Erste Schritte

Data Infrastructure Insights

NetApp
December 19, 2024

Inhalt

Erste Schritte . . . 1
- Erste Schritte mit Workload Security . . . 1
- Anforderungen An Security Agent Für Workloads . . . 1
- Installation Von Workload Security Agent . . . 5
- Löschen eines Workload Security Agent . . . 12
- Konfigurieren eines Active Directory (AD)-Benutzerverzeichnissammler . . . 13
- Konfigurieren eines LDAP Directory Server Collectors . . . 19
- Konfiguration des ONTAP SVM Data Collector . . . 25
- Konfiguration des Cloud Volumes ONTAP und Amazon FSX für NetApp ONTAP Collector . . . 33
- Benutzerverwaltung . . . 34
- SVM Event Rate Checker (Agent Sizing Guide) . . . 35

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" "Agent Hinzufügen" "**Video**: Agentenbereitstellung"
Konfigurieren Sie einen User Directory Connector	"Fügen Sie Den User Directory Connector Hinzu" "**Video**: Active Directory-Verbindung"
Konfigurieren Sie Datensammler	Klicken Sie auf **Workload Security > Collectors** Klicken Sie auf den Datensammler, den Sie konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt „Data Collector Vendor Reference“ der Dokumentation. "**Video**: ONTAP SVM Verbindung"
Erstellen Von Benutzerkonten	"Benutzerkonten Verwalten"
Fehlerbehebung	"**Video**: Fehlerbehebung"

Auch die Workload-Sicherheit lässt sich in andere Tools integrieren. Beispielsweise zur "Siehe diesen Leitfaden"Integration in Splunk.

Anforderungen An Security Agent Für Workloads

Sie müssen "Installieren Sie einen Agenten"Informationen von Ihren Datensammlern 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 mit einer lizenzierten Version von einer der folgenden Versionen: * CentOS 8 24,04 11 9,4 Stream (64 64 64-Bit), CentOS 9 9.3 Stream, SELinux * openSUSE Leap 64 bis 20.04 (64-Bit) * Oracle Linux 64 - 15, 15 bis 8.8 (9.2-Bit) * Red hat Enterprise Linux 9.4 bis 9.4, 9.1 bis 9.4 (8.6-Bit), SELinux * Rocky 64 - 8.6 (15.3-Bit), SELinux * 8.8-Bit * (LTS * 9.1-22.04-Bit) und 64-15.5-Bit) (LmaTS * 64-10-Bit) Es wird ein dedizierter Server empfohlen.
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 36 GB (mindestens 35 GB freier Speicherplatz nach der Dateisystemerstellung) Hinweis: Es wird empfohlen, etwas zusätzlichen Speicherplatz zuzuweisen, um die Erstellung des Dateisystems zu ermöglichen. Stellen Sie sicher, dass mindestens 35 GB freier Speicherplatz im Dateisystem vorhanden ist. Wenn /opt ein eingebrachter Ordner aus einem NAS-Speicher ist, stellen Sie sicher, dass lokale Benutzer Zugriff auf diesen Ordner haben. Agent oder Data Collector können möglicherweise nicht installiert werden, wenn lokale Benutzer keine Berechtigung für diesen Ordner haben. Weitere Informationen finden Sie im Abschnitt."Fehlerbehebung"
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 installiert werden wie eine Data Infrastructure Insights Erfassungseinheit und/oder ein Agent. 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 * -Arbeitsumgebungen:

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	<site_Name>.cs01.cloudinsights.netapp.com <site_Name>.c01.cloudinsights.netapp.com <site_Name>.c02.cloudinsights.netapp.com	Einblick in die Dateninfrastruktur
TCP	443	Workload Security Agent	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Zugriff auf Authentifizierungsservices

Für **Europa-basierte** Arbeitslastsicherheitsumgebungen:

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	<site_Name>.cs01-eu-1.cloudinsights.netapp.com <site_Name>.c01-eu-1.cloudinsights.netapp.com <site_Name>.c02-eu-1.cloudinsights.netapp.com	Einblick in die Dateninfrastruktur
TCP	443	Workload Security Agent	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsservices

Für * APAC-basierte * -Arbeitsumgebungen:

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	443	Workload Security Agent	<site_Name>.cs01-ap-1.cloudinsights.netapp.com <site_Name>.c01-ap-1.cloudinsights.netapp.com <site_Name>.c02-ap-1.cloudinsights.netapp.com	Einblick in die Dateninfrastruktur
TCP	443	Workload Security Agent	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsservices

Netzwerkregeln

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	389 (LDAP) 636 (LDAPS/Start-tls)	Workload Security Agent	LDAP-Server-URL	Mit LDAP verbinden
TCP	443	Workload Security Agent	Cluster- oder SVM-Management-IP-Adresse (abhängig von der SVM-Collector-Konfiguration)	API-Kommunikation mit ONTAP

Protokoll	Port	Quelle	Ziel	Beschreibung
TCP	35000 - 55000	SVM-Daten-LIF-IP-Adressen	Workload Security Agent	Kommunikation von ONTAP zum Workload Security Agent für FPolicy-Ereignisse. Diese Ports müssen gegenüber dem Workload Security Agent geöffnet werden, damit ONTAP Ereignisse an ihn senden kann, einschließlich jeglicher Firewall auf dem Workload Security Agent selbst (falls vorhanden). BEACHTEN SIE, dass Sie nicht **all** dieser Ports reservieren müssen, aber die Ports, die Sie dafür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, mit der Reservierung von ~100 Ports zu beginnen, und bei Bedarf zu erhöhen.
TCP	7	Workload Security Agent	SVM-Daten-LIF-IP-Adressen	Echo vom Agent zu SVM-Daten-LIFs
SSH	22	Workload Security Agent	Cluster-Management	Erforderlich für das Blockieren von CIFS/SMB-Benutzern.

Systemgröße

Informationen zur Dimensionierung finden Sie in der "Ereignisprüfung" Dokumentation.

Installation Von Workload Security Agent

Workload Security (ehemals Cloud Secure) erfasst Daten zu Benutzeraktivitäten mithilfe eines oder mehrerer Agenten. Agenten stellen eine Verbindung zu Geräten auf Ihrem Mandanten her und sammeln Daten, die zur Analyse an die Workload Security SaaS-Schicht gesendet werden. Informationen zum Konfigurieren einer Agent-VM finden Sie

unter"Anforderungen An Den Agenten".

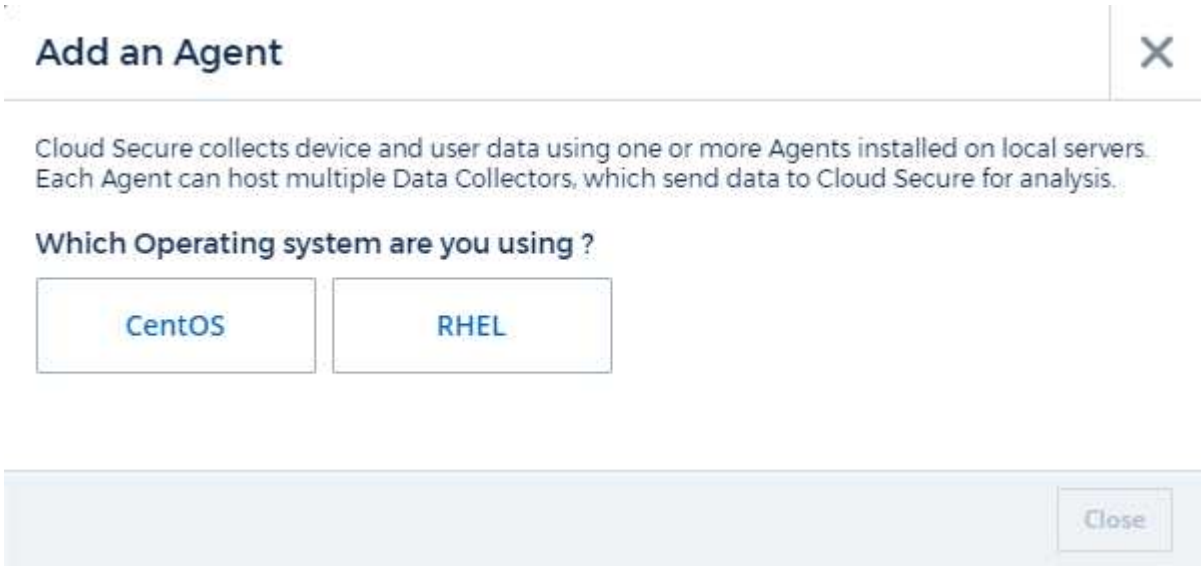
Bevor Sie Beginnen

- 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.
- Erfahren Sie mehr über Data Infrastructure Insights Security "Hier".

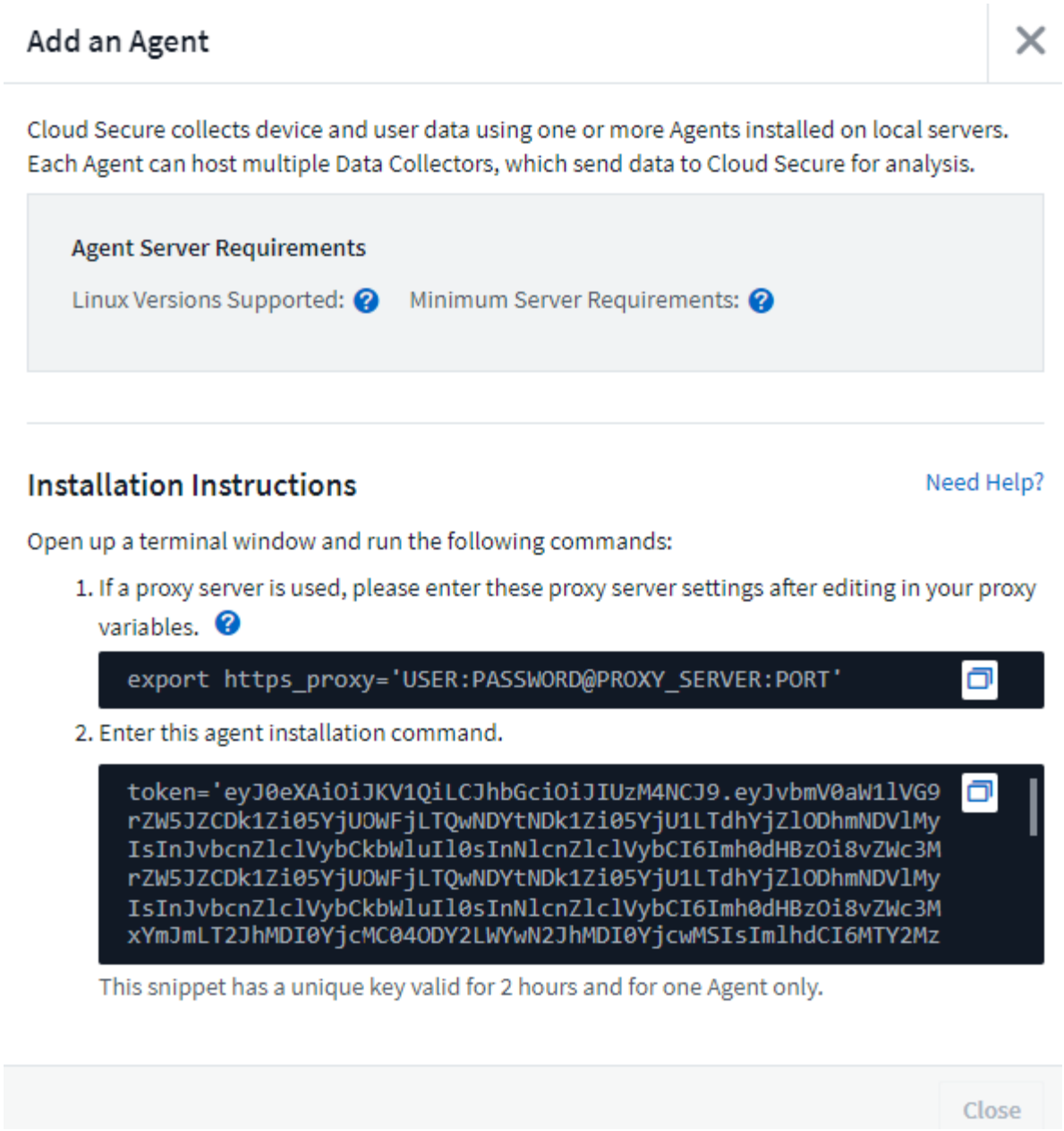
Schritte zum Installieren von Agent

1. Melden Sie sich als Administrator oder Account-Inhaber an Ihrer Workload Security-Umgebung an.
2. Wählen Sie **Collectors > Agenten > +Agent**

   Das System zeigt die Seite Agent hinzufügen an:



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:

Nach Dem Beenden

1. Sie müssen eine 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
```

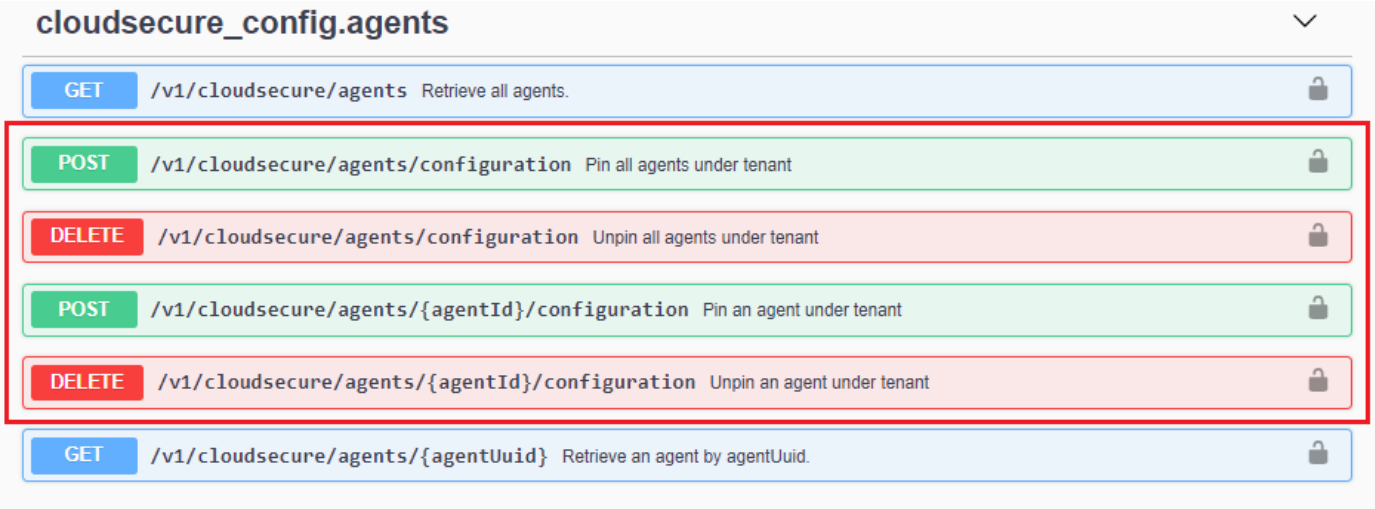
„Pinning“ an einen Agenten in der aktuellen Version

Standardmäßig aktualisiert Data Infrastructure Insights Workload Security die Agenten automatisch. Einige Kunden möchten die automatische Aktualisierung anhalten, sodass ein Agent die aktuelle Version verwendet, bis eine der folgenden Aktionen durchgeführt wird:

- Der Kunde nimmt die automatischen Agentenaktualisierungen wieder auf.
- 30 Tage sind vergangen. Beachten Sie, dass die 30 Tage am Tag der letzten Agentenaktualisierung beginnen, nicht an dem Tag, an dem der Agent angehalten wurde.

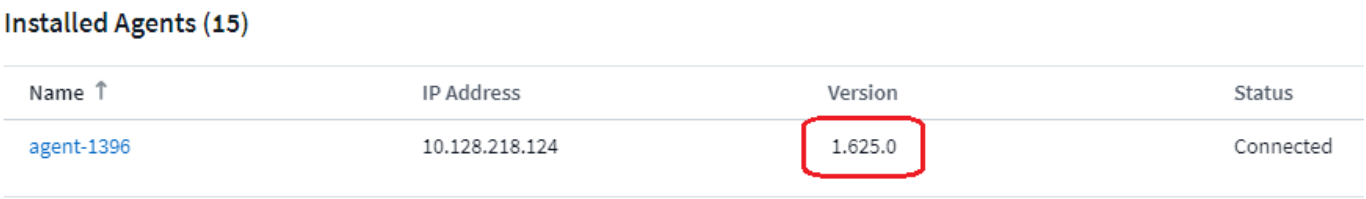
In jedem dieser Fälle wird der Agent bei der nächsten Aktualisierung der Workload-Sicherheit aktualisiert.

Um automatische Agentenaktualisierungen anzuhalten oder fortzusetzen, verwenden Sie die APIs *cloudSecure_config.Agents*:



Beachten Sie, dass es bis zu fünf Minuten dauern kann, bis die Aktion Pause oder Wiederaufnahme wirksam wird.

Sie können Ihre aktuellen Agentenversionen auf der Seite **Workload Security > Collectors** auf der Registerkarte **Agents** anzeigen.



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 an die Standardausgabe umgeleitet und ist mit dem `journalctl -u cloudsecure-agent.service` Befehl im Service-Protokoll sichtbar. Dieser Befehl kann zur weiteren Problembehandlung verwendet werden. est
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".

Problem:	Auflösung:
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.
Agent wurde installiert und wurde ausgeführt. Der Agent ist jedoch plötzlich angehalten.	SSH an den Agent-Rechner. Überprüfen Sie den Status des Agentendienstes über `sudo systemctl status cloudsecure-agent.service`. 1. Überprüfen Sie, ob in den Protokollen die Meldung „Workload Security Daemon Service konnte nicht gestartet werden“ angezeigt wird. 2. Prüfen Sie, ob cssys Benutzer auf dem Agent-Computer 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, hat eine zentralisierte Überwachungsrichtlinie möglicherweise den cssys-Benutzer gelöscht. 4. Erstellen Sie cssys Benutzer und Gruppe manuell, indem Sie die folgenden Befehle ausführen. `sudo useradd cssys` `sudo groupadd cssys` 5. Starten Sie anschließend den Agentendienst neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service` 6. Wenn es immer noch nicht ausgeführt wird, überprüfen Sie die anderen Optionen zur Fehlerbehebung.
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 anschließend den Agentendienst neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service` 3. Überprüfen Sie den Status des Agentendienstes über `sudo systemctl status cloudsecure-agent.service`. 4. Agent sollte in den Status „VERBUNDEN“ wechseln.

Problem:	Auflösung:
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.
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. Ein neues Verzeichnis mit dem Namen „CloudSecure“ erstellen. 2. Gehen Sie zu diesem Verzeichnis. 3. Kopieren Sie den vollständigen Installationsbefehl “Token=…… … ./cloudsecure-Agent-install.sh“ 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 Seriennummer von Data Infrastructure Insights an, um einen Fall zu öffnen und Protokolle wie angegeben an den Fall anzuhängen.	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 cssys B. gruppiert cssys c. CAT /etc/os-Release
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.

Problem:	Auflösung:
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.
Agent wird nach der Installation nicht ausgeführt. *Systemctl Status cloudsecure-agent.service* cloudsecure-agent.service: 12:26 zeigt Folgendes an: [Root@Demo ~]# systemctl Status cloudsecure-agent.service agent.service 03 21 126 cloudsecure-agent.service – Workload Security Agent Daemon Dienst geladen: Geladen (/usr/lib/systemd/System/cloudsecure-agent.service; 12:26 03 21 aktiviert; Herstellervorgabe: Deaktiviert) aktiv: Aktivieren (Auto-restart) (Ergebnis: Exit-Code) seit dem 2021-126:25889 PDT; vor 2 Tagen Prozess: 25889=ExecStart=/bin/bash /opt/NetApp/Systemcode verlassen: 08-03 21=12:26, Status 1/Systemcode = 126 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 die folgenden 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 Agenten neu: 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 **Workload-Sicherheit > Collectors > Agents**

   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 Data Infrastructure Insights Administrator oder Account Owner sein, um diese Aufgabe ausführen zu können.
- 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-Sicherheit auf: **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. Zum Beispiel: *username@companyname.com* oder *username@domainname.com* Zusätzlich ist eine schreibgeschützte Domain-Berechtigung erforderlich. Der Benutzer muss Mitglied der Sicherheitsgruppe *Read-Only Domain Controller* sein.
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
Status	Bundesland
Abteilung	Abteilung
Foto	Daumennagelfoto
ManagerDN	manager an
Gruppen	Mitgliedschafts

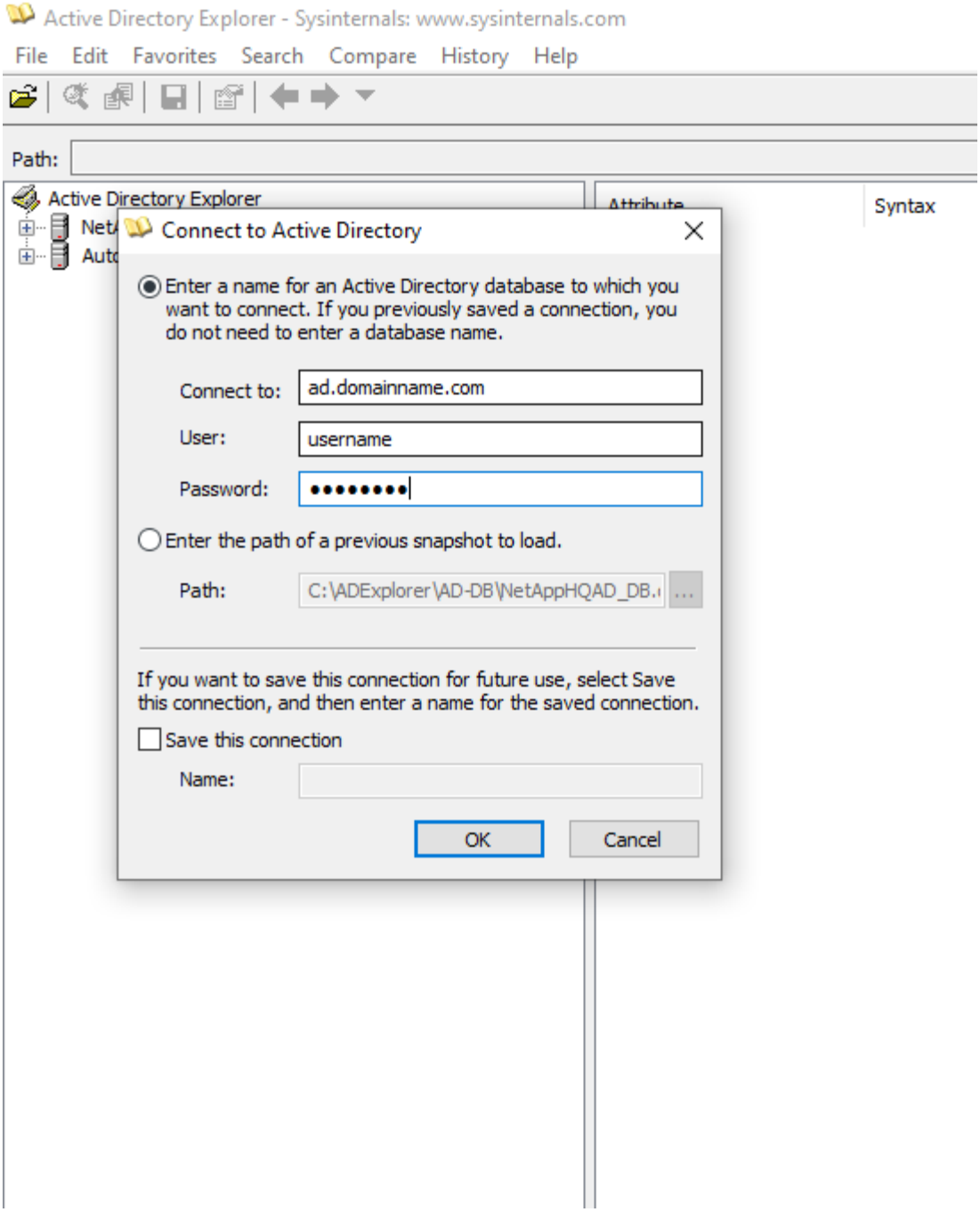
Die Konfiguration Des Benutzerverzeichnissammler Wird Getestet

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 den AD Explorer, um in einer AD-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 "AD-Explorer" auf jedem Windows-Rechner, der eine Verbindung zum AD-Server herstellen kann.
  - Stellen Sie eine Verbindung mit dem AD-Server unter Verwendung des Benutzernamens/Kennworts des AD-Verzeichnisservers her.



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.

Problem:	Auflösung:
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.
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 ein falscher 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 ein falscher 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.

Problem:	Auflösung:
Wann erfolgt die AD-Synchronisierung nach dem Neustart des Collectors?	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.
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 bestimmten Active Directory-Collector, der die Benutzerinformationen aus Active Directory abruft. 2. Hinweis unter den optionalen Attributen gibt es einen Feldnamen „Telefonnummer“, der dem Active Directory-Attribut ‘Telefonnummer’ 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 es in Active Directory ein Attribut namens ‘telephonnumber’ gibt, das tatsächlich die Telefonnummer des Benutzers hat. 5. Sagen wir in Active Directory, dass es in ‘phonenumber’ geändert wurde. 6. Bearbeiten Sie dann den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich ‘Telefonnummerierung’ durch ‘Phonenumber’. 7. Speichern Sie den Active Directory-Collector, der Collector wird neu gestartet, erhält die Telefonnummer des Benutzers und zeigt diese auf der Seite Benutzerprofil an.
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.

Problem:	Auflösung:
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 Data Infrastructure Insights Administrator oder Account Owner sein, um diese Aufgabe ausführen zu können.
- 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-Sicherheit auf: **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 for a user 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
Status	Bundesland
Abteilung	Abteilnummer
Foto	Foto
ManagerDN	manager an
Gruppen	Mitgliedschafts

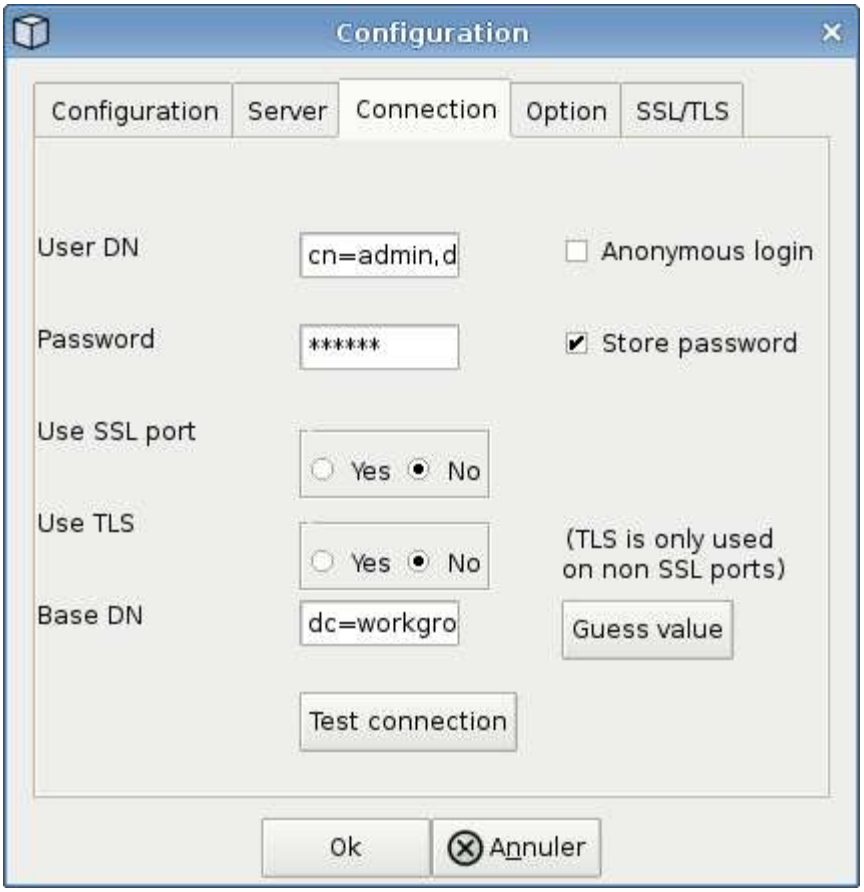
Die Konfiguration Des Benutzerverzeichnissammler Wird Getestet

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 LDAP Explorer (http://ldaptool.sourceforge.net/) oder Java LDAP Explorer (http://jxplorer.org/) auf jedem Windows-Rechner, der sich mit dem LDAP-Server verbinden kann.
  - Stellen Sie eine Verbindung mit dem LDAP-Server unter Verwendung des Benutzernamens/Kennworts des LDAP-Verzeichnisservers her.



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.

Problem:	Auflösung:
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 richtige Server-IP und die richtige Suchbasis bereitgestellt 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
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 ein falscher 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.

Problem:	Auflösung:
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.
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 bestimmten Active Directory-Collector, der die Benutzerinformationen aus Active Directory abruft. 2. Hinweis unter den optionalen Attributen gibt es einen Feldnamen „Telefonnummer“, der dem Active Directory-Attribut ‘Telefonnummer’ zugeordnet ist. 4. Verwenden Sie jetzt das oben beschriebene Active Directory Explorer-Tool, um den LDAP-Verzeichnisserver zu durchsuchen und den korrekten Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass im LDAP-Verzeichnis ein Attribut namens ‘telephonnumber’ vorhanden ist, das tatsächlich die Telefonnummer des Benutzers hat. 5. Sagen wir im LDAP-Verzeichnis, dass es in ‘phonenumber’ geändert wurde. 6. Bearbeiten Sie dann den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich ‘Telefonnummerierung’ durch ‘Phonenumber’. 7. Speichern Sie den Active Directory-Collector, der Collector wird neu gestartet, erhält die Telefonnummer des Benutzers und zeigt diese auf der Seite Benutzerprofil an.
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. Verwenden Sie für die beste Performance eine Data ONTAP-Version über 9.13.1.
  - SMB-Protokollversion 3.1 und früher.
  - NFS-Versionen bis einschließlich NFS 4.1 mit ONTAP 9.15.1 oder höher
  - 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.
- • ONTAP persistenter Speicher wird von 9.14.1 unterstützt.
- 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 nicht in der Lage sind oder nicht bereit sind, den vollständigen Benutzernamen und das Kennwort für die Verwaltung des Administratorclusters/der SVM zu verwenden, können Sie einen benutzerdefinierten Benutzer mit einer geringeren Privileges erstellen, wie im folgenden Abschnitt erwähnt„Ein Hinweis über Berechtigungen“. 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. Siehe auch die "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:

```
Vserver: svmname
                                                                  Second
User/Group                  Authentication                 Acct   Authentication
Name           Application  Method        Role Name        Locked Method
-------------- -----------  ------------  ---------------- ------ --------------
vsadmin        http         password      vsadmin          no     none
vsadmin        ontapi       password      vsadmin          no     none
vsadmin        ssh          password      vsadmin          no     none
3 entries were displayed.
```

- Stellen Sie sicher, dass für die SVM ein CIFS-Server konfiguriert 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 benutzerdefinierte 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 benutzerdefinierte 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 eine dedizierte Management-LIF zum Hinzufügen der SVM verwenden. 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.

  Informationen zur Konfiguration finden Sie unter"Anforderungen an den Agenten". 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.

Voraussetzungen für die Sperrung des Benutzerzugriffs

Beachten Sie Folgendes für"Sperrung Des Benutzerzugriffs":

Für diese Funktion sind Anmeldedaten auf Cluster-Ebene erforderlich.

Wenn Sie Anmeldedaten für die Cluster-Administration verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *cscuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, führen Sie die folgenden Schritte aus, um Workload Security-Berechtigungen zum Blockieren des Benutzers zu erteilen.

Führen Sie für CSuser mit Cluster-Anmeldedaten die folgenden Schritte in der ONTAP-Befehlszeile aus:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

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
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

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

Protobuf-Modus

Workload Security konfiguriert die FPolicy-Engine im Protobuf-Modus, wenn diese Option in den *Advanced Configuration*-Einstellungen des Collectors aktiviert ist. Der Protobuf-Modus wird in ONTAP Version 9.15 und höher unterstützt.

Weitere Informationen zu dieser Funktion finden Sie in der "ONTAP-Dokumentation".

Für Protobuf sind bestimmte Berechtigungen erforderlich (einige oder alle dieser Berechtigungen sind möglicherweise bereits vorhanden):

Clustermodus:

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

VServer-Modus:

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

Berechtigungen für autonomen ONTAP-Ransomware-Schutz und ONTAP-Zugriff verweigert

Wenn Sie Anmeldedaten für die Cluster-Administration verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, befolgen Sie die folgenden Schritte, um Workload Security-Berechtigungen zum Sammeln von ARP-bezogenen Informationen aus ONTAP zu erteilen.

Weitere Informationen finden Sie unter "Integration mit ONTAP-Zugriff verweigert"

Und "Integration in ONTAP Autonomous Ransomware Protection"

Konfigurieren Sie den Datensammler

Schritte zur Konfiguration

1. Melden Sie sich als Administrator oder Account Owner bei Ihrer Data Infrastructure Insights-Umgebung an.
2. Klicken Sie Auf **Workload Security > Collectors > +Data Collectors**

   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.
Name SVM	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 stehen folgende Optionen zur Verfügung: 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 MetroCluster

Für MetroCluster wird Folgendes empfohlen:

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

Wenn Sie die Service Policy mit ONTAP **Version 9.9.1 oder neuer** verwenden, um eine Verbindung zum Data Source Collector herzustellen, ist der *Data-fpolicy-Client*-Dienst 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.

Data Collector Wiedergeben/Anhalten

2 neue Operationen werden jetzt auf dem Kebab-Menü des Sammlers angezeigt (PAUSE und WIEDERAUFNAHME).

Wenn sich der Data Collector im Status *Running* befindet, können Sie die Erfassung anhalten. Öffnen Sie das Menü „drei Punkte“ für den Collector und wählen Sie PAUSE. Während der Collector angehalten wird, werden keine Daten von ONTAP erfasst und keine Daten vom Collector an ONTAP gesendet. Dies bedeutet, dass keine FPolicy-Ereignisse vom ONTAP zum Datensammler und von dort zu Dateninfrastruktureinblicken übertragen werden.

Wenn neue Volumes usw. auf ONTAP erstellt werden, während der Collector angehalten ist, erfasst Workload Security die Daten nicht, und diese Volumes usw. werden nicht in Dashboards oder Tabellen angezeigt.

Beachten Sie Folgendes:

- Das Löschen von Snapshots geschieht nicht gemäß den Einstellungen, die auf einem angehaltenen Collector konfiguriert wurden.
- EMS-Ereignisse (wie ONTAP ARP) werden nicht auf einem angehaltenen Collector verarbeitet. Das heißt, wenn ONTAP einen Ransomware-Angriff identifiziert, kann Data Infrastructure Insights Workload Security

dieses Ereignis nicht erfassen.

- Für einen angehaltenen Collector werden KEINE Integritätsbenachrichtigungen-E-Mails gesendet.
- Manuelle oder automatische Aktionen (wie Snapshot oder Benutzerblockierung) werden auf einem angehaltenen Collector nicht unterstützt.
- Bei Agent- oder Collector-Upgrades, Neustart/Neustart der Agent-VM oder Neustart des Agent-Dienstes bleibt ein angehaltener Collector im Status „*Paused*“.
- Wenn sich der Datensammler im Status *Error* befindet, kann der Collector nicht in den Status *Paused* geändert werden. Die Schaltfläche Pause wird nur aktiviert, wenn der Status des Collectors *Running* lautet.
- Wenn die Verbindung zum Agenten unterbrochen wird, kann der Collector nicht in den Status *Paused* geändert werden. Der Collector geht in den Status *stopped* und die Schaltfläche Pause wird deaktiviert.

Persistenter Speicher

Persistenter Speicher wird von ONTAP 9.14.1 und höher unterstützt. Beachten Sie, dass die Anweisungen für Volume-Namen von ONTAP 9.14 bis 9.15 variieren.

Persistenter Speicher kann durch Aktivieren des Kontrollkästchens auf der Seite Collector Edit/Add aktiviert werden. Nach dem Aktivieren des Kontrollkästchens wird ein Textfeld für die Annahme des Volume-Namens angezeigt. Der Volume-Name ist ein obligatorisches Feld für die Aktivierung von Persistent Store.

- Für ONTAP 9.14.1 müssen Sie das Volume erstellen, bevor Sie die Funktion aktivieren, und den gleichen Namen im Feld „*Volume Name*“ eingeben. Die empfohlene Volume-Größe beträgt 16 GB.
- Für ONTAP 9.15.1 wird das Volume automatisch mit 16 GB Größe vom Collector erstellt. Dabei wird der Name verwendet, der im Feld *Volume Name* angegeben ist.

Für Persistent Store sind bestimmte Berechtigungen erforderlich (einige oder alle dieser Berechtigungen sind möglicherweise bereits vorhanden):

Clustermodus:

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

VServer-Modus:

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

Fehlerbehebung

Tipps zur Fehlerbehebung finden Sie auf der "Fehlerbehebung für den SVM Collector" Seite.

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 finden Sie Informationen zur Konfiguration einer Single-Node-/HA-AWS-Instanz zum Hosten des Workload Security Agent: https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html

Befolgen Sie nach Abschluss der Konfiguration die Schritte zur Einrichtung Ihrer SVM: 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 ein RHEL oder CentOS AMI 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 Owner bei Ihrer Data Infrastructure Insights-Umgebung an.

2. Navigieren Sie zu Workload Security **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. Auf diese Weise wird der Workload Security Agent installiert, der alle "Agent-Voraussetzungen"erfüllt.

Detaillierte Schritte finden Sie unter diesem 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 Workload-Sicherheit werden über Data Infrastructure Insights gemanagt.

Data Infrastructure 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 auf die Seite User Management von Data Infrastructure 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 in der Dokumentation zu Data Infrastructure Insights"Benutzerrolle".

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 folgenden Befehl 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 Größenbemessung. Sie können die Anzahl der Kerne und/oder des Speichers erhöhen, um die Anzahl der unterstützten Datensammler zu erhöhen, bis zu maximal 50 Datensammler:

Agent-Gerätekonfiguration	Anzahl der SVM Data Collectors	Max. Ereignisrate, die der Agent-Rechner verarbeiten kann
4 Kerne, 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
Weitere Voraussetzungen und Anforderungen finden Sie auf der
xref:{relative_path}concept_cs_agent_requirements.html["Anforderungen An
Den Agenten"] Seite.
```

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 läuft für maximal 5 Minuten, auch wenn sich die Anzahl der SVMs erhöht.
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, auch 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.