



# Sicherheit Von Storage-Workloads

## Cloud Insights

NetApp  
May 25, 2023

# Inhaltsverzeichnis

- Sicherheit Von Storage-Workloads ..... 1
  - Allgemeines Zur Storage Workload Security ..... 1
  - Erste Schritte ..... 1
  - Meldungen ..... 39
  - Forensik ..... 42
  - Automatisierte Antwortrichtlinien ..... 49
  - Integration in ONTAP Autonomous Ransomware Protection ..... 51
  - Blockieren Des Benutzerzugriffs ..... 54
  - Workload Security: Simulation eines Angriffs ..... 59
  - Konfigurieren von E-Mail-Benachrichtigungen für Warnungen, Warnungen und den Zustand des Agent/Data Source Collectors ..... 63
  - Workload-Sicherheits-API ..... 63

# Sicherheit Von Storage-Workloads

## Allgemeines Zur Storage Workload Security

Die Cloud Insights Storage Workload Security (ehemals Cloud Secure) schützt Ihre Daten mithilfe intelligenter Funktionen vor Bedrohungen von innen. Es ermöglicht eine zentrale Übersicht und Kontrolle über den Zugriff auf alle Unternehmensdaten in Hybrid-Cloud-Umgebungen, damit Sicherheits- und Compliance-Ziele erfüllt werden.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

### Übersicht

Verschaffen Sie sich einen zentralen Überblick und kontrollieren Sie den Benutzerzugriff auf wichtige Unternehmensdaten, die lokal oder in der Cloud gespeichert sind.

Ersetzen Sie Tools und manuelle Prozesse, die nicht zeitgerecht und präzise Einblicke in Datenzugriff und -Kontrolle bieten. Workload Security wird auf einzigartige Weise in der Cloud und in lokalen Storage-Systemen ausgeführt, sodass Sie über schädliches Benutzerverhalten in Echtzeit benachrichtigt werden können.

### Darstellt

Dank erweitertem Machine Learning und Anomalieerkennung werden Unternehmensdaten vor Missbrauch durch böswillige oder kompromittierte Benutzer geschützt.

Benachrichtigt Sie über erweitertes Machine Learning und Anomalieerkennung des Benutzerverhaltens bei ungewöhnlichen Datenzugriff.

### Compliance

Durch Auditing von Benutzerzugriffen auf lokal oder in der Cloud gespeicherte wichtige Unternehmensdaten wird die unternehmensinterne Compliance gewahrt.

## Erste Schritte

### Erste Schritte mit Workload Security

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



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

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" " <b>Video</b> : Agentenbereitstellung"
Konfigurieren Sie einen User Directory Connector	"Fügen Sie Den User Directory Connector Hinzufügen" " <b>Video</b> : Active Directory-Verbindung"
Konfigurieren Sie Datensammler	Klicken Sie auf <b>Admin &gt; Datensammler</b> Klicken Sie auf den Datensammler, den Sie konfigurieren möchten. Weitere Informationen finden Sie im Abschnitt Data Collector Vendor Reference in der Dokumentation." <b>Video</b> : ONTAP SVM Verbindung"
Erstellen Von Benutzerkonten	"Benutzerkonten Verwalten"
Fehlerbehebung	" <b>Video</b> : 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.



Storage Workload Security ist in der Cloud Insights Bundesausgabe nicht verfügbar.

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

Komponente	Linux-Anforderungen Erfüllt
Verfügbare 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 " <a href="#">Fehlerbehebung</a> " 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:

Verfügbare 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 <site_Name>.c01.cloudinsights.netapp.com <site_Name>.c02.cloudinsights.netapp.com	Abgehender Anruf	Zugriff auf Cloud Insights
TCP	443	gateway.c01.cloudinsights.netapp.com 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 <site_Name>.c01-eu-1.cloudinsights.netapp.com <site_Name>.c02-eu-1.cloudinsights.netapp.com	Abgehender Anruf	Zugriff auf Cloud Insights
TCP	443	gateway.c01.cloudinsights.netapp.com 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

Protokoll	Port	Ziel	Richtung	Beschreibung
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	Kommunikation mit ONTAP bei FPolicy-Ereignissen
TCP	7	SVM-Daten-LIF-IP-Adressen	Abgehender Anruf	Unidirektional zwischen ONTAP und Workload-Sicherheit. Agent pingt die SVM-LIFs an.
SSH	22	Cluster-Management	Abgehender Anruf	Erforderlich für das Blockieren von CIFS/SMB-Benutzern.

## 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:



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

### 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





## Nach Dem Beenden

1. Sie müssen ein konfigurieren "[Benutzerverzeichnissammler](#)".
2. Sie müssen einen oder mehrere Data Collectors konfigurieren.

## Netzwerkconfiguration

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 <code>/opt/netapp/cloudSecure/Agent/logs/agent.log</code> nicht erstellt, und die Datei <code>install.log</code> 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 <code>journalctl -u cloudsecure-agent.service</code> Befehl. Dieser Befehl kann zur weiteren Fehlerbehebung verwendet werden.

Problem:	Auflösung:
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 " <a href="#">Anforderungen An Den Agenten</a> ".
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 Agent-Dienstes über <code>sudo systemctl status cloudsecure-agent.service</code> . 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. <code>sudo id cssys sudo groups cssys`3</code> . 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. <code>`sudo useradd cssys`sudo groupadd cssys`5</code> . Starten Sie danach den Agent-Service neu, indem Sie den folgenden Befehl ausführen: <code>`sudo systemctl restart cloudsecure-agent.service`6</code> . 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 handeln.
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: <code>sudo systemctl restart cloudsecure-agent.service`3</code> . Prüfen Sie den Status des Agent-Service über <code>`sudo systemctl status cloudsecure-agent.service</code> . 4. Agent sollte in DEN ANGESCHLOSSENEN Zustand gehen.

Problem:	Auflösung:
<p>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.</p>	<p>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.</p>
<p>Bei der Installation des Agenten bleibt die Installation nach dem Entpacken hängen.</p>	<p>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.</p>
<p>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.</p>	<p>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</p>
<p>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</p>	<p>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.</p>

Problem:	Auflösung:
<p>Agent-Installation schlägt bei useradd fehl: Verzeichnis /Home/cssys kann nicht erstellt werden</p>	<p>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: <i>Sudo useradd user_Name -m -d HOME_dir -m</i> :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, <i>sudo useradd cssys -m -d /cssys</i>, fügt einen Benutzer_cssys_ hinzu und erstellt sein Login-Verzeichnis unter root.</p>
<p>Agent wird nach der Installation nicht ausgeführt. <i>Systemctl Status cloudsecure-agent.service</i> 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.</p>	<p>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.</p>
<p>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?</p>	<p>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: <i>cd /opt/netapp/cloudSecure/conf</i> 2. Öffnen Sie die Datei <i>agent.properties</i> mit Ihrem bevorzugten Texteditor zum Bearbeiten. 3. Fügen Sie folgende Zeilen hinzu oder ändern Sie sie: <i>AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com</i> <i>AGENT_PROXY_PORT=80</i> <i>AGENT_PROXY_USER=pxuser</i> <i>AGENT_PROXY_PASSWORD=pass1234</i> 4. Speichern Sie die Datei. 5. Starten Sie den Agent: <i>Sudo systemctl restart cloudsecure-agent.service</i></p>

## 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: <i>GlobalADCollector</i>
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: <i>X.y.z</i> ⇒ direkter Domainname, wie Sie ihn auf Ihrer SVM haben. [Beispiel: <i>hq.companyname.com</i> ] <i>DC=x,DC=y,DC=z</i> ⇒ relative Distinguished Names [Beispiel: <i>DC=hq,DC=commeryname,DC=com</i> ] oder Sie können wie folgt angeben: <i>OU=Engineering,DC=hq,DC=commeryname,DC=com</i> [nach spezifischer OU-Technik filtern] <i>CN=username,OU=Engineering,DC=comcompyname,DC=netapp,DC=com</i> [um nur bestimmte Benutzer mit <username> von OU <Engineering> zu erhalten] <i>_CN=Acrobat</i> Nutzer, <i>CN=Benutzer,DC=hq,DC=commeryname,DC=</i> alle Benutzer innerhalb von Boston, die innerhalb der Organisation unterstützt werden.
DN binden	Benutzer erlaubt, das Verzeichnis zu durchsuchen. Beispiel: <i>username@companyname.com</i> oder <i>username@domainname.com</i>
Kennwort BINDEN	Kennwort des Verzeichnisservers (d. h. Kennwort für in Bind DN verwendeten Benutzernamen)
Protokoll	Idap, Idaps, Idap-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 Benutzerverzeichnisses 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-Verzeichnisseservers 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.

<b>Problem:</b>	<b>Auflösung:</b>
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 <i>Neustart</i> 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 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.



<b>Problem:</b>	<b>Auflösung:</b>
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 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 „Phonenummer“ geändert wurde. 6. Dann bearbeiten Sie den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich 'Telefonnummerierung' durch 'Phonenummer'. 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-Serverschlüsselung, 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: <i>GlobalLDAPCollector</i>
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= companyname,DC=com] oder Sie können wie folgt angeben: OU= <i>Engineering</i> ,DC= <i>hq</i> ,DC= <i>companyname</i> ,DC= <i>com</i> [nach spezifischer OU-Technik filtern] CN= <i>username</i> ,OU= <i>Engineering</i> ,DC= <i>companyname</i> , DC= <i>netapp</i> , DC= <i>com</i> [um nur bestimmte Benutzer mit <username> von OU <Engineering> zu bekommen] _CN=Acrobat Nutzer,CN=Benutzer,DC=hq,DC=companyname,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 <a href="mailto:john@dorp.company.com">john@dorp.company.com</a> . dorp.company.com
--Konten	--user
--john	--anna
Kennwort BINDEN	Kennwort des Verzeichnisseservers (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 Verzeichnisseserver
Anzeigename	Name
UNIXID	Nummer der Uidnummer
Benutzername	uid

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

Merkmale	Attributname im Verzeichnisseserver
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 Benutzerverzeichnissesammler 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 Oder Java LDAP Explorer 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-Verzeichnisseservers 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 <i>Neustart</i> klicken.

Problem:	Auflösung:
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
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.

<b>Problem:</b>	<b>Auflösung:</b>
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: ACceptSecurityContext 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 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 „Phonenummer“ geändert wurde. 6. Dann bearbeiten Sie den CloudSecure User Directory Collector. Ersetzen Sie im optionalen Attributbereich 'Telefonnummerierung' durch 'Phonenummer'. 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-Serverschlüsselung, 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 <vservename> -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 <vserversname> 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 <b>CloudSecure &gt; Aktivitätsforensics &gt; Alle Aktivitäten</b> 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:
<p>Collector meldet Fehlermeldung: „Keine lokale IP-Adresse auf dem Anschluss gefunden, die die Datenschnittstellen der SVM erreichen kann“.</p>	<p>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-Datenlif oder dem Management- lif 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: <code>Network ping -vserver &lt;vserver Name&gt; -Destination &lt;Agent IP&gt; -lif &lt;Lif Name&gt; -show-Detail</code> 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 <code>https://&lt;cluster_mgmt_ip&gt;/spi/&lt;clustername&gt;/etc/log/packet_traces/</code> 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 "<a href="#">Netapp Support</a>" Für weitere Unterstützung.</p>

<b>Problem:</b>	<b>Auflösung:</b>
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:
<p>Fehlermeldung: „Konnektor befindet sich im Fehlerzustand. Service.name: Audit. Grund für Fehlschlag: Externer fpolicy-Server beendet.“</p>	<p>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.</p> <p>2. Geben Sie den folgenden Befehl in das Feld Agent ein und stellen Sie sicher, dass der Port-Bereich geöffnet ist. <i>Sudo iptables-save 3500*</i>  Beispielausgabe sollte aussehen wie: <i>-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEU -j ACCEPT</i></p> <p>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. <i>Systemdienste Firewall show Systemdienste Firewall-Policy show_ "Überprüfen Sie die Firewall-Befehle"</i> Auf der ONTAP-Seite.</p> <p>4. SSH an die SVM/Cluster, die Sie überwachen möchten. <i>Ping the Agent Box from the SVM Data lif (with CIFS, NFS Protocols Support) und Sicherstellen, dass Ping funktioniert: _Network ping -vserver &lt;vserver Name&gt; -Destination &lt;Agent IP&gt; -lif &lt;Lif Name&gt; -show-Detail</i> Wenn nicht pingfähig, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, damit der Agent-Rechner pingfähig ist.</p> <p>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.</p> <p>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.</p> <p>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.</p>

Problem:	Auflösung:
<p>Auf der Aktivitätsseite werden keine Ereignisse angezeigt.</p>	<p>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. <code>&lt;SVM&gt;Ereignisprotokoll show -source fpolicy</code> 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: <code>&lt;SVM&gt;fpolicy show</code> 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.</p>
<p>SVM Data Collector befindet sich im Fehlerzustand und Fehlermeldung „Agent konnte keine Verbindung zum Collector herstellen“</p>	<p>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.</p>
<p>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“)</p>	<p>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: <code>Event Log show -source fpolicy</code>, die das Fehlerereignisprotokoll <code>show -source fpolicy -fields Event,Action,Beschreibung</code> zeigt, die weitere Details. <a href="#">Überprüfen Sie die Firewall-Befehle</a> Auf der ONTAP-Seite.</p>
<p>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.“</p>	<p>Stellen Sie sicher, dass es eine Betriebssystemschnittstelle gibt (Rolle als Daten und Datenprotokoll als CIFS/NFS).</p>



Problem:	Auflösung:
<p>Der Datensammler wechselt in den Fehlerzustand und geht nach einiger Zeit in DEN LAUFENDEN Zustand, dann wieder zurück zu Fehler. Dieser Zyklus wiederholt sich.</p>	<p>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.</p>
<p>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'</p>	<p>Die Freigabennamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die DSC-Konfiguration der ONTAP SVM, um die Freigabennamen zu korrigieren. <i>Aktien einschließen und ausschließen</i> 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.</p>
<p>Im Cluster gibt es bereits Richtlinien, die nicht verwendet werden. Was sollte vor der Installation von Workload Security getan werden?</p>	<p>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: <i>fpolicy show</i> Steps zum Löschen von fpolicy-Konfigurationen: <i>fpolicy disable -vserver &lt;svmname&gt; -Policy-Name &lt;Policy_Name&gt; fpolicy-Name_vserver_Name_vmserver_delete -vmserver_name_vmserver_list_vmserver_delete_vengine_Name_vmserver_vengine_Name_vmserver_vmserver_list_vmserver_&lt;_vmengine_Name_vmserver_&lt;_vmengine_list_Name_vmserver_&lt;_vmserver_nement-Name_&lt;_vmserver_vmserver_Name_vmserver_&lt;_vmserver_list_vmserver_Name_&lt;&lt;&lt;_next-</i></p>
<p>Nach Aktivierung der Workload-Sicherheit beeinträchtigt die ONTAP-Performance: Sporadisch steigt die Latenz an und IOPS werden sporadisch niedrig.</p>	<p>Stellen Sie sicher, dass Sie dort eine Data ONTAP-Version verwenden "<a href="#">Diese Ausgabe</a>" 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.</p>

Problem:	Auflösung:
<p>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. „</p>	<p>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.</p>
<p>Der Data Collector zeigt die Fehlermeldung „Fehler: Fehler: Fehler, den Zustand des Collectors innerhalb von 2 Wiederholungen zu ermitteln. Versuchen Sie erneut, den Collector neu zu starten (Fehlercode: AGENT008)“.</p>	<p>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 <i>Bearbeiten</i>. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche <i>Save</i> 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 "<a href="#">Auf dieser Seite</a>".</p>

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](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](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](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
---------	-----------

<p>„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).</p>	<p>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.</p>
--	--

## 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 _sshpass_ auf dem linux-Rechner. Es gibt zwei Möglichkeiten, es zu installieren:
```

- a. Führen Sie den Befehl „Folwing“ aus:

```
linux_prompt> yum install sshpass  
.. Wenn das nicht funktioniert, laden Sie _sshpass_ 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.

## Meldungen

Die Seite „Workload Security Alerts“ zeigt eine Zeitleiste aktueller Angriffe und/oder Warnungen an und ermöglicht Ihnen, Details zu jedem Problem anzuzeigen.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

[Alarmliste]

### Alarm

In der Alarmliste wird ein Diagramm angezeigt, in dem die Gesamtanzahl der potenziellen Angriffe und/oder Warnungen angezeigt wird, die im ausgewählten Zeitraum angehoben wurden, gefolgt von einer Liste der Angriffe und/oder Warnungen, die in diesem Zeitraum aufgetreten sind. Sie können den Zeitbereich ändern, indem Sie die Schieberegler für Startzeit und Endzeit in der Grafik anpassen.

Für jede Meldung wird Folgendes angezeigt:

#### Potentielle Angriffe:

- Der *Potential Attack*-Typ (z. B. Ransomware oder Sabotage)
- Datum und Uhrzeit des potenziellen Angriffs wurde *entdeckt*
- Der *Status* der Warnmeldung:
  - **Neu:** Dies ist der Standard für neue Warnmeldungen.
  - **In Bearbeitung:** Der Alarm wird von einem Teammitglied oder Mitgliedern untersucht.
  - **Behoben:** Der Alarm wurde von einem Teammitglied als gelöst markiert.
  - **Abgeschieden:** Der Alarm wurde als falsch positives oder erwartetes Verhalten abgewiesen.

Ein Administrator kann den Status der Warnmeldung ändern und eine Notiz hinzufügen, um die Untersuchung zu unterstützen.

[Ändern Sie Den Alarmstatus]

- Der *User*, dessen Verhalten die Warnung ausgelöst hat
- *Nachweis* des Angriffs (zum Beispiel wurde eine große Anzahl von Dateien verschlüsselt)
- Die *Aktion wurde ausgeführt* (zum Beispiel wurde ein Snapshot erstellt)

#### Warnungen:

- Das *anormale Verhalten*, das die Warnung ausgelöst hat
- Das Datum und die Uhrzeit, zu der das Verhalten erkannt wurde\_

- Der *Status* der Warnmeldung (Neu, wird ausgeführt usw.)
- Der *User*, dessen Verhalten die Warnung ausgelöst hat
- Eine Beschreibung des *Change* (z. B. eine abnormale Erhöhung des Dateizugriffs)
- Die *Aktion Ausgeführt*

## Filteroptionen

Sie können Warnungen nach folgenden Kriterien filtern:

- Der *Status* der Warnmeldung
- Spezifischer Text in der *Note*
- Die Art von *attacks/Warnings*
- Der *\_Benutzer\_*, dessen Aktionen die Warnung/Warnung ausgelöst haben

## Die Seite „Warndetails“

Sie können auf der Seite mit den Warnmeldungen auf einen Alarm-Link klicken, um eine Detailseite für die Meldung zu öffnen. Die Alarmdetails können je nach Angriffstyp oder Alarmtyp variieren. Eine Seite mit den Details zum Angriff durch Ransomware kann beispielsweise folgende Informationen enthalten:

### Zusammenfassung:

- Angriffstyp (Ransomware, Sabotage) und Alarm-ID (zugewiesen durch Workload-Sicherheit)
- Datum und Uhrzeit des Angriffs
- Es wurde eine Aktion ausgeführt (beispielsweise ein automatischer Snapshot erstellt. Die Zeit des Snapshots wird direkt unter der Zusammenfassung angezeigt)
- Status (Neu, in Bearbeitung usw.)

### Abschnitt „Angriffsergebnisse“:

- Anzahl der betroffenen Volumes und Dateien
- Eine begleitende Zusammenfassung der Detektion
- Ein Diagramm mit Dateiaktivitäten während des Angriffs

### Abschnitt „Verwandte Benutzer“:

In diesem Abschnitt werden Details zu dem Benutzer angezeigt, der an dem potenziellen Angriff beteiligt ist, einschließlich einer Grafik der Top-Aktivität für den Benutzer.

Seite zu Warnungen (Dieses Beispiel zeigt einen potenziellen Ransomware-Angriff auf):[Beispiel Für Ransomware-Warnungen]

Detailseite (dieses Beispiel zeigt einen potenziellen Ransomware-Angriff.):[Beispiel Für Die Detailseite Von Ransomware]

## Snapshot Aktion durchführen

Workload Security schützt Ihre Daten, indem bei Erkennung schädlicher Aktivitäten automatisch ein Snapshot erstellt wird. So wird sichergestellt, dass Ihre Daten sicher gesichert werden.

Sie können definieren "[Automatisierte Antwortrichtlinien](#)" Die einen Snapshot machen, wenn Ransomware-Angriff oder eine andere abnormale Benutzeraktivität erkannt wird. Sie können einen Snapshot auch manuell von der Warnungsseite aus erstellen.

Automatische Momentaufnahme:[Aktionsbildschirm Für Warnmeldungen, 1000]

Manuelle Momentaufnahme:[Aktionsbildschirm Für Warnmeldungen, 1000]

## Warnbenachrichtigungen

Für jede Aktion der Warnmeldung werden E-Mail-Benachrichtigungen an eine Benachrichtigungsliste gesendet. Um Warnungsempfänger zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie für jeden Empfänger eine E-Mail-Adresse ein.

## Aufbewahrungsrichtlinie

Warnungen und Warnungen werden 13 Monate lang aufbewahrt. Warnungen und Warnungen, die älter als 13 Monate sind, werden gelöscht. Wenn die Workload-Sicherheitsumgebung gelöscht wird, werden auch alle mit der Umgebung verknüpften Daten gelöscht.

## Fehlerbehebung

Problem:	Versuchen Sie Das:
Gibt es für durch Workload-Sicherheit (CS) ergriffene Snapshots eine Spülzeit/Archivierungsdauer für CS-Snapshots?	Nein Für CS-Snapshots ist kein Spülzeitraum/Archivierungszeitraum festgelegt. Der Benutzer muss die Spülrichtlinie für CS-Snapshots definieren. Weitere Informationen finden Sie im " <a href="#">ONTAP-Dokumentation</a> " Über das Einrichten der Richtlinien.
Es besteht die Situation, dass ONTAP stündliche Snapshots pro Tag erstellt. Werden Workload Security (CS) Snapshots dies beeinträchtigen? Wird CS Schnappschuss den stündlichen Snapshot-Platz machen? Wird der stündliche StandardSnapshot angehalten?	Arbeitslastsicherheit Schnappschüsse werden die stündlichen Schnappschüsse nicht beeinflussen. CS Snapshots nehmen keinen stündlichen Snapshot-Platz in Anspruch und sollten wie zuvor fortgesetzt werden. Der standardmäßige stündliche Snapshot wird nicht angehalten.
Was geschieht, wenn die Maximalanzahl der Snapshots in ONTAP erreicht wird?	Wenn die maximale Anzahl an Snapshots erreicht wird, schlägt das nachfolgende Erstellen eines Snapshots fehl, und die Workload-Sicherheit weist eine Fehlermeldung auf, dass der Snapshot voll ist. Benutzer müssen Snapshot-Richtlinien definieren, um die ältesten Snapshots zu löschen, sonst werden keine Snapshots erstellt. Ab ONTAP 9.3 und älteren Versionen kann ein Volume bis zu 255 Snapshot Kopien enthalten. Ab ONTAP 9.4 kann ein Volume bis zu 1023 Snapshot Kopien enthalten. Weitere Informationen finden Sie in der ONTAP-Dokumentation " <a href="#">Richtlinie zum Löschen von Snapshots wird festgelegt</a> ".

Problem:	Versuchen Sie Das:
Workload Security kann überhaupt keine Snapshots erstellen.	Stellen Sie sicher, dass die Rolle, die zum Erstellen von Snapshots verwendet wird, Link hat: <a href="#">proper Rechte zugewiesen</a> . Stellen Sie sicher, dass <i>csrole</i> mit entsprechenden Zugriffsrechten für die Erstellung von Snapshots erstellt wird: Security Login role create -vserver <vserversname> -role csrolle -cmddirname „Volume Snapshot“ -Access all
Snapshots versagen bei älteren Warnmeldungs-Warnungen auf SVMs, die aus der Workload Security entfernt und anschließend wieder hinzugefügt wurden. Für neue Warnmeldungen, die nach dem erneuten Hinzufügen der SVM auftreten, werden Snapshots erstellt.	Dies ist ein seltenes Szenario. Falls dies der Fall ist, melden Sie sich bei ONTAP an und erstellen Sie die Snapshots manuell, um die älteren Meldungen zu erhalten.
Auf der Seite „Details der Warnmeldung“ wird die Meldung „Letzter Versuch fehlgeschlagen“ unter der Schaltfläche „Take Snapshot“ angezeigt. Wenn Sie den Fehler bewegen, wird „API-Befehl aufrufen hat Timeout für den Datensammler mit id“ angezeigt.	Dies kann passieren, wenn ein Datensammler zur Workload-Sicherheit über SVM Management IP hinzugefügt wird, wenn sich die LIF der SVM in ONTAP in „ <i>dedisabled State</i> “ befindet. Aktivieren Sie die bestimmte LIF in ONTAP und lösen Sie <i>_Snapshot</i> manuell aus der Workload-Sicherheit aus. Die Aktion „Snapshot“ wird dann erfolgreich ausgeführt.

## Forensik

### Forensik - Alle Aktivitäten

Auf der Seite Alle Aktivitäten können Sie die Aktionen verstehen, die für Einheiten in der Workload-Sicherheitsumgebung durchgeführt werden.

#### Alle Aktivitätsdaten Werden Untersucht

Klicken Sie auf **Forensics > Vorgangsforensics** und klicken Sie auf die Registerkarte **Alle Aktivitäten**, um die Seite Alle Aktivitäten aufzurufen. Diese Seite bietet einen Überblick über Aktivitäten in Ihrer Umgebung und hebt die folgenden Informationen hervor:

- Ein Diagramm mit „*Aktivitätsverlauf*“ (Zugriff pro Minute/pro 5 Minuten/pro 10 Minuten basierend auf dem ausgewählten globalen Zeitbereich)

Sie können das Diagramm vergrößern, indem Sie ein Rechteck im Diagramm herausziehen. Die gesamte Seite wird geladen, um den vergrößerten Zeitbereich anzuzeigen. Wenn der Zoom vergrößert wird, wird eine Schaltfläche angezeigt, mit der der Benutzer zoomen kann.

- Ein Diagramm mit „*Aktivitätstypen*“. Um die Vorgangshistorie-Daten nach Aktivitätstyp zu erhalten, klicken Sie auf den entsprechenden x-Achse-Label-Link.
- Ein Diagramm der Aktivität auf *\_Entity Types\_*. Um Vorgangsdaten nach Entitätstyp zu erhalten, klicken Sie auf den entsprechenden Link für die X-Achse-Bezeichnung.
- Eine Liste der Daten „*Alle Aktivitäten*“

Die Tabelle *\*Alle Aktivitäten\** enthält die folgenden Informationen. Beachten Sie, dass standardmäßig nicht alle dieser Spalten angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das

Zahnrad-Symbol klicken [Zahnrad-Symbol].

- Die **Zeit**, auf die ein Unternehmen zugegriffen wurde, einschließlich Jahr, Monat, Tag und Uhrzeit des letzten Zugriffs.
- Der \* Benutzer\*, der mit einem Link auf das Entity zugegriffen hat "[Benutzerinformationen](#)".
- Die **Aktivität**, die der Benutzer durchgeführt hat. Folgende Typen werden unterstützt:
  - **Gruppeneigentum ändern** - Gruppeneigentum ist von Datei oder Ordner geändert. Weitere Informationen zu Gruppeneigentum finden Sie unter "[Dieser Link](#)."
  - **Eigentümer ändern** - das Eigentum an Datei oder Ordner wird zu einem anderen Benutzer geändert.
  - **Berechtigung ändern** - Datei- oder Ordnerrechte wurde geändert.
  - **Erstellen** - Erstellen Sie Datei oder Ordner.
  - **Löschen** - Datei oder Ordner löschen. Wenn ein Ordner gelöscht wird, werden *delete* Ereignisse für alle Dateien in diesem Ordner und Unterordnern abgerufen.
  - **Lesen** - Datei wird gelesen.
  - **Metadaten lesen** - nur bei Option zur Ordnerüberwachung. Wird beim Öffnen eines Ordners unter Windows erzeugt oder „ls“ innerhalb eines Ordners unter Linux ausgeführt.
  - **Umbenennen** - Umbenennen Sie die Datei oder den Ordner.
  - **Schreiben** - Daten werden in eine Datei geschrieben.
  - **Metadaten schreiben** - Dateimetadaten werden geschrieben, zum Beispiel, Berechtigung geändert.
  - **Andere Änderung** - jedes andere Ereignis, das oben nicht beschrieben wird. Alle nicht zugeordneten Ereignisse werden dem Aktivitätstyp „andere Änderung“ zugeordnet. Gilt für Dateien und Ordner.
- Der **Pfad** zur Entität mit einem Link zum "[Entity Detail-Daten](#)"
- **Entity Type**, einschließlich der Endung Entity (d. h. Datei) (.doc, .docx, .tmp usw.)
- Das **Gerät**, in dem sich die Entitäten befinden
- Das **Protokoll** zum Abrufen von Ereignissen.
- Der **Original-Pfad**, der bei der Umbenennung der Originaldatei verwendet wird. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie die Spaltenauswahl, um diese Spalte zur Tabelle hinzuzufügen.
- Das **Volumen**, in dem sich die Entitäten befinden. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie die Spaltenauswahl, um diese Spalte zur Tabelle hinzuzufügen.

## Filtern Forensischer Vorgangshistorie-Daten

Es gibt zwei Methoden, mit denen Sie Daten filtern können.

1. Bewegen Sie den Mauszeiger über das Feld in der Tabelle, und klicken Sie auf das angezeigte Filtersymbol. Der Wert wird den entsprechenden Filtern in der oberen Liste *Filter by* hinzugefügt.
2. Filtern Sie die Daten, indem Sie das Feld *Filter by* eingeben:

Wählen Sie den entsprechenden Filter aus dem oberen Widget 'Filtern nach' aus, indem Sie auf die Schaltfläche **[+]** klicken:

[Entity Filer, width=500]

Geben Sie den Suchtext ein

Drücken Sie die Eingabetaste, oder klicken Sie außerhalb des Filterfelds, um den Filter anzuwenden.

Sie können forensische Aktivitätsdaten nach folgenden Feldern filtern:

- Der Typ **Aktivität**.
- **Quell-IP**, auf die das Element zugegriffen wurde. Sie müssen eine gültige Quell-IP-Adresse in doppelten Anführungszeichen angeben, z. B. „10.1.1.1.“. Unvollständige IPs wie „10.1.1.“, „**10.1.**“ usw. funktionieren nicht.
- **Protokoll** zum Abrufen protokollspezifischer Aktivitäten.
- **Benutzername** des Benutzers, der die Aktivität ausführt. Sie müssen den genauen Benutzernamen angeben, um sie zu filtern. Die Suche mit teilweisen Nutzernamen oder teilweisen Nutzernamen, vorfixiert oder mit '\*' abgestickt, funktioniert nicht.
- **Rauschunterdrückung** zum Filtern von Dateien, die in den letzten 2 Stunden vom Benutzer erstellt werden. Sie wird auch zum Filtern temporärer Dateien (z. B. .tmp-Dateien) verwendet, auf die der Benutzer Zugriff hat.

Die folgenden Felder unterliegen speziellen Filterregeln:

- **Entity Type**, mit Entity (file) Extension
- **Pfad** der Entität
- **Benutzer** die Aktivität durchführen
- **Gerät** (SVM), in dem sich Entitäten befinden
- **Volumen**, in dem sich Entitäten befinden
- Der **Original-Pfad**, der bei der Umbenennung der Originaldatei verwendet wird.

Die vorhergehenden Felder unterliegen beim Filtern folgenden Kriterien:

- Der genaue Wert sollte in Anführungszeichen liegen: Beispiel: "suchtext"
- Platzhalter-Strings dürfen keine Anführungszeichen enthalten: Beispiel: suchtext, \*suchtext\*, filtert nach Zeichenfolgen, die 'seartext' enthalten.
- String mit einem Präfix, Beispiel: suchtext\* , sucht alle Strings, die mit 'seartext' beginnen.

## Forensische Vorgangshistorie-Daten Sortieren

Sie können Vorgangshistorie-Daten nach `_Time`, `User`, `Source IP`, `Activity`, `Path_` und `_Entity Type_` sortieren. Standardmäßig wird die Tabelle nach absteigender `_Time_`-Reihenfolge sortiert, was bedeutet, dass die neuesten Daten zuerst angezeigt werden. Die Sortierung ist für die Felder *Device* und *Protocol* deaktiviert.

## Alle Aktivitäten Werden Exportiert

Sie können den Vorgangsverlauf in eine CSV-Datei exportieren, indem Sie über der Tabelle „Vorgangsverlauf“ auf die Schaltfläche „Export“ klicken. Beachten Sie, dass nur die 100,000 wichtigsten Datensätze exportiert werden. Je nach Datenmenge kann es einige Sekunden bis zu mehreren Minuten dauern, bis der Export abgeschlossen ist.

## Spaltenauswahl für Alle Aktivitäten

In der Tabelle *Alle Aktivitäten* werden standardmäßig ausgewählte Spalten angezeigt. Um die Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle und

wählen Sie aus der Liste der verfügbaren Spalten aus.

[Aktivitätsauswahl, width=30%]

### Aufbewahrung Des Aktivitätsverlaufs

Der Aktivitätsverlauf wird 13 Monate lang in aktiven Workload-Sicherheitsumgebungen aufbewahrt.

### Anwendbarkeit von Filtern in Forensics Seite

Filtern	Das macht es	Beispiel	In welchen Filtern anwendbar?	Gilt nicht für welche Filter	Ergebnis
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	Auto*03172022	Benutzer, PFAD, Einheitstyp, Gerätetyp, Volume, Ursprünglicher Pfad		Gibt alle Ressourcen zurück, die mit „Auto“ beginnen und mit „03172022“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	AutoSabotageUser1_03172022?	Benutzer, Einheitstyp, Gerät, Volume		Gibt AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225 usw. zurück
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022	Benutzer, Domäne, Benutzername, PFAD, Einheitstyp, Gerät, Originalpfad		Gibt eine beliebige von AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022 zurück
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen	NICHT automatisch BefreiUser4_03162022	Benutzer, Domäne, Benutzername, PFAD, Einheitstyp, Ursprünglicher PFAD, Volume	Gerät	Gibt alles zurück, was nicht mit "AutoBefreiUser4_03162022" beginnt
Keine	Sucht in allen Feldern nach Null-Werten	Keine	Domäne		Gibt Ergebnisse an, bei denen das Zielfeld leer ist

## Pfadsuche/Original-Pfadsuche

Suchergebnisse mit und ohne / werden unterschiedlich sein

/AutoDir1/AutoFile	Funktioniert
AutoDir1/AutoFile	Funktioniert nicht
/AutoDir1/AutoFile (Dir1)	Dir1 partielle Substring funktioniert nicht
„/AutoDir1/AutoFile03242022“	Genaue Suche funktioniert
Auto*03242022	Funktioniert nicht
AutoSabotageUser1_03172022?	Funktioniert nicht
/AutoDir1/AutoFile03242022 ODER /AutoDir1/AutoFile03242022	Funktioniert
NICHT /AutoDir1/AutoFile03242022	Funktioniert
NICHT /AutoDir1	Funktioniert
NICHT /AutoFile03242022	Funktioniert nicht
*	Zeigt alle Einträge an

## Fehlerbehebung

Problem	Versuchen Sie Dies
In der Tabelle „Alle Aktivitäten“ in der Spalte ‘Benutzer‘ wird der Benutzername wie folgt angezeigt: „ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817“ oder LDAP:default:80038003“	Mögliche Gründe sind: 1. Es wurden noch keine User Directory Collectors konfiguriert. Um einen hinzuzufügen, gehen Sie zu <b>Admin &gt; Data Collectors &gt; User Directory Collectors</b> und klicken Sie auf <b>+User Directory Collector</b> . Wählen Sie <i>Active Directory</i> oder <i>LDAP Directory Server</i> . 2. Ein Benutzerverzeichnissammler wurde konfiguriert, ist jedoch angehalten oder befindet sich im Fehlerzustand. Gehen Sie zu <b>Admin &gt; Data Collectors &gt; User Directory Collectors</b> und überprüfen Sie den Status. Siehe " <a href="#">Fehlerbehebung für Benutzerverzeichnissammler</a> " Der Dokumentation für Tipps zur Fehlerbehebung. Nach der ordnungsgemäßen Konfiguration wird der Name innerhalb von 24 Stunden automatisch behoben. Wenn die Lösung immer noch nicht behoben wird, überprüfen Sie, ob Sie den korrekten Benutzer-Data Collector hinzugefügt haben. Stellen Sie sicher, dass der Benutzer tatsächlich Teil des hinzugefügten Active Directory/LDAP Directory Servers ist.



Einige NFS-Ereignisse werden in der UI nicht angezeigt.

Überprüfen Sie Folgendes: 1. Ein Benutzer-Verzeichnis-Collector für AD-Server mit POSIX-Attributen sollte mit dem unixid-Attribut ausgeführt werden, das über UI aktiviert ist. 2. Jeder Benutzer, der NFS-Zugang macht, sollte angezeigt werden, wenn er in der Benutzerseite von UI 3 durchsucht wird. RAW-Ereignisse (Ereignisse, für die der Benutzer noch nicht erkannt wurde) werden für NFS 4 nicht unterstützt. Anonymer Zugriff auf den NFS-Export wird nicht überwacht. 5. Stellen Sie sicher, dass die NFS-Version in weniger als NFS4.1 verwendet wird.

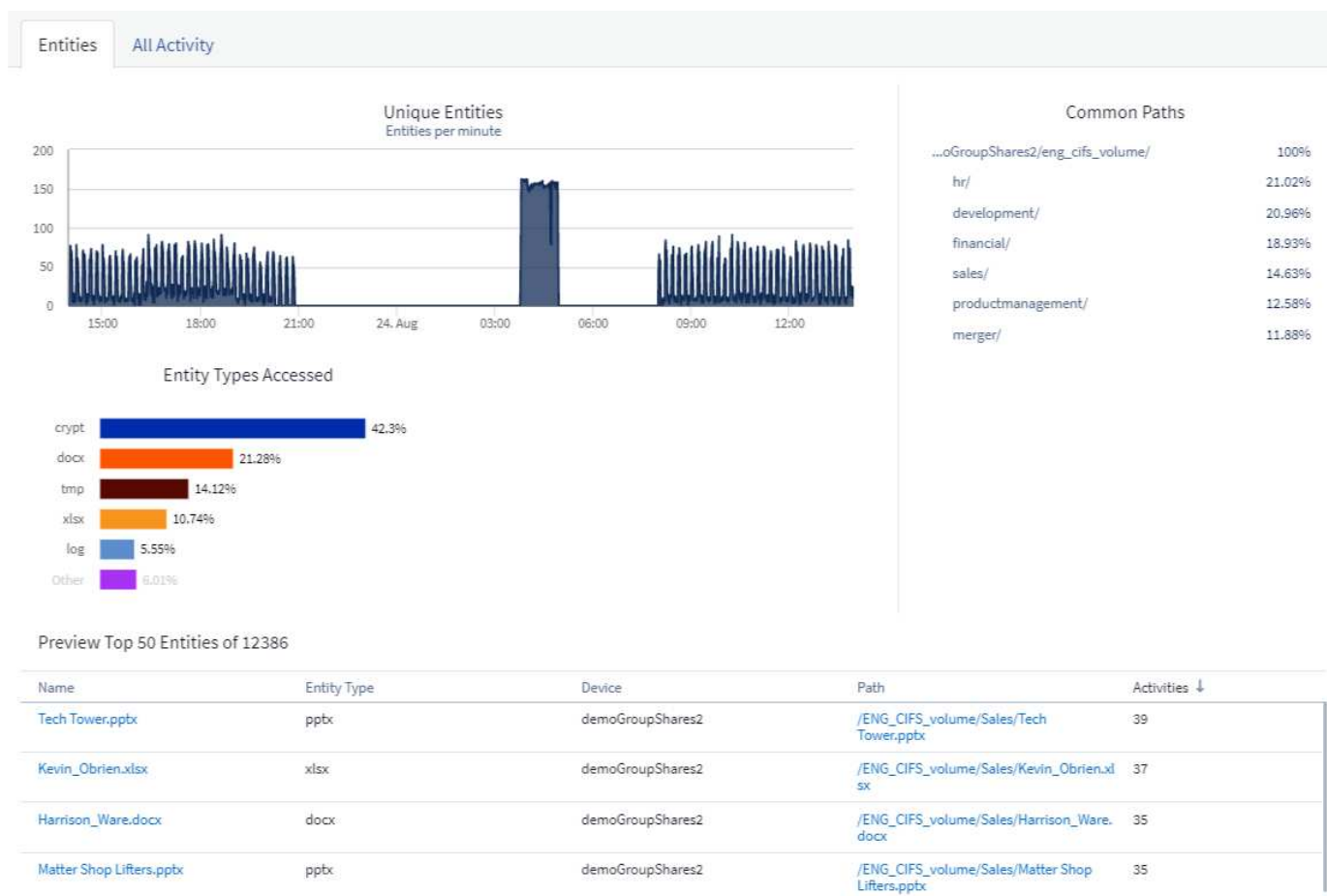
## Seite Mit Forensischen Einheiten

Die Seite Forensics Entities enthält detaillierte Informationen über die Aktivität der Entität in Ihrer Umgebung.

### Untersuchung Von Informationen Zur Einheit

Klicken Sie auf **Forensics > Vorgangsforensics**, und klicken Sie auf die Registerkarte *Entities*, um die Seite Entities aufzurufen.

Auf dieser Seite erhalten Sie einen Überblick über die Aktivitäten der Einheit in Ihrer Umgebung, und Sie können die folgenden Informationen hervorheben: \* Ein Diagramm mit eindeutigen Entitäten Zugriffsberechtigung pro Minute \* Ein Diagramm mit Entity-Typen, auf die zugegriffen wurde \* Eine Aufschlüsselung der Common Paths \* Eine Liste der Top 50 Entities von der Gesamtanzahl der Entitäten



Durch Klicken auf eine Entität in der Liste wird eine Übersichtsseite für die Entität geöffnet, auf der ein Profil der Entität mit Details wie Name, Typ, Geräte-Name, IP-Adresse und Pfad sowie das Entity-Verhalten wie Benutzer, IP, Und die Zeit, zu der das Unternehmen zuletzt aufgerufen wurde.



Entity Overview

Entity Profile

Name Kevin_Obrien.xlsx	Most Accessed Location 10.197.144.115	Size 91 KB
Type xlsx	Device Name demoGroupShares2	Path /ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx

Entity Behaviour

Recent Activity	Operations (last 7 days)
Last accessed : 12 minutes ago Aug 24, 2020 2:02 PM	Read :89
Last accessed by: Tyrique Ray	Read Metadata :22
Last accessed from : 10.197.144.115	Other Activities :43

## Übersicht Über Forensische Benutzer

Informationen zu jedem Benutzer finden Sie in der Benutzerübersicht. Verwenden Sie diese Ansichten, um Benutzereigenschaften, zugehörige Einheiten und aktuelle Aktivitäten zu verstehen.

### Benutzerprofil

Zu den Benutzerprofilinformationen gehören die Kontaktinformationen und der Standort des Benutzers. Das Profil enthält folgende Informationen:

- Name des Benutzers
- E-Mail-Adresse des Benutzers
- Benutzermanager
- Telefonkontakt für den Benutzer
- Standort des Benutzers

### Benutzerverhalten

Die Informationen zum Benutzerverhalten identifizieren aktuelle Aktivitäten und Vorgänge, die vom Benutzer durchgeführt werden. Zu diesen Informationen gehören:

- Aktuelle Aktivität
  - Letzter Zugriffsort
  - Aktivitätsdiagramm
  - Meldungen
- Betrieb der letzten sieben Tage

- Anzahl an Operationen

### **Intervall Aktualisieren**

Die Benutzerliste wird alle 12 Stunden aktualisiert.

### **Aufbewahrungsrichtlinie**

Wenn die Benutzerliste nicht erneut aktualisiert wird, wird sie 13 Monate lang aufbewahrt. Nach 13 Monaten werden die Daten gelöscht. Wenn die Workload-Sicherheitsumgebung gelöscht wird, werden alle der Umgebung zugeordneten Daten gelöscht.

## **Automatisierte Antwortrichtlinien**

Antwortrichtlinien lösen Aktionen aus, wie z. B. das Erstellen eines Snapshots oder das Einschränken des Benutzerzugriffs bei einem Angriff oder einem anormalen Benutzerverhalten.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

Sie können Richtlinien für bestimmte Geräte oder alle Geräte festlegen. Um eine Antwortrichtlinie festzulegen, wählen Sie **Admin > Automated Response Policies** und klicken Sie auf die entsprechende \*Policy Schaltfläche. Sie können Richtlinien für Angriffe oder Warnungen erstellen.

## Add Attack Policy ✕

Policy Name\*

---

**For Ransomware Attacks**  
Currently Cloud Secure discovers and tracks possible Ransomware attacks.  
*Coming Soon:* Tracking for additional attack types, including Identity Theft, Sabotage, and Snooping.

On Device

[+ Another Device](#)

---

Actions

Take Snapshot i

Sie müssen die Richtlinie mit einem eindeutigen Namen speichern.

Um eine automatische Antwortzeit zu deaktivieren (z. B. Snapshot erstellen), überprüfen Sie einfach die Aktion und speichern Sie die Richtlinie.

Wenn eine Warnung für die angegebenen Geräte (oder alle Geräte, falls ausgewählt) ausgelöst wird, erstellt die Richtlinie zur automatischen Reaktion einen Snapshot Ihrer Daten. Sie können den Snapshot-Status auf der sehen "[Details zu Warnmeldungen](#)".

Siehe "[Einschränken Des Benutzerzugriffs](#)" Seite für weitere Details zur Einschränkung des Benutzerzugriffs durch IP.

Sie können eine Richtlinie für automatische Reaktionen ändern oder anhalten, indem Sie die Option im Dropdown-Menü der Richtlinie auswählen.

Workload Security löscht automatisch Snapshots einmal pro Tag auf Basis der Snapshot-Einstellungen.

## Snapshot Purge Settings



Define purge periods to automatically delete snapshots taken by Cloud Secure.

### Attack Automated Response

Delete Snapshot after

### Warning Automated Response

Delete Snapshot after

### User Created

Delete Snapshot after

Cancel

Save

## Integration in ONTAP Autonomous Ransomware Protection

Die Funktion ONTAP Autonomous Ransomware Protection (ARP) verwendet Workload-Analysen in NAS-Umgebungen (NFS und SMB), um ungewöhnliche Dateiaktivitäten proaktiv zu erkennen und zu warnen, die auf einen Ransomware-Angriff hinweisen könnten.

Weitere Details und Lizenzanforderungen zu ARP finden Sie ["Hier"](#).

Workload Security ist in ONTAP integriert, um ARP-Ereignisse zu empfangen, und bietet zusätzliche Analysen und automatische Antwortebenen.

Workload Security erhält die ARP-Ereignisse vom ONTAP und ergreift die folgenden Maßnahmen:

1. Korreliert Ereignisse der Volume-Verschlüsselung mit den Benutzeraktivitäten, um zu ermitteln, wer den Schaden verursacht.
2. Implementierung von Richtlinien zur automatischen Reaktion (falls definiert)
3. Bietet forensische Funktionen:
  - Ermöglichen Sie Kunden die Durchführung von Untersuchungen zu Datensicherheitsverletzungen.
  - Erkennen Sie, welche Dateien betroffen waren, sodass das Recovery schneller erfolgt und Untersuchungen zu Datensicherheitsverletzungen durchgeführt werden können.

### Voraussetzungen

1. Minimale ONTAP-Version: 9.11.1

2. ARP-aktivierte Volumes. Einzelheiten zur Aktivierung von ARP finden Sie ["Hier"](#). ARP muss über den OnCommand System Manager aktiviert sein. Workload Security kann ARP nicht aktivieren.
3. Workload Security Collector sollte über Cluster-IP hinzugefügt werden.
4. Für diese Funktion sind Anmeldedaten auf Cluster-Ebene erforderlich. Das bedeutet, dass beim Hinzufügen der SVM Anmeldedaten für die Cluster-Ebene verwendet werden müssen.

## Benutzerberechtigungen erforderlich

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

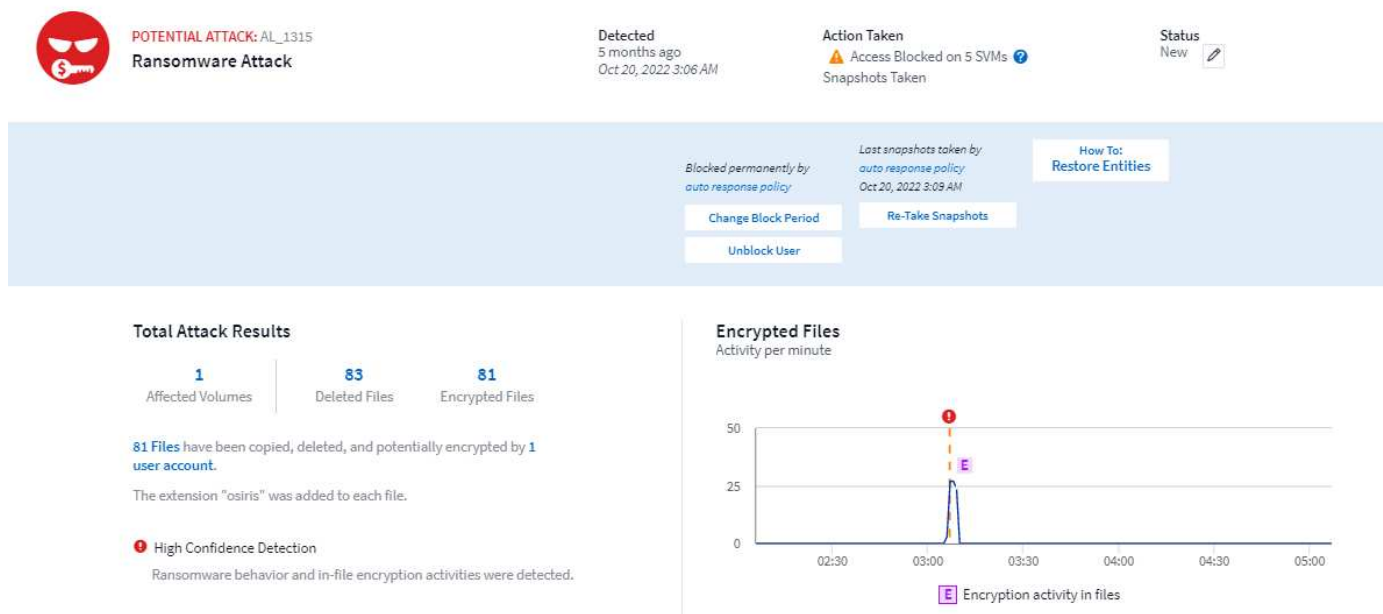
Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit den dem Benutzer angegebenen Berechtigungen verwenden, befolgen Sie die folgenden Schritte, um Workload Security-Berechtigungen zum Sammeln von ARP-bezogenen Informationen aus ONTAP zu erteilen.

Führen Sie für *csuser* mit Cluster-Anmeldedaten folgende Schritte in der ONTAP-Befehlszeile aus:

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

## Beispielalarm

Im Folgenden wird eine Beispielwarnung angezeigt, die aufgrund eines ARP-Ereignisses generiert wurde:



## Related Users



**Jamelia Graham**  
Business Partner  
HR

User/IP Access ?

**Blocked**

**81**  
Encrypted Files

Detected  
5 months ago  
Oct 20, 2022 3:06 AM



**Username**  
us024

**Domain**  
cslab.netapp.com

**Email**  
Graham@netapp.com

**Phone**  
9251140014

**Department**  
HR

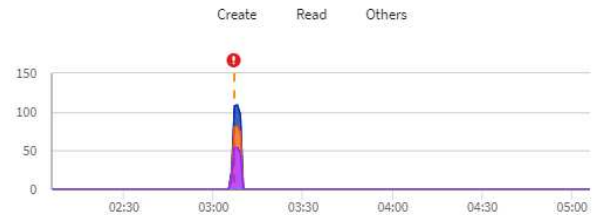
**Manager**  
Iwan Holt

**Location**  
WA

### Top Activity Types

Activity per minute  
Last accessed from: 10.193.113.247

[View Activity Detail](#)



### Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	Block <a href="#">more detail</a>	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	Block <a href="#">more detail</a>	1h		Automatic	10.197.144.115

### Affected Devices/Volumes

Device ↑	Volume	Encrypted Files	Associated Snapshot Taken
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM cloudsecure_attack_auto Automatic _1666249787062 <a href="#">Take Snapshot</a>

Ein hochvertrauliches Banner zeigt auf, dass der Angriff das Verhalten von Ransomware zusammen mit Dateiverschlüsselungsaktivitäten gezeigt hat. Das Diagramm der verschlüsselten Dateien gibt den Zeitstempel an, mit dem die Volume-Verschlüsselungsaktivität von der ARP-Lösung erkannt wurde.

## Einschränkungen

Wenn eine SVM nicht durch Workload-Sicherheit überwacht wird, aber durch ONTAP ARP-Ereignisse generiert werden, dann werden die Ereignisse weiterhin durch die Workload-Sicherheit empfangen und angezeigt. Es werden jedoch keine forensischen Informationen bezüglich der Warnmeldung und auch keine Benutzerzuordnung erfasst oder angezeigt.

## Fehlerbehebung

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

Problem:	Auflösung:
<p>E-Mail-Alarme werden 24 Stunden nach einem Angriff empfangen. In der UI werden die Alarme 24 Stunden vorher angezeigt, wenn die E-Mails von der Cloud Insights-Workload-Sicherheit empfangen werden.</p>	<p>Wenn ONTAP das Ereignis <i>Ransomware Detected</i> an die Sicherheit des Cloud Insights Workloads (d. h. Workload-Sicherheit) sendet, wird die E-Mail gesendet. Das Ereignis enthält eine Liste von Angriffen und Zeitstempel. Die Workload Security UI zeigt den Warnungszeitstempel der ersten angegriffenen Datei an. ONTAP sendet das <i>Ransomware Detected</i> -Ereignis an Cloud Insights, wenn eine bestimmte Anzahl von Dateien codiert ist. Daher kann es einen Unterschied geben zwischen dem Zeitpunkt, zu dem die Warnung in der UI angezeigt wird, und dem Zeitpunkt, zu dem die E-Mail gesendet wird.</p>

## Blockieren Des Benutzerzugriffs

Sobald ein Angriff erkannt wurde, kann Workload Security den Angriff beenden, indem der Benutzerzugriff auf das Dateisystem blockiert wird. Der Zugriff kann automatisch mithilfe von Automated Response Policies oder manuell über die Alarm- oder Benutzerdetails-Seiten gesperrt werden.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

Beim Blockieren des Benutzerzugriffs sollten Sie einen Sperrzeitraum festlegen. Nach Ende des ausgewählten Zeitraums wird der Benutzerzugriff automatisch wiederhergestellt. Das Zugriffssperre wird sowohl für SMB- als auch für NFS-Protokolle unterstützt.

Benutzer ist direkt für SMB gesperrt und die IP-Adresse der Host Machines, die den Angriff verursachen, wird für NFS blockiert. Diese Computer-IP-Adressen dürfen nicht auf alle Storage Virtual Machines (SVMs) zugreifen, die durch Workload Security überwacht werden.

Zum Beispiel, sagen wir, Workload Security verwaltet 10 SVMs und die automatische Antwortrichtlinie ist für vier dieser SVMs konfiguriert. Wenn der Angriff in einer der vier SVMs stammt, wird der Zugriff des Benutzers in allen 10 SVMs blockiert. Auf der ursprünglichen SVM wird noch ein Snapshot erstellt.

Falls vier SVMs mit einer für SMB konfigurierten SVM und eine für NFS konfigurierte SVM und die übrigen beiden für NFS und SMB konfiguriert sind, werden alle SVMs blockiert, wenn der Angriff aus einer der vier SVMs stammt.

### Voraussetzungen für die 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
```

## Wie wird die Funktion aktiviert?

- Navigieren Sie unter Workload Security zu **Admin > Automated Response Policies > Response Policy Settings > Block User Access**.
- Legen Sie „Benutzerzugriff sperren aktivieren“ auf „*Enabled*“ fest.

## Wie richten Sie die automatische Sperrung des Benutzerzugriffs ein?

- Erstellen Sie eine neue Angriffsrichtlinie oder bearbeiten Sie eine vorhandene Angriffsrichtlinie.
- Wählen Sie die SVMs aus, auf denen die Angriffsrichtlinie überwacht werden soll.
- Klicken Sie auf das Kontrollkästchen „Benutzerdateizugriff blockieren“. Die Funktion wird aktiviert, wenn diese Option ausgewählt ist.
- Wählen Sie unter „Zeitraum“ die Zeit aus, bis die Blockierung angewendet werden soll.
- Um die automatische Blockierung von Benutzern zu testen, können Sie einen Angriff über ein simulieren ["Simuliertes Skript"](#).

## Wie kann man wissen, ob es blockierte Benutzer im System gibt?

- Auf der Seite Alarmlisten wird ein Banner oben auf dem Bildschirm angezeigt, falls ein Benutzer blockiert ist.
- Durch Klicken auf das Banner gelangen Sie zur Seite „Benutzer“, wo die Liste der blockierten Benutzer angezeigt wird.
- Auf der Seite „Benutzer“ befindet sich eine Spalte mit dem Namen „Benutzer/IP-Zugriff“. In dieser Spalte wird der aktuelle Status der Benutzerblockierung angezeigt.

## Benutzerzugriff manuell einschränken und verwalten

- Sie können zu den Warnungsdetails oder Benutzerdetails gehen und einen Benutzer dann manuell von diesen Bildschirmen blockieren oder wiederherstellen.

## Verlauf Der Benutzerzugriffsbeschränkung

Auf der Seite Warnungsdetails und Benutzerdetails im Bedienfeld können Sie eine Prüfung des Zugriffsbegrenzungsverlaufs des Benutzers anzeigen: Zeit, Aktion (Blockieren, Entsperren), Dauer, Aktion ausgeführt von, Manuelle/automatische und betroffene IPs für NFS.

## Wie wird die Funktion deaktiviert?

Sie können die Funktion jederzeit deaktivieren. Wenn es eingeschränkte Benutzer im System gibt, müssen Sie zuerst den Zugriff wiederherstellen.

- Navigieren Sie unter Workload Security zu **Admin > Automated Response Policies > Response Policy Settings > Block User Access**
- Deaktivieren Sie die Option „Benutzerzugriff blockieren aktivieren“.

Die Funktion wird von allen Seiten ausgeblendet.

## Manuelle Wiederherstellung der IPs für NFS

Führen Sie die folgenden Schritte aus, um IP-Adressen von ONTAP manuell wiederherzustellen, wenn Ihre Workload-Sicherheitsstudie abläuft oder wenn der Agent/Collector nicht verfügbar ist.

1. Listen Sie alle Exportrichtlinien auf einer SVM auf.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
      Policy          Rule    Access   Client      RO
Vserver  Name              Index  Protocol Match      Rule
-----  -
-----
svm0     default           1      nfs3,      cloudsecure_rule,  never
                           1      nfs4,      10.11.12.13
                           2      cifs
svm1     default           4      cifs,      0.0.0.0/0          any
                           3      nfs
svm2     test              1      nfs3,      cloudsecure_rule,  never
                           1      nfs4,      10.11.12.13
                           2      cifs
svm3     test              3      cifs,      0.0.0.0/0          any
                           1      nfs,
                           2      flexcache
4 entries were displayed.
```

2. Löschen Sie die Regeln über alle Richtlinien auf der SVM, die als Client Match „cloudSecure\_rule“ haben, indem Sie den entsprechenden RegellIndex angeben. Workload-Sicherheitsregel liegt in der Regel bei 1.

```
contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Stellen Sie sicher, dass die Sicherheitsregel für Workloads gelöscht
wird (optionaler Schritt zur Bestätigung).
```

```

contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
      Policy          Rule   Access  Client      RO
Vserver  Name             Index  Protocol Match      Rule
-----  -
-----
svm0     default          4      cifs,      0.0.0.0/0      any
          nfs
svm2     test             3      cifs,      0.0.0.0/0      any
          nfs,
          flexcache
2 entries were displayed.

```

## Benutzer für SMB manuell wiederherstellen

Führen Sie die folgenden Schritte aus, um alle Benutzer von ONTAP manuell wiederherzustellen, wenn Ihre Testversion für die Workload-Sicherheit abläuft oder wenn der Agent/Collector nicht verfügbar ist.

Sie können die Liste der in Workload Security blockierten Benutzer auf der Benutzer-Listenseite abrufen.

1. Melden Sie sich mit Cluster\_admin\_-Anmeldedaten beim ONTAP Cluster an (wo Sie die Blockierung von Benutzern aufheben möchten). (Bei Amazon FSX melden Sie sich mit FSX-Anmeldeinformationen an).
2. Führen Sie den folgenden Befehl aus, um alle durch Workload Security für SMB blockierten Benutzer in allen SVMs aufzulisten:

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

```

Vserver:  <vservename>
Direction: win-unix
Position Hostname          IP Address/Mask
-----  -
1         -                    -                Pattern: CSLAB\\US040
          Replacement:
2         -                    -                Pattern: CSLAB\\US030
          Replacement:
2 entries were displayed.

```

In der obigen Ausgabe wurden 2 Benutzer (US030, US040) mit Domain CSLAB blockiert.

1. Führen Sie den folgenden Befehl aus, um den Benutzer zu entsperren, wenn Sie die Position aus der obigen Ausgabe identifiziert haben:

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

. Bestätigen Sie, dass die Sperrung der Benutzer aufgehoben wird, indem Sie den folgenden Befehl ausführen:

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

Für die zuvor blockierten Benutzer sollten keine Einträge angezeigt werden.

## Fehlerbehebung

Problem	Versuchen Sie Dies
Einige der Benutzer werden nicht eingeschränkt, obwohl es einen Angriff gibt.	1. Stellen Sie sicher, dass sich der Data Collector und der Agent für die SVMs im Status <i>running</i> befinden. Workload Security kann keine Befehle senden, wenn der Data Collector und der Agent angehalten sind. 2. Dies liegt daran, dass der Benutzer möglicherweise von einem Computer mit einer neuen IP-Adresse auf den Speicher zugegriffen hat, die zuvor nicht verwendet wurde. Die Einschränkung erfolgt über die IP-Adresse des Hosts, über den der Benutzer auf den Speicher zugreift. Überprüfen Sie in der UI (Warndetails > Zugriffsbegrenzungsverlauf für diesen Benutzer > betroffene IP-Adressen) die Liste der eingeschränkten IP-Adressen. Wenn der Benutzer von einem Host aus auf Speicher zugreift, der eine andere IP als die eingeschränkten IP hat, kann der Benutzer weiterhin über die nicht eingeschränkte IP auf den Speicher zugreifen. Wenn der Benutzer versucht, von den Hosts, deren IP-Adressen eingeschränkt sind, auf den Speicher zuzugreifen, wird nicht zugegriffen werden können.
Manuelles Klicken auf Zugriff beschränken gibt „IP-Adressen dieses Benutzers wurden bereits eingeschränkt“.	Die zu beschränkte IP wird bereits von einem anderen Benutzer eingeschränkt.
Richtlinie konnte nicht geändert werden. Grund: Nicht autorisiert für diesen Befehl.	Überprüfen Sie, ob Sie cscuser verwenden, dass dem Benutzer Berechtigungen wie oben beschrieben erteilt werden.

Problem	Versuchen Sie Dies
<p>Benutzer (IP-Adresse) Blockieren für NFS funktioniert, aber für SMB / CIFS, sehe ich eine Fehlermeldung: "SID to DomainName Transformation fehlgeschlagen. Grund-Timeout: Socket wurde nicht hergestellt"</p>	<p>Dies kann vorkommen, dass <i>csuser</i> nicht über die Berechtigung verfügt, ssh auszuführen. (Stellen Sie die Verbindung auf Cluster-Ebene sicher, und stellen Sie dann sicher, dass der Benutzer ssh ausführen kann.) <i>Csuser</i> Rolle erfordert diese Berechtigungen. <a href="https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking">https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking</a>Führen Sie für <i>csuser</i> mit Cluster-Anmeldeinformationen über die ONTAP-Befehlszeile Folgendes aus: Sicherheits-Login Rolle create -role csrole -cmddirname "vserver Export-Policy rule" -Access all Security Login role create -role csrdname 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 Rolle create -role csrole -cmddirname "vserver Name-Mapping" -Access all Wenn <i>csuser</i> nicht verwendet wird und wenn Admin-Benutzer auf Cluster-Ebene verwendet wird, stellen Sie sicher, dass der Admin-Benutzer SSH-Berechtigung für ONTAP hat.</p>

## Workload Security: Simulation eines Angriffs

Mithilfe der Anweisungen auf dieser Seite können Sie einen Angriff für das Testen oder Demonieren der Workload-Sicherheit mithilfe des im Lieferumfang enthaltenen Skripts Ransomware Simulation simulieren.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

### Dinge zu beachten, bevor Sie beginnen

- Das Ransomware-Simulationsskript funktioniert nur auf Linux.
- Das Skript wird mit den Installationsdateien des Workload Security Agent bereitgestellt. Sie ist auf jedem Computer verfügbar, auf dem ein Workload Security Agent installiert ist.
- Sie können das Skript auf dem Workload Security Agent-Rechner selbst ausführen; es ist nicht erforderlich, einen anderen Linux-Rechner vorzubereiten. Wenn Sie jedoch das Skript lieber auf einem anderen System ausführen möchten, kopieren Sie einfach das Skript und führen es dort aus.

### Mindestens 1,000 Beispieldateien haben

Dieses Skript sollte auf einer SVM mit einem Ordner ausgeführt werden, der Dateien verschlüsselt. Es wird empfohlen, mindestens 1,000 Dateien in diesem Ordner und allen Unterordnern zu haben. Die Dateien dürfen nicht leer sein. Erstellen Sie die Dateien nicht und verschlüsseln Sie sie mit demselben Benutzer. Workload Security berücksichtigt diese Aktivität mit niedrigem Risiko und erzeugt daher keine Warnmeldung (d. h. der gleiche Benutzer ändert die Dateien, die er gerade erstellt hat).

Siehe unten für Anweisungen zu ["Programmgesteuertes Erstellen nicht leerer Dateien"](#).

## Richtlinien vor dem Ausführen des Simulators:

1. Stellen Sie sicher, dass verschlüsselte Dateien nicht leer sind.
2. Vergewissern Sie sich, dass Sie > 50 Dateien verschlüsseln. Eine kleine Anzahl von Dateien wird ignoriert.
3. Führen Sie keinen Angriff mit demselben Benutzer mehrmals durch. Nach einigen Fällen wird CS das Benutzerverhalten kennen und davon ausgehen, dass es sich um das normale Verhalten des Benutzers handelt.
4. Verschlüsseln Sie keine Dateien, die gerade von demselben Benutzer erstellt wurden. Das Ändern einer Datei, die gerade von einem Benutzer erstellt wurde, wird nicht als riskante Aktivität betrachtet. Verwenden Sie stattdessen Dateien, die von einem anderen Benutzer erstellt wurden, ODER warten Sie ein paar Stunden zwischen Erstellung und Verschlüsselung der Dateien.

## Bereiten Sie das System vor

Zunächst das Zielvolumen auf die Maschine montieren. Sie können entweder ein NFS-Mount oder einen CIFS-Export mounten.

So mounten Sie den NFS-Export in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvoll /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Mounten Sie NFS Version 4.1 nicht; es wird von FPolicy nicht unterstützt.

So mounten Sie CIFS in Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
Richten Sie als Nächstes einen Data Collector ein:
```

1. Konfigurieren Sie den Workload Security Agent, falls er noch nicht ausgeführt wurde.
2. Konfigurieren Sie den SVM-Datensammler, falls noch nicht geschehen.

## Führen Sie das Skript Ransomware Simulator aus

1. Melden Sie sich (ssh) beim Workload Security Agent-Rechner an.
2. Navigieren Sie zu: `/opt/netapp/cloudSecure/Agent/install`
3. Rufen Sie das Simulator-Skript ohne Parameter auf, um die Verwendung zu sehen:

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

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

## Verschlüsseln Sie Ihre Testdateien

Um die Dateien zu verschlüsseln, führen Sie den folgenden Befehl aus:

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

## Stellen Sie Dateien wieder her

Führen Sie zum Entschlüsseln den folgenden Befehl aus:

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

## Führen Sie das Skript mehrmals aus

Nachdem ein Ransomware-Angriff für einen Benutzer generiert wurde, wechseln Sie zu einem anderen Benutzer, um einen zusätzlichen Angriff zu generieren. Workload Security erlernt das Benutzerverhalten und warnt bei wiederholten Ransomware-Angriffen innerhalb kurzer Zeit für denselben Benutzer nicht.

## Dateien programmatisch erstellen

Bevor Sie die Dateien erstellen, müssen Sie zunächst die Verarbeitung des Datensammlers beenden. Führen Sie die folgenden Schritte aus, bevor Sie den Datensammler zum Agenten hinzufügen. Wenn Sie den Datensammler bereits hinzugefügt haben, bearbeiten Sie einfach den Datensammler, geben Sie ein ungültiges Kennwort ein und speichern Sie es. Dadurch wird der Datensammler vorübergehend in einen Fehlerzustand versetzt. HINWEIS: Achten Sie darauf, dass Sie das ursprüngliche Passwort beachten!

Bevor Sie die Simulation ausführen, müssen Sie zuerst Dateien hinzufügen, die verschlüsselt werden sollen. Sie können die zu verschlüsselenden Dateien entweder manuell in den Zielordner kopieren oder die Dateien mithilfe eines Skripts (siehe Beispiel unten) programmatisch erstellen. Kopieren Sie mindestens 1,000 Dateien, unabhängig von der verwendeten Methode.

Wenn Sie die Dateien programmatisch erstellen möchten, gehen Sie wie folgt vor:

1. Melden Sie sich im Feld Agent an.
2. Mounten Sie einen NFS-Export aus der SVM des Filers auf die Agent Maschine. CD in diesen Ordner.
3. Erstellen Sie in diesem Ordner eine Datei mit dem Namen createfiles.sh
4. Kopieren Sie die folgenden Zeilen in diese Datei.

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

5. Speichern Sie die Datei.
6. Stellen Sie sicher, dass Sie die Berechtigung für die Ausführung der Datei ausführen:

```
chmod 777 ./createfiles.sh
. Ausführen des Skripts:
```

```
./createfiles.sh
```

Im aktuellen Ordner werden 1000 Dateien erstellt.

7. Aktivieren Sie den Datensammler erneut

Wenn Sie den Datensammler in Schritt 1 deaktiviert haben, bearbeiten Sie den Datensammler, geben Sie das richtige Passwort ein, und speichern Sie es. Stellen Sie sicher, dass der Datensammler wieder in Betrieb ist.



# Konfigurieren von E-Mail-Benachrichtigungen für Warnungen, Warnungen und den Zustand des Agent/Data Source Collectors

Um die Empfänger von Benachrichtigungen für die Workload-Sicherheit zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie für jeden Empfänger eine E-Mail-Adresse in die entsprechenden Abschnitte ein.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

## Potenzielle Angriffs- und Warnhinweise

Um Benachrichtigungen zu potenziellen Angriffen zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „potenzielle Angriffswarnungen senden“ ein. Für jede Aktion der Warnmeldung werden E-Mail-Benachrichtigungen an die Benachrichtigungsliste gesendet.

Um Warnhinweise zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „Warnhinweise senden“ ein.

## Statusüberwachung von Agent und Data Collector

Sie können den Zustand von Agenten und Datenquellen über Benachrichtigungen überwachen.

Um Benachrichtigungen zu erhalten, wenn ein Agent oder Datenquellensammler nicht funktioniert, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „*Data Collection Health Alerts*“ ein.

Beachten Sie Folgendes:

- Zustandswarnmeldungen werden erst gesendet, nachdem der Agent/Sammler mindestens eine Stunde lang die Meldung beendet hat.
- Es wird nur eine E-Mail-Benachrichtigung an die vorgesehenen Empfänger in einem bestimmten Zeitraum von 24 Stunden gesendet, auch wenn der Agent oder der Datensammler länger getrennt ist.
- Bei einem Agent-Fehler wird eine Warnung gesendet (nicht eine pro Collector). Die E-Mail enthält eine Liste aller betroffenen SVMs.
- Active Directory-Sammlung Fehler wird als Warnung gemeldet; es hat keine Auswirkungen auf Ransomware-Erkennung.
- Die Setup-Liste „erste Schritte“ enthält jetzt eine neue Phase „*E-Mail-Benachrichtigungen konfigurieren*“.

## Workload-Sicherheits-API

Die Workload-Sicherheits-API ermöglicht NetApp Kunden und unabhängigen Software-Anbietern (ISVs) die Integration der Workload-Sicherheit in andere Applikationen wie CMDB- oder andere Ticketsysteme.



Workload-Sicherheit ist in der Cloud Insights Bundesausgabe nicht verfügbar.

Anforderungen für API-Zugriff:

- Ein API-Zugriffstoken-Modell wird verwendet, um den Zugriff zu gewähren.
- Das Management von API-Token wird von Workload Security-Benutzern mit der Administratorrolle durchgeführt.

## API-Dokumentation (Swagger)

Die neuesten API-Informationen finden Sie, indem Sie sich bei Workload Security anmelden und zu **Admin > API Access** navigieren. Klicken Sie auf den Link **API Documentation**. Die API-Dokumentation ist Swagger-basiert, die eine kurze Beschreibung und Verwendungsinformationen für die API enthält und Sie können es in Ihrer Umgebung ausprobieren.

## API-Zugriffs-Tokens

Bevor Sie die Workload Security API verwenden, müssen Sie ein oder mehrere **API Access Token** erstellen. Access Tokens gewähren Leseberechtigungen. Sie können auch die Ablauffrist für jedes Access Token festlegen.

So erstellen Sie ein Access Token:

- Klicken Sie auf **Admin > API Access**
- Klicken Sie auf **+API Access Token**
- Geben Sie **Tokenname** Ein
- Geben Sie **Token Expiration** An



Ihr Token kann nur während des Erstellungsvorgangs in die Zwischenablage kopiert und gespeichert werden. Token können nicht abgerufen werden, nachdem sie erstellt wurden. Daher wird dringend empfohlen, das Token zu kopieren und an einem sicheren Ort zu speichern. Sie werden aufgefordert, auf die Schaltfläche API-Zugriffstoken kopieren zu klicken, bevor Sie den Bildschirm zur Token-Erstellung schließen können.

Sie können Token deaktivieren, aktivieren und widerrufen. Deaktivierte Token können aktiviert werden.

Tokens gewähren aus Kundensicht allgemeinen Zugang zu APIs und verwalten den Zugriff auf APIs im Umfang ihrer eigenen Umgebung.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Access Token dann als Berechtigung, wenn es die Ziel-API anruft. Das übergebene Token informiert die API, dass der Inhaber des Tokens berechtigt ist, auf die API zuzugreifen und bestimmte Aktionen basierend auf dem Umfang auszuführen, den während der Autorisierung gewährt wurde.

Der HTTP-Header, in dem das Access Token übergeben wird, ist **X-CloudInsights-ApiKey**:

Verwenden Sie zum Abrufen von Lagerbeständen beispielsweise Folgendes:

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

Wobei `<API_Access-Token>` das Token ist, das Sie bei der Erstellung des API-Zugriffsschlüssels gespeichert haben.

Detaillierte Informationen finden Sie im Link *API Documentation* unter **Admin > API Access**.

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.