組態變更都會繼續套用。

Workload Security / Collectors / Edit Data Collector

Edit ONTAP SVM

Name*	Agent
<input type="text" value="CI_SVM"/>	<div>fp-cs-1-agent (CONNECTED) ▼ agent-1537 (CONNECTED) agent-jptsc (CONNECTED) fp-cs-1-agent (CONNECTED) fp-cs-2-agent (CONNECTED) GSSC_girton (CONNECTED)</div>
Connect via Management IP for:	
<input checked="" type="radio"/> Cluster	
<input type="radio"/> SVM	

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。


ONTAP SVM 資料收集器疑難排解

「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。您可以在這裡找到疑難排解此收集器問題的秘訣。

如需設定此收集器的說明、請參閱["設定 SVM Collector"](#)頁面。

發生錯誤時，您可以按一下「已安裝的資料收集器」頁面 _ 狀態 _ 欄中的 _ 更多詳細資料 _，以取得有關錯誤的詳細資料。

Installed Data Collectors

Name	Status	Type	Agent
9.8_vs1	 Error more detail	ONTAP SVM	agent-11

已知問題及其解決方法如下所述。

- 問題：* 資料收集器會執行一段時間，並在隨機時間後停止，失敗的原因是：「錯誤訊息：Connector 處於錯誤狀態。服務名稱：稽核。故障原因：外部fpolicy伺服器過載。」
- 試試看：* ONTAP 的事件率遠高於 Agent Box 的處理率。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。

如果代理程式安裝在 2021 年 3 月 4 日之前的代理程式方塊中，請在代理程式方塊中執行下列命令：

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

重新調整大小後，從 UI 重新啟動收集器。

- 問題：* 收集器回報錯誤訊息：「連接器上找不到可連接 SVM 資料介面的本機 IP 位址」。* 試試看：
* 這很可能是因為 ONTAP 端的網路問題。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 Agent VM 中進行 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 可以 Ping：

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

如果無法 Ping、請確定 ONTAP 中的網路設定正確、以便值機員機器可以 Ping。

3. 如果您嘗試透過叢集 IP 連線，但無法正常運作，請嘗試直接透過 SVM IP 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，並嘗試透過該 Lif 進行連線。確定子網路遮罩設定正確。
6. 進階偵錯：
 - a. 在 ONTAP 中啟動封包追蹤。
 - b. 嘗試從 CloudSecure UI 將資料收集器連線至 SVM。
 - c. 請等待錯誤出現。停止ONTAP 封包追蹤。
 - d. 從 ONTAP 開啟封包追蹤。您可以在這個位置使用此功能

```
https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
```

- .. 請確定 ONTAP 到值機員方塊有一個 SYN。
- .. 如果 ONTAP 沒有 SYN，則 ONTAP 中的防火牆會發生問題。
- .. 在 ONTAP 中開啟防火牆，讓 ONTAP 能夠連線到代理程式方塊。

7. 如果仍無法運作，請諮詢網路團隊，確定沒有外部防火牆封鎖從 ONTAP 到值機員信箱的連線。
8. 如果上述任何一項都無法解決問題，請開啟案例["NetApp支援"](#)以取得進一步協助。

- 問題：* 訊息：「無法判斷 ONTAP [主機名稱： <IP Address> 。原因：連線錯誤至儲存系統 <IP Address> ：無法連線主機（無法連線至主機） * 請嘗試以下操作： *

1. 確認已提供正確的 SVM IP 管理位址或叢集管理 IP。
2. SSH 連接至 SVM 或您要連線的叢集。連線後、請確認SVM或叢集名稱正確無誤。

- 問題：* 錯誤訊息：「Connector is in error state 。service.name：稽核。故障原因：外部fpolicy伺服器已終止。」試用：

1. 防火牆很可能會封鎖代理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 Agent （代理）框中鍵入以下命令，確保端口範圍已打開。

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

輸出範例應如下所示：

```
-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack  
-ctstate NEW -j ACCEPT  
. 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。
```

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

"檢查防火牆命令"在 ONTAP 側。

3. 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 作業正常：

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

如果無法 Ping 、請確定 ONTAP 中的網路設定正確、以便值機員機器可以 Ping 。

4. 如果透過 2 個資料收集器將單一 SVM 新增兩次至租用戶，則會顯示此錯誤。透過UI刪除其中一個資料收集器。然後透過UI重新啟動其他資料收集器。然後資料收集器會顯示「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。

5. 如果在兩個不同的工作負載安全環境（租戶）中新增相同的 SVM ，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。
6. 如果服務原則設定不正確，也可能發生此錯誤。使用支援支援支援功能的支援功能9.8或更新版本時、若要連線至資料來源收集器、則需要資料服務資料服務、例如NFS和/或資料- CIFS、以提供資料- fpolicy-Client服務ONTAP 。此外、資料fpolicy-Client服務必須與受監控SVM的資料LIF相關聯。

- 問題：* 活動頁面上沒有任何事件。試用：

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. 如果看不到任何活動，請登入 SVM 並輸入下列命令。

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

請確定 fpolicy 沒有相關錯誤。

3. 如果看不到任何活動，請登入 SVM 。輸入下列命令：

```
<SVM>fpolicy show
```

檢查是否已設定名為「cloudsecured_」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。

- 問題：* SVM Data Collector 處於錯誤狀態，錯誤訊息為「Agent failed to connect to the collector」
* 請嘗試以下操作：*

1. 代理程式很可能超載，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線至 Agent 。
3. 同時在 UI 的「All Activity)」頁面中檢查資料流率。
4. 如果每秒的活動數量相當高，請安裝另一個 Agent，並將部分資料來源收集器移至新的 Agent 。

- 問題：* SVM Data Collector 顯示錯誤訊息「fpolicy.server.connectError: Node failed to 建置與 FPolicy 伺服器的連線「12.195.15.146」（原因：「Select Timed Out」（選取逾時)）」* 請嘗試：
* SVM/ 叢集已啟用防火牆。因此fpolicy引擎無法連線至fpolicy伺服器。ONTAP 中的 CLI 可用來取得更多資訊，包括：

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

"[檢查防火牆命令](#)"在 ONTAP 側。

- 問題：* 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）。」* 嘗試：* 確保有一個作業介面（作為資料和資料傳輸協定的角色，如 CIFS/NFS 。

- 問題：* 資料收集器進入錯誤狀態，過一段時間後進入執行中狀態，然後再回到錯誤。此週期會重複。* 請嘗試：* 這通常發生在下列情況：
 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. 確保只有 1 個資料收集器連線至 1 個 SVM。
 4. 刪除連接至同一個 SVM 的其他資料收集器。

- 問題：* Connector 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.scote-modify 中指定的 'hare-to -include' 元素的值無效： "Federal * 請嘗試以下操作：* 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。

- 問題：* 叢集中有未使用的現有 fpolicies。在安裝工作負載安全性之前、應該如何處理這些問題？* 請嘗試：* 建議刪除所有現有的未使用 fpolicy 設定，即使它們處於中斷連線狀態。「工作負載安全性」會以「cloudseced_」開頭的字元建立fpolicy。可以刪除所有其他未使用的fpolicy組態。

顯示 fpolicy 清單的 CLI 命令：

```
fpolicy show
刪除 fpolicy 組態的步驟：
```

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

| 啟用工作負載安全功能後，ONTAP 效能會受到影響：延遲有時會變得很高，IOPs 偶爾會變得很低。| 使用 ONTAP 搭配工作負載安全功能時，有時會在 ONTAP 中看到延遲問題。有許多可能的原因如下所述：["1372994"](#)，["1415152"](#)，["1438207"](#)，["1479704"](#) ["1354659"](#)。所有這些問題都已在 ONTAP 9.13.1 及更新版本中修正、強烈建議您使用這些更新版本之一。

- 問題： * 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。」 * 試試看： *
 1. 從只設定NFS服務的新SVM開始著手。
 2. 在ONTAP 工作負載安全性中新增一個功能不全的SVM資料收集器。CIFS被設定為SVM允許的傳輸協定、同時在ONTAP 工作負載安全性中加入SVM Data Collector。
 3. 等到工作負載安全性中的資料收集器顯示錯誤。
 4. 由於未在SVM上設定CIFS伺服器、因此工作負載安全性會顯示左圖所示的錯誤。
 5. 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。

- 問題： * 資料收集器會顯示錯誤訊息：「錯誤：無法在 2 次重試內判斷收集器的健全狀況，請嘗試重新啟動收集器（錯誤代碼： AGENT008 ）」。試用：
 1. 在「資料收集器」頁面上、捲動至資料收集器右側、顯示錯誤訊息、然後按一下「3點」功能表。選取 編輯。再次輸入資料收集器的密碼。按下「Sav_」按鈕以儲存資料收集器。資料收集器會重新啟動、錯誤應該會解決。
 2. Agent 機器可能沒有足夠的 CPU 或 RAM 保留空間，這就是 DSC 故障的原因。請檢查新增至機器代理程式的資料收集器數量。如果超過20個、請增加代理機器的CPU和RAM容量。CPU和RAM增加之後、DSC就會進入初始化、然後自動進入執行狀態。請參閱上的尺寸調整指南["本頁"](#)。

- 問題： * 選取 SVM 模式時， Data Collector 發生錯誤。 * 嘗試： * 在 SVM 模式下連線時，如果使用叢集管理 IP 來連線，而非 SVM 管理 IP，則連線將會錯誤。請確定使用正確的 SVM IP。

- 問題： * 啟用「存取遭拒」功能時，資料收集器會顯示錯誤訊息：「Connector 處於錯誤狀態。服務名稱：稽核。失敗原因：無法在 SVM test_SVM 上設定 fpolicy。原因：使用者未經授權。」 * 嘗試此操作： * 使用者可能缺少「存取遭拒」功能所需的剩餘權限。請依照上的指示["本頁"](#)來設定權限。

一旦設定權限，請重新啟動收集器。

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 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/cloudinsights/task_cs_add_agent.html#Steps to 安裝代理程式](https://docs.NetApp.com/us-en/cloudinsights/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 / 或記憶體的数量、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]#
```

疑難排解

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执行程序？	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。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。