# Erste Schritte

## Cloud Insights

NetApp
March 17, 2023

# Inhaltsverzeichnis

# Erste Schritte

## Erste Schritte mit Workload Security

Es müssen Konfigurationsaufgaben abgeschlossen werden, bevor Sie mit Workload Security beginnen können, um die Benutzeraktivitäten zu überwachen.

Das Workload Security-System verwendet einen Agenten, um Zugriffsdaten von Speichersystemen und Benutzerinformationen von Directory Services-Servern zu erfassen.

Sie müssen Folgendes konfigurieren, bevor Sie mit dem Erfassen von Daten beginnen können:

| Aufgabe | Verwandte Informationen |
| --- | --- |
| Konfigurieren eines Agenten | "Anforderungen An Den Agenten"<br><br>"Agent Hinzufügen"<br><br>"**Video**: Agentenbereitstellung" |
| Konfigurieren Sie einen User Directory Connector | "Fügen Sie Den User Directory Connector Hinzu"<br><br>"**Video**: Active Directory-Verbindung" |
| Konfigurieren Sie Datensammler | Klicken Sie auf **Admin > Datensammler** Klicken Sie auf den Datensammler, den Sie konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt Data Collector Vendor Reference in der Dokumentation."**Video**: ONTAP SVM Verbindung" |
| Erstellen Von Benutzerkonten | "Benutzerkonten Verwalten" |
| Fehlerbehebung | "**Video**: Fehlerbehebung" |

Auch die Workload-Sicherheit lässt sich in andere Tools integrieren. Beispiel: "Siehe diesen Leitfaden" Bei der Integration mit Splunk:

## Anforderungen An Security Agent Für Workloads

Unbedingt "Installieren Sie einen Agenten" Um Informationen von Ihren Datensammlern zu erhalten. Bevor Sie den Agent installieren, sollten Sie sicherstellen, dass Ihre Umgebung den Anforderungen an Betriebssystem, CPU, Arbeitsspeicher und Speicherplatz entspricht.

| Komponente | Linux-Anforderungen Erfüllt |
| --- | --- |
| Betriebssystem | Ein Computer, auf dem eine lizenzierte Version von einer der folgenden Versionen läuft: Red hat Enterprise Linux 7.x, 8.x 64-Bit CentOS 7.x 64-Bit CentOS 8 Stream Ubuntu 20 bis 22 64-Bit Rocky 8.x 64-Bit, Rocky 9.x 64-Bit auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Es wird ein dedizierter Server empfohlen. SE (Security Enhanced) Linux wird nicht unterstützt. |
| Befehle | Für die Installation ist „entpacken“ erforderlich. Darüber hinaus ist für die Installation, das Ausführen von Skripten und die Deinstallation der Befehl 'udo su –' erforderlich. |
| CPU | 4 CPU-Kerne |
| Speicher | 16 GB RAM |
| Verfügbarer Festplattenspeicher | Speicherplatz sollte auf diese Weise zugewiesen werden: /Opt/netapp 35 GB (Minimum) Wenn /opt ein gemounteter Ordner aus einem NAS-Speicher ist, stellen Sie sicher, dass lokale Benutzer Zugriff auf diesen Ordner haben. Agent oder Data Collector können nicht installiert werden, wenn lokale Benutzer nicht über die Berechtigung zu diesem Ordner verfügen. Siehe "Fehlerbehebung" Weitere Informationen finden Sie in diesem Abschnitt. |
| Netzwerk | 100 Mbit/s bis 1 Gbit/s Ethernet-Verbindung, statische IP-Adresse, IP-Konnektivität zu allen Geräten und ein erforderlicher Port zur Workload Security-Instanz (80 oder 443). |

Hinweis: Der Workload Security Agent kann auf demselben Rechner wie ein Cloud Insights-Erfassungsgerät und/oder -Agent installiert werden. Es ist jedoch eine Best Practice, diese in separaten Maschinen zu installieren. Wenn diese auf demselben Rechner installiert sind, weisen Sie den Festplattenspeicherplatz wie unten gezeigt zu:

| | |
| --- | --- |
| Verfügbarer Festplattenspeicher | 50-55 GB für Linux sollte auf diese Weise Speicherplatz zugewiesen werden: /Opt/netapp 25-30 GB /var/log/netapp 25 GB |

## Zusätzliche Empfehlungen

- Es wird dringend empfohlen, die Zeit auf dem ONTAP-System und dem Agent-Rechner mit **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

## Zugriffsregeln Für Das Cloud-Netzwerk

Für * US-basierte * -Sicherheitsumgebungen:

| Protokoll | Port | Ziel | Richtung | Beschreibung |
|---|---|---|---|---|
| TCP | 443 | <site_Name>.cs01.cloudinsights.netapp.com<br><site_Name>.c01.cloudinsights.netapp.com<br><site_Name>.c02.cloudinsights.netapp.com | Abgehender Anruf | Zugriff auf Cloud Insights |
| TCP | 443 | gateway.c01.cloudinsights.netapp.com<br>agentlogin.cs01.cloudinsights.netapp.com | Abgehender Anruf | Zugriff auf Authentifizierungsservices |

Für **Europa-basierte** Arbeitslastsicherheitsumgebungen:

| Protokoll | Port | Ziel | Richtung | Beschreibung |
|---|---|---|---|---|
| TCP | 443 | <site_Name>.cs01-eu-1.cloudinsights.netapp.com<br><site_Name>.c01-eu-1.cloudinsights.netapp.com<br><site_Name>.c02-eu-1.cloudinsights.netapp.com | Abgehender Anruf | Zugriff auf Cloud Insights |
| TCP | 443 | gateway.c01.cloudinsights.netapp.com<br>agentlogin.cs01-eu-1.cloudinsights.netapp.com | Abgehender Anruf | Zugriff auf Authentifizierungsservices |

Für * APAC-basierte * -Arbeitsumgebungen:

| Protokoll | Port | Ziel | Richtung | Beschreibung |
|---|---|---|---|---|
| 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 | Abgehender Anruf | Zugriff auf Cloud Insights |
| TCP | 443 | gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com | Abgehender Anruf | Zugriff auf Authentifizierungsservices |

## Netzwerkregeln

Beachten Sie, dass beim Hinzufügen von *"CSuser"*, dieser Benutzer benötigt SSH-Zugriff auf die ONTAP Management-LIF.

| Protokoll | Port | Ziel | Richtung | Beschreibung |
|---|---|---|---|---|
| TCP | 389 (LDAP) 636 (LDAPS/Start-tls) | LDAP-Server-URL | Abgehender Anruf | Mit LDAP verbinden |
| TCP | 443 | Cluster- oder SVM-Management-IP-Adresse (abhängig von der SVM-Collector-Konfiguration) | Abgehender Anruf | API-Kommunikation mit ONTAP |
| TCP | 35000 - 55000 | SVM-Daten-LIF-IP-Adressen | Eingehend/Ausgehend | Kommunikation mit ONTAP bei FPolicy-Ereignissen |
| TCP | 7 | SVM-Daten-LIF-IP-Adressen | Bidirektional | Bidirektional zwischen ONTAP und Workload Security. Agent pingt die SVM-LIFs an. |

## Systemgröße

Siehe "Ereignisprüfung" Dokumentation für Informationen zur Größenanpassung

# Installation Von Workload Security Agent

Workload Security (ehemals Cloud Secure) erfasst Daten zu Benutzeraktivitäten mithilfe eines oder mehrerer Agenten. Mitarbeiter stellen Verbindungen zu Geräten in Ihrer Umgebung her und erfassen Daten, die zur Analyse an die SaaS-Ebene für die Workload-Sicherheit gesendet werden. Siehe "Anforderungen An Den Agenten" So konfigurieren Sie eine Agent-VM:

## Bevor Sie Beginnen

- Die sudo-Berechtigung ist für die Installation, das Ausführen von Skripten und die Deinstallation erforderlich.
- Während der Installation des Agenten werden ein lokaler Benutzer *cssys* und eine lokale Gruppe *cssys* auf dem Computer erstellt. Wenn die Berechtigungseinstellungen die Erstellung eines lokalen Benutzers nicht zulassen und stattdessen Active Directory benötigen, muss im Active Directory-Server ein Benutzer mit dem Benutzernamen *csys* erstellt werden.

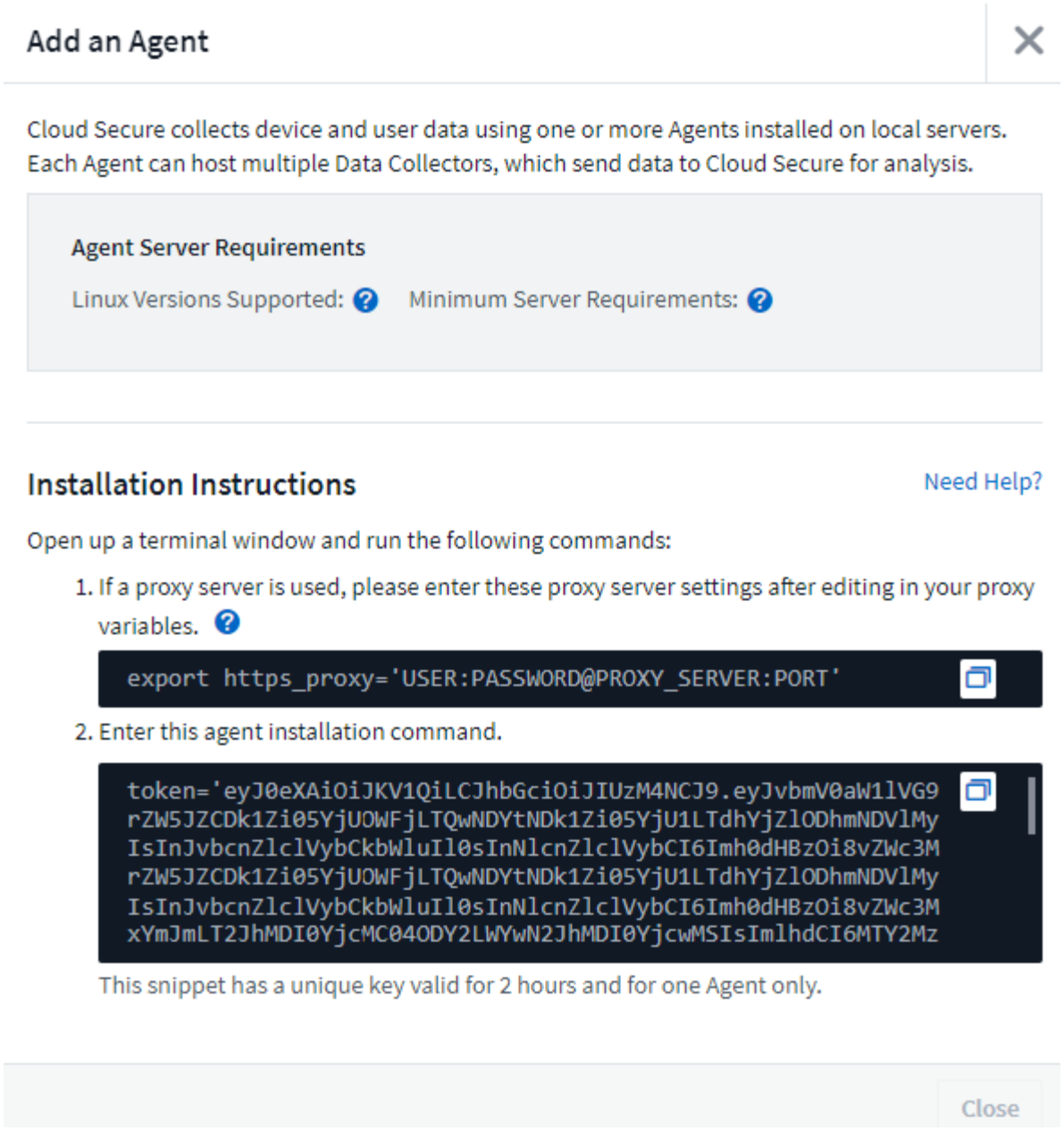
## Schritte zum Installieren von Agent

1. Melden Sie sich als Administrator oder Account-Inhaber an Ihrer Workload Security-Umgebung an.
2. Wählen Sie im Menü **Sicherheit** die Option **Admin > Data Collectors > Agents > +Agent** aus

   Das System zeigt die Seite Agent hinzufügen an:

   [Agenten 1 hinzufügen] | *Add-agent-1.png*

3. Vergewissern Sie sich, dass der Agent-Server die Mindestsystemanforderungen erfüllt.
4. Um zu überprüfen, ob auf dem Agent-Server eine unterstützte Version von Linux ausgeführt wird, klicken Sie auf *Version supported (i)*.
5. Wenn Ihr Netzwerk Proxy-Server verwendet, legen Sie die Proxy-Server-Details fest. Befolgen Sie dazu die Anweisungen im Proxy-Abschnitt.




6. Klicken Sie auf das Symbol in Zwischenablage kopieren, um den Installationsbefehl zu kopieren.
7. Führen Sie den Installationsbefehl in einem Terminalfenster aus.
8. Das System zeigt die folgende Meldung an, wenn die Installation erfolgreich abgeschlossen wurde:

   [Erkennung eines neuen Agenten] | *new-agent-detect.png*

**Nach Dem Beenden**

1. Sie müssen ein konfigurieren "Benutzerverzeichnissammler".
2. Sie müssen einen oder mehrere Data Collectors konfigurieren.

## Netzwerkkonfiguration

Führen Sie auf dem lokalen System die folgenden Befehle aus, um Ports zu öffnen, die von Workload Security verwendet werden. Wenn ein Sicherheitsbedenken bezüglich des Portbereichs bestehen, können Sie einen kleineren Portbereich verwenden, z. B. *35000:35100*. Jede SVM verwendet zwei Ports.

**Schritte**

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

Befolgen Sie die nächsten Schritte nach Ihrer Plattform:

**CentOS 7.x / RHEL 7.x**:

1. `sudo iptables-save | grep 35000`

Probenausgabe:

```
 -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` (Für CentOS 8)

Probenausgabe:

```
35000-55000/tcp
```

## Fehlerbehebung Bei Agentenfehlern

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

| Problem: | Auflösung: |
| --- | --- |
| Bei der Installation des Agenten wird der Ordner /opt/netapp/cloudSecure/Agent/logs/agent.log nicht erstellt, und die Datei install.log enthält keine relevanten Informationen. | Dieser Fehler tritt beim Bootstrapping des Agenten auf. Der Fehler wird nicht in Protokolldateien protokolliert, da er vor der Initialisierung des Loggers auftritt. Der Fehler wird auf die Standardausgabe umgeleitet und ist über den im Service-Protokoll sichtbar `journalctl -u cloudsecure-agent.service` Befehl. Dieser Befehl kann zur weiteren Fehlerbehebung verwendet werden. |
| Agent-Installation schlägt fehl mit ‘Diese linux-Distribution wird nicht unterstützt. Beenden der Installation“. | Dieser Fehler wird angezeigt, wenn Sie versuchen, den Agent auf einem nicht unterstützten System zu installieren. Siehe "Anforderungen An Den Agenten". |
| Agent-Installation fehlgeschlagen mit dem Fehler "-bash: Unzip: Command not found" | Installieren Sie unzip und führen Sie dann den Installationsbefehl erneut aus. Wenn Yum auf dem Computer installiert ist, versuchen Sie „yum install unzip“, um unzip Software zu installieren. Danach kopieren Sie den Befehl von der Agent Installations-UI erneut, und fügen ihn in die CLI ein, um die Installation erneut auszuführen. |

| Problem: | Auflösung: |
| --- | --- |
| Agent wurde installiert und wurde ausgeführt. Der Agent ist jedoch plötzlich angehalten. | SSH an den Agent-Rechner. Überprüfen Sie den Status des Agent-Dienstes über `sudo systemctl status cloudsecure-agent.service`. 1. Überprüfen Sie, ob die Protokolle eine Meldung „Workload Security Daemon Service konnte nicht gestartet werden“ anzeigen. 2. Prüfen, ob csys-Benutzer in der Agent-Maschine vorhanden ist oder nicht. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus, und überprüfen Sie, ob der Benutzer und die Gruppe der csys vorhanden sind. `sudo id cssys sudo groups cssys`3. Wenn keine vorhanden ist, kann eine zentrale Überwachungsrichtlinie den csys-Benutzer gelöscht haben. 4. Erstellen Sie csys Benutzer und Gruppe manuell durch die Ausführung der folgenden Befehle. `sudo useradd cssys `sudo groupadd cssys`5. Starten Sie danach den Agent-Service neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service`6. Wenn es noch nicht ausgeführt wird, überprüfen Sie bitte die anderen Fehlerbehebungsoptionen. |
| Es können nicht mehr als 50 Datensammler zu einem Agenten hinzugefügt werden. | Es können nur 50 Datensammler zu einem Agenten hinzugefügt werden. Dabei kann es sich um eine Kombination aller Collector-Typen, z. B. Active Directory, SVM und anderer Collectors handelt. |
| UI zeigt an, dass der Agent im Status „NOT_CONNECTED“ steht. | Schritte zum Neustart des Agenten. 1. SSH an den Agent-Rechner. 2. Starten Sie danach den Agent-Service neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service`3. Prüfen Sie den Status des Agent-Service über `sudo systemctl status cloudsecure-agent.service`. 4. Agent sollte in DEN ANGESCHLOSSENEN Zustand gehen. |
| Agent VM befindet sich hinter Zscaler Proxy und die Agent-Installation ist gescheitert. Wegen der SSL-Inspektion von Zscaler Proxy werden die Workload Security-Zertifikate präsentiert, da sie von Zscaler CA signiert ist, so dass der Agent die Kommunikation nicht anvertraut. | Deaktivieren Sie die SSL-Inspektion im Zscaler Proxy für die *.cloudinsights.netapp.com url. Wenn Zscaler die SSL-Prüfung übernimmt und die Zertifikate ersetzt, funktioniert Workload Security nicht. |

| Problem: | Auflösung: |
| --- | --- |
| Bei der Installation des Agenten bleibt die Installation nach dem Entpacken hängen. | Der Befehl „chmod 755 -RF“ schlägt fehl. Der Befehl schlägt fehl, wenn der Agent-Installationsbefehl von einem nicht-Root-Sudo-Benutzer ausgeführt wird, der Dateien im Arbeitsverzeichnis hat, die zu einem anderen Benutzer gehören, und die Berechtigungen dieser Dateien können nicht geändert werden. Wegen des fehlerhaften chmod-Befehls wird die restliche Installation nicht ausgeführt. 1. Erstellen Sie ein neues Verzeichnis namens „cloudSecure“. 2. Gehen Sie zu diesem Verzeichnis. 3. Kopieren Sie und fügen Sie die vollständige “Token=…… … ./cloudSecure-Agent-install.sh“-Installationsbefehl und drücken Sie die Eingabetaste. 4. Die Installation sollte fortgesetzt werden können. |
| Falls der Agent sich immer noch nicht mit Saas verbinden kann, öffnen Sie bitte einen Fall mit dem NetApp Support. Geben Sie die Cloud Insights Seriennummer an, um einen Fall zu öffnen, und hängen Sie wie erwähnt Protokolle an den Fall an. | Protokolle an den Fall anhängen: 1. Führen Sie das folgende Skript mit Root-Berechtigung aus und teilen Sie die Ausgabedatei (cloudSecure-Agent-symptoms.zip). a. /Opt/netapp/cloudSecure/Agent/bin/cloudsecure-agent-symptom-collector.sh 2. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus und teilen Sie die Ausgabe. a. id csys B. Gruppen cssys c. CAT /etc/os-Freigabe |
| Das Skript cloudsecure-agent-symptom-collector.sh schlägt mit folgendem Fehler fehl. [Root@Machine tmp]# /opt/netapp/cloudSecure/Agent/bin/cloudsecure-agent-symptom-collector.sh Service-Protokoll erfassen Erfassung von Anwendungsprotokollen Erfassung von Agent-Konfigurationen Aufnahme des Service-Status-Snapshots unter Verwendung von Agent-Verzeichnisstruktur-Snapshot …… . …… . /Opt/netapp/cloudSecure/Agent/bin/cloudSecure-Agent-Symptom-Collector.sh: Zeile 52: ZIP: Befehl nicht gefunden FEHLER: /Tmp/cloudsecure-agent-symptoms.zip konnte nicht erstellt werden | Zip-Werkzeug ist nicht installiert. Installieren Sie das Zip-Tool, indem Sie den Befehl „yum install zip“ ausführen. Führen Sie dann die cloudsecure-agent-symptom-collector.sh erneut aus. |
| Agent-Installation schlägt bei useradd fehl: Verzeichnis /Home/cssys kann nicht erstellt werden | Dieser Fehler kann auftreten, wenn das Login-Verzeichnis des Benutzers unter /Home nicht erstellt werden kann, da keine Berechtigungen vorhanden sind. Die Problemumgehung wäre, csys Benutzer zu erstellen und sein Login-Verzeichnis manuell mit dem folgenden Befehl hinzuzufügen: *Sudo useradd user_Name -m -d HOME_dir* -m :Erstellen Sie das Home-Verzeichnis des Benutzers, wenn es nicht existiert. -D : der neue Benutzer wird mit HOME_dir als Wert für das Login-Verzeichnis des Benutzers erstellt. Zum Beispiel, *sudo useradd cssys -m -d /cssys*, fügt einen Benutzer_cssys_ hinzu und erstellt sein Login-Verzeichnis unter root. |

| Problem: | Auflösung: |
| --- | --- |
| Agent wird nach der Installation nicht ausgeführt. *Systemctl Status cloudsecure-agent.service* zeigt Folgendes an: [Root@Demo ~]# systemctl Status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service loaded: Loaded (/usr/lib/systemd/System/cloudsecure-agent.service; enabled; Vendor Preset: Deabled: Disabled) Active: Actiting (Auto-restart) (Ergebnis: Exit-Code) since Di 2021-08-03 21:12 126:26 PDT; 2s ago Process: 25889 Start=/bin/bash /opt/Secure-Agent/cloudcode 25889 (Code=verlassen, Status=126), Aug 03 21:12:26 Demo-System[1]: cloudsecure-agent.service: Hauptprozess beendet, Code=verlassen, Status=126/n/a Aug 03 21:12:26 Demo-System[1]: Einheit cloudsecure-agent.service hat den Status fehlgeschlagen. Aug 03 21:12:26 Demo-System[1]: cloudsecure-agent.service fehlgeschlagen. | Dies kann fehlschlagen, da *csys*-Benutzer möglicherweise nicht über die Berechtigung zur Installation verfügt. Wenn /opt/netapp ein NFS-Mount ist und wenn der Benutzer *cssys* keinen Zugriff auf diesen Ordner hat, schlägt die Installation fehl. *Csys* ist ein lokaler Benutzer, der vom Workload Security Installer erstellt wurde und möglicherweise nicht über die Berechtigung zum Zugriff auf die gemountete Freigabe verfügt. Sie können dies überprüfen, indem Sie versuchen, über *cssys* user auf /opt/netapp/cloudSecure/Agent/bin/cloudSecure-Agent zuzugreifen. Wenn die „Berechtigung verweigert“ zurückgegeben wird, ist keine Installationsberechtigung vorhanden. Installieren Sie anstelle eines bereitgestellten Ordners in einem lokalen Verzeichnis auf dem Computer. |
| Der Agent wurde zunächst über einen Proxy-Server verbunden und während der Installation des Agenten wurde der Proxy festgelegt. Jetzt hat sich der Proxy-Server geändert. Wie kann die Proxy-Konfiguration des Agenten geändert werden? | Sie können die Datei agent.properties bearbeiten, um die Proxydetails hinzuzufügen. Führen Sie folgende Schritte aus: 1. Wechseln Sie in den Ordner mit der Eigenschaftendatei: cd /opt/netapp/cloudSecure/conf 2. Öffnen Sie die Datei *agent.properties* mit Ihrem bevorzugten Texteditor zum Bearbeiten. 3. Fügen Sie folgende Zeilen hinzu oder ändern Sie sie: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Speichern Sie die Datei. 5. Starten Sie den Agent: Sudo systemctl restart cloudsecure-agent.service |

# Löschen eines Workload Security Agent

Wenn Sie einen Workload Security Agent löschen, müssen alle dem Agent zugeordneten Datensammler zuerst gelöscht werden.

## Löschen eines Agenten

Durch das Löschen eines Agenten werden alle dem Agenten zugeordneten Datensammler gelöscht. Wenn Sie die Datensammler mit einem anderen Agenten konfigurieren möchten, sollten Sie vor dem Löschen des Agenten ein Backup der Data Collector-Konfigurationen erstellen.

**Bevor Sie beginnen**

1. Stellen Sie sicher, dass alle mit dem Agenten verknüpften Datensammler aus dem Workload Security-Portal gelöscht werden.

   Hinweis: Ignorieren Sie diesen Schritt, wenn sich alle zugehörigen Kollektoren im STATUS „GESTOPPT“ befinden.

**Schritte zum Löschen eines Agenten:**

1. SSH in der Agent VM und führen Sie den folgenden Befehl aus. Wenn Sie dazu aufgefordert werden, geben Sie „y“ ein, um fortzufahren.

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

2. Klicken Sie Auf **Admin > Datensammler > Agenten**

   Das System zeigt die Liste der konfigurierten Agenten an.

3. Klicken Sie auf das Optionsmenü für den Agenten, den Sie löschen möchten.
4. Klicken Sie Auf **Löschen**.

   Das System zeigt die Seite **Agent löschen** an.

5. Klicken Sie auf **Löschen**, um den Löschvorgang zu bestätigen.

# Konfigurieren eines Active Directory (AD)-Benutzerverzeichnissammler

Workload Security kann so konfiguriert werden, dass Benutzerattribute von Active Directory-Servern erfasst werden.

**Bevor Sie beginnen**

- Sie müssen ein Cloud Insights-Administrator oder -Kontoinhaber sein, um diese Aufgabe auszuführen.
- Sie müssen über die IP-Adresse des Servers verfügen, der den Active Directory-Server hostet.
- Ein Agent muss konfiguriert werden, bevor Sie einen Benutzerverzeichnisanschluss konfigurieren.

**Schritte zum Konfigurieren eines Benutzerverzeichnissammler**

1. Klicken Sie im Menü Workload Security auf: **Admin > Data Collectors > User Directory Collectors > + User Directory Collector** und wählen Sie **Active Directory**

   Das System zeigt den Bildschirm Benutzerverzeichnis hinzufügen an.

Konfigurieren Sie den User Directory Collector, indem Sie die erforderlichen Daten in die folgenden Tabellen eingeben:

| Name | Beschreibung |
|---|---|
| Name | Eindeutiger Name für das Benutzerverzeichnis. Beispiel: *GlobalADCollector* |
| Agent | Wählen Sie einen konfigurierten Agenten aus der Liste aus |
| Server-IP/Domain-Name | IP-Adresse oder Fully-Qualified Domain Name (FQDN) des Servers, der das Active Directory hostet |

| | |
|---|---|
| Waldname | Gesamtebene der Verzeichnisstruktur. Forest Name ermöglicht beide Formate: *X. y.y.z* ⇒ direkter Domainname, wie Sie ihn auf Ihrer SVM haben. [Beispiel: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ relative Distinguished Names [Beispiel: DC=hq,DC= commeryname,DC=com] oder Sie können wie folgt angeben: *OU=Engineering,DC=hq,DC= commeryname,DC=com* [nach spezifischer OU-Technik filtern] *CN=username,OU=Engineering,DC=comcompyname , DC=netapp, DC=com* [um nur bestimmte Benutzer mit <username> von OU <Engineering> zu erhalten] _CN=Acrobat Nutzer,CN=Benutzer,DC=hq,DC=commeryname,DC= alle Benutzer innerhalb von Boston, die innerhalb der Organisation unterstützt werden. |
| DN binden | Benutzer erlaubt, das Verzeichnis zu durchsuchen. Beispiel: *username@companyname.com* oder *username@domainname.com* |
| Kennwort BINDEN | Kennwort des Verzeichnisservers (d. h. Kennwort für in Bind DN verwendeten Benutzernamen) |
| Protokoll | ldap, ldaps, ldap-Start-tls |
| Ports | Wählen Sie Port |

Geben Sie die folgenden Directory Server-erforderlichen Attribute ein, wenn die Standardattributnamen in Active Directory geändert wurden. Meistens werden diese Attributnamen in Active Directory geändert, in diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

| Merkmale | Attributname im Verzeichnisserver |
|---|---|
| Anzeigename | Name |
| SID | Objektsid |
| Benutzername | SAMAccountName |

Klicken Sie auf Optionale Attribute einschließen, um eines der folgenden Attribute hinzuzufügen:

| Merkmale | Attributname im Verzeichnisserver |
|---|---|
| E-Mail-Adresse | E-Mail |
| Telefonnummer | Telefonnummerierung |
| Rolle | Titel |
| Land | Co |
| Bundesland | Bundesland |
| Abteilung | Abteilung |
| Foto | Daumennagelfoto |

| | |
|---|---|
| ManagerDN | manager an |
| Gruppen | Mitgliedschafts |

## Die Konfiguration Des Benutzerverzeichnissammler Wird Getestet

Sie können LDAP-Benutzerberechtigungen und Attributdefinitionen mithilfe der folgenden Verfahren validieren:

- Verwenden Sie den folgenden Befehl, um die Berechtigung für LDAP-Benutzer für die Workload-Sicherheit zu validieren:

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

- Verwenden Sie AD Explorer, um in einer AD-Datenbank zu navigieren, Objekteigenschaften und -Attribute anzuzeigen, Berechtigungen anzuzeigen, das Schema eines Objekts anzuzeigen, ausgefeilte Suchen auszuführen, die Sie speichern und erneut ausführen können.
  - Installieren "AD-Explorer" Auf jedem Windows-Rechner, der eine Verbindung zum AD-Server herstellen kann.
  - Stellen Sie eine Verbindung zum AD-Server mit dem Benutzernamen/Passwort des AD-Verzeichnisservers her.

[AD-Verbindung]

## Fehlerbehebung Bei Konfigurationsfehlern Des Benutzerverzeichnisses

In der folgenden Tabelle werden bekannte Probleme und Auflösungen beschrieben, die während der Kollektor-Konfiguration auftreten können:

| **Problem:** | **Auflösung:** |
|---|---|
| Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt, „ungültige Anmeldeinformationen für LDAP-Server bereitgestellt“. | Benutzername oder Passwort falsch angegeben. Bearbeiten und geben Sie den korrekten Benutzernamen und das richtige Passwort an. |
| Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt: „Das Objekt, das DN=DC=hq,DC=Domainname,DC=com als Waldname angegeben hat, konnte nicht abgerufen werden.“ | Falscher Waldname angegeben. Bearbeiten und geben Sie den richtigen Namen für die Gesamtstruktur an. |
| Die optionalen Attribute des Domänenbenutzers werden auf der Seite „Workload Security User Profile“ nicht angezeigt. | Dies ist wahrscheinlich auf eine Diskrepanz zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bearbeiten und geben Sie die korrekten optionalen Attributnamen an. |
| Datensammler im Fehlerzustand mit „LDAP-Benutzer konnten nicht abgerufen werden. Grund für Fehler: Verbindung auf dem Server nicht möglich, Verbindung ist Null“ | Starten Sie den Kollektor neu, indem Sie auf die Schaltfläche *Neustart* klicken. |

| Problem: | Auflösung: |
| --- | --- |
| Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. | Stellen Sie sicher, dass Sie für die erforderlichen Felder gültige Werte angegeben haben (Server, Forest-Name, BIND-DN, BIND-Password). Vergewissern Sie sich, dass die Eingabe von BIND-DN immer als ‘Administrator@<Domain_Forest_Name>’ oder als Benutzerkonto mit Administratorrechten für die Domäne angegeben wird. |
| Das Hinzufügen eines Benutzerverzeichnissteckers führt zum ‘reVERSUCH’ Status. Zeigt den Fehler „kann den Status des Collectors nicht definieren,Grund TCP Befehl [Connect(localhost:35012,None,List(),some(,seconds),true)] fehlgeschlagen, weil java.net.ConnectionException:Connection abgelehnt wurde.“ | Für den AD-Server wurde eine falsche IP- oder FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN. |
| Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt: „LDAP-Verbindung konnte nicht hergestellt werden“. | Für den AD-Server wurde eine falsche IP- oder FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN. |
| Das Hinzufügen eines Benutzerverzeichnissteckers führt zum Status ‘Fehler’. Fehler sagt, “die Einstellungen konnten nicht geladen werden. Grund: Datasource Configuration hat einen Fehler. Spezifischer Grund: /Connector/conf/Application.conf: 70: ldap.ldap-Port hat type STRING statt NUMBER“ | Falscher Wert für Port angegeben. Versuchen Sie, die Standardanschlusswerte oder die korrekte Portnummer für den AD-Server zu verwenden. |
| Ich begann mit den obligatorischen Attributen, und es funktionierte. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen. | Dies ist wahrscheinlich auf eine Diskrepanz zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bearbeiten und geben Sie den korrekten obligatorischen oder optionalen Attributnamen an. |
| Wann erfolgt nach dem Neustart des Collectors die AD-Synchronisierung? | DIE ANZEIGENSYNCHRONISATION erfolgt sofort nach dem Neustart des Collectors. Es dauert etwa 15 Minuten, bis Benutzerdaten von etwa 300.000 Benutzern abgerufen wurden. Und wird automatisch alle 12 Stunden aktualisiert. |
| Benutzerdaten werden von AD zu CloudSecure synchronisiert. Wann werden die Daten gelöscht? | Benutzerdaten werden 13 Monate lang aufbewahrt, wenn keine Aktualisierung erfolgt. Wenn der Mandant gelöscht wird, werden die Daten gelöscht. |
| Der Benutzerverzeichnisanschluss hat den Status ‘Fehler’. „Der Stecker befindet sich im Fehlerzustand. Dienstname: UsersLdap. Grund für Fehler: Abrufen von LDAP-Benutzern fehlgeschlagen. Grund für Fehlschlag: 80090308: LdapErr: DSID-0C090453, Kommentar: ACkeptSecurityContext error, Data 52e, v3839“ | Falscher Waldname angegeben. Siehe oben, wie Sie den richtigen Namen für die Gesamtstruktur angeben. |

| Problem: | Auflösung: |
| --- | --- |
| Die Telefonnummer wird nicht auf der Benutzerprofilseite ausgefüllt. | Dies ist wahrscheinlich auf ein Problem bei der Attributzuordnung mit dem Active Directory zurückzuführen. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Informationen des Benutzers aus Active Directory abrufen wird. 2. Hinweis unter optionalen Attributen gibt es einen Feldnamen „Telefonnummer“, der dem Active Directory-Attribut ‘Telefonnummernnummer’ zugeordnet ist. 4. Verwenden Sie jetzt das Active Directory Explorer-Tool wie oben beschrieben, um das Active Directory zu durchsuchen und den korrekten Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass in Active Directory ein Attribut namens ‘Telefonnummernnummer’, das in der Tat die Telefonnummer des Benutzers hat, vorhanden ist. 5. Sagen wir ‘Active Directory, dass es in „Phonenumber“ geändert wurde. 6. Dann bearbeiten Sie den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich ‘Telefonnummerierung’ durch ‘Phonenumber’. 7. Speichern Sie den Active Directory-Collector, wird der Sammler neu starten und erhalten die Telefonnummer des Benutzers und die gleiche in der Benutzerprofil Seite. |
| Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen. | Deaktivieren Sie die AD-Serververschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurde, wird es dort für 13 Monate sein. Wenn der AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Um erneut abzurufen, muss der Benutzer-Verzeichnis-Collector mit AD verbunden sein. |
| Daten aus Active Directory sind in CloudInsights Security vorhanden. Alle Benutzerinformationen von CloudInsights löschen möchten. | Active Directory-Benutzerinformationen können nicht NUR von CloudInsights Security gelöscht werden. Um den Benutzer zu löschen, muss der gesamte Mandant gelöscht werden. |

# Konfigurieren eines LDAP Directory Server Collectors

Sie konfigurieren die Workload Security so, dass Benutzerattribute von LDAP Directory-Servern erfasst werden.

**Bevor Sie beginnen**

- Sie müssen ein Cloud Insights-Administrator oder -Kontoinhaber sein, um diese Aufgabe auszuführen.
- Sie müssen über die IP-Adresse des Servers verfügen, der den LDAP-Directory-Server hostet.
- Ein Agent muss konfiguriert werden, bevor Sie einen LDAP-Directory-Konnektor konfigurieren.

**Schritte zum Konfigurieren eines Benutzerverzeichnissammler**

1. Klicken Sie im Menü Workload Security auf: **Admin > Data Collectors > User Directory Collectors > + User Directory Collector** und wählen Sie **LDAP Directory Server**

   Das System zeigt den Bildschirm Benutzerverzeichnis hinzufügen an.

Konfigurieren Sie den User Directory Collector, indem Sie die erforderlichen Daten in die folgenden Tabellen eingeben:

| Name | Beschreibung |
|---|---|
| Name | Eindeutiger Name für das Benutzerverzeichnis. Beispiel: *GlobalLDAPCollector* |
| Agent | Wählen Sie einen konfigurierten Agenten aus der Liste aus |
| Server-IP/Domain-Name | IP-Adresse oder vollqualifizierter Domain-Name (FQDN) des Servers, der den LDAP-Verzeichnisserver hostet |
| Suchbasis | Search Base des LDAP-Servers Search Base ermöglicht die beiden folgenden Formate: *X. y.y.z* ⇒ Direkter Domänenname, wie Sie ihn auf Ihrer SVM haben. [Beispiel: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ relative Distinguished Names [Beispiel: DC=hq,DC= commeryname,DC=com] oder Sie können wie folgt angeben: *OU=Engineering,DC=hq,DC= commeryname,DC=com* [nach spezifischer OU-Technik filtern] *CN=username,OU=Engineering,DC=comcompyname , DC=netapp, DC=com* [um nur bestimmte Benutzer mit <username> von OU <Engineering> zu bekommen] _CN=Acrobat Nutzer,CN=Benutzer,DC=hq,DC=commeryname,DC= alle Benutzer innerhalb der Organisation zu bekommen, die innerhalb von Boston, C=S=e, |
| DN binden | Benutzer erlaubt, das Verzeichnis zu durchsuchen. Beispiel: uid=ldapuser,cn=users,cn=Accounts,dc=Domain,dc=companyname,dc=com uid=john,cn=Users,cn=Accounts,dc=dorp,dc=company,dc=com für einen Benutzer john@dorp.company.com. dorp.company.com |
| --Konten | --user |
| --john | --anna |
| Kennwort BINDEN | Kennwort des Verzeichnisservers (d. h. Kennwort für in Bind DN verwendeten Benutzernamen) |
| Protokoll | ldap, ldaps, ldap-Start-tls |
| Ports | Wählen Sie Port |

Geben Sie die folgenden Directory Server-erforderlichen Attribute ein, wenn die Standardattributnamen im

LDAP Directory-Server geändert wurden. Meistens werden diese Attributnamen in LDAP Directory Server geändert, in diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

| Merkmale | Attributname im Verzeichnisserver |
|---|---|
| Anzeigename | Name |
| UNIXID | Nummer der Uidnummer |
| Benutzername | uid |

Klicken Sie auf Optionale Attribute einschließen, um eines der folgenden Attribute hinzuzufügen:

| Merkmale | Attributname im Verzeichnisserver |
|---|---|
| E-Mail-Adresse | E-Mail |
| Telefonnummer | Telefonnummerierung |
| Rolle | Titel |
| Land | Co |
| Bundesland | Bundesland |
| Abteilung | Abteilnummer |
| Foto | Foto |
| ManagerDN | manager an |
| Gruppen | Mitgliedschafts |

## Die Konfiguration Des Benutzerverzeichnissammler Wird Getestet

Sie können LDAP-Benutzerberechtigungen und Attributdefinitionen mithilfe der folgenden Verfahren validieren:

- Verwenden Sie den folgenden Befehl, um die Berechtigung für LDAP-Benutzer für die Workload-Sicherheit zu validieren:

```
 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
* Verwenden Sie den LDAP Explorer, um in einer LDAP-Datenbank zu
navigieren, Objekteigenschaften und -Attribute anzuzeigen,
Berechtigungen anzuzeigen, das Schema eines Objekts anzuzeigen und
komplexe Suchen auszuführen, die Sie speichern und erneut ausführen
können.
```

  - Installieren Sie den LDAP Explorer (http://ldaptool.sourceforge.net/) Oder Java LDAP Explorer (http://jxplorer.org/) Auf jedem Windows-Rechner, der eine Verbindung zum LDAP-Server herstellen kann.
  - Stellen Sie eine Verbindung mit dem LDAP-Server unter Verwendung des Benutzernamens/Kennworts des LDAP-Verzeichnisservers her.

[LDAP-Verbindung]

## Fehlerbehebung bei LDAP Directory Collector-Konfigurationsfehlern

In der folgenden Tabelle werden bekannte Probleme und Auflösungen beschrieben, die während der Kollektor-Konfiguration auftreten können:

| **Problem:** | **Auflösung:** |
|---|---|
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. Fehler sagt, „ungültige Anmeldeinformationen für LDAP-Server bereitgestellt“. | Falscher Bind-DN oder Bind-Kennwort oder die Suchbasis angegeben. Bearbeiten Sie die richtigen Informationen, und geben Sie sie an. |
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. Fehler sagt: „Das Objekt, das DN=DC=hq,DC=Domainname,DC=com als Waldname angegeben hat, konnte nicht abgerufen werden.“ | Falsche Suchbasis angegeben. Bearbeiten und geben Sie den richtigen Namen für die Gesamtstruktur an. |
| Die optionalen Attribute des Domänenbenutzers werden auf der Seite „Workload Security User Profile“ nicht angezeigt. | Dies ist wahrscheinlich auf eine Diskrepanz zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bei Feldern wird die Groß-/Kleinschreibung beachtet. Bearbeiten und geben Sie die korrekten optionalen Attributnamen an. |
| Datensammler im Fehlerzustand mit „LDAP-Benutzer konnten nicht abgerufen werden. Grund für Fehler: Verbindung auf dem Server nicht möglich, Verbindung ist Null“ | Starten Sie den Kollektor neu, indem Sie auf die Schaltfläche *Neustart* klicken. |
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. | Stellen Sie sicher, dass Sie für die erforderlichen Felder gültige Werte angegeben haben (Server, Forest-Name, BIND-DN, BIND-Password). Stellen Sie sicher, dass die Eingabe von Bind-DN immer als uid=ldapuser,cn=users,cn=Accounts,dc=Domain,dc=commeryname,dc=com angegeben ist. |
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum ‘reVERSUCH’-Status. Zeigt Fehler „Fehler bei der Ermittlung des Zustands des Kollektors und damit erneuter Versuch“ an. | Stellen Sie sicher, dass die Server-IP und die Search Base korrekt sind /// |
| Beim Hinzufügen des LDAP-Verzeichnisses wird der folgende Fehler angezeigt: „Fehler bei der Ermittlung des Zustands des Collectors innerhalb von 2 Wiederholungen, versuchen Sie erneut, den Collector neu zu starten (Fehlercode: AGENT008)“ | Stellen Sie sicher, dass die Server-IP-Adresse und die Suchbasis korrekt sind |

| Problem: | Auflösung: |
| --- | --- |
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum ‘reVERSUCH’-Status. Zeigt den Fehler „kann den Status des Collectors nicht definieren,Grund TCP Befehl [Connect(localhost:35012,None,List(),some(,seconds),true)] fehlgeschlagen, weil java.net.ConnectionException:Connection abgelehnt wurde.“ | Für den AD-Server wurde eine falsche IP- oder FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN. //// |
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. Fehler sagt: „LDAP-Verbindung konnte nicht hergestellt werden“. | Für den LDAP-Server wurde eine falsche IP oder ein falscher FQDN bereitgestellt. Bearbeiten Sie die korrekte IP-Adresse oder den korrekten FQDN. Oder falscher Wert für den angegebenen Port. Versuchen Sie, die Standardanschlusswerte oder die korrekte Portnummer für den LDAP-Server zu verwenden. |
| Das Hinzufügen eines LDAP-Directory-Connectors führt zum Status ‘Fehler’. Fehler sagt, “die Einstellungen konnten nicht geladen werden. Grund: Datasource Configuration hat einen Fehler. Spezifischer Grund: /Connector/conf/Application.conf: 70: ldap.ldap-Port hat type STRING statt NUMBER“ | Falscher Wert für Port angegeben. Versuchen Sie, die Standardanschlusswerte oder die korrekte Portnummer für den AD-Server zu verwenden. |
| Ich begann mit den obligatorischen Attributen, und es funktionierte. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen. | Dies ist wahrscheinlich auf eine Diskrepanz zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory zurückzuführen. Bearbeiten und geben Sie den korrekten obligatorischen oder optionalen Attributnamen an. |
| Wann erfolgt die LDAP-Synchronisierung nach dem Neustart des Collectors? | Die LDAP-Synchronisierung erfolgt unmittelbar nach dem Neustart des Collectors. Es dauert etwa 15 Minuten, bis Benutzerdaten von etwa 300.000 Benutzern abgerufen wurden. Und wird automatisch alle 12 Stunden aktualisiert. |
| Benutzerdaten werden von LDAP zu CloudSecure synchronisiert. Wann werden die Daten gelöscht? | Benutzerdaten werden 13 Monate lang aufbewahrt, wenn keine Aktualisierung erfolgt. Wenn der Mandant gelöscht wird, werden die Daten gelöscht. |
| Der LDAP-Directory-Konnektor führt zum ‘Fehler’-Status. „Der Stecker befindet sich im Fehlerzustand. Dienstname: UsersLdap. Grund für Fehler: Abrufen von LDAP-Benutzern fehlgeschlagen. Grund für Fehlschlag: 80090308: LdapErr: DSID-0C090453, Kommentar: ACkeptSecurityContext error, Data 52e, v3839“ | Falscher Waldname angegeben. Siehe oben, wie Sie den richtigen Namen für die Gesamtstruktur angeben. |

| Problem: | Auflösung: |
| --- | --- |
| Die Telefonnummer wird nicht auf der Benutzerprofilseite ausgefüllt. | Dies ist wahrscheinlich auf ein Problem bei der Attributzuordnung mit dem Active Directory zurückzuführen. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Informationen des Benutzers aus Active Directory abrufen wird. 2. Hinweis unter optionalen Attributen gibt es einen Feldnamen „Telefonnummer“, der dem Active Directory-Attribut ‘Telefonnummernnummer’ zugeordnet ist. 4. Verwenden Sie jetzt das Active Directory Explorer-Tool wie oben beschrieben, um den LDAP Directory-Server zu durchsuchen und den korrekten Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass im LDAP-Verzeichnis ein Attribut namens ‘Telefonnummernnummer’ vorhanden ist, das tatsächlich die Telefonnummer des Benutzers hat. 5. Sagen wir ‘LDAP-Verzeichnis, dass es in „Phonenumber“ geändert wurde. 6. Dann bearbeiten Sie den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich ‘Telefonnummerierung’ durch ‘Phonenumber’. 7. Speichern Sie den Active Directory-Collector, wird der Sammler neu starten und erhalten die Telefonnummer des Benutzers und die gleiche in der Benutzerprofil Seite. |
| Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen. | Deaktivieren Sie die AD-Serververschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurde, wird es dort für 13 Monate sein. Wenn der AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Um wieder abrufen zu können, muss der Benutzer-Verzeichnis-Collector mit AD verbunden sein. |

# Konfiguration des ONTAP SVM Data Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen.

## Bevor Sie beginnen

- Dieser Datensammler wird unterstützt durch:
  - Data ONTAP 9.2 und höher. Um die beste Performance zu erzielen, verwenden Sie eine Data ONTAP-Version "Diese Ausgabe" Ist fest.
  - SMB-Protokollversion 3.1 und früher. Workload Security funktioniert nicht in SMB-Konfigurationen, die FlexCache verwenden. Ab ONTAP9.7 wird FPolicy nur in einer NFS-Umgebung unterstützt.
  - NFS-Protokoll Version 4.0 und früher
  - FlexGroup wird von ONTAP 9.4 und höheren Versionen unterstützt

- ONTAP Select wird unterstützt

- Es werden nur SVMs vom Datentyp unterstützt. SVMs mit Infinite Volumes werden nicht unterstützt.
- SVM hat mehrere Untertypen. Davon werden nur *default*, *Sync_source* und *Sync_Destination* unterstützt.
- Ein Agent "Muss konfiguriert sein" Bevor Sie Datensammler konfigurieren können.
- Stellen Sie sicher, dass Sie über einen richtig konfigurierten User Directory Connector verfügen, sonst werden bei Ereignissen kodierte Benutzernamen und nicht der tatsächliche Name des Benutzers (wie in Active Directory gespeichert) auf der Seite „Activity Forensics“ angezeigt.
- Um eine optimale Performance zu erzielen, sollten Sie den FPolicy-Server so konfigurieren, dass er sich im gleichen Subnetz wie das Storage-System befindet.
- Sie müssen eine SVM mit einer der folgenden beiden Methoden hinzufügen:
  - Mit Cluster-IP, SVM-Name und Cluster-Management-Benutzername und -Passwort. ***Dies ist die empfohlene Methode.***
    - Der SVM-Name muss exakt wie in ONTAP angegeben sein und bei Groß-/Kleinschreibung beachtet werden.
  - Mit SVM Vserver Management IP, Benutzername und Passwort
  - Wenn Sie den vollständigen Administrator-Benutzernamen und -Kennwort für Cluster-/SVM-Management nicht verwenden können oder nicht bereit sind, können Sie einen benutzerdefinierten Benutzer mit geringeren Berechtigungen erstellen, wie im erwähnt "„Ein Hinweis über Berechtigungen“" Abschnitt unten. Dieser benutzerdefinierte Benutzer kann für einen SVM- oder Cluster-Zugriff erstellt werden.
    - o Sie können auch einen AD-Benutzer mit einer Rolle verwenden, die mindestens die Berechtigungen von csrolle hat, wie im Abschnitt „Hinweis auf Berechtigungen“ unten erwähnt. Weitere Informationen finden Sie im "ONTAP-Dokumentation".
- Stellen Sie sicher, dass die korrekten Applikationen für die SVM festgelegt sind, indem Sie den folgenden Befehl ausführen:

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

Beispielausgabe:[Beispiel für eine SVM-Befehlsausgabe]

- Stellen Sie sicher, dass für die SVM ein konfigurierter CIFS-Server ist: Clustershell:> `vserver cifs show`

  Das System gibt den Namen des Vservers, den CIFS-Servernamen und weitere Felder zurück.

- Legen Sie ein Passwort für den SVM vsadmin Benutzer fest. Wenn Sie benutzerdefinierten Benutzer oder Cluster-Admin-Benutzer verwenden, überspringen Sie diesen Schritt. Clustershell:> `security login password -username vsadmin -vserver svmname`
- Der SVM vsadmin-Benutzer für externen Zugriff entsperren. Wenn Sie benutzerdefinierten Benutzer oder Cluster-Admin-Benutzer verwenden, überspringen Sie diesen Schritt. Clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Stellen Sie sicher, dass die Firewall-Policy der Daten-LIF auf ‘mgmt’ (nicht ‘data’) eingestellt ist. Überspringen Sie diesen Schritt, wenn Sie die SVM mit einem dedizierten Management- lif hinzufügen. Clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy`

`mgmt`

- Wenn eine Firewall aktiviert ist, muss eine Ausnahme definiert sein, die TCP-Datenverkehr für den Port unter Verwendung des Data ONTAP Data Collectors zulässt.

  Siehe "Anforderungen an den Agenten" Für Konfigurationsinformationen. Dies gilt für lokale Agenten und Agenten, die in der Cloud installiert sind.

- Wenn ein Agent in einer AWS EC2 Instanz zum Monitoring einer Cloud ONTAP SVM installiert wird, müssen sich der Agent und der Storage in derselben VPC befinden. Wenn sie in separaten VPCs sind, muss es eine gültige Route zwischen den VPC geben.

## Ein Hinweis zu Berechtigungen

**Berechtigungen beim Hinzufügen über Cluster Management IP:**

Wenn Sie den Cluster Management Administrator-Benutzer nicht verwenden können, um Workload Security den Zugriff auf den ONTAP SVM-Datensammler zu erlauben, können Sie einen neuen Benutzer namens „cscuser“ mit den Rollen erstellen, wie in den Befehlen unten gezeigt. Verwenden Sie den Benutzernamen „CSuser“ und das Passwort für „cscuser“, wenn Sie den Workload Security Data Collector für die Verwendung der Cluster Management IP konfigurieren.

Um den neuen Benutzer zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clustermanagements-Administrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus:

```
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
```

**Berechtigungen beim Hinzufügen über Vserver Management IP:**

Wenn Sie den Cluster Management Administrator-Benutzer nicht verwenden können, um Workload Security den Zugriff auf den ONTAP SVM-Datensammler zu erlauben, können Sie einen neuen Benutzer namens „cscuser“ mit den Rollen erstellen, wie in den Befehlen unten gezeigt. Verwenden Sie den Benutzernamen „CSuser“ und das Passwort für „cscuser“, wenn Sie den Workload Security Data Collector für die Verwendung von Vserver Management IP konfigurieren.

Um den neuen Benutzer zu erstellen, melden Sie sich mit dem Benutzernamen/Kennwort des Clustermanagements-Administrators bei ONTAP an, und führen Sie die folgenden Befehle auf dem ONTAP-Server aus. Die folgenden Befehle sollten einfacher in einen Text Editor kopiert und vor der Ausführung der folgenden Befehle auf ONTAP den <vservername> mit Ihrem Vserver-Namen ersetzt werden:

```
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>
```

## Konfigurieren Sie den Datensammler

**Schritte zur Konfiguration**

1. Melden Sie sich als Administrator oder Account-Inhaber in Ihrer Cloud Insights-Umgebung an.
2. Klicken Sie Auf **Admin > Datensammler > +Datensammler**

   Das System zeigt die verfügbaren Datensammler an.

3. Bewegen Sie den Mauszeiger über die Kachel **NetApp SVM und klicken Sie auf *+Monitor**.

   Das System zeigt die Konfigurationsseite der ONTAP SVM an. Geben Sie die erforderlichen Daten für die einzelnen Felder ein.

| Feld | Beschreibung |
|---|---|
| Name | Eindeutiger Name für den Data Collector |
| Agent | Wählen Sie einen konfigurierten Agenten aus der Liste aus. |
| Verbindung über Management-IP herstellen für: | Wählen Sie eine Cluster-IP oder eine SVM-Management-IP aus |
| Management-IP-Adresse für Cluster/SVM | Je nach Ihrer obigen Auswahl die IP-Adresse für das Cluster oder die SVM. |
| SVM-Name | Name der SVM (dieses Feld ist erforderlich, wenn eine Verbindung über Cluster-IP hergestellt wird) |

| | |
|---|---|
| Benutzername | Benutzername für den Zugriff auf die SVM/Cluster beim Hinzufügen über Cluster IP die Optionen sind: 1. Cluster-Admin 2. 'Cuser' 3. AD-User mit ähnlicher Rolle wie CSuser. Beim Hinzufügen über SVM IP haben Sie folgende Optionen: 4. Vsadmin 5. 'Cuser' 6. AD-Benutzername mit ähnlicher Rolle wie CSuser. |
| Passwort | Kennwort für den oben genannten Benutzernamen |
| Freigaben/Volumes Filtern | Wählen Sie aus, ob Freigaben/Volumes aus der Ereignissammlung einbezogen oder ausgeschlossen werden sollen |
| Geben Sie vollständige Freigabennamen ein, die ausgeschlossen/include werden sollen | Kommagetrennte Liste von Freigaben, die ausgeschlossen oder (je nach Bedarf) aus der Ereignissammlung aufgenommen werden sollen |
| Geben Sie vollständige Volume-Namen ein, die ausgeschlossen/include werden sollen | Kommagetrennte Liste von Volumes zum Ausschließen oder Einschließen (je nach Bedarf) aus der Ereignissammlung |
| Überwachen Sie Den Ordnerzugriff | Wenn diese Option aktiviert ist, werden Ereignisse für die Überwachung des Ordnerzugriffs aktiviert. Beachten Sie, dass Ordner erstellen/umbenennen und löschen auch ohne diese Option überwacht werden. Wenn Sie diese Option aktivieren, erhöht sich die Anzahl der überwachten Ereignisse. |
| Festlegen der Puffergröße für ONTAP-Senden | Legt die Größe des ONTAP FPolicy-Sendepuffers fest. Wenn eine ONTAP-Version vor 9.8p7 verwendet wird und Performance-Problem auftritt, kann die Puffergröße des ONTAP send geändert werden, um die ONTAP-Leistung zu verbessern. Wenden Sie sich an den NetApp Support, wenn diese Option nicht angezeigt wird und Sie sie erkunden möchten. |

**Nachdem Sie fertig sind**

- Auf der Seite installierte Datensammler können Sie den Datensammler über das Optionsmenü rechts neben jedem Collector bearbeiten. Sie können den Datensammler neu starten oder die Konfigurationsattribute des Datensammlers bearbeiten.

## Empfohlene Konfiguration für Metro Cluster

Die folgenden Empfehlungen für MetroCluster:

1. Verbinden Sie zwei Data Collectors – eine mit der Quell-SVM und eine andere mit der Ziel-SVM.
2. Die Datensammler sollten durch *Cluster IP* verbunden werden.
3. Zu jedem Zeitpunkt sollte ein Datensammler in Betrieb sein, ein anderer wird im Fehler sein.

   Der aktuelle 'running' SVM-Datensammler wird als *running* angezeigt. Der Datensammler der aktuellen 'stovered' SVM wird als *Error* angezeigt.

4. Bei jeder Umschaltung ändert sich der Zustand des Datensammlers von 'running' zu 'error' und umgekehrt.
5. Es dauert bis zu zwei Minuten, bis der Datensammler den Fehlerstatus in den Ausführungszustand wechselt.

## Service-Richtlinie

Bei Verwendung der Service-Policy aus ONTAP Version 9.9.1, um eine Verbindung zum Datenquellensammler herzustellen, ist der Dienst *Data-fpolicy-Client* zusammen mit dem Datendienst *Data-nfs* und/oder *Data-cifs* erforderlich.

Beispiel:

```
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)
```

In Versionen von ONTAP vor 9.9 muss *Data-fpolicy-Client* nicht gesetzt werden.

## Fehlerbehebung

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

Im Fehlerfall klicken Sie in der Spalte *Status* auf *more Detail*, um Details zum Fehler zu erhalten.

[]

| **Problem:** | **Auflösung:** |
| --- | --- |
| Data Collector wird einige Zeit ausgeführt und stoppt nach einer zufälligen Zeit, schlägt fehl mit: "Fehlermeldung: Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für Fehler: Externer fpolicy-Server überlastet.“ | Die Ereignisrate von ONTAP war weit höher als die, die das Feld Agent verarbeiten kann. Damit wurde die Verbindung beendet. Überprüfen Sie den Peak Traffic in CloudSecure, wenn die Verbindung unterbrochen wurde. Dies können Sie auf der Seite **CloudSecure > Aktivitätsforensics > Alle Aktivitäten** überprüfen. Wenn der maximale aggregierte Datenverkehr höher ist als der, was die Agent Box verarbeiten kann, lesen Sie die Seite Event Rate Checker zur Dimensionierung der Collector-Bereitstellung in einer Agent-Box. Wenn der Agent vor dem 4. März 2021 in der Agent-Box installiert wurde, führen Sie die folgenden Befehle in der Agent-Box aus: Echo 'net.Core.rmem_max=8388608' >> /etc/sysctl.conf Echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p Neustart des Sammlers von der UI nach der Größenänderung. |

| Problem: | Auflösung: |
| --- | --- |
| Collector meldet Fehlermeldung: „Keine lokale IP-Adresse auf dem Anschluss gefunden, die die Datenschnittstellen der SVM erreichen kann“. | Dies ist sehr wahrscheinlich auf der Seite des ONTAP-Netzwerks zurückzuführen. Bitte führen Sie folgende Schritte aus: 1. Stellen Sie sicher, dass es keine Firewalls auf der SVM-Datenlüf oder dem Management- l gibt, welche die Verbindung von der SVM blockieren. 2. Beim Hinzufügen einer SVM über eine Cluster-Management-IP, stellen Sie bitte sicher, dass die Daten- und Management- lif der SVM von der Agent-VM pingfähig sind. Bei Problemen prüfen Sie Gateway, Netzmaske und Routen für den Lif. Sie können auch versuchen, sich mithilfe von ssh unter Verwendung der Cluster-Management-IP beim Cluster anzumelden und die Agent-IP zu pingen. Stellen Sie sicher, dass die Agent-IP pingfähig ist: *Network ping -vserver <vserver Name> -Destination <Agent IP> -lif <Lif Name> -show-Detail* Wenn Sie nicht pingfähig sind, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, so dass der Agent-Rechner pingfähig ist. 3. Wenn Sie eine Verbindung über Cluster-IP versucht haben und es nicht funktioniert, versuchen Sie, direkt über SVM-IP zu verbinden. Die Schritte zur Verbindung über SVM IP finden Sie oben. 4. Beim Hinzufügen des Collectors über SVM IP und vsadmin Zugangsdaten prüfen, ob die SVM Lif die Data PLUS Mgmt-Rolle aktiviert hat. In diesem Fall funktioniert der Ping an die SVM Lif, allerdings funktioniert SSH an die SVM Lif nicht. Wenn ja, erstellen Sie ein SVM Management-only-Lif und versuchen Sie, eine Verbindung über diese SVM-Management-only-Lizenz herzustellen. 5. Wenn es immer noch nicht funktioniert, erstellen Sie eine neue SVM-Lif und versuchen Sie eine Verbindung über diese Lif. Stellen Sie sicher, dass die Subnetzmaske richtig eingestellt ist. 6. Erweitertes Debugging: A) Starten Sie eine Paketverfolgung in ONTAP. b) Try to Connect a Data Collector to the SVM from CloudSecure UI. c) warten, bis der Fehler angezeigt wird. Stoppen Sie die Paketverfolgung in ONTAP. d) Öffnen Sie die Paketverfolgung von ONTAP. Er ist an diesem Standort verfügbar *https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/* e) stellen Sie sicher, dass ein SYN von ONTAP zur Agent-Box kommt. f) Wenn es kein SYN von ONTAP gibt, dann ist es ein Problem mit Firewall in ONTAP. G) Öffnen Sie die Firewall in ONTAP, so dass ONTAP in der Lage ist, die Agent-Box zu verbinden. 7. Wenn es noch nicht funktioniert, wenden Sie sich bitte an das Netzwerkteam, um sicherzustellen, dass keine externe Firewall die Verbindung von ONTAP zur Agent Box blockiert. 8. Wenn keiner der oben genannten Probleme löst, öffnen Sie einen Fall mit "Netapp Support" Für weitere Unterstützung. |

| Problem: | Auflösung: |
| --- | --- |
| Nachricht: „Es konnte der ONTAP-Typ für [Hostname: <IP-Adresse> nicht ermittelt werden. Grund: Verbindungsfehler zum Speichersystem <IP-Adresse>: Host ist nicht erreichbar (Host nicht erreichbar)“ | 1. Überprüfen Sie, ob die richtige SVM-IP-Management-Adresse oder Cluster-Management-IP angegeben wurde. 2. SSH zu der SVM oder dem Cluster, mit dem Sie beabsichtigen zu verbinden. Sobald Sie eine Verbindung hergestellt haben, stellen Sie sicher, dass der SVM oder der Cluster-Name korrekt ist. |

| Problem: | Auflösung: |
| --- | --- |
| Fehlermeldung: „Konnektor befindet sich im Fehlerzustand. Service.name: Audit. Grund für Fehlschlag: Externer fpolicy-Server beendet.“ | 1. Es ist sehr wahrscheinlich, dass eine Firewall die notwendigen Ports in der Agent-Maschine blockiert. Überprüfen Sie, ob der Port-Bereich 35000-55000/tcp geöffnet ist, damit der Agent-Rechner eine Verbindung von der SVM herstellen kann. Stellen Sie außerdem sicher, dass keine Firewalls von der ONTAP-Seite aus aktiviert sind, die die Kommunikation mit dem Agenten-Rechner blockieren. 2. Geben Sie den folgenden Befehl in das Feld Agent ein und stellen Sie sicher, dass der Port-Bereich geöffnet ist. *Sudo iptables-save 3500** Beispielausgabe sollte aussehen wie: *-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEU -j ACCEPT* 3. Melden Sie sich bei SVM an, geben Sie die folgenden Befehle ein und überprüfen Sie, ob für die Kommunikation mit ONTAP keine Firewall eingerichtet ist. *Systemdienste Firewall show Systemdienste Firewall-Policy show_"Überprüfen Sie die Firewall-Befehle" Auf der ONTAP-Seite. 4. SSH an die SVM/Cluster, die Sie überwachen möchten. Ping the Agent Box from the SVM Data lif (with CIFS, NFS Protocols Support) und Sicherstellen, dass Ping funktioniert: _Network ping -vserver <vserver Name> -Destination <Agent IP> -lif <Lif Name> -show-Detail* Wenn nicht pingfähig, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, damit der Agent-Rechner pingfähig ist. 5.Wenn eine einzelne SVM über 2 Datensammler zweimal zu einem Mandanten hinzugefügt wird, wird dieser Fehler angezeigt. Löschen Sie einen der Datensammler über die UI. Starten Sie dann den anderen Datensammler über die UI neu. Dann wird der Data Collector den Status „RUNNING“ anzeigen und beginnt, Ereignisse von der SVM zu empfangen. Im Prinzip sollte in einem Mandanten nur eine SVM über 1 Datensammler hinzugefügt werden. 1 SVM sollte nicht zweimal über 2 Datensammler hinzugefügt werden. 6. In Fällen, in denen in zwei verschiedenen Workload-Sicherheitsumgebungen (Mandanten) dieselbe SVM hinzugefügt wurde, wird der letzte Aspekt immer erfolgreich sein. Der zweite Collector konfiguriert fpolicy mit seiner eigenen IP-Adresse und startet die erste. So wird der Sammler in der ersten aufhören, Ereignisse zu empfangen, und sein "Audit"-Service wird in Fehlerzustand. Um dies zu verhindern, konfigurieren Sie jede SVM in einer einzigen Umgebung. 7. Dieser Fehler kann auch auftreten, wenn Dienstrichtlinien nicht richtig konfiguriert sind. Mit ONTAP 9.8 oder höher ist zur Verbindung mit dem Data Source Collector der datenrichtlinienclient-Dienst zusammen mit dem Datenservice Data-nfs und/oder Data-cifs erforderlich. Darüber hinaus muss der datenrichtlinienclient-Service den Daten-Lif(s) für die überwachte SVM zugeordnet werden. |

| Problem: | Auflösung: |
| --- | --- |
| Auf der Aktivitätsseite werden keine Ereignisse angezeigt. | 1. Prüfen, ob ONTAP Collector im „LAUFENDEN“ Zustand ist. Wenn ja, stellen Sie sicher, dass einige cifs-Ereignisse auf den cifs-Client-VMs durch das Öffnen einiger Dateien generiert werden. 2. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bei der SVM an und geben Sie den folgenden Befehl ein. *<SVM>Ereignisprotokoll show -source fpolicy* Stellen Sie sicher, dass fpolicy keine Fehler enthält. 3. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bei der SVM an. Geben Sie den folgenden Befehl ein: *<SVM>fpolicy show* Überprüfen Sie, ob die fpolicy mit dem Präfix „cloudSecure_“ festgelegt wurde und der Status „ein“ lautet. Ist er nicht eingestellt, kann der Agent die Befehle in der SVM höchstwahrscheinlich nicht ausführen. Stellen Sie sicher, dass alle Voraussetzungen, die am Anfang der Seite beschrieben sind, eingehalten wurden. |
| SVM Data Collector befindet sich im Fehlerzustand und Fehlermeldung „Agent konnte keine Verbindung zum Collector herstellen“ | 1. Höchstwahrscheinlich ist der Agent überlastet und kann keine Verbindung zu den Datenquellenkollektoren herstellen. 2. Überprüfen Sie, wie viele Datenquellensammler mit dem Agenten verbunden sind. 3. Überprüfen Sie auch die Datenflussrate auf der Seite „Alle Aktivitäten“ in der UI. 4. Wenn die Anzahl der Vorgänge pro Sekunde signifikant hoch ist, installieren Sie einen anderen Agenten und verschieben einige der Datenquellensammler auf den neuen Agenten. |
| SVM Data Collector zeigt die Fehlermeldung „fpolicy.server.connectError: Node konnte keine Verbindung zum FPolicy-Server „12.195.15.146“ herstellen ( Grund: „Select Timed Out“)“ | Firewall ist in SVM/Cluster aktiviert. fpolicy Engine kann also keine Verbindung zum fpolicy-Server herstellen. CLIs in ONTAP, die verwendet werden können, um weitere Informationen zu erhalten sind: Event Log show -source fpolicy, die das Fehlerereignisprotokoll show -source fpolicy -fields Event,Action,Beschreibung zeigt, die weitere Details.“Überprüfen Sie die Firewall-Befehle" Auf der ONTAP-Seite. |
| Fehlermeldung: „Connector befindet sich im Fehlerzustand. Dienstname:Audit. Grund für Fehler: Keine gültige Datenschnittstelle (Rolle: Daten, Datenprotokolle: NFS oder CIFS oder beides, Status: Up) auf der SVM gefunden.“ | Stellen Sie sicher, dass es eine Betriebsschnittstelle gibt (Rolle als Daten und Datenprotokoll als CIFS/NFS. |

| Problem: | Auflösung: |
| --- | --- |
| Der Datensammler wechselt in den Fehlerzustand und geht nach einiger Zeit in DEN LAUFENDEN Zustand, dann wieder zurück zu Fehler. Dieser Zyklus wiederholt sich. | Dies geschieht typischerweise im folgenden Szenario: 1. Es werden mehrere Datensammler hinzugefügt. 2. Die Datensammler, die diese Art von Verhalten zeigen, haben 1 SVM zu diesen Datensammlern hinzugefügt. Das bedeutet, dass 2 oder mehr Datensammler mit 1 SVM verbunden sind. 3. Sicherstellen, dass 1 Datensammler eine Verbindung mit nur 1 SVM herstellt. 4. Löschen Sie die anderen Datensammler, die mit derselben SVM verbunden sind. |
| Der Anschluss befindet sich im Fehlerzustand. Dienstname: Audit. Grund für Fehler: Konnte nicht konfiguriert werden (Richtlinie auf SVM svmname. Grund: Ungültiger Wert angegeben für Element 'shares-to-include' in 'fpolicy.Policy.Scope-modify: "Federal' | Die Freigabennamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die DSC-Konfiguration der ONTAP SVM, um die Freigabennamen zu korrigieren. *Aktien einschließen und ausschließen* ist nicht für eine lange Liste von Share-Namen gedacht. Verwenden Sie stattdessen Filtern nach Volume, wenn eine große Anzahl an Shares enthalten oder ausschließen muss. |
| Im Cluster gibt es bereits frichtlinien, die nicht verwendet werden. Was sollte vor der Installation von Workload Security getan werden? | Es wird empfohlen, alle vorhandenen nicht verwendeten fpolicy-Einstellungen zu löschen, selbst wenn sie sich im getrennten Zustand befinden. Workload Security erstellt fpolicy mit dem Präfix „cloudSecure_“. Alle anderen nicht verwendeten fpolicy-Konfigurationen können gelöscht werden. CLI-Befehl zum Anzeigen der fpolicy-Liste: *fpolicy show* Steps zum Löschen von fpolicy-Konfigurationen: *fpolicy disable -vserver <svmname> -Policy-Name <Policy_Name>* fpolicy-Name_vserver_Name_vmserver_delete -vmserver_name_vmserver_list_vmserver_delete_vengine_Name_vmserver_vengine_Name_vmserver_vmserver_list_vmserver_<_vmgine_Name_vmserver_<_vmgine_list_Name_vmserver_<_vmserver_nement-Name_<_vmserver_vmserver_Name_vmserver_<_vmserver_list_vmserver_Name_<<<_next- |
| Nach Aktivierung der Workload-Sicherheit beeinträchtigt die ONTAP-Performance: Sporadisch steigt die Latenz an und IOPS werden sporadisch niedrig. | Stellen Sie sicher, dass Sie dort eine Data ONTAP-Version verwenden "Diese Ausgabe" Ist fest. Die empfohlene Mindestversion von ONTAP ist 9.8P7. Wenn eine ONTAP-Version vor 9.8p7 verwendet wird und dieses Performance-Problem auftritt, kann die Puffergröße des ONTAP send geändert werden, um die ONTAP-Leistung zu verbessern. Wenden Sie sich an den NetApp Support, wenn Sie diese Option erkunden möchten und diese Einstellung nicht anzeigen möchten, wenn Sie einen neuen Datensammler hinzufügen oder einen vorhandenen bearbeiten. |

| Problem: | Auflösung: |
| --- | --- |
| Datensammler ist fehlerhaft, zeigt diese Fehlermeldung an. „Fehler: Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für Fehler: Richtlinie konnte nicht für SVM svm_Test konfiguriert werden. Grund: Fehlender Wert für zapi Feld: Ereignisse. „ | Beginnen Sie mit einer neuen SVM, wobei nur ein NFS-Service konfiguriert ist. Hinzufügen eines ONTAP SVM-Datensammlers zur Workload-Sicherheit CIFS ist als zulässiges Protokoll für die SVM konfiguriert und fügt den ONTAP SVM Data Collector zur Workload-Sicherheit hinzu. Warten Sie, bis der Datensammler in Workload Security einen Fehler anzeigt. Da der CIFS-Server NICHT auf der SVM konfiguriert ist, wird dieser Fehler, wie in der linken Seite dargestellt, durch Workload Security angezeigt. Bearbeiten Sie den ONTAP SVM Data Collector und deaktivieren Sie die Prüfung CIFS als zulässiges Protokoll. Speichern Sie den Datensammler. Er wird erst ausgeführt, wenn das NFS-Protokoll aktiviert ist. |
| Der Data Collector zeigt die Fehlermeldung „Fehler: Fehler: Fehler: Fehler, den Zustand des Collectors innerhalb von 2 Wiederholungen zu ermitteln. Versuchen Sie erneut, den Collector neu zu starten (Fehlercode: AGENT008)“. | 1. Scrollen Sie auf der Seite Data Collectors rechts vom Datensammler, der den Fehler gibt, und klicken Sie auf das Menü mit 3 Punkten. Wählen Sie *Bearbeiten*. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche *Save* drücken. Der Data Collector wird neu gestartet, und der Fehler sollte behoben werden. 2. Der Agent-Rechner kann nicht genügend CPU- oder RAM-Reserve, deshalb sind die DSCs gescheitert. Überprüfen Sie die Anzahl der Datensammler, die dem Agenten auf dem Computer hinzugefügt werden. Wenn es mehr als 20 ist, erhöhen Sie die CPU- und RAM-Kapazität des Agent-Rechners. Sobald die CPU und der RAM erhöht sind, werden die DSCs in die Initialisierung und dann automatisch in den laufenden Zustand versetzt. Schauen Sie sich den Leitfaden zur Größenanpassung an "Auf dieser Seite". |

Wenn Sie immer noch Probleme haben, wenden Sie sich an die auf der Seite * Hilfe > Support* genannten Support-Links.

# Konfiguration des Cloud Volumes ONTAP und Amazon FSX für NetApp ONTAP Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen.

## Cloud Volumes ONTAP Storage-Konfiguration

In der OnCommand Cloud Volumes ONTAP-Dokumentation können Sie eine AWS-Instanz mit einem Node/HA für das Hosting des Workload Security Agent konfigurieren:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Führen Sie nach Abschluss der Konfiguration die Schritte aus, um die SVM einzurichten:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

## Unterstützte Plattformen

- Cloud Volumes ONTAP, unterstützt bei allen verfügbaren Cloud-Service-Providern. Zum Beispiel Amazon, Azure, Google Cloud.
- ONTAP Amazon FSX

## Agent-Gerätekonfiguration

Die Agent-Maschine muss in den jeweiligen Subnetzen der Cloud-Service-Provider konfiguriert sein. Weitere Informationen zum Netzwerkzugriff finden Sie unter [Agent-Anforderungen].

Unten sind die Schritte für die Installation von Agenten in AWS aufgeführt. Die entsprechenden Schritte, die für den Cloud-Service-Provider gelten, können für die Installation in Azure oder Google Cloud befolgt werden.

Konfigurieren Sie in AWS die Maschine, die als Workload Security Agent verwendet werden soll, mit den folgenden Schritten:

Konfigurieren Sie die Maschine, die als Workload Security Agent verwendet werden soll, wie folgt:

**Schritte**

1. Melden Sie sich bei der AWS Konsole an, und navigieren Sie zur Seite EC2-instances, und wählen Sie *Launch Instance* aus.
2. Wählen Sie eine RHEL- oder CentOS AMI-Lösung mit der entsprechenden Version aus, wie auf dieser Seite erwähnt:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Wählen Sie die VPC und das Subnetz aus, in der die Cloud-ONTAP-Instanz residiert.
4. Wählen Sie *t2.xlarge* (4 vcpus und 16 GB RAM) als zugewiesene Ressourcen aus.
    a. Erstellen Sie die EC2-Instanz.
5. Installieren Sie die erforderlichen Linux-Pakete mithilfe des YUM-Paketmanagers:
    a. Installieren Sie die nativen Linux-Pakete *wget* und *unzip*.

## Installieren Sie den Workload Security Agent

1. Melden Sie sich als Administrator oder Account-Inhaber in Ihrer Cloud Insights-Umgebung an.
2. Navigieren Sie zu Workload Security **Admin > Data Collectors** und klicken Sie auf die Registerkarte **Agents**.
3. Klicken Sie auf **+Agent** und geben Sie RHEL als Zielplattform an.
4. Kopieren Sie den Befehl Agenteninstallation.
5. Fügen Sie den Befehl „Agent Installation“ in die RHEL EC2-Instanz ein, bei der Sie angemeldet sind. Dadurch wird der Workload Security Agent installiert, der alle zur Verfügung stellt "Agent-Voraussetzungen" Werden erfüllt.

Ausführliche Schritte finden Sie über den folgenden Link: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

## Fehlerbehebung

Bekannte Probleme und deren Lösungen sind in der folgenden Tabelle beschrieben.

| Problem | Auflösung |
| --- | --- |
| „Workload-Sicherheit: Fehler beim ermitteln des ONTAP-Typs für Amazon FxSN Datensammler“ Fehler wird vom Data Collector angezeigt. Der Kunde kann den neuen Amazon FSxN Data Collector nicht zur Workload Security hinzufügen. Die Verbindung zum FSxN-Cluster an Port 443 vom Agenten ist zeitabhängig. Für die Kommunikation sind Firewall- und AWS Sicherheitsgruppen die erforderlichen Regeln aktiviert. Ein Agent wurde bereits bereitgestellt und befindet sich auch im selben AWS Konto. Dieser Agent wird verwendet, um die verbleibenden NetApp-Geräte zu verbinden und zu überwachen (und alle funktionieren). | Lösen Sie dieses Problem, indem Sie fsxadmin LIF-Netzwerksegment zur Sicherheitsregel des Agenten hinzufügen. Erlaubt alle Ports, wenn Sie sich nicht sicher über die Ports sind. |

# Benutzerverwaltung

## Benutzerkonten für die Workload-Sicherheit werden über Cloud Insights gemanagt.

Cloud Insights bietet vier Benutzerkontoebenen: Kontoinhaber, Administrator, Benutzer und Gast. Jedem Konto werden bestimmte Berechtigungsebenen zugewiesen. Ein Benutzerkonto mit Administratorrechten kann Benutzer erstellen oder ändern und jedem Benutzer eine der folgenden Workload-Sicherheitsrollen zuweisen:

| Rolle | Zugriff Auf Die Workload-Sicherheit |
| --- | --- |
| Verwalter | Alle Workload-Sicherheitsfunktionen, einschließlich derer für Warnmeldungen, Forensik, Datensammler, automatisierte Antwortrichtlinien und APIs für Workload-Sicherheit, sind möglich. Ein Administrator kann auch andere Benutzer einladen, kann aber nur Workload-Sicherheitsrollen zuweisen. |
| Benutzer | Kann Warnungen anzeigen und verwalten und Forensik anzeigen. Benutzer können den Alarmstatus ändern, eine Notiz hinzufügen, Snapshots manuell erstellen und den Benutzerzugriff einschränken. |
| Gast | Kann Warnungen und Forensik anzeigen. Gastrolle kann den Alarmstatus nicht ändern, Notizen hinzufügen, Snapshots manuell erstellen oder den Benutzerzugriff einschränken. |

**Schritte**

1. Melden Sie sich bei Workload Security an
2. Klicken Sie im Menü auf **Admin > Benutzerverwaltung**

   Sie werden zur Seite User Management von Cloud Insights weitergeleitet.

3. Wählen Sie die gewünschte Rolle für jeden Benutzer aus.

Wählen Sie beim Hinzufügen eines neuen Benutzers einfach die gewünschte Rolle aus (normalerweise Benutzer oder Gast).

Weitere Informationen zu Benutzerkonten und Rollen finden Sie im Cloud Insights "Benutzerrolle" Dokumentation.

# SVM Event Rate Checker (Agent Sizing Guide)

Das Event Rate Checker wird verwendet, um die kombinierte Ereignisrate von NFS/SMB in der SVM zu prüfen, bevor Sie einen ONTAP SVM Data Collector installieren, um zu ermitteln, wie viele SVMs ein Agent Machine überwachen können. Verwenden Sie den Event Rate Checker als Leitfaden zur Größenbestimmung, um Ihre Sicherheitsumgebung zu planen.

Ein Agent kann bis zu 50 Datensammler unterstützen.

## Voraussetzungen:

- Cluster-IP
- Benutzername und Passwort für den Cluster-Admin

Wenn dieses Skript ausgeführt wird, sollte kein ONTAP SVM Data Collector für die SVM ausgeführt werden, für die die Ereignisrate ermittelt wird.

Schritte

1. Installieren Sie den Agent, indem Sie die Anweisungen in CloudSecure befolgen.
2. Führen Sie nach der Installation des Agent das Skript *Server_Data_Rate_Checker.sh* als Sudo-Benutzer aus:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Dieses Skript erfordert die Installation von _sshapass_ auf dem linux-
Rechner. Es gibt zwei Möglichkeiten, es zu installieren:
```

   a. Führen Sie den Befehl „Fiolwing“ aus:

```
 linux_prompt> yum install sshpass
.. Wenn das nicht funktioniert, laden Sie _sshapass_ aus dem Internet
auf den linux-Rechner herunter, und führen Sie den folgenden Befehl
aus:
```

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

3. Geben Sie die richtigen Werte ein, wenn Sie dazu aufgefordert werden. Ein Beispiel hierfür finden Sie unten.
4. Das Skript dauert etwa 5 Minuten.
5. Nach Abschluss des Durchlaufs wird die Ereignisrate vom SVM gedruckt. Sie können die Ereignisrate pro

SVM in der Konsolenausgabe überprüfen:

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

Jeder ONTAP SVM Data Collector kann einer einzelnen SVM zugeordnet werden. Dies bedeutet, dass jeder Data Collector die Anzahl der von einer einzelnen SVM generierten Ereignisse erhalten kann.

Beachten Sie Folgendes:

A) Verwenden Sie diese Tabelle als allgemeinen Leitfaden zur Größenbestimmung:

| Agent-Gerätekonfiguration | Anzahl der SVM Data Collectors | Max. Ereignisrate, die der Agent-Rechner verarbeiten kann |
|---|---|---|
| 4 Cores, 16 GB | 10 Datensammler | 20.000 Ereignisse/Sek. |
| 4 Kerne, 32 GB | 20 Datensammler | 20.000 Ereignisse/Sek. |

B) um Ihre gesamten Ereignisse zu berechnen, fügen Sie die für alle SVMs erzeugten Ereignisse für diesen Agenten hinzu.

C) Wenn das Skript nicht während der Stoßzeiten ausgeführt wird oder der Spitzenverkehr schwer vorherzusagen ist, dann einen Ereignissatz-Puffer von 30 % behalten.

B + C sollte kleiner Als A sein, andernfalls kann der Agent-Rechner nicht überwacht werden.

Mit anderen Worten, die Anzahl der Datensammler, die einem einzelnen Agenten-Rechner hinzugefügt werden können, sollte der folgenden Formel entsprechen:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Siehe
xref:{relative_path}concept_cs_agent_requirements.html["Anforderungen An
Den Agenten"] Seite für zusätzliche Voraussetzungen und Anforderungen.
```

## Beispiel

Lassen Sie uns sagen, wir haben drei SVMS mit Ereignissätzen von 100, 200 und 300 Ereignissen pro Sekunde.

Wir verwenden die Formel:

```
 (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.
```

Die Konsolenausgabe ist auf dem Agent-Rechner im Dateinamen *_fpolicy_stat*<SVM Name>.log_ im vorliegenden Arbeitsverzeichnis verfügbar.

Das Skript kann in den folgenden Fällen fehlerhafte Ergebnisse liefern:

- Falsche Anmeldedaten, IP oder SVM-Name werden angegeben.
- Eine bereits vorhandene fpolicy mit demselben Namen, der gleichen Sequenznummer usw. gibt einen Fehler.
- Das Skript wird während des Laufs abrupt unterbrochen.

Ein Beispiel für einen Skriptdurchlauf ist unten dargestellt:

```
[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]#
```

## Fehlerbehebung

| Frage | Antwort |
| --- | --- |
| Wenn ich dieses Skript auf einer SVM ausführe, die bereits für die Workload-Sicherheit konfiguriert ist, verwendet es einfach die bestehende fpolicy-Konfiguration auf der SVM oder richtet es eine temporäre ein und führt den Prozess aus? | Der Event Rate Checker kann auch für eine bereits für Workload Security konfigurierte SVM einwandfrei ausgeführt werden. Es sollte keine Auswirkungen geben. |
| Kann ich die Anzahl der SVMs erhöhen, auf denen das Skript ausgeführt werden kann? | Ja. Bearbeiten Sie einfach das Skript und ändern Sie die maximale Anzahl der SVMs von 5 in eine beliebige Zahl. |
| Wenn ich die Anzahl der SVMs vergrössern möchte, wird sich damit die Ausführung des Skripts verlängern? | Nein Das Skript wird für maximal 5 Minuten ausgeführt, selbst wenn die Anzahl der SVMs erhöht wird. |
| Kann ich die Anzahl der SVMs erhöhen, auf denen das Skript ausgeführt werden kann? | Ja. Sie müssen das Skript bearbeiten und die maximale Anzahl an SVMs von 5 in eine beliebige andere Maximalzahl ändern. |
| Wenn ich die Anzahl der SVMs vergrössern möchte, wird sich damit die Ausführung des Skripts verlängern? | Nein Das Skript läuft für maximal 5 Minuten, selbst wenn die Anzahl der SVMs erhöht wird. |

| | |
|---|---|
| Was passiert, wenn ich die Ereignisratsprüfung mit einem vorhandenen Agenten durchführe? | Wenn Sie die Ereignisratenprüfung für einen bereits vorhandenen Agenten ausführen, kann dies zu einer Erhöhung der Latenz auf der SVM führen. Diese Erhöhung ist temporär, während die Ereignisratenprüfung ausgeführt wird. |