Workload-Sicherheit

Data Infrastructure Insights

NetApp
February 03, 2026

Inhalt

Workload-Sicherheit

Informationen zur Speicher-Workload-Sicherheit

Data Infrastructure Insights Storage Workload Security (früher Cloud Secure) hilft Ihnen, Ihre Daten mit verwertbaren Informationen zu Insider-Bedrohungen zu schützen. Es bietet eine zentrale Sichtbarkeit und Kontrolle aller Unternehmensdatenzugriffe in Hybrid-Cloud-Umgebungen, um sicherzustellen, dass Sicherheits- und Compliance-Ziele erreicht werden.

Sichtweite

Erhalten Sie zentrale Transparenz und Kontrolle über den Benutzerzugriff auf Ihre kritischen Unternehmensdaten, die vor Ort oder in der Cloud gespeichert sind.

Ersetzen Sie Tools und manuelle Prozesse, die keinen zeitnahen und genauen Einblick in den Datenzugriff und die Datenkontrolle bieten. Workload Security funktioniert auf einzigartige Weise sowohl auf Cloud- als auch auf lokalen Speichersystemen und warnt Sie in Echtzeit vor böswilligem Benutzerverhalten.

Schutz

Schützen Sie Unternehmensdaten durch fortschrittliches maschinelles Lernen und Anomalieerkennung vor Missbrauch durch böswillige oder kompromittierte Benutzer.

Warnt Sie bei abnormalen Datenzugriffen durch fortschrittliches maschinelles Lernen und Anomalieerkennung des Benutzerverhaltens.

Einhaltung

Stellen Sie die Unternehmenskonformität sicher, indem Sie den Benutzerdatenzugriff auf Ihre kritischen Unternehmensdaten prüfen, die vor Ort oder in der Cloud gespeichert sind.

Erste Schritte

Erste Schritte mit Workload-Sicherheit

Workload Security hilft Ihnen, die Benutzeraktivität zu überwachen und potenzielle Sicherheitsbedrohungen in Ihrer Speicherumgebung zu erkennen. Bevor Sie mit der Überwachung beginnen können, müssen Sie Agenten, Datensammler und Verzeichnisdienste konfigurieren, um die Grundlage für eine umfassende Sicherheitsüberwachung zu schaffen.

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

Bevor Sie mit der Datenerfassung beginnen können, müssen Sie Folgendes konfigurieren:

Aufgabe	Ähnliche Informationen

Konfigurieren eines Agenten	"Agentenanforderungen" "Agent hinzufügen"
Konfigurieren eines Benutzerverzeichnis-Connectors	"Benutzerverzeichnis-Connector hinzufügen"
Konfigurieren von Datensammlern	Klicken Sie auf **Workload-Sicherheit > Collector**. Klicken Sie auf den Datensammler, den Sie konfigurieren möchten. Informationen zu den Datensammlern finden Sie im Abschnitt „Referenz der Datensammler-Anbieter“ der Dokumentation.
Benutzerkonten erstellen	"Benutzerkonten verwalten"

Workload Security kann auch in andere Tools integriert werden. Zum Beispiel,"siehe diese Anleitung" zur Integration mit Splunk.

Anforderungen für den Workload Security Agent

Setzen Sie Workload Security Agents auf dedizierten Servern ein, die die Mindestanforderungen an Betriebssystem, CPU, Arbeitsspeicher und Festplattenspeicher erfüllen, um eine optimale Überwachung und Bedrohungserkennung zu gewährleisten. Dieser Leitfaden beschreibt die Hardware- und Netzwerkvoraussetzungen, die vor "Installation Ihres Workload Security Agent" erforderlich sind, einschließlich unterstützter Linux-Distributionen, Netzwerkverbindungsregeln und Hinweise zur Systemdimensionierung.

Komponente	Linux-Anforderungen
Betriebssystem	Ein Computer, auf dem eine lizenzierte Version eines der folgenden Betriebssysteme ausgeführt wird: * AlmaLinux 9.4 (64 Bit) bis 9.5 (64 Bit), 10 (64 Bit), einschließlich SELinux * CentOS Stream 9 (64 Bit) * Debian 11 (64 Bit), 12 (64 Bit), einschließlich SELinux * OpenSUSE Leap 15.3 (64 Bit) bis 15.6 (64 Bit) * Oracle Linux 8.10 (64 Bit), 9.1 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux * Red Hat Enterprise Linux 8.10 (64 Bit), 9.1 (64 Bit) bis 9.6 (64 Bit), 10 (64 Bit), einschließlich SELinux * Rocky 9.4 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux * SUSE Linux Enterprise Server 15 SP4 (64-Bit) bis 15 SP6 (64-Bit), einschließlich SELinux * Ubuntu 20.04 LTS (64-Bit), 22.04 LTS (64-Bit), 24.04 LTS (64-Bit) Auf diesem Computer sollte keine andere Software auf Anwendungsebene ausgeführt werden. Ein dedizierter Server wird empfohlen.
Befehle	Für die Installation ist „Entpacken“ erforderlich. Darüber hinaus ist der Befehl „sudo su –“ für die Installation, das Ausführen von Skripts und die Deinstallation erforderlich.
CPU	4 CPU-Kerne
Erinnerung	16 GB RAM

Komponente	Linux-Anforderungen
Verfügbarer Speicherplatz	Der Speicherplatz sollte folgendermaßen zugewiesen werden: /opt/netapp 36 GB (mindestens 35 GB freier Speicherplatz nach der Erstellung des Dateisystems). Hinweis: Es wird empfohlen, etwas zusätzlichen Speicherplatz zuzuweisen, um die Erstellung des Dateisystems zu ermöglichen. Stellen Sie sicher, dass im Dateisystem mindestens 35 GB freier Speicherplatz vorhanden sind. Wenn es sich bei /opt um einen bereitgestellten Ordner aus einem NAS-Speicher handelt, stellen Sie sicher, dass lokale Benutzer Zugriff auf diesen Ordner haben. Die Installation des Agenten oder Datensammlers schlägt möglicherweise fehl, wenn lokale Benutzer keine Berechtigung für diesen Ordner haben. Weitere Informationen finden Sie im"Fehlerbehebung" Weitere Einzelheiten finden Sie im Abschnitt „Informationen zur Sicherheit“.
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).

Bitte beachten: Der Workload Security-Agent kann auf derselben Maschine wie eine Data Infrastructure Insights Erfassungseinheit und/oder ein Agent installiert werden. Es empfiehlt sich jedoch, diese auf separaten Maschinen zu installieren. Falls diese auf derselben Maschine installiert sind, weisen Sie den Speicherplatz wie unten gezeigt zu:

Verfügbarer Speicherplatz	50–55 GB Für Linux sollte der Speicherplatz folgendermaßen zugewiesen werden: /opt/netapp 25–30 GB /var/log/netapp 25 GB

Zusätzliche Empfehlungen

- Es wird dringend empfohlen, die Zeit sowohl auf dem ONTAP -System als auch auf der Agent-Maschine mithilfe von **Network Time Protocol (NTP)** oder **Simple Network Time Protocol (SNTP)** zu synchronisieren.

Cloud-Netzwerkzugriffsregeln

Für **US-basierte** Workload Security-Umgebungen:

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	443	Workload-Sicherheitsagent	<Sitename>.cs01.cloudinsights.netapp.com <Sitename>.c01.cloudinsights.netapp.com <Sitename>.c02.cloudinsights.netapp.com	Zugriff auf Data Infrastructure Insights
TCP	443	Workload-Sicherheitsagent	agentlogin.cs01.cloudinsights.netapp.com	Zugriff auf Authentifizierungsdienste

Für **in Europa ansässige** Workload Security-Umgebungen:

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	443	Workload-Sicherheitsagent	<Sitename>.cs01-eu-1.cloudinsights.netapp.com <Sitename>.c01-eu-1.cloudinsights.netapp.com <Sitename>.c02-eu-1.cloudinsights.netapp.com	Zugriff auf Data Infrastructure Insights
TCP	443	Workload-Sicherheitsagent	agentlogin.cs01-eu-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsdienste

Für **APAC-basierte** Workload Security-Umgebungen:

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	443	Workload-Sicherheitsagent	<Sitename>.cs01-ap-1.cloudinsights.netapp.com <Sitename>.c01-ap-1.cloudinsights.netapp.com <Sitename>.c02-ap-1.cloudinsights.netapp.com	Zugriff auf Data Infrastructure Insights
TCP	443	Workload-Sicherheitsagent	agentlogin.cs01-ap-1.cloudinsights.netapp.com	Zugriff auf Authentifizierungsdienste

Netzwerkinterne Regeln

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	389 (LDAP) 636 (LDAPs / Start-TLS)	Workload-Sicherheitsagent	LDAP-Server-URL	Mit LDAP verbinden
TCP	443	Workload-Sicherheitsagent	Cluster- oder SVM-Verwaltungs-IP-Adresse (abhängig von der SVM-Collector-Konfiguration)	API-Kommunikation mit ONTAP

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000 - 55000	SVM-Daten-LIF-IP-Adressen	Workload-Sicherheitsagent	Kommunikation von ONTAP an den Workload Security Agent für Fpolicy-Ereignisse. Diese Ports müssen für den Workload Security Agent geöffnet werden, damit ONTAP Ereignisse an ihn senden kann, einschließlich einer Firewall auf dem Workload Security Agent selbst (sofern vorhanden). BEACHTEN Sie, dass Sie nicht **alle** dieser Ports reservieren müssen, aber die Ports, die Sie dafür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, zunächst etwa 100 Ports zu reservieren und diese bei Bedarf zu erhöhen.

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000-55000	Cluster-Verwaltungs-IP	Workload-Sicherheitsagent	Kommunikation von der ONTAP Cluster Management IP zum Workload Security Agent für **EMS-Ereignisse**. Diese Ports müssen für den Workload Security Agent geöffnet werden, damit ONTAP **EMS-Ereignisse** an ihn senden kann, einschließlich einer Firewall auf dem Workload Security Agent selbst (sofern vorhanden). BEACHTEN Sie, dass Sie nicht **alle** dieser Ports reservieren müssen, aber die Ports, die Sie dafür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, zunächst etwa 100 Ports zu reservieren und diese bei Bedarf zu erhöhen.
SSH	22	Workload-Sicherheitsagent	Clusterverwaltung	Wird für die CIFS/SMB-Benutzerblockierung benötigt.

Systemdimensionierung

Siehe die"Event-Raten-Checker" Informationen zur Größenbestimmung finden Sie in der Dokumentation.

Workload-Sicherheitsagenten bereitstellen

Workload Security-Agenten sind unerlässlich, um die Benutzeraktivitäten zu überwachen und potenzielle Sicherheitsbedrohungen in Ihrer Speicherinfrastruktur zu erkennen. Dieser Leitfaden enthält eine schrittweise Installationsanleitung, Best Practices für die Agentenverwaltung (einschließlich Pause-/Fortsetzungs- und Anheft-/Entfernungsfunktionen) sowie Konfigurationsanforderungen nach der Bereitstellung. Bevor Sie beginnen, stellen Sie sicher, dass Ihr Agentenserver die folgenden Anforderungen erfüllt: "Systemanforderungen"Die

Bevor Sie beginnen

- Für die Installation, das Ausführen von Skripts und die Deinstallation ist das Sudo-Privileg erforderlich.
- Während der Installation des Agenten werden auf dem Computer ein lokaler Benutzer *cssys* und eine lokale Gruppe *cssys* erstellt. Wenn die Berechtigungseinstellungen die Erstellung eines lokalen Benutzers nicht zulassen und stattdessen Active Directory erfordern, muss auf dem Active Directory-Server ein Benutzer mit dem Benutzernamen *cssys* erstellt werden.
- Sie können mehr über die Sicherheit von Data Infrastructure Insights lesen"hier," .

Bewährte Verfahren

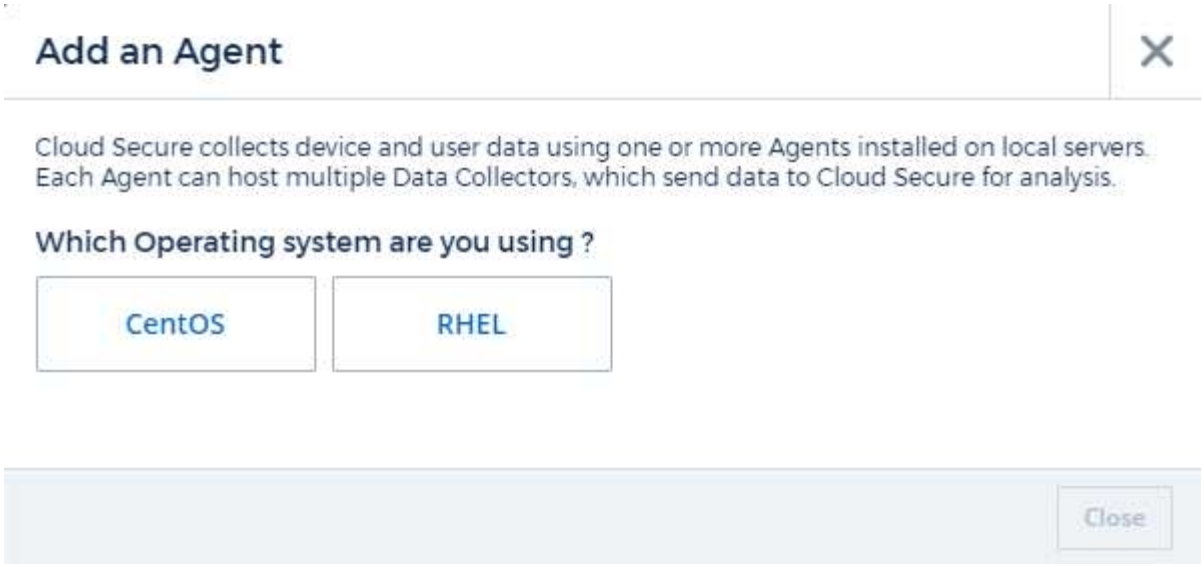
Beachten Sie Folgendes, bevor Sie Ihren Workload Security-Agenten konfigurieren.

Pause und Fortsetzung	Pause: Entfernt fpolicies aus ONTAP. Wird typischerweise verwendet, wenn Kunden umfangreiche Wartungsarbeiten durchführen, die viel Zeit in Anspruch nehmen können, wie z. B. Neustarts von Agenten-VMs oder den Austausch von Speichermedien. Zusammenfassung: Fügt fpolicies wieder zu ONTAP hinzu.
Anheften und Lösen	Unpin ruft sofort die neueste Version ab (sofern verfügbar) und aktualisiert Agent und Collector. Während dieses Upgrades werden die fpolicies-Verbindungen getrennt und wiederhergestellt. Diese Funktion ist für Kunden gedacht, die den Zeitpunkt automatischer Aktualisierungen selbst bestimmen möchten. Siehe unten fürAnleitung zum Einstecken/Entfernen der Stifte Die
Empfohlene Vorgehensweise	Bei großen Konfigurationen empfiehlt es sich, Pin und Unpin anstelle von pausierenden Kollektoren zu verwenden. Beim Anheften und Aufheben der Fixierung ist kein Pausieren und Fortsetzen erforderlich. Kunden können ihre Agenten und Sammler beibehalten und haben nach Erhalt einer E-Mail-Benachrichtigung über eine neue Version 30 Tage Zeit, die Agenten einzeln zu aktualisieren. Dieser Ansatz minimiert die Latenzauswirkungen auf fpolicies und ermöglicht eine bessere Kontrolle über den Upgrade-Prozess.

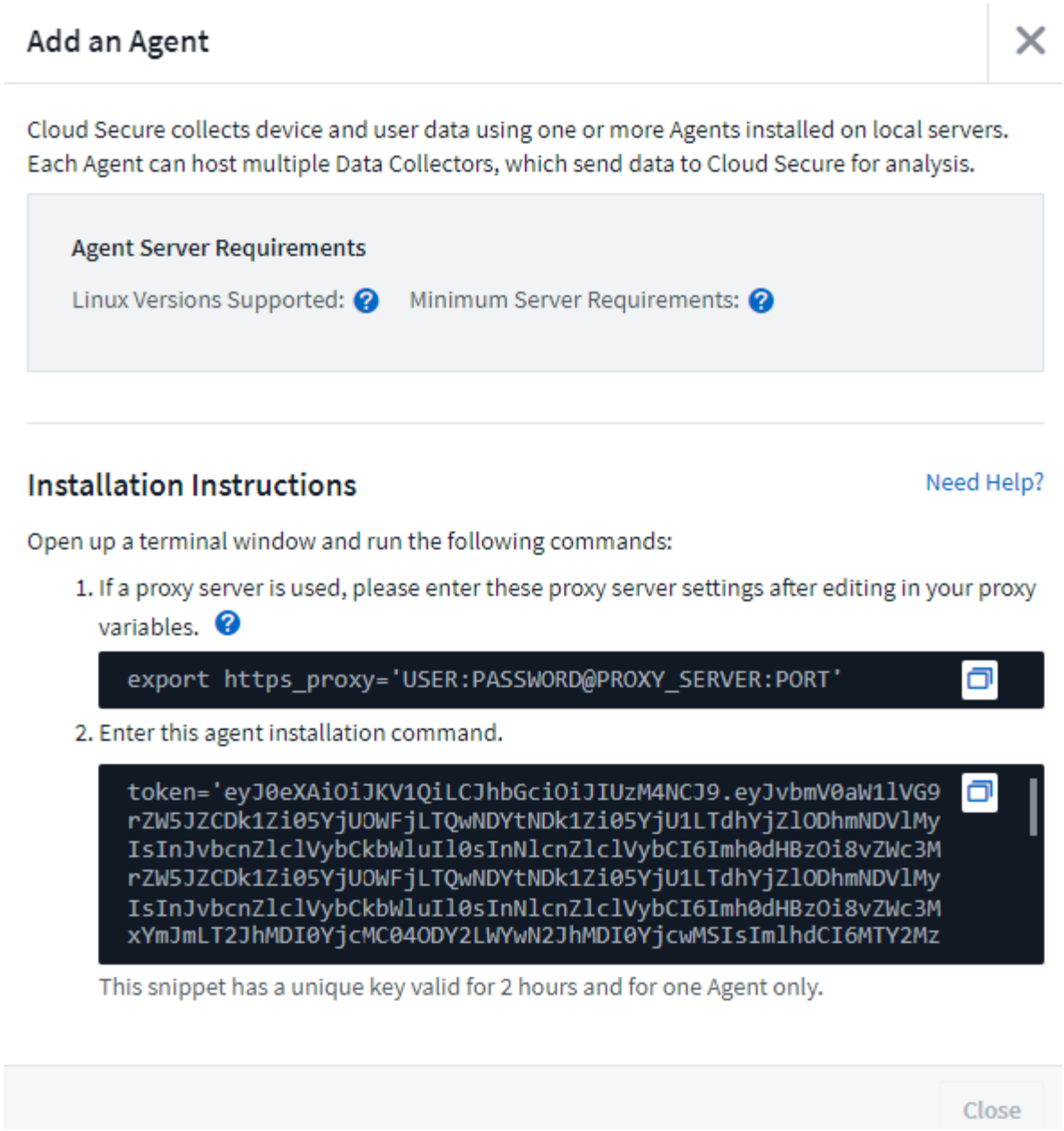
Schritte zum Installieren des Agenten

1. Melden Sie sich als Administrator oder Kontobesitzer bei Ihrer Workload Security-Umgebung an.
2. Wählen Sie **Sammler > Agenten > +Agent**

   Das System zeigt die Seite „Agent hinzufügen“ an:



3. Stellen Sie sicher, dass der Agent-Server die Mindestsystemanforderungen erfüllt.
4. Um zu überprüfen, ob auf dem Agent-Server eine unterstützte Linux-Version ausgeführt wird, klicken Sie auf *Unterstützte Versionen (i)*.
5. Wenn Ihr Netzwerk einen Proxyserver verwendet, legen Sie die Proxyserverdetails fest, indem Sie den Anweisungen im Abschnitt „Proxy“ folgen.



6. Klicken Sie auf das Symbol „In die Zwischenablage kopieren“, um den Installationsbefehl zu kopieren.
7. Führen Sie den Installationsbefehl in einem Terminalfenster aus.
8. Wenn die Installation erfolgreich abgeschlossen ist, zeigt das System die folgende Meldung an:

Nach Abschluss

1. Sie müssen eine"Benutzerverzeichnis-Sammler" .
2. Sie müssen einen oder mehrere Datensammler konfigurieren.

Netzwerkkonfiguration

Führen Sie die folgenden Befehle auf dem lokalen System aus, um Ports zu öffnen, die von Workload Security verwendet werden. Wenn Sicherheitsbedenken hinsichtlich des Portbereichs bestehen, können Sie einen kleineren Portbereich verwenden, beispielsweise *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 entsprechend Ihrer Plattform:

CentOS 7.x / RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Beispielausgabe:

```
 -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)

Beispielausgabe:

```
35000-55000/tcp
```

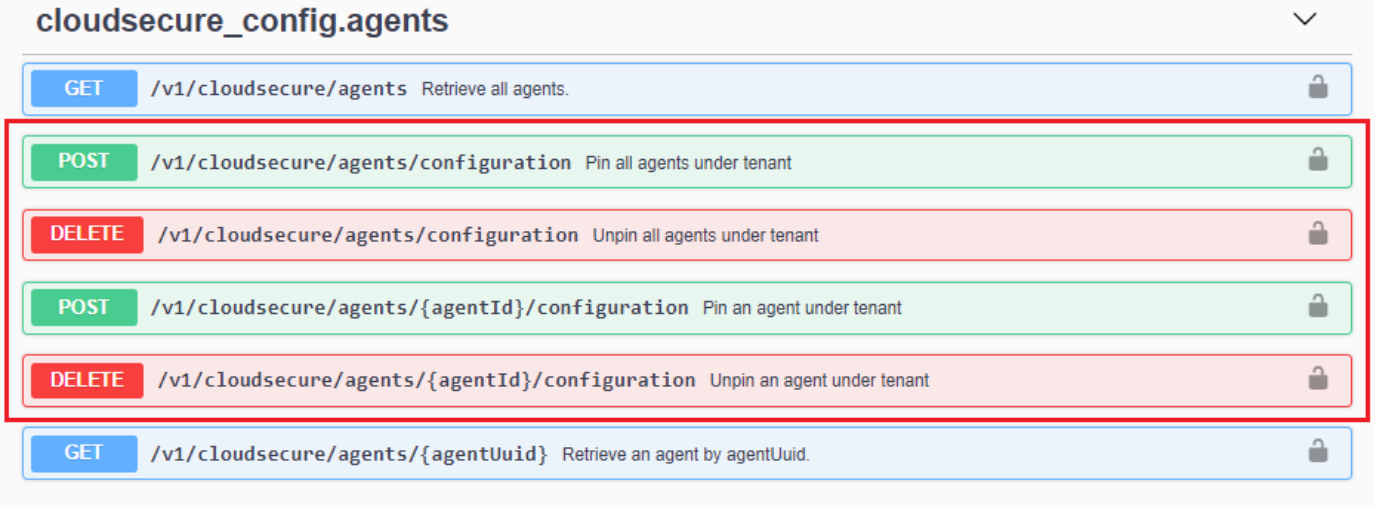
Einen Agenten auf der aktuellen Version „fixieren“

Standardmäßig aktualisiert Data Infrastructure Insights Workload Security Agents automatisch. Einige Kunden möchten die automatische Aktualisierung möglicherweise anhalten, wodurch ein Agent auf seiner aktuellen Version verbleibt, bis eines der folgenden Ereignisse eintritt:

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

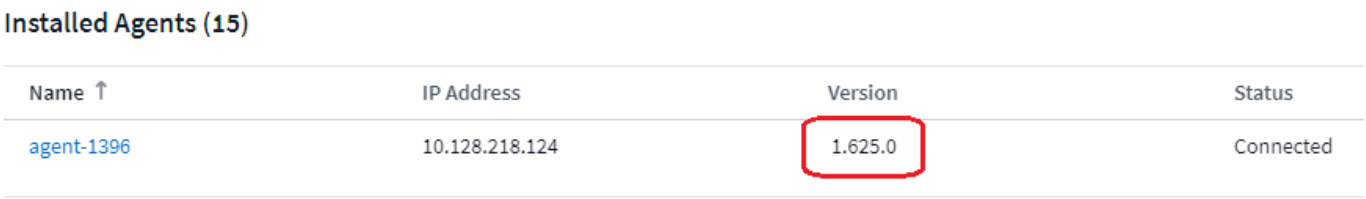
In jedem dieser Fälle wird der Agent bei der nächsten Aktualisierung der Workload-Sicherheit aktualisiert.

Um automatische Agent-Updates anzuhalten oder fortzusetzen, verwenden Sie die *cloudsecure_config.agents* -APIs:



Beachten Sie, dass es bis zu fünf Minuten dauern kann, bis die Pausen- oder Fortsetzungsaktion wirksam wird.

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



Fehlerbehebung bei Agentenfehlern

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

Problem:	Auflösung:
Bei der Agent-Installation kann der Ordner /opt/netapp/cloudsecure/agent/logs/agent.log nicht erstellt werden und die Datei install.log enthält keine relevanten Informationen.	Dieser Fehler tritt beim Bootstrapping des Agenten auf. Der Fehler wird nicht in den Protokolldateien protokolliert, da er vor der Initialisierung des Loggers auftritt. Der Fehler wird zur Standardausgabe umgeleitet und ist im Serviceprotokoll mit dem `journalctl -u cloudsecure-agent.service` Befehl. Dieser Befehl kann zur weiteren Fehlerbehebung des Problems verwendet werden. est
Die Agenteninstallation schlägt mit der Meldung „Diese Linux-Distribution wird nicht unterstützt“ fehl. Beenden der Installation‘.	Dieser Fehler tritt auf, wenn Sie versuchen, den Agenten auf einem nicht unterstützten System zu installieren. Sehen "Agentenanforderungen" .

Problem:	Auflösung:
Die Agenteninstallation ist mit folgendem Fehler fehlgeschlagen: „-bash: unzip: Befehl nicht gefunden“	Installieren Sie „Unzip“ und führen Sie den Installationsbefehl erneut aus. Wenn Yum auf dem Computer installiert ist, versuchen Sie „yum install unzip“, um die Entpackungssoftware zu installieren. Kopieren Sie anschließend den Befehl erneut aus der Benutzeroberfläche der Agent-Installation und fügen Sie ihn in die CLI ein, um die Installation erneut auszuführen.

Der Agent wurde installiert und lief. Der Agent hat jedoch plötzlich aufgehört.	Stellen Sie eine SSH-Verbindung zum Agent-Computer her. Überprüfen Sie den Status des Agentendienstes über `sudo systemctl status cloudsecure-agent.service` . 1. Überprüfen Sie, ob in den Protokollen die Meldung „Workload Security-Daemon-Dienst konnte nicht gestartet werden“ angezeigt wird. 2. Überprüfen Sie, ob der CSSY-Benutzer auf dem Agent-Computer vorhanden ist oder nicht. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus und prüfen Sie, ob der Benutzer und die Gruppe CSSYS vorhanden sind.
	`sudo id cssys`
	`sudo groups cssys` 3. Wenn keines vorhanden ist, wurde der CSSY-Benutzer möglicherweise durch eine zentralisierte Überwachungsrichtlinie gelöscht. 4. Erstellen Sie den CSSY-Benutzer und die CSSY-Gruppe manuell, indem Sie die folgenden Befehle ausführen.
	`sudo useradd cssys`
	`sudo groupadd cssys` 5. Starten Sie den Agentendienst anschließend neu, indem Sie den folgenden Befehl ausführen:
	`sudo systemctl restart cloudsecure-agent.service` 6. Wenn es immer noch nicht läuft, prüfen Sie bitte die anderen Optionen zur Fehlerbehebung.

Es können nicht mehr als 50 Datensammler zu einem Agenten hinzugefügt werden.	Einem Agenten können nur 50 Datensammler hinzugefügt werden. Dies kann eine Kombination aller Collector-Typen sein, beispielsweise Active Directory, SVM und andere Collector.
Die Benutzeroberfläche zeigt, dass sich der Agent im Status NOT_CONNECTED befindet.	Schritte zum Neustart des Agenten. 1. Stellen Sie eine SSH-Verbindung zum Agent-Computer her. 2. Starten Sie den Agentendienst anschließend neu, indem Sie den folgenden Befehl ausführen: `sudo systemctl restart cloudsecure-agent.service` 3. Überprüfen Sie den Status des Agentendienstes über `sudo systemctl status cloudsecure-agent.service` . 4. Der Agent sollte in den Status „VERBUNDEN“ wechseln.

Problem:	Auflösung:
Die Agent-VM befindet sich hinter dem Zscaler-Proxy und die Agent-Installation schlägt fehl. Aufgrund der SSL-Prüfung des Zscaler-Proxys werden die Workload-Sicherheitszertifikate so angezeigt, als wären sie von der Zscaler-Zertifizierungsstelle signiert, sodass der Agent der Kommunikation nicht vertraut.	Deaktivieren Sie die SSL-Prüfung im Zscaler-Proxy für die URL *.cloudinsights.netapp.com. Wenn Zscaler eine SSL-Prüfung durchführt und die Zertifikate ersetzt, funktioniert Workload Security nicht.
Während der Installation des Agenten bleibt die Installation nach dem Entpacken hängen.	Der Befehl „chmod 755 -Rf“ schlägt fehl. Der Befehl schlägt fehl, wenn der Agent-Installationsbefehl von einem Nicht-Root-Sudo-Benutzer ausgeführt wird, der Dateien im Arbeitsverzeichnis hat, die einem anderen Benutzer gehören, und die Berechtigungen dieser Dateien nicht geändert werden können. Aufgrund des fehlgeschlagenen chmod-Befehls wird der Rest der Installation nicht ausgeführt. 1. Erstellen Sie ein neues Verzeichnis mit dem Namen „cloudsecure“. 2. Gehen Sie zu diesem Verzeichnis. 3. Kopieren Sie den vollständigen Installationsbefehl „token=…… … ./cloudsecure-agent-install.sh“, fügen Sie ihn ein und drücken Sie die Eingabetaste. 4. Die Installation sollte fortgesetzt werden können.
Wenn der Agent immer noch keine Verbindung zu Saas herstellen kann, öffnen Sie bitte einen Fall beim NetApp Support. Geben Sie die Seriennummer von Data Infrastructure Insights an, um einen Fall zu öffnen, und hängen Sie die Protokolle wie angegeben an den Fall an.	So fügen Sie Protokolle an den Koffer an: 1. Führen Sie das folgende Skript mit Root-Berechtigung aus und geben Sie die Ausgabedatei (cloudsecure-agent-symptoms.zip) frei. a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Führen Sie die folgenden Befehle nacheinander mit Root-Berechtigung aus und teilen Sie die Ausgabe. a. id cssys b. groups cssys c. cat /etc/os-release
Das Skript cloudsecure-agent-symptom-collector.sh schlägt mit dem folgenden Fehler fehl. [root@machine tmp]# /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh Dienstprotokoll sammeln Anwendungsprotokolle sammeln Agentenkonfigurationen sammeln Servicestatus-Snapshot erstellen Snapshot der Agentenverzeichnisstruktur erstellen …… …… /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.	Das Zip-Tool ist nicht installiert. Installieren Sie das Zip-Tool, indem Sie den Befehl „yum install zip“ ausführen. Führen Sie dann cloudsecure-agent-symptom-collector.sh erneut aus.

Problem:	Auflösung:
Die Agenteninstallation schlägt mit useradd fehl: Verzeichnis /home/cssys kann nicht erstellt werden	Dieser Fehler kann auftreten, wenn das Anmeldeverzeichnis des Benutzers aufgrund fehlender Berechtigungen nicht unter /home erstellt werden kann. Die Problemumgehung besteht darin, einen CSSY-Benutzer zu erstellen und sein Anmeldeverzeichnis manuell mit dem folgenden Befehl hinzuzufügen: *sudo useradd user_name -m -d HOME_DIR* -m: Erstellen Sie das Home-Verzeichnis des Benutzers, falls es nicht vorhanden ist. -d: Der neue Benutzer wird mit HOME_DIR als Wert für das Anmeldeverzeichnis des Benutzers erstellt. Beispielsweise fügt *sudo useradd cssys -m -d /cssys* einen Benutzer *cssys* hinzu und erstellt sein Anmeldeverzeichnis unter root.
Der Agent wird nach der Installation nicht ausgeführt. *Systemctl status cloudsecure-agent.service* zeigt Folgendes: [root@demo ~]# systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service Loaded: geladen (/usr/lib/systemd/system/cloudsecure-agent.service; aktiviert; Vendor-Vorgabe: deaktiviert) Active: Aktivierung (automatischer Neustart) (Ergebnis: Exitcode) seit Dienstag, 03.08.2021, 21:12:26 PDT; Vor 2 Sekunden Prozess: 25889 ExecStart=/bin/bash /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent (Code=exited Status=126) Haupt-PID: 25889 (Code=exited, Status=126), 3. August 21:12:26 Demo systemd[1]: cloudsecure-agent.service: Hauptprozess beendet, Code=exited, Status=126/n/a 3. August 21:12:26 Demo systemd[1]: Einheit cloudsecure-agent.service ist in den Zustand „Fehler“ gewechselt. 03. Aug. 21:12:26 Demo systemd[1]: cloudsecure-agent.service fehlgeschlagen.	Dies kann fehlschlagen, weil der Benutzer *cssys* möglicherweise keine Berechtigung zur Installation hat. Wenn es sich bei /opt/netapp um einen NFS-Mount handelt und der Benutzer *cssys* keinen Zugriff auf diesen Ordner hat, schlägt die Installation fehl. *cssys* ist ein lokaler Benutzer, der vom Workload Security-Installationsprogramm erstellt wurde und möglicherweise keine Berechtigung zum Zugriff auf die bereitgestellte Freigabe hat. Sie können dies überprüfen, indem Sie versuchen, mit dem Benutzer *cssys* auf /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent zuzugreifen. Wenn die Meldung „Berechtigung verweigert“ angezeigt wird, liegt keine Installationsberechtigung vor. Installieren Sie die Software nicht in einem bereitgestellten Ordner, sondern in einem lokalen Verzeichnis auf dem Computer.
Der Agent wurde ursprünglich über einen Proxyserver verbunden und der Proxy wurde während der Agentinstallation festgelegt. Jetzt hat sich der Proxyserver geändert. Wie kann die Proxy-Konfiguration des Agenten geändert werden?	Sie können die agent.properties bearbeiten, um die Proxy-Details hinzuzufügen. Gehen Sie folgendermaßen vor: 1. Wechseln Sie in den Ordner, der die Eigenschaftendatei enthält: cd /opt/netapp/cloudsecure/conf 2. Öffnen Sie die Datei *agent.properties* zur Bearbeitung mit Ihrem bevorzugten Texteditor. 3. Fügen Sie die folgenden Zeilen hinzu oder ändern Sie sie: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Speichern Sie die Datei. 5. Starten Sie den Agenten neu: sudo systemctl restart cloudsecure-agent.service

Löschen eines Workload Security Agent

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

Löschen eines Agenten

> Durch das Löschen eines Agenten werden alle mit dem Agenten verknüpften Datensammler gelöscht. Wenn Sie die Datensammler mit einem anderen Agenten konfigurieren möchten, sollten Sie vor dem Löschen des Agenten eine Sicherungskopie der Datensammlerkonfigurationen 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 Collector im Status STOPPED befinden.

Schritte zum Löschen eines Agenten:

1. Melden Sie sich per SSH bei der Agent-VM an und führen Sie den folgenden Befehl aus. Geben Sie bei der entsprechenden Aufforderung „y“ ein, um fortzufahren.

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

2. Klicken Sie auf **Workload-Sicherheit > Collectors > Agents**

   Das System zeigt die Liste der konfigurierten Agenten an.

3. Klicken Sie auf das Optionsmenü für den Agenten, den Sie löschen.
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)-Benutzerverzeichnis-Collectors

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

Bevor Sie beginnen

- Sie müssen ein Data Infrastructure Insights Administrator oder Kontoinhaber sein, um diese Aufgabe auszuführen.
- Sie müssen über die IP-Adresse des Servers verfügen, auf dem der Active Directory-Server gehostet wird.
- Bevor Sie einen Benutzerverzeichnis-Connector konfigurieren, muss ein Agent konfiguriert werden.

Schritte zum Konfigurieren eines Benutzerverzeichnis-Collectors

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

   Das System zeigt den Bildschirm „Benutzerverzeichnis hinzufügen“ an.

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

Name	Beschreibung
Name	Eindeutiger Name für das Benutzerverzeichnis. Zum Beispiel *GlobalADCollector*
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus
Server-IP/Domänenname	IP-Adresse oder vollqualifizierter Domänenname (FQDN) des Servers, auf dem das Active Directory gehostet wird
Waldname	Gesamtstrukturebene der Verzeichnisstruktur. Der Gesamtstrukturname lässt die beiden folgenden Formate zu: *x.y.z* ⇒ direkter Domänenname, wie er auf Ihrem SVM vorhanden ist. [Beispiel: hq.firmenname.com] *DC=x,DC=y,DC=z* ⇒ Relative Distinguished Names [Beispiel: DC=hq,DC= Firmenname,DC=com] Oder Sie können Folgendes angeben: *OU=Engineering,DC=hq,DC= Firmenname,DC=com* [um nach einer bestimmten OU Engineering zu filtern] *CN=Benutzername,OU=Engineering,DC=Firmennam e, DC=NetApp, DC=com* [um nur bestimmte Benutzer mit <Benutzername> aus der OU <Engineering> abzurufen] *CN=Acrobat-Benutzer,CN=Benutzer,DC=hq,DC=Firmenname,DC= com,O= Firmenname,L=Boston,S=MA,C=US* [um alle Acrobat-Benutzer innerhalb der Benutzer in dieser Organisation abzurufen] Vertrauenswürdige Active Directory-Domänen werden ebenfalls unterstützt.
Bind-DN	Der Benutzer darf das Verzeichnis durchsuchen. Beispiel: *Benutzername@Firmenname.com* oder *Benutzername@Domänenname.com*. Außerdem ist die Berechtigung „Nur Lesen“ für die Domäne erforderlich. Der Benutzer muss Mitglied der Sicherheitsgruppe „Schreibgeschützte Domänencontroller“ sein.
BIND-Passwort	Kennwort für den Verzeichnisserver (d. h. Kennwort für den im Bind-DN verwendeten Benutzernamen)
Protokoll	ldap, ldaps, ldap-start-tls
Häfen	Port auswählen

Geben Sie die folgenden für Directory Server erforderlichen Attribute ein, wenn die Standardattributnamen in Active Directory geändert wurden. Meistens werden diese Attributnamen in Active Directory *nicht* geändert. In

diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

Eigenschaften	Attributname im Verzeichnisserver
Anzeigename	Name
SID	Objekt-ID
Benutzername	sAMAccountName

Klicken Sie auf „Optionale Attribute einschließen“, um die folgenden Attribute hinzuzufügen:

Eigenschaften	Attributname im Verzeichnisserver
E-Mail-Adresse	mail
Telefonnummer	Telefonnummer
Rolle	Titel
Land	co
Status	Zustand
Abteilung	Abteilung
Foto	Miniaturfoto
ManagerDN	Manager
Gruppen	Mitglied von

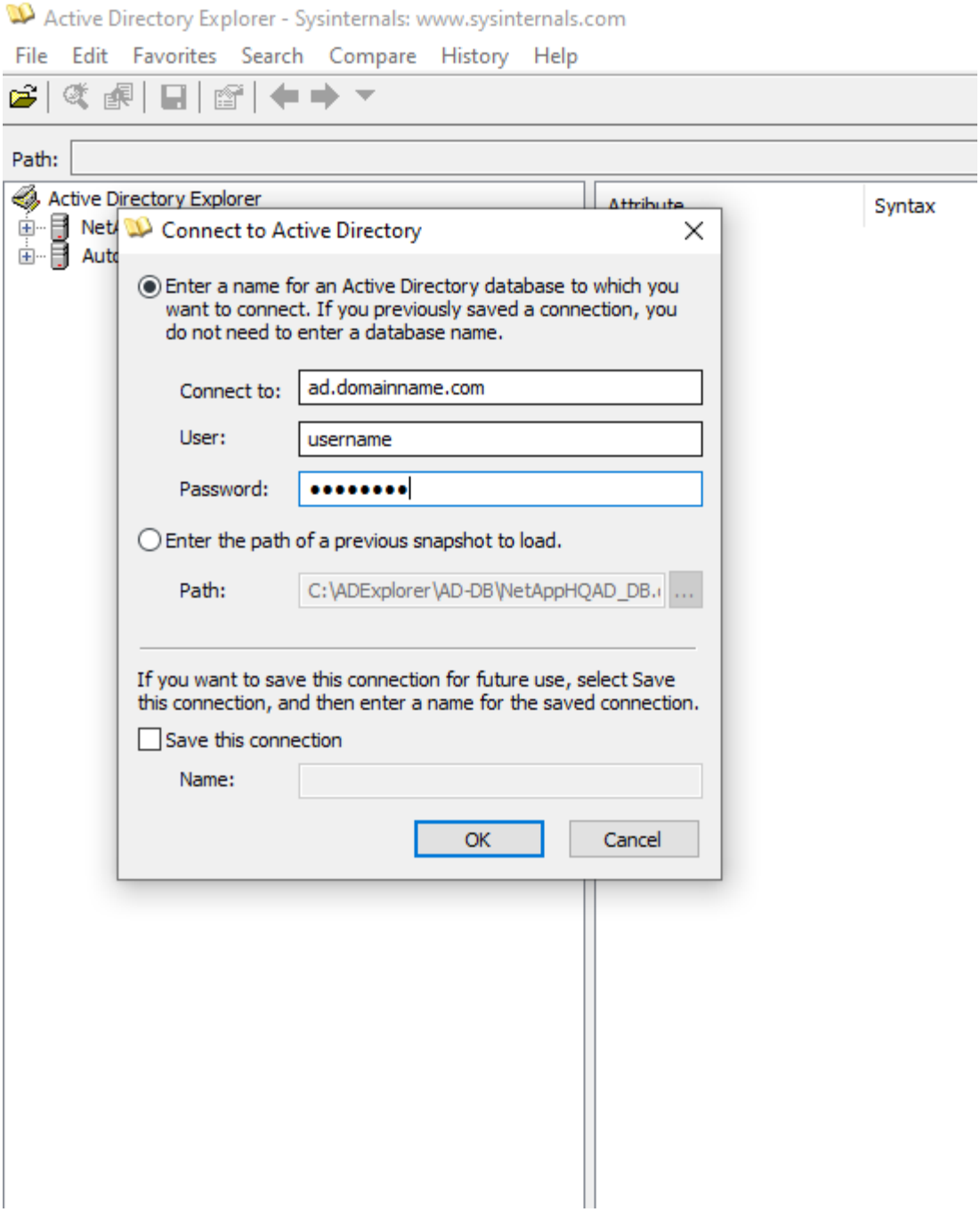
Testen der Konfiguration Ihres Benutzerverzeichnis-Collectors

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

- Verwenden Sie den folgenden Befehl, um die LDAP-Benutzerberechtigung für Workload Security 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 und komplexe Suchvorgänge auszuführen, die Sie speichern und erneut ausführen können.
  - Installieren"AD Explorer" auf jedem Windows-Computer, der eine Verbindung zum AD-Server herstellen kann.
  - Stellen Sie mit dem Benutzernamen/Passwort des AD-Verzeichnisservers eine Verbindung zum AD-Server her.



Fehlerbehebung bei Konfigurationsfehlern des User Directory Collector

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

Problem:	Auflösung:
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „Ungültige Anmeldeinformationen für LDAP-Server angegeben.“	Falscher Benutzername oder falsches Passwort angegeben. Bearbeiten Sie den richtigen Benutzernamen und das richtige Passwort und geben Sie es ein.

Problem:	Auflösung:
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „Das Objekt, das DN=DC=hq,DC=domainname,DC=com entspricht und als Gesamtstrukturname angegeben wurde, konnte nicht abgerufen werden.“	Falscher Gesamtstrukturname angegeben. Bearbeiten Sie den Vorgang und geben Sie den richtigen Gesamtstrukturnamen ein.
Die optionalen Attribute des Domänenbenutzers werden auf der Workload Security-Benutzerprofilseite nicht angezeigt.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory. Bearbeiten Sie die Datei und geben Sie die korrekten optionalen Attributnamen an.
Datensammler im Fehlerzustand mit „Fehler beim Abrufen der LDAP-Benutzer.“ Grund für den Fehler: „Verbindung zum Server nicht möglich, die Verbindung ist null“	Starten Sie den Collector neu, indem Sie auf die Schaltfläche *Neustart* klicken.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“.	Stellen Sie sicher, dass Sie für die erforderlichen Felder (Server, Gesamtstrukturname, Bind-DN, Bind-Passwort) gültige Werte angegeben haben. Stellen Sie sicher, dass die Bind-DN-Eingabe immer als „Administrator@<Domänengesamtstrukturname>“ oder als Benutzerkonto mit Domänenadministratorrechten erfolgt.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „WIEDERHOLT“. Zeigt den Fehler „Der Status des Collectors konnte nicht definiert werden, Grund: Der TCP-Befehl [Connect(localhost:35012,None,List(),Some(,seconds),true)] ist aufgrund von java.net.ConnectionException:Connection refused fehlgeschlagen.“	Für den AD-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „LDAP-Verbindung konnte nicht hergestellt werden.“	Für den AD-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein.
Das Hinzufügen eines Benutzerverzeichnis-Konnektors führt zum Status „Fehler“. Der Fehler lautet: „Die Einstellungen konnten nicht geladen werden.“ Grund: Die Datenquellenkonfiguration weist einen Fehler auf. Spezifischer Grund: /connector/conf/application.conf: 70: ldap.ldap-port hat den Typ STRING statt NUMBER“	Falscher Wert für Port angegeben. Versuchen Sie, die Standard-Portwerte oder die richtige Portnummer für den AD-Server zu verwenden.
Ich habe mit den obligatorischen Attributen begonnen und es hat funktioniert. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory. Bearbeiten Sie den korrekten obligatorischen oder optionalen Attributnamen und geben Sie ihn an.

Problem:	Auflösung:
Wann erfolgt die AD-Synchronisierung nach dem Neustart des Collectors?	Die AD-Synchronisierung erfolgt unmittelbar nach dem Neustart des Collectors. Das Abrufen der Benutzerdaten von etwa 300.000 Benutzern dauert etwa 15 Minuten und wird alle 12 Stunden automatisch aktualisiert.
Benutzerdaten werden von AD mit CloudSecure synchronisiert. Wann werden die Daten gelöscht?	Benutzerdaten werden 13 Monate lang gespeichert, wenn keine Aktualisierung erfolgt. Bei Löschung des Mandanten werden auch die Daten gelöscht.
Der Benutzerverzeichnis-Connector führt zum Status „Fehler“. „Der Connector befindet sich im Fehlerzustand. Dienstname: usersLdap. Grund für den Fehler: LDAP-Benutzer konnten nicht abgerufen werden. Grund für den Fehler: 80090308: LdapErr: DSID-0C090453, Kommentar: AcceptSecurityContext-Fehler, Daten 52e, v3839"	Falscher Gesamtstrukturname angegeben. Informationen zum Angeben des richtigen Gesamtstrukturnamens finden Sie oben.
Die Telefonnummer wird auf der Benutzerprofilseite nicht eingetragen.	Dies liegt höchstwahrscheinlich an einem Attributzuordnungsproblem mit Active Directory. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Benutzerinformationen aus Active Directory abruft. 2. Beachten Sie, dass unter den optionalen Attributen ein Feldname „Telefonnummer“ vorhanden ist, der dem Active Directory-Attribut „Telefonnummer“ zugeordnet ist. 4. Verwenden Sie nun das Tool „Active Directory Explorer“ wie oben beschrieben, um das Active Directory zu durchsuchen und den richtigen Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass es im Active Directory ein Attribut mit dem Namen „Telefonnummer“ gibt, das tatsächlich die Telefonnummer des Benutzers enthält. 5. Nehmen wir an, es wurde im Active Directory in „Telefonnummer“ geändert. 6. Bearbeiten Sie dann den CloudSecure-Benutzerverzeichnis-Collector. Ersetzen Sie im Abschnitt „Optionale Attribute“ „Telefonnummer“ durch „Telefonnummer“. 7. Speichern Sie den Active Directory-Collector. Der Collector wird neu gestartet, ruft die Telefonnummer des Benutzers ab und zeigt diese auf der Benutzerprofilseite an.
Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen.	Deaktivieren Sie die AD-Server-Verschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurden, bleiben sie 13 Monate lang dort. Wenn die Verbindung zum AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Zum erneuten Abrufen muss der Benutzerverzeichnis-Collector mit AD verbunden sein.

Problem:	Auflösung:
Daten aus Active Directory sind in CloudInsights Security vorhanden. Möchten Sie alle Benutzerinformationen aus CloudInsights löschen.	Es ist nicht möglich, NUR Active Directory-Benutzerinformationen aus CloudInsights Security zu löschen. Um den Benutzer zu löschen, muss der gesamte Mandant gelöscht werden.

Konfigurieren eines LDAP-Verzeichnisserver-Collectors

Sie konfigurieren Workload Security, um Benutzerattribute von LDAP-Verzeichnisservern zu erfassen.

Bevor Sie beginnen

- Sie müssen ein Data Infrastructure Insights Administrator oder Kontoinhaber sein, um diese Aufgabe auszuführen.
- Sie müssen über die IP-Adresse des Servers verfügen, auf dem der LDAP-Verzeichnisserver gehostet wird.
- Bevor Sie einen LDAP-Verzeichnis-Connector konfigurieren, muss ein Agent konfiguriert werden.

Schritte zum Konfigurieren eines Benutzerverzeichnis-Collectors

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

   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. Zum Beispiel *GlobalLDAPCollector*
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus
Server-IP/Domänenname	IP-Adresse oder vollqualifizierter Domänenname (FQDN) des Servers, auf dem der LDAP-Verzeichnisserver gehostet wird

Suchbasis	Suchbasis des LDAP-Servers. Suchbasis erlaubt die beiden folgenden Formate: *x.y.z* ⇒ direkter Domänenname, wie Sie ihn auf Ihrem SVM haben. [Beispiel: hq.firmenname.com] *DC=x,DC=y,DC=z* ⇒ Relative Distinguished Names [Beispiel: DC=hq,DC=Firmenname,DC=com] Oder Sie können Folgendes angeben: *OU=Engineering,DC=hq,DC=Firmenname,DC=com* [um nach einer bestimmten OU Engineering zu filtern] *CN=Benutzername,OU=Engineering,DC=Firmenname, DC=NetApp, DC=com* [um nur bestimmte Benutzer mit <Benutzername> aus der OU <Engineering> abzurufen] *CN=Acrobat-Benutzer,CN=Benutzer,DC=hq,DC=Firmenname,DC=com,O= Firmenname,L=Boston,S=MA,C=US* [um alle Acrobat-Benutzer innerhalb der Benutzer in dieser Organisation abzurufen]
Bind-DN	Der Benutzer darf das Verzeichnis durchsuchen. Beispiel: uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com für einen Benutzer john@dorp.company.com. dorp.company.com
--accounts	--users
--John	--anna
BIND-Passwort	Kennwort für den Verzeichnisserver (d. h. Kennwort für den im Bind-DN verwendeten Benutzernamen)
Protokoll	ldap, ldaps, ldap-start-tls
Häfen	Port auswählen

Geben Sie die folgenden für den Verzeichnisserver erforderlichen Attribute ein, wenn die Standardattributnamen im LDAP-Verzeichnisserver geändert wurden. Meistens werden diese Attributnamen im LDAP-Verzeichnisserver *nicht* geändert. In diesem Fall können Sie einfach mit dem Standardattributnamen fortfahren.

Eigenschaften	Attributname im Verzeichnisserver
Anzeigename	Name
UNIXID	UID-Nummer
Benutzername	UID

Klicken Sie auf „Optionale Attribute einschließen“, um die folgenden Attribute hinzuzufügen:

Eigenschaften	Attributname im Verzeichnisserver
E-Mail-Adresse	mail
Telefonnummer	Telefonnummer

Rolle	Titel
Land	co
Status	Zustand
Abteilung	Abteilungsnummer
Foto	Foto
ManagerDN	Manager
Gruppen	Mitglied von

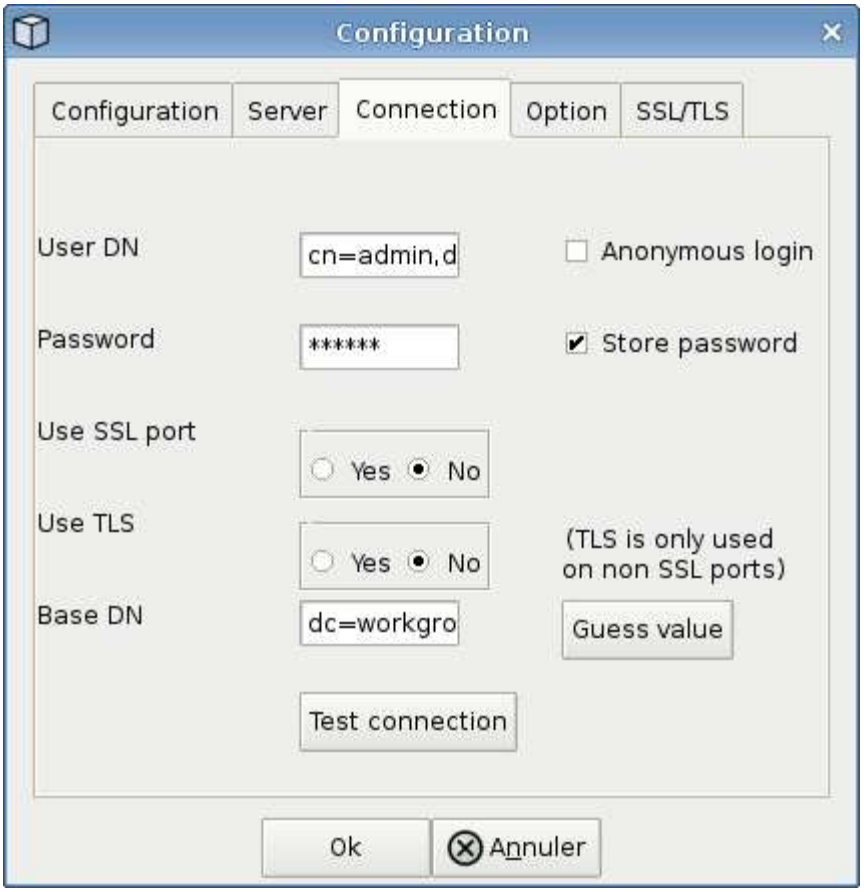
Testen der Konfiguration Ihres Benutzerverzeichnis-Collectors

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

- Verwenden Sie den folgenden Befehl, um die LDAP-Benutzerberechtigung für Workload Security 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 Suchvorgänge auszuführen, die Sie speichern und erneut
ausführen können.
```

  - Installieren Sie den LDAP Explorer(http://ldaptool.sourceforge.net/) oder Java LDAP Explorer(http://jxplorer.org/) auf jedem Windows-Computer, der eine Verbindung zum LDAP-Server herstellen kann.
  - Stellen Sie mit dem Benutzernamen/Passwort des LDAP-Verzeichnisservers eine Verbindung zum LDAP-Server her.



Fehlerbehebung bei Konfigurationsfehlern des LDAP-Verzeichnissammlers

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

Problem:	Auflösung:
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „Ungültige Anmeldeinformationen für LDAP-Server angegeben.“	Falscher Bind-DN oder falsches Bind-Passwort oder falsche Suchbasis angegeben. Bearbeiten und geben Sie die richtigen Informationen ein.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „Das Objekt, das DN=DC=hq,DC=domainname,DC=com entspricht und als Gesamtstrukturname angegeben wurde, konnte nicht abgerufen werden.“	Falsche Suchbasis angegeben. Bearbeiten Sie den Vorgang und geben Sie den richtigen Gesamtstrukturnamen ein.
Die optionalen Attribute des Domänenbenutzers werden auf der Workload Security-Benutzerprofilseite nicht angezeigt.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den Namen der in CloudSecure hinzugefügten optionalen Attribute und den tatsächlichen Attributnamen in Active Directory. Bei den Feldern wird zwischen Groß- und Kleinschreibung unterschieden. Bearbeiten Sie die Datei und geben Sie die korrekten optionalen Attributnamen an.

Problem:	Auflösung:
Datensammler im Fehlerzustand mit „Fehler beim Abrufen der LDAP-Benutzer.“ Grund für den Fehler: „Verbindung zum Server nicht möglich, die Verbindung ist null“	Starten Sie den Collector neu, indem Sie auf die Schaltfläche *Neustart* klicken.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“.	Stellen Sie sicher, dass Sie für die erforderlichen Felder (Server, Gesamtstrukturname, Bind-DN, Bind-Passwort) gültige Werte angegeben haben. Stellen Sie sicher, dass die Bind-DN-Eingabe immer als uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyname,dc=com bereitgestellt wird.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „WIEDERHOLT“. Zeigt den Fehler „Fehler beim Ermitteln des Zustands des Collectors, daher erneuter Versuch“ an.	Stellen Sie sicher, dass die richtige Server-IP und Suchbasis angegeben ist ////
Beim Hinzufügen des LDAP-Verzeichnisses wird der folgende Fehler angezeigt: „Der Zustand des Collectors konnte innerhalb von 2 Versuchen nicht ermittelt werden. Versuchen Sie, den Collector erneut neu zu starten (Fehlercode: AGENT008)“	Stellen Sie sicher, dass die richtige Server-IP und Suchbasis angegeben ist
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „WIEDERHOLT“. Zeigt den Fehler „Der Status des Collectors konnte nicht definiert werden, Grund: Der TCP-Befehl [Connect(localhost:35012,None,List(),Some(,seconds),true)] ist aufgrund von java.net.ConnectionException:Connection refused fehlgeschlagen.“	Für den AD-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein. ////
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „LDAP-Verbindung konnte nicht hergestellt werden.“	Für den LDAP-Server wurde eine falsche IP-Adresse oder ein falscher FQDN angegeben. Bearbeiten und geben Sie die richtige IP-Adresse oder den richtigen FQDN ein. Oder falscher Wert für den angegebenen Port. Versuchen Sie, die Standard-Portwerte oder die richtige Portnummer für den LDAP-Server zu verwenden.
Das Hinzufügen eines LDAP-Verzeichniskonnektors führt zum Status „Fehler“. Der Fehler lautet: „Die Einstellungen konnten nicht geladen werden.“ Grund: Die Datenquellenkonfiguration weist einen Fehler auf. Spezifischer Grund: /connector/conf/application.conf: 70: ldap.ldap-port hat den Typ STRING statt NUMBER“	Falscher Wert für Port angegeben. Versuchen Sie, die Standard-Portwerte oder die richtige Portnummer für den AD-Server zu verwenden.
Ich habe mit den obligatorischen Attributen begonnen und es hat funktioniert. Nach dem Hinzufügen der optionalen Attribute werden die Daten der optionalen Attribute nicht aus AD abgerufen.	Dies liegt wahrscheinlich an einer Nichtübereinstimmung zwischen den in CloudSecure hinzugefügten optionalen Attributen und den tatsächlichen Attributnamen in Active Directory. Bearbeiten Sie den korrekten obligatorischen oder optionalen Attributnamen und geben Sie ihn an.

Problem:	Auflösung:
Wann erfolgt die LDAP-Synchronisierung nach dem Neustart des Collectors?	Die LDAP-Synchronisierung erfolgt unmittelbar nach dem Neustart des Collectors. Das Abrufen der Benutzerdaten von etwa 300.000 Benutzern dauert etwa 15 Minuten und wird alle 12 Stunden automatisch aktualisiert.
Benutzerdaten werden von LDAP mit CloudSecure synchronisiert. Wann werden die Daten gelöscht?	Benutzerdaten werden 13 Monate lang gespeichert, wenn keine Aktualisierung erfolgt. Bei Löschung des Mandanten werden auch die Daten gelöscht.
Der LDAP-Verzeichnis-Connector führt zum Status „Fehler“. „Der Connector befindet sich im Fehlerzustand. Dienstname: usersLdap. Grund für den Fehler: LDAP-Benutzer konnten nicht abgerufen werden. Grund für den Fehler: 80090308: LdapErr: DSID-0C090453, Kommentar: AcceptSecurityContext-Fehler, Daten 52e, v3839"	Falscher Gesamtstrukturname angegeben. Informationen zum Angeben des richtigen Gesamtstrukturnamens finden Sie oben.
Die Telefonnummer wird auf der Benutzerprofilseite nicht eingetragen.	Dies liegt höchstwahrscheinlich an einem Attributzuordnungsproblem mit Active Directory. 1. Bearbeiten Sie den jeweiligen Active Directory-Collector, der die Benutzerinformationen aus Active Directory abruft. 2. Beachten Sie, dass unter den optionalen Attributen ein Feldname „Telefonnummer“ vorhanden ist, der dem Active Directory-Attribut „Telefonnummer“ zugeordnet ist. 4. Verwenden Sie nun das Tool „Active Directory Explorer“ wie oben beschrieben, um den LDAP-Verzeichnisserver zu durchsuchen und den richtigen Attributnamen anzuzeigen. 3. Stellen Sie sicher, dass im LDAP-Verzeichnis ein Attribut mit dem Namen „Telefonnummer“ vorhanden ist, das tatsächlich die Telefonnummer des Benutzers enthält. 5. Nehmen wir an, im LDAP-Verzeichnis wurde es in „Telefonnummer“ geändert. 6. Bearbeiten Sie dann den CloudSecure-Benutzerverzeichnis-Collector. Ersetzen Sie im Abschnitt „Optionale Attribute“ „Telefonnummer“ durch „Telefonnummer“. 7. Speichern Sie den Active Directory-Collector. Der Collector wird neu gestartet, ruft die Telefonnummer des Benutzers ab und zeigt diese auf der Benutzerprofilseite an.
Wenn das Verschlüsselungszertifikat (SSL) auf dem Active Directory (AD)-Server aktiviert ist, kann der Workload Security User Directory Collector keine Verbindung zum AD-Server herstellen.	Deaktivieren Sie die AD-Server-Verschlüsselung, bevor Sie einen User Directory Collector konfigurieren. Sobald die Benutzerdetails abgerufen wurden, bleiben sie 13 Monate lang dort. Wenn die Verbindung zum AD-Server nach dem Abrufen der Benutzerdetails getrennt wird, werden die neu hinzugefügten Benutzer in AD nicht abgerufen. Zum erneuten Abrufen muss der Benutzerverzeichnis-Collector mit AD verbunden sein.

Konfigurieren des ONTAP SVM-Datenkollektors

Der ONTAP SVM Data Collector ermöglicht Workload Security die Überwachung von Datei- und Benutzerzugriffsaktivitäten auf NetApp ONTAP Storage Virtual Machines (SVMs). Dieses Handbuch führt Sie durch die Konfiguration und Verwaltung des SVM-Datensammlers, um eine umfassende Sicherheitsüberwachung Ihrer ONTAP Umgebung zu gewährleisten.

Bevor Sie beginnen

- Dieser Datensammler wird mit Folgendem unterstützt:
  - Data ONTAP 9.2 und spätere Versionen. Verwenden Sie für optimale Leistung eine Data ONTAP Version höher als 9.13.1.
  - SMB-Protokollversion 3.1 und früher.
  - NFS-Versionen bis einschließlich NFS 4.1 (Beachten Sie, dass NFS 4.1 mit ONTAP 9.15 oder höher unterstützt wird).
  - Flexgroup wird ab ONTAP 9.4 und späteren Versionen unterstützt
  - FlexCache wird für NFS mit ONTAP 9.7 und späteren Versionen unterstützt.
  - FlexCache wird für SMB mit ONTAP 9.14.1 und späteren Versionen unterstützt.
  - ONTAP Select wird unterstützt
- Es werden nur Datentyp-SVMs unterstützt. SVMs mit unbegrenzten Volumes werden nicht unterstützt.
- SVM hat mehrere Untertypen. Davon werden nur *default*, *sync_source* und *sync_destination* unterstützt.
- Ein Agent"muss konfiguriert werden" bevor Sie Datensammler konfigurieren können.
- Stellen Sie sicher, dass Sie über einen ordnungsgemäß konfigurierten Benutzerverzeichnis-Connector verfügen. Andernfalls werden auf der Seite „Aktivitätsforensik“ verschlüsselte Benutzernamen und nicht der tatsächliche Name des Benutzers (wie in Active Directory gespeichert) angezeigt.
- ONTAP Persistent Store wird ab Version 9.14.1 unterstützt.
- Für eine optimale Leistung sollten Sie den FPolicy-Server so konfigurieren, dass er sich im selben Subnetz wie das Speichersystem befindet.
- Ausführliche Best Practices und Empfehlungen zur Konfiguration der Workload Security FPolicy finden Sie unter"KB-Artikel zu Best Practices für FPolice" Die
- Sie müssen eine SVM mit einer der folgenden beiden Methoden hinzufügen:
  - Durch Verwendung der Cluster-IP, des SVM-Namens sowie des Benutzernamens und Kennworts für die Clusterverwaltung. ***Dies ist die empfohlene Methode.***
    - Der SVM-Name muss genau so lauten, wie er in ONTAP angezeigt wird, und die Groß-/Kleinschreibung muss beachtet werden.
  - Durch Verwendung von SVM Vserver Management IP, Benutzername und Passwort
  - Wenn Sie den vollständigen Benutzernamen und das Kennwort für die Cluster-/SVM-Verwaltung des Administrators nicht verwenden können oder möchten, können Sie einen benutzerdefinierten Benutzer mit geringeren Berechtigungen erstellen, wie im Abschnitt„Ein Hinweis zu Berechtigungen“ Abschnitt unten. Dieser benutzerdefinierte Benutzer kann entweder für den SVM- oder Cluster-Zugriff erstellt werden.
    - Alternativ können Sie einen AD-Benutzer mit einer Rolle verwenden, die mindestens die

Berechtigungen der Rolle „csrole“ besitzt, wie im Abschnitt „Hinweis zu Berechtigungen“ weiter unten beschrieben. Siehe auch die"ONTAP-Dokumentation" Die

- Stellen Sie sicher, dass die richtigen Anwendungen für die SVM eingestellt sind, indem Sie den folgenden Befehl ausführen:

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

Beispielausgabe:

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

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

  Das System gibt den VServer-Namen, den CIFS-Servernamen und zusätzliche Felder zurück.

- Legen Sie ein Kennwort für den SVM-Benutzer vsadmin fest. Wenn Sie einen benutzerdefinierten Benutzer oder einen Cluster-Administratorbenutzer verwenden, überspringen Sie diesen Schritt. clustershell:> `security login password -username vsadmin -vserver svmname`
- Entsperren Sie den SVM-Benutzer vsadmin für den externen Zugriff. Wenn Sie einen benutzerdefinierten Benutzer oder einen Cluster-Administratorbenutzer verwenden, überspringen Sie diesen Schritt. clustershell:> `security login unlock -username vsadmin -vserver svmname`
- Stellen Sie sicher, dass die Firewall-Richtlinie des Daten-LIF auf „mgmt“ (nicht „data“) eingestellt ist. Überspringen Sie diesen Schritt, wenn Sie zum Hinzufügen der SVM ein dediziertes Management-LIF verwenden. clustershell:> `network interface modify -lif <SVM_data_LIF_name> -firewall -policy mgmt`
- Wenn eine Firewall aktiviert ist, müssen Sie eine Ausnahme definiert haben, um TCP-Verkehr für den Port zuzulassen, der den Data ONTAP Data Collector verwendet.

  Sehen"Agentenanforderungen" für Konfigurationsinformationen. Dies gilt für lokale Agenten und in der Cloud installierte Agenten.

- Wenn ein Agent in einer AWS EC2-Instanz installiert wird, um eine Cloud ONTAP SVM zu überwachen, müssen sich Agent und Speicher im selben VPC befinden. Wenn sie sich in separaten VPCs befinden, muss eine gültige Route zwischen den VPCs vorhanden sein.

Testen der Konnektivität für Datensammler

Die Funktion zum Testen der Konnektivität (eingeführt im März 2025) soll Endbenutzern dabei helfen, die spezifischen Ursachen von Fehlern beim Einrichten von Datensammlern in Data Infrastructure Insights (DII) Workload Security zu identifizieren. Dadurch können die Benutzer Probleme im Zusammenhang mit der Netzwerkkommunikation oder fehlenden Rollen selbst beheben.

Mithilfe dieser Funktion können Benutzer vor dem Einrichten eines Datensammlers feststellen, ob alle netzwerkbezogenen Prüfungen durchgeführt wurden. Darüber hinaus werden Benutzer über die Funktionen informiert, auf die sie basierend auf der ONTAP Version, den Rollen und den ihnen in ONTAP zugewiesenen Berechtigungen zugreifen können.

Testkonnektivität wird für Benutzerverzeichnis-Collectors nicht unterstützt.

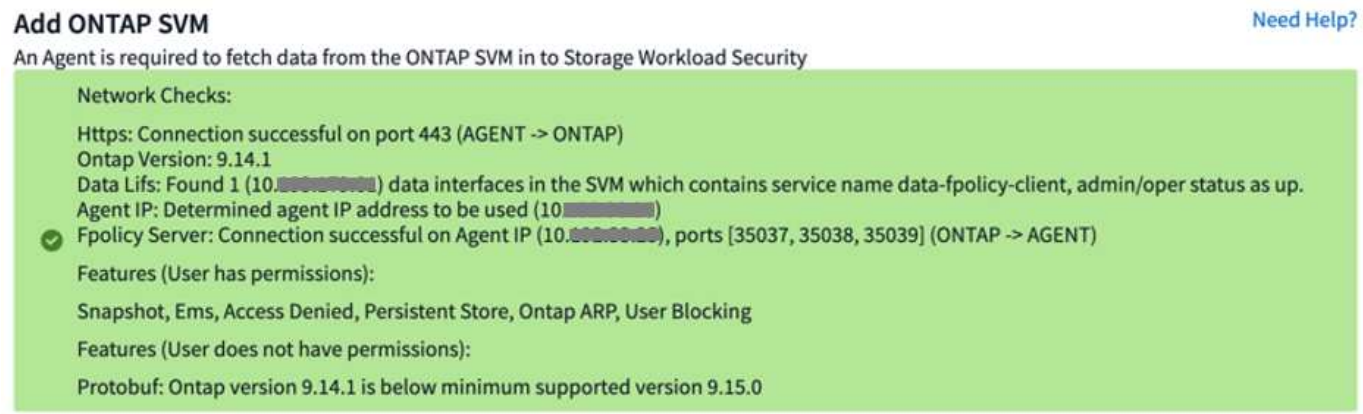
Voraussetzungen für den Verbindungstest

- Damit diese Funktion vollständig funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich.
- Die Überprüfung des Funktionszugriffs wird im SVM-Modus nicht unterstützt.
- Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.
- Wenn Sie einen benutzerdefinierten Benutzer verwenden (z. B. *csuser*), geben Sie die erforderlichen Berechtigungen und funktionsspezifischen Berechtigungen für die Funktionen an, die Sie verwenden möchten.

Lesen Sie unbedingt dieBerechtigungen Abschnitt weiter unten.

Testen der Verbindung

Der Benutzer kann zur Seite „Collector hinzufügen/bearbeiten“ gehen, die Details auf Clusterebene (im Clustermodus) oder auf SVM-Ebene (im SVM-Modus) eingeben und auf die Schaltfläche **Verbindung testen** klicken. Workload Security verarbeitet dann die Anfrage und zeigt eine entsprechende Erfolgs- oder Fehlermeldung an.



Wichtige Hinweise zu ONTAP Multi Admin Verify (MAV)

Einige Funktionen, wie das Erstellen und Löschen von Snapshots oder das Blockieren von Benutzern (SMB), funktionieren möglicherweise nicht basierend auf den in Ihrer Version von ONTAP hinzugefügten MAV-Befehlen.

Führen Sie die folgenden Schritte aus, um Ausnahmen zu Ihren MAV-Befehlen hinzuzufügen, die es Workload Security ermöglichen, Snapshots zu erstellen oder zu löschen und Benutzer zu blockieren.

Befehle zum Erstellen und Löschen von Snapshots:

```
multi-admin-verify rule modify -operation "volume snapshot create" -query
"-snapshot !*cloudsecure_*"
multi-admin-verify rule modify -operation "volume snapshot delete" -query
"-snapshot !*cloudsecure_*"
```

Befehl, um das Blockieren von Benutzern zu erlauben:

```
multi-admin-verify rule delete -operation set
```

Voraussetzungen für die Benutzerzugriffssperre

Beachten Sie Folgendes für"Sperrung des Benutzerzugriffs" :

Damit diese Funktion funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich.

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

Wenn Sie einen benutzerdefinierten Benutzer (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen verwenden, befolgen Sie die Schritte in"Sperrung des Benutzerzugriffs" um Workload Security die Berechtigung zum Blockieren von Benutzern zu erteilen.

Ein Hinweis zu Berechtigungen

Berechtigungen beim Hinzufügen über Cluster Management IP:

Wenn Sie den Clusterverwaltungsadministratorbenutzer nicht verwenden können, um Workload Security Zugriff auf den ONTAP SVM-Datensammler zu gewähren, können Sie einen neuen Benutzer namens „csuser“ mit den in den folgenden Befehlen gezeigten Rollen erstellen. Verwenden Sie den Benutzernamen „csuser“ und das Kennwort für „csuser“, wenn Sie den Workload Security-Datenkollektor für die Verwendung der Cluster Management-IP konfigurieren.

Hinweis: Sie können eine einzelne Rolle erstellen, die für alle Funktionsberechtigungen eines benutzerdefinierten Benutzers verwendet wird. Wenn ein Benutzer vorhanden ist, löschen Sie zuerst den vorhandenen Benutzer und die Rolle mit diesen Befehlen:

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

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

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
security login role create -role csrole -cmddirname "cluster application-
record" -access all
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
security login create -user-or-group-name csuser -application http
-authmethod password -role csrole
```

Berechtigungen beim Hinzufügen über Vserver Management IP:

Wenn Sie den Clusterverwaltungsadministratorbenutzer nicht verwenden können, um Workload Security Zugriff auf den ONTAP SVM-Datensammler zu gewähren, können Sie einen neuen Benutzer namens „csuser“ mit den in den folgenden Befehlen gezeigten Rollen erstellen. Verwenden Sie den Benutzernamen „csuser“ und das Kennwort für „csuser“, wenn Sie den Workload Security-Datensammler für die Verwendung der Vserver Management IP konfigurieren.

Hinweis: Sie können eine einzelne Rolle erstellen, die für alle Funktionsberechtigungen eines benutzerdefinierten Benutzers verwendet wird. Wenn ein Benutzer vorhanden ist, löschen Sie zuerst den vorhandenen Benutzer und die Rolle mit diesen Befehlen:

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

Um den neuen Benutzer zu erstellen, melden Sie sich mit dem Benutzernamen/Passwort des Clusterverwaltungsadministrators bei ONTAP an und führen Sie die folgenden Befehle auf dem ONTAP Server aus. Kopieren Sie diese Befehle der Einfachheit halber in einen Texteditor und ersetzen Sie <vservername> durch Ihren Vserver-Namen, bevor Sie diese Befehle auf ONTAP ausführen:

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

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

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

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

Protobuf-Modus

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

Weitere Einzelheiten zu dieser Funktion finden Sie im"ONTAP-Dokumentation" .

Für protobuf sind bestimmte Berechtigungen erforderlich (einige oder alle davon sind möglicherweise bereits vorhanden):

Cluster-Modus:

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
VServer-Modus:
```

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

Berechtigungen für ONTAP Autonomous Ransomware Protection und ONTAP Access Denied

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

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

Weitere Informationen finden Sie unter"Integration mit ONTAP Access Denied"

Und"Integration mit ONTAP Autonomous Ransomware Protection"

Konfigurieren des Datensammlers

Schritte zur Konfiguration

1. Melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
2. Klicken Sie auf **Workload-Sicherheit > Collectors > +Datensammler**

   Das System zeigt die verfügbaren Datensammler an.

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

   Das System zeigt die ONTAP SVM-Konfigurationsseite an. Geben Sie für jedes Feld die erforderlichen Daten ein.

Feld	Beschreibung
Name	Eindeutiger Name für den Datensammler
Agent	Wählen Sie einen konfigurierten Agenten aus der Liste aus.
Verbindung über Management-IP für:	Wählen Sie entweder Cluster-IP oder SVM-Verwaltungs-IP
Cluster-/SVM-Verwaltungs-IP-Adresse	Die IP-Adresse für den Cluster oder die SVM, abhängig von Ihrer obigen Auswahl.
Name SVM	Der Name der SVM (dieses Feld ist erforderlich, wenn eine Verbindung über die Cluster-IP hergestellt wird)
Benutzername	Benutzername für den Zugriff auf SVM/Cluster. Beim Hinzufügen über die Cluster-IP sind die Optionen: 1. Cluster-Administrator 2. 'csuser' 3. AD-Benutzer mit ähnlicher Rolle wie csuser. Beim Hinzufügen über die SVM-IP sind die Optionen: 4. vsadmin 5. 'csuser' 6. AD-Benutzername mit ähnlicher Rolle wie csuser.
Passwort	Passwort für den oben genannten Benutzernamen

Filtern von Anteilen/Volumes	Wählen Sie, ob Freigaben/Volumes in die Ereigniserfassung einbezogen oder ausgeschlossen werden sollen
Geben Sie die vollständigen Freigabenamen ein, die ausgeschlossen/eingeschlossen werden sollen	Durch Kommas getrennte Liste von Freigaben, die (je nach Bedarf) aus der Ereignissammlung ausgeschlossen oder eingeschlossen werden sollen
Geben Sie vollständige Volumenamen ein, die ausgeschlossen/eingeschlossen werden sollen	Durch Kommas getrennte Liste der Datenträger, die (je nach Bedarf) von der Ereigniserfassung ausgeschlossen oder eingeschlossen werden sollen
Ordnerzugriff überwachen	Wenn diese Option aktiviert ist, werden Ereignisse für die Ordnerzugriffsüberwachung aktiviert. Beachten Sie, dass das Erstellen/Umbenennen und Löschen von Ordnern auch ohne Auswahl dieser Option überwacht wird. Durch die Aktivierung wird die Anzahl der überwachten Ereignisse erhöht.
ONTAP Sendepuffergröße festlegen	Legt die Größe des ONTAP Fpolicy-Sendepuffers fest. Wenn eine ONTAP Version vor 9.8p7 verwendet wird und Leistungsprobleme auftreten, kann die Größe des ONTAP Sendepuffers geändert werden, um die ONTAP Leistung zu verbessern. Wenden Sie sich an den NetApp -Support, wenn Sie diese Option nicht sehen und sie ausprobieren möchten.

Nach Abschluss

- Verwenden Sie auf der Seite „Installierte Datensammler“ das Optionsmenü rechts neben jedem Sammler, um den Datensammler zu bearbeiten. Sie können den Datensammler neu starten oder die Konfigurationsattribute des Datensammlers bearbeiten.

Empfohlene Konfiguration für MetroCluster

Folgendes wird für MetroCluster empfohlen:

1. Verbinden Sie zwei Datensammler, einen mit dem Quell-SVM und einen mit dem Ziel-SVM.
2. Die Datensammler sollten über *Cluster-IP* verbunden sein.
3. Der Datensammler des aktuell „laufenden“ SVM wird jederzeit als „*Läuft*“ angezeigt. Der aktuell „gestoppte“ Datensammler des SVM wird als *Gestoppt* angezeigt.
4. Bei jeder Umschaltung ändert sich der Status des Datensammlers von *Läuft* zu *Gestoppt* und umgekehrt.
5. Es dauert bis zu zwei Minuten, bis der Datensammler vom Status „Gestoppt“ in den Status „Läuft“ wechselt.

Servicerichtlinie

Wenn Sie die Servicerichtlinie mit ONTAP **Version 9.9.1 oder neuer** verwenden, ist zum Herstellen einer Verbindung mit dem Data Source Collector 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 ONTAP -Versionen vor 9.9.1 muss *data-fpolicy-client* nicht festgelegt werden.

Play-Pause-Datensammler

Wenn sich der Datensammler im Status „Wird ausgeführt“ befindet, können Sie die Sammlung anhalten. Öffnen Sie das „Drei-Punkte“-Menü für den Collector und wählen Sie PAUSE. Während der Collector angehalten ist, werden keine Daten von ONTAP gesammelt und keine Daten vom Collector an ONTAP gesendet. Dies bedeutet, dass keine Fpolicy-Ereignisse von ONTAP zum Datensammler und von dort zu Data Infrastructure Insights fließen.

Beachten Sie, dass Workload Security die Daten nicht sammelt, wenn auf ONTAP neue Volumes usw. erstellt werden, während der Collector angehalten ist, und dass diese Volumes usw. nicht in Dashboards oder Tabellen angezeigt werden.

Ein Collector kann nicht angehalten werden, wenn er über eingeschränkte Benutzer verfügt. Stellen Sie den Benutzerzugriff wieder her, bevor Sie den Collector anhalten.

Beachten Sie Folgendes:

- Gemäß den für einen angehaltenen Collector konfigurierten Einstellungen wird keine Snapshot-Bereinigung durchgeführt.
- EMS-Ereignisse (wie ONTAP ARP) werden auf einem pausierten Collector nicht verarbeitet. Das bedeutet, wenn ONTAP einen Dateimanipulationsangriff erkennt, kann Data Infrastructure Insights Workload Security dieses Ereignis nicht erfassen.
- Für einen pausierten Collector werden KEINE E-Mails mit Gesundheitsbenachrichtigungen gesendet.
- Manuelle oder automatische Aktionen (wie Snapshot oder Benutzerblockierung) werden bei einem angehaltenen Collector nicht unterstützt.
- Bei Agent- oder Collector-Upgrades, Neustarts/Neustarts der Agent-VM oder Neustarts des Agent-Dienstes bleibt ein angehaltener Collector im Status *Angehalten*.
- Wenn sich der Datensammler im Status *Fehler* befindet, kann der Sammler nicht in den Status *Pausiert* geändert werden. Die Schaltfläche „Pause“ wird nur aktiviert, wenn der Status des Collectors „Wird ausgeführt“ ist.
- Wenn die Verbindung zum Agenten getrennt wird, kann der Collector nicht in den Status *Pausiert* versetzt werden. Der Collector wechselt in den Status „Gestoppt“ und die Schaltfläche „Pause“ wird deaktiviert.

Persistenter Speicher

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

Der persistente Speicher kann durch Aktivieren des Kontrollkästchens auf der Seite „Bearbeiten/Hinzufügen“ des Collectors aktiviert werden. Nach dem Aktivieren des Kontrollkästchens wird ein Textfeld zur Annahme des Datenträgernamens angezeigt. Der Volumename ist ein Pflichtfeld zum Aktivieren des persistenten Speichers.

- Für ONTAP 9.14.1 müssen Sie das Volume vor der Aktivierung der Funktion erstellen und im Feld *Volume Name* denselben Namen angeben. Die empfohlene Volumegröße beträgt 16 GB.
- Für ONTAP 9.15.1 wird das Volume vom Collector automatisch mit einer Größe von 16 GB erstellt, wobei der im Feld *Volume Name* angegebene Name verwendet wird.

Für den persistenten Speicher sind bestimmte Berechtigungen erforderlich (einige oder alle davon sind möglicherweise bereits vorhanden):

Cluster-Modus:

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

VServer-Modus:

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

Migrieren von Collectoren

Sie können einen Workload Security-Collector problemlos von einem Agenten auf einen anderen migrieren und so einen effizienten Lastenausgleich der Collector-Instanzen zwischen den Agenten ermöglichen.

Voraussetzungen

- Der Quellagent muss sich im Status *verbunden* befinden.
- Der zu migrierende Collector muss sich im Status „Laufend“ befinden.

Hinweis:

- Migrate wird sowohl für Daten- als auch für Benutzerverzeichnis-Sammler unterstützt.
- Die Migration eines Collectors wird für manuell verwaltete Mandanten nicht unterstützt.

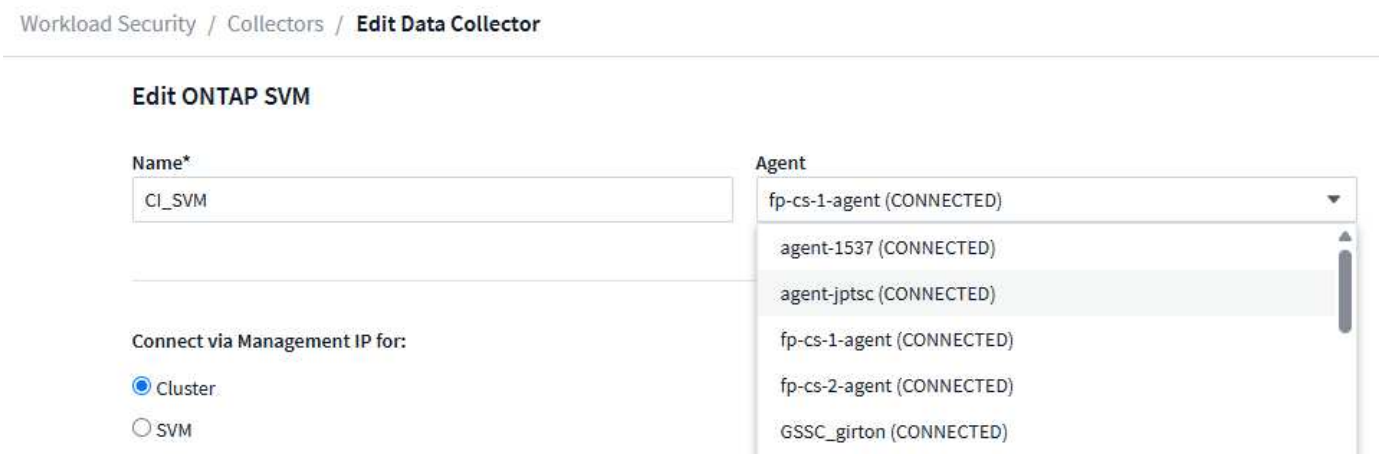
Migrieren des Collectors

Um einen Collector zu migrieren, führen Sie die folgenden Schritte aus:

1. Gehen Sie zur Seite „Collector bearbeiten“.
2. Wählen Sie einen Zielagenten aus der Agenten-Dropdownliste aus.
3. Klicken Sie auf die Schaltfläche „Collector speichern“.

Workload Security verarbeitet die Anfrage. Nach erfolgreicher Migration wird der Benutzer zur Seite mit der Sammlerliste weitergeleitet. Im Fehlerfall wird auf der Bearbeitungsseite eine entsprechende Meldung angezeigt.

Hinweis: Alle zuvor auf der Seite „Collector bearbeiten“ vorgenommenen Konfigurationsänderungen bleiben auch nach der erfolgreichen Migration des Collectors zum Zielagenten wirksam.



Fehlerbehebung

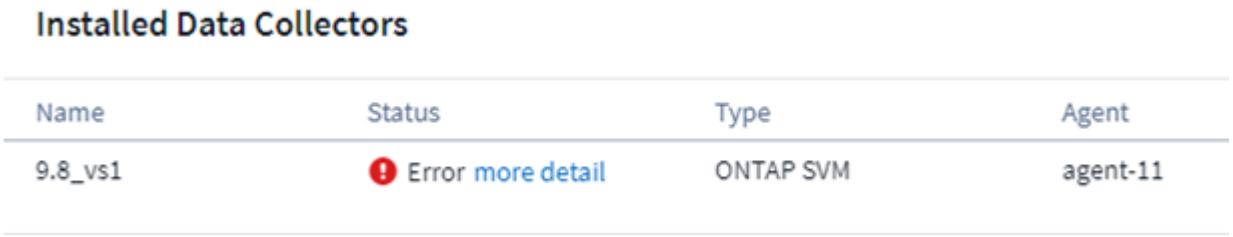
Siehe die"Fehlerbehebung beim SVM Collector" Seite für Tipps zur Fehlerbehebung.

Fehlerbehebung beim ONTAP SVM Data Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen. Hier finden Sie Tipps zur Behebung von Problemen mit diesem Collector.

Siehe die"Konfigurieren des SVM-Collectors" Seite für Anweisungen zum Konfigurieren dieses Collectors.

Im Falle eines Fehlers können Sie auf der Seite „Installierte Datensammler“ in der Spalte „Status“ auf „Weitere Details“ klicken, um Einzelheiten zum Fehler anzuzeigen.



Bekannte Probleme und deren Lösungen werden unten beschrieben.

Problem: Der Datensammler läuft eine Zeit lang und stoppt nach einer zufälligen Zeit mit der Fehlermeldung: „Fehlermeldung: Connector befindet sich im Fehlerzustand.“ Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server überlastet." **Versuchen Sie Folgendes:** Die Ereignisrate von ONTAP war viel höher als das, was die Agent-Box verarbeiten kann. Daher wurde die Verbindung beendet.

Überprüfen Sie den Spitzenverkehr in CloudSecure, als die Verbindung getrennt wurde. Dies können Sie auf der Seite **CloudSecure > Aktivitätsforensik > Alle Aktivitäten** überprüfen.

Wenn der aggregierte Spitzenverkehr höher ist als das, was die Agent Box verarbeiten kann, lesen Sie auf der

Seite „Event Rate Checker“ nach, wie Sie die Größe für die Collector-Bereitstellung in einer Agent Box festlegen.

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
```

Starten Sie den Collector nach der Größenänderung über die Benutzeroberfläche neu.

{leer}

Problem: Der Collector meldet die Fehlermeldung: „Auf dem Connector wurde keine lokale IP-Adresse gefunden, die die Datenschnittstellen der SVM erreichen kann.“ **Versuchen Sie Folgendes:** Dies liegt höchstwahrscheinlich an einem Netzwerkproblem auf der ONTAP Seite. Bitte befolgen Sie diese Schritte:

1. Stellen Sie sicher, dass auf der SVM-Daten- oder Verwaltungsebene keine Firewalls vorhanden sind, die die Verbindung von der SVM blockieren.
2. Wenn Sie eine SVM über eine Cluster-Management-IP hinzufügen, stellen Sie sicher, dass die Datenlebensdauer und die Managementlebensdauer der SVM von der Agent-VM aus pingbar sind. Überprüfen Sie bei Problemen das Gateway, die Netzmaske und die Routen für das Leben.

   Sie können auch versuchen, sich über SSH mit der Cluster-Verwaltungs-IP beim Cluster anzumelden und die Agent-IP anzupingen. Stellen Sie sicher, dass die Agent-IP pingbar ist:

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

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.
3. Wenn Sie versucht haben, eine Verbindung über die Cluster-IP herzustellen, und dies nicht funktioniert hat, versuchen Sie, eine direkte Verbindung über die SVM-IP herzustellen. Die Schritte zum Herstellen einer Verbindung über die SVM-IP finden Sie oben.
4. Überprüfen Sie beim Hinzufügen des Collectors über die SVM-IP und die VSadmin-Anmeldeinformationen, ob für SVM Lif die Rolle „Data plus Mgmt“ aktiviert ist. In diesem Fall funktioniert ein Ping zum SVM Lif, ein SSH zum SVM Lif funktioniert jedoch nicht. Wenn ja, erstellen Sie ein SVM Mgmt Only Lif und versuchen Sie, über dieses SVM Management Only Lif eine Verbindung herzustellen.
5. Wenn es immer noch nicht funktioniert, erstellen Sie ein neues SVM-Lif und versuchen Sie, über dieses Lif eine Verbindung herzustellen. Stellen Sie sicher, dass die Subnetzmaske richtig eingestellt ist.
6. Erweitertes Debuggen:
   a. Starten Sie eine Paketverfolgung in ONTAP.
   b. Versuchen Sie, einen Datensammler über die CloudSecure-Benutzeroberfläche mit dem SVM zu verbinden.

c. Warten Sie, bis der Fehler auftritt. Stoppen Sie die Paketverfolgung in ONTAP.

d. Öffnen Sie die Paketverfolgung von ONTAP. Es ist an diesem Standort verfügbar

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Stellen Sie sicher, dass ein SYN von ONTAP zur Agent-Box vorhanden
ist.
.. Wenn kein SYN von ONTAP vorhanden ist, liegt ein Problem mit der
Firewall in ONTAP vor.
.. Öffnen Sie die Firewall in ONTAP, damit ONTAP eine Verbindung zur
Agent-Box herstellen kann.
```

7. Wenn es immer 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 keine der oben genannten Maßnahmen das Problem löst, eröffnen Sie einen Fall bei"Netapp-Support" für weitere Unterstützung.

{leer}

Problem: Meldung: „ ONTAP -Typ für [Hostname: <IP-Adresse>] konnte nicht ermittelt werden. Grund: Verbindungsfehler zum Speichersystem <IP-Adresse>: Host ist nicht erreichbar (Host nicht erreichbar)" **Versuchen Sie Folgendes:**

1. Überprüfen Sie, ob die richtige SVM-IP-Verwaltungsadresse oder Cluster-Verwaltungs-IP angegeben wurde.
2. Stellen Sie per SSH eine Verbindung zum SVM oder Cluster her, zu dem Sie eine Verbindung herstellen möchten. Sobald Sie verbunden sind, stellen Sie sicher, dass der SVM- oder Clustername korrekt ist.

{leer}

Problem: Fehlermeldung: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server beendet." **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich blockiert eine Firewall die erforderlichen Ports auf dem Agent-Computer. Überprüfen Sie, ob der Portbereich 35000–55000/TCP für die Agent-Maschine geöffnet ist, damit sie eine Verbindung vom SVM herstellen kann. Stellen Sie außerdem sicher, dass auf der ONTAP -Seite keine Firewalls aktiviert sind, die die Kommunikation mit dem Agent-Computer blockieren.
2. Geben Sie den folgenden Befehl in das Agent-Feld ein und stellen Sie sicher, dass der Portbereich geöffnet ist.

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

   Die Beispielausgabe sollte folgendermaßen aussehen:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
NEW -j ACCEPT
. Melden Sie sich bei SVM an, geben Sie die folgenden Befehle ein und
überprüfen Sie, dass keine Firewall eingerichtet ist, die die
Kommunikation mit ONTAP blockiert.
```

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

"Firewall-Befehle prüfen"auf der ONTAP -Seite.

3. Stellen Sie per SSH eine Verbindung zum SVM/Cluster her, den Sie überwachen möchten. Pingen Sie die Agent-Box vom SVM-Datenlebenszyklus aus (mit Unterstützung für CIFS- und NFS-Protokolle) und stellen Sie sicher, dass der Ping funktioniert:

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

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.

4. Wenn ein einzelner SVM über zwei Datensammler zweimal zu einem Mandanten hinzugefügt wird, wird dieser Fehler angezeigt. Löschen Sie einen der Datensammler über die Benutzeroberfläche. Starten Sie dann den anderen Datensammler über die Benutzeroberfläche neu. Anschließend zeigt der Datensammler den Status „RUNNING“ an und beginnt mit dem Empfang von Ereignissen vom SVM.

   Grundsätzlich sollte in einem Mandanten 1 SVM nur einmal über 1 Datensammler hinzugefügt werden. 1 SVM sollte nicht zweimal über 2 Datensammler hinzugefügt werden.

5. In Fällen, in denen dieselbe SVM in zwei verschiedenen Workload Security-Umgebungen (Mandanten) hinzugefügt wurde, ist die letzte immer erfolgreich. Der zweite Collector konfiguriert fpolicy mit seiner eigenen IP-Adresse und wirft den ersten raus. Der Collector im ersten empfängt also keine Ereignisse mehr und sein „Audit“-Dienst wechselt in einen Fehlerzustand. Um dies zu verhindern, konfigurieren Sie jede SVM in einer einzelnen Umgebung.
6. Dieser Fehler kann auch auftreten, wenn die Servicerichtlinien nicht richtig konfiguriert sind. Um bei ONTAP 9.8 oder höher eine Verbindung zum Data Source Collector herzustellen, ist der Dienst data-fpolicy-client zusammen mit dem Datendienst data-nfs und/oder data-cifs erforderlich. Darüber hinaus muss der Dienst „data-fpolicy-client“ mit den Datenlebensdauern für die überwachte SVM verknüpft werden.

{leer}

Problem: Auf der Aktivitätsseite wurden keine Ereignisse angezeigt. **Versuchen Sie Folgendes:**

1. Überprüfen Sie, ob sich der ONTAP Collector im Status „RUNNING“ befindet. Wenn ja, stellen Sie sicher, dass einige CIFS-Ereignisse auf den CIFS-Client-VMs generiert werden, indem Sie einige Dateien öffnen.

2. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an und geben Sie den folgenden Befehl ein.

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

   Bitte stellen Sie sicher, dass keine Fehler im Zusammenhang mit fpolicy vorliegen.

3. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an. Geben Sie den folgenden Befehl ein:

   ```
   <SVM>fpolicy show
   ```

   Überprüfen Sie, ob die fpolicy-Richtlinie mit dem Präfix „cloudsecure_“ festgelegt wurde und der Status „Ein“ ist. Wenn nicht festgelegt, kann der Agent die Befehle im SVM höchstwahrscheinlich nicht ausführen. Bitte stellen Sie sicher, dass alle Voraussetzungen, wie am Anfang der Seite beschrieben, erfüllt sind.

{leer}

Problem: Der SVM-Datensammler befindet sich im Fehlerzustand und die Fehlermeldung lautet „Der Agent konnte keine Verbindung zum Sammler herstellen.“ **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich ist der Agent überlastet und kann keine Verbindung zu den Datenquellen-Sammlern 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 Benutzeroberfläche.
4. Wenn die Anzahl der Aktivitäten pro Sekunde sehr hoch ist, installieren Sie einen anderen Agenten und verschieben Sie einige der Datenquellensammler auf den neuen Agenten.

{leer}

Problem: SVM Data Collector zeigt die Fehlermeldung „fpolicy.server.connectError: Knoten konnte keine Verbindung mit dem FPolicy-Server „12.195.15.146“ herstellen (Grund: „Select Timed out“)“ an. **Versuchen Sie Folgendes:** Die Firewall ist in SVM/Cluster aktiviert. Daher kann die fpolicy-Engine keine Verbindung zum fpolicy-Server herstellen. CLIs in ONTAP , die zum Abrufen weiterer Informationen verwendet werden können, sind:

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

"Firewall-Befehle prüfen"auf der ONTAP -Seite.

{leer}

Problem: Fehlermeldung: „Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Auf der SVM wurde keine gültige Datenschnittstelle (Rolle: Daten, Datenprotokolle: NFS oder CIFS oder beide, Status: aktiv) gefunden.“ **Versuchen Sie Folgendes:** Stellen Sie sicher, dass eine funktionsfähige Schnittstelle vorhanden ist (mit der Rolle „Daten“ und dem Datenprotokoll „CIFS/NFS“).

{leer}

Problem: Der Datensammler wechselt in den Fehlerzustand und nach einiger Zeit in den RUNNING-Zustand und dann wieder zurück in den Fehlerzustand. Dieser Zyklus wiederholt sich. **Versuchen Sie Folgendes:** Dies geschieht normalerweise im folgenden Szenario:

1. Es wurden mehrere Datensammler hinzugefügt.
2. Den Datensammlern, die dieses Verhalten zeigen, wird 1 SVM hinzugefügt. Das bedeutet, dass zwei oder mehr Datensammler mit einem SVM verbunden sind.
3. Stellen Sie sicher, dass 1 Datensammler nur mit 1 SVM verbunden ist.
4. Löschen Sie die anderen Datensammler, die mit derselben SVM verbunden sind.

{leer}

Problem: Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren (Richtlinie auf SVM svmname). Grund: Ungültiger Wert für das Element „shares-to-include“ in „fpolicy.policy.scope-modify: „Federal“ angegeben. **Versuchen Sie Folgendes:** *Die Freigabenamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die ONTAP SVM DSC-Konfiguration, um die Freigabenamen zu korrigieren.

Freigaben einschließen und ausschließen ist nicht für eine lange Liste von Freigabenamen vorgesehen. Verwenden Sie stattdessen die Filterung nach Volumen, wenn Sie eine große Anzahl von Aktien ein- oder ausschließen möchten.

{leer}

Problem: Es gibt im Cluster vorhandene fpolicies, die nicht verwendet werden. Was sollte vor der Installation von Workload Security damit geschehen? **Versuchen Sie Folgendes:** Es wird empfohlen, alle vorhandenen, nicht verwendeten fpolicy-Einstellungen zu löschen, auch wenn sie getrennt sind. Workload Security erstellt fpolicy mit dem Präfix „cloudsecure_“. Alle anderen nicht verwendeten fpolicy-Konfigurationen können gelöscht werden.

CLI-Befehl zum Anzeigen der fpolicy-Liste:

```
 fpolicy show
Schritte zum Löschen von fpolicy-Konfigurationen:
```

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

{leer}

Problem: Nach Aktivierung der Workload-Sicherheit wird die ONTAP Performance beeinträchtigt: Die Latenz steigt sporadisch stark an, die IOPS sinken sporadisch stark ab. **Probieren Sie Folgendes aus:** Bei der Verwendung von ONTAP mit Workload Security können gelegentlich Latenzprobleme in ONTAP auftreten. Dafür gibt es eine Reihe möglicher Gründe, wie im Folgenden erläutert wird:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" Die Alle diese Probleme wurden in ONTAP 9.13.1 und höher behoben. Es wird dringend empfohlen, eine dieser neueren Versionen zu verwenden.

{leer}

Problem: Der Datensammler zeigt die Fehlermeldung an: „Fehler: Der Zustand des Sammlers konnte innerhalb von 2 Versuchen nicht ermittelt werden. Versuchen Sie, den Sammler erneut neu zu starten (Fehlercode: AGENT008)“. **Versuchen Sie Folgendes:**

1. Scrollen Sie auf der Seite „Datensammler“ nach rechts neben den Datensammler, der den Fehler ausgibt, und klicken Sie auf das Menü mit den drei Punkten. Wählen Sie *Bearbeiten*. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche *Speichern* klicken. Data Collector wird neu gestartet und der Fehler sollte behoben sein.
2. Die Agent-Maschine verfügt möglicherweise nicht über genügend CPU- oder RAM-Reserve, weshalb die DSCs ausfallen. Bitte überprüfen Sie die Anzahl der Datensammler, die dem Agenten auf der Maschine hinzugefügt wurden. Wenn es mehr als 20 sind, erhöhen Sie bitte die CPU- und RAM-Kapazität der Agent-Maschine. Sobald die CPU und der RAM erhöht werden, wechseln die DSCs automatisch in den Initialisierungs- und dann in den Ausführungszustand. Schauen Sie in die Größentabelle auf"diese Seite" .

{leer}

Problem: Der Datensammler gibt einen Fehler aus, wenn der SVM-Modus ausgewählt ist. **Versuchen Sie Folgendes:** Wenn beim Verbinden im SVM-Modus die Cluster-Management-IP anstelle der SVM-Management-IP zum Verbinden verwendet wird, tritt ein Verbindungsfehler auf. Stellen Sie sicher, dass die richtige SVM-IP verwendet wird.

{leer}

Problem: Der Datensammler zeigt eine Fehlermeldung an, wenn die Funktion „Zugriff verweigert“ aktiviert ist: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren von fpolicy auf SVM test_svm. Grund: Der Benutzer ist nicht autorisiert." **Versuchen Sie**

Folgendes: Dem Benutzer fehlen möglicherweise die REST-Berechtigungen, die für die Funktion „Zugriff verweigert“ erforderlich sind. Bitte folgen Sie den Anweisungen auf"diese Seite" um die Berechtigungen festzulegen.

Starten Sie den Collector neu, sobald die Berechtigungen festgelegt sind.

{leer}

Problem: Der Collector befindet sich im Fehlerzustand mit der Meldung: Connector befindet sich im Fehlerzustand. Grund für den Fehler: Konfiguration des persistenten Speichers auf SVM <SVM-Name> fehlgeschlagen. Grund: Es konnte kein geeignetes Aggregat für das Volumen "<volumeName>" in der SVM "<SVM Name>" gefunden werden. Grund: Leistungsdaten für das Aggregat "<aggregateName>" sind derzeit nicht verfügbar. Warten Sie ein paar Minuten und versuchen Sie den Befehl erneut. Dienstname: Audit. Fehlergrund: Fehler beim Konfigurieren des persistenten Speichers auf der SVM <SVM name="">.</SVM> Ursache: Es konnte kein passendes Aggregat für Volume "<volumeName>" in der SVM "<SVM name=""></SVM></volumeName>gefunden werden". Ursache: Performance-Informationen für das Aggregat "<aggregateName>" sind derzeit nicht verfügbar.</aggregateName> Warten Sie einige Minuten, und versuchen Sie es erneut.

Versuchen Sie Folgendes: Warten Sie einige Minuten und starten Sie dann den Collector neu.

{leer}

Wenn weiterhin Probleme auftreten, verwenden Sie die Support-Links auf der Seite **Hilfe > Support**.

Konfigurieren des Cloud Volumes ONTAP und Amazon FSx for NetApp ONTAP

Überwachen Sie den Datei- und Benutzerzugriff in Ihrer Cloud-Speicherinfrastruktur, indem Sie Workload Security-Datensammler für Cloud Volumes ONTAP und Amazon FSx for NetApp ONTAP konfigurieren. Dieser Leitfaden bietet eine Schritt-für-Schritt-Anleitung zum Bereitstellen von Agents in AWS und zum Verbinden dieser Agents mit Ihren Cloud-Speicherinstanzen.

Cloud Volumes ONTAP Speicherkonfiguration

Informationen zum Konfigurieren einer AWS-Instanz mit einem einzelnen Knoten/HA zum Hosten des Workload Security Agent finden Sie in der OnCommand Cloud Volumes ONTAP Dokumentation:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Nachdem die Konfiguration abgeschlossen ist, befolgen Sie die Schritte zum Einrichten Ihres SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Unterstützte Plattformen

- Cloud Volumes ONTAP, wird von allen verfügbaren Cloud-Service-Anbietern unterstützt, sofern verfügbar. Zum Beispiel: Amazon, Azure, Google Cloud.
- ONTAP Amazon FSx

Agent-Computerkonfiguration

Die Agent-Maschine muss in den jeweiligen Subnetzen der Cloud-Dienstanbieter konfiguriert werden. Weitere Informationen zum Netzwerkzugriff finden Sie in den [Agentenanforderungen].

Nachfolgend finden Sie die Schritte zur Agenteninstallation in AWS. Für die Installation können in Azure oder Google Cloud die entsprechenden Schritte ausgeführt werden, sofern diese für den Cloud-Dienstanbieter gelten.

Führen Sie in AWS die folgenden Schritte aus, um die Maschine für die Verwendung als Workload Security Agent zu konfigurieren:

Führen Sie die folgenden Schritte aus, um die Maschine für die Verwendung als Workload Security Agent zu konfigurieren:

Schritte

1. Melden Sie sich bei der AWS-Konsole an, navigieren Sie zur Seite „EC2-Instances“ und wählen Sie „Instanz starten“ aus.
2. Wählen Sie ein RHEL- oder CentOS-AMI mit der entsprechenden Version aus, wie auf dieser Seite erwähnt:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Wählen Sie die VPC und das Subnetz aus, in denen sich die Cloud ONTAP -Instanz befindet.
4. Wählen Sie *t2.xlarge* (4 vcpus und 16 GB RAM) als zugewiesene Ressourcen.
    a. Erstellen Sie die EC2-Instanz.
5. Installieren Sie die erforderlichen Linux-Pakete mit dem YUM-Paketmanager:
    a. Installieren Sie *wget* und *unzip* native Linux-Pakete.

Installieren des Workload Security Agent

1. Melden Sie sich als Administrator oder Kontoinhaber bei Ihrer Data Infrastructure Insights Umgebung an.
2. Navigieren Sie zu Workload Security **Collectors** und klicken Sie auf die Registerkarte **Agents**.
3. Klicken Sie auf **+Agent** und geben Sie RHEL als Zielplattform an.
4. Kopieren Sie den Befehl zur Agenteninstallation.
5. Fügen Sie den Agent-Installationsbefehl in die RHEL EC2-Instanz ein, bei der Sie angemeldet sind. Dadurch wird der Workload Security-Agent installiert, der alle"Agentenvoraussetzungen" erfüllt sind.

Detaillierte Schritte finden Sie unter diesem Link: https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Fehlerbehebung

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

Problem	Auflösung

Der Datensammler zeigt den Fehler „Workload-Sicherheit: ONTAP -Typ für Amazon FxSN-Datensammler konnte nicht ermittelt werden“ an. Der Kunde kann keinen neuen Amazon FSxN-Datensammler zu Workload Security hinzufügen. Bei der Verbindung vom Agenten zum FSxN-Cluster auf Port 443 kommt es zu einer Zeitüberschreitung. Für Firewall- und AWS-Sicherheitsgruppen sind die erforderlichen Regeln aktiviert, um die Kommunikation zu ermöglichen. Ein Agent ist bereits bereitgestellt und befindet sich auch im selben AWS-Konto. Derselbe Agent wird zum Verbinden und Überwachen der verbleibenden NetApp -Geräte verwendet (und alle funktionieren).	Lösen Sie dieses Problem, indem Sie der Sicherheitsregel des Agenten das LIF-Netzwerksegment fsxadmin hinzufügen. Alle Ports zulassen, wenn Sie sich bei den Ports nicht sicher sind.

Benutzerverwaltung

Workload Security-Benutzerkonten werden über Data Infrastructure Insights verwaltet.

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

Rolle	Workload-Sicherheitszugriff
Administrator	Kann alle Workload-Sicherheitsfunktionen ausführen, einschließlich der Funktionen für Warnungen, Forensik, Datensammler, Richtlinien für automatisierte Reaktionen und APIs für Workload-Sicherheit. Ein Administrator kann auch andere Benutzer einladen, aber nur Workload-Sicherheitsrollen zuweisen.
Benutzer	Kann Warnungen anzeigen und verwalten sowie forensische Daten anzeigen. Die Benutzerrolle kann den Alarmstatus ändern, eine Notiz hinzufügen, manuell Schnappschüsse machen und den Benutzerzugriff einschränken.
Gast	Kann Warnungen und Forensik anzeigen. Mit der Gastrolle können Sie den Alarmstatus nicht ändern, keine Notiz hinzufügen, manuell Schnappschüsse 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 Benutzerverwaltungsseite von Data Infrastructure Insights weitergeleitet.

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

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

Weitere Informationen zu Benutzerkonten und Rollen finden Sie in den Data Infrastructure Insights"Benutzerrolle" Dokumentation.

Event Rate Checker: Leitfaden zur Agentengröße

Ermitteln Sie die optimale Größe der Agentenmaschinen, indem Sie die von Ihren SVMs generierten NFS- und SMB-Ereignisraten vor der Bereitstellung der Datensammler messen. Das Skript zur Überprüfung der Ereignisrate hilft Ihnen, die Kapazitätsgrenzen (maximal 50 Datensammler pro Agent) zu verstehen und sicherzustellen, dass Ihre Agenteninfrastruktur das erwartete Ereignisvolumen für eine zuverlässige Bedrohungserkennung bewältigen kann.

Anforderungen:

- Cluster-IP
- Benutzername und Kennwort des Clusteradministrators

Beim Ausführen dieses Skripts sollte kein ONTAP SVM Data Collector für die SVM ausgeführt werden, für die die Ereignisrate bestimmt wird.

Schritte:

1. Installieren Sie den Agenten, indem Sie den Anweisungen in CloudSecure folgen.
2. Sobald der Agent installiert ist, führen Sie das Skript *server_data_rate_checker.sh* als Sudo-Benutzer aus:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Für dieses Skript muss _sshpass_ auf der Linux-Maschine installiert
sein.  Es gibt zwei Möglichkeiten, es zu installieren:
```

   a. Führen Sie den folgenden Befehl aus:

```
 linux_prompt> yum install sshpass
.. Wenn das nicht funktioniert, laden Sie _sshpass_ aus dem Internet
auf die Linux-Maschine 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 finden Sie unten.
4. Die Ausführung des Skripts dauert ungefähr 5 Minuten.
5. Nach Abschluss des Laufs druckt das Skript die Ereignisrate vom SVM. Sie können die Ereignisrate pro SVM in der Konsolenausgabe überprüfen:

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

Jeder Ontap SVM-Datensammler kann mit einem einzelnen SVM verknüpft werden, was bedeutet, dass jeder Datensammler die Anzahl der Ereignisse empfangen kann, die ein einzelnes SVM generiert.

Beachten Sie Folgendes:

A) Verwenden Sie diese Tabelle als allgemeine Größenrichtlinie. Sie können die Anzahl der Kerne und/oder den Speicher erhöhen, um die Anzahl der unterstützten Datensammler auf bis zu 50 Datensammler zu erhöhen:

Agent-Computerkonfiguration	Anzahl der SVM-Datensammler	Maximale Ereignisrate, die der Agent-Computer verarbeiten kann
4 Kerne, 16 GB	10 Datensammler	20.000 Ereignisse/Sek.
4 Kerne, 32 GB	20 Datensammler	20.000 Ereignisse/Sek.

B) Um Ihre Gesamtereignisse zu berechnen, addieren Sie die für alle SVMs für diesen Agenten generierten Ereignisse.

C) Wenn das Skript nicht während der Spitzenzeiten ausgeführt wird oder wenn der Spitzenverkehr schwer vorherzusagen ist, halten Sie einen Ereignisratenpuffer von 30 % ein.

B + C sollte kleiner als A sein, sonst schlägt die Überwachung durch die Agent-Maschine fehl.

Mit anderen Worten: Die Anzahl der Datensammler, die einer einzelnen Agentenmaschine 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 dielink:concept_cs_agent_requirements.html["Agentenanforderungen"]
Seite für zusätzliche Voraussetzungen und Anforderungen.
```

Beispiel

Nehmen wir an, wir haben drei SVMS, die Ereignisraten von 100, 200 bzw. 300 Ereignissen pro Sekunde generieren.

Wir wenden die Formel an:

```
 (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 der Agent-Maschine unter dem Dateinamen *fpolicy_stat_<SVM-Name>.log* im aktuellen Arbeitsverzeichnis verfügbar.

Das Skript kann in den folgenden Fällen fehlerhafte Ergebnisse liefern:

- Es wurden falsche Anmeldeinformationen, IP-Adressen oder SVM-Namen angegeben.
- Eine bereits vorhandene fpolicy mit demselben Namen, derselben Sequenznummer usw. führt zu einem Fehler.
- Das Skript wird während der Ausführung abrupt gestoppt.

Ein Beispiel für die Ausführung eines Skripts wird unten angezeigt:

```
[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]#
```

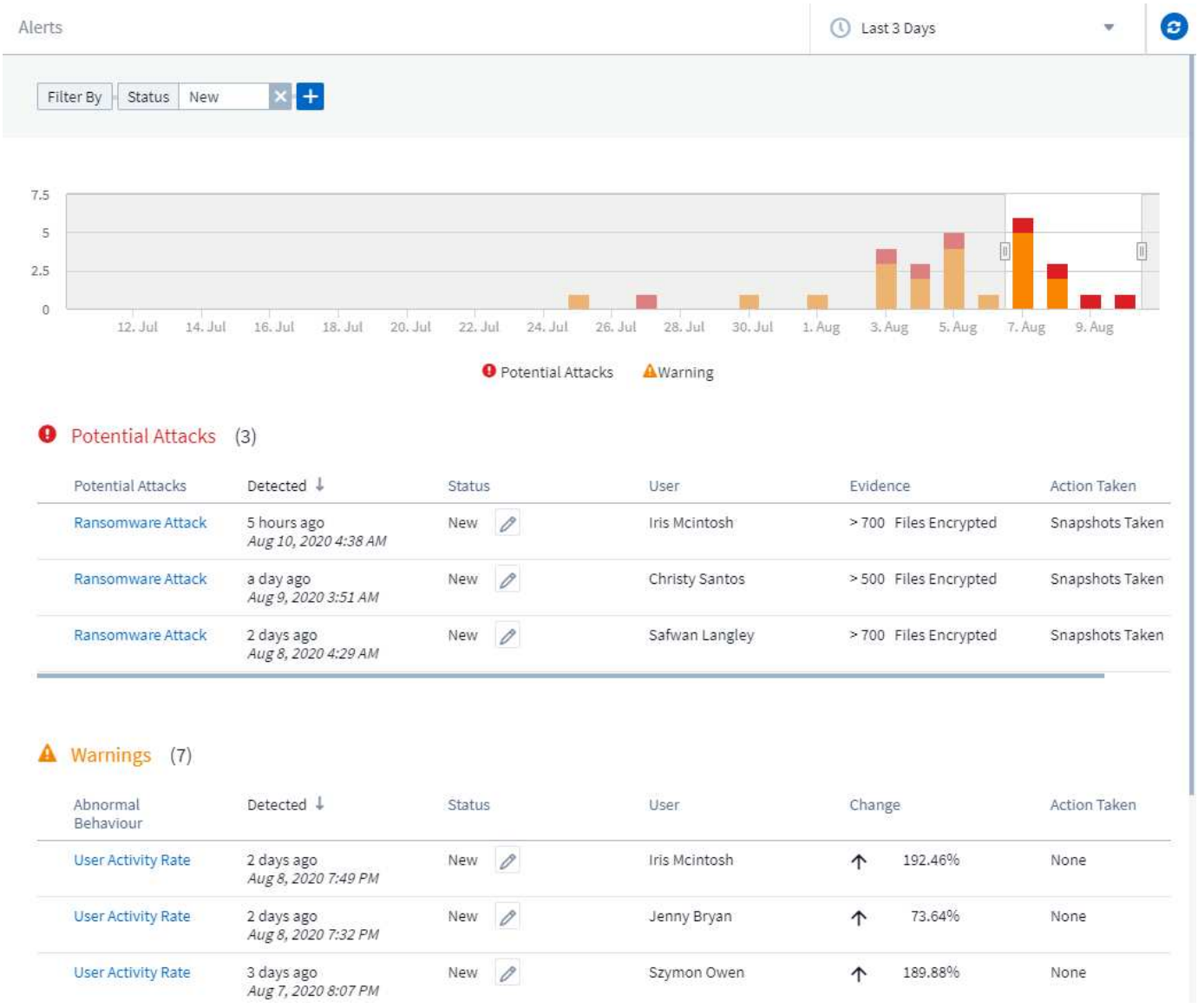
Fehlerbehebung

Frage	Antwort
Wenn ich dieses Skript auf einer SVM ausführe, die bereits für Workload Security konfiguriert ist, verwendet es dann einfach die vorhandene fpolicy-Konfiguration auf der SVM oder richtet es eine temporäre ein und führt den Prozess aus?	Der Event Rate Checker kann auch für eine SVM, die bereits für Workload Security konfiguriert ist, 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 von SVMs von 5 auf eine beliebige Zahl.
Wenn ich die Anzahl der SVMs erhöhe, verlängert sich dann die Ausführungszeit des Skripts?	Nein. Das Skript wird maximal 5 Minuten lang ausgeführt, auch 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 von SVMs von 5 auf eine beliebige Zahl ändern.
Wenn ich die Anzahl der SVMs erhöhe, verlängert sich dann die Ausführungszeit des Skripts?	Nein. Das Skript wird maximal 5 Minuten lang ausgeführt, auch wenn die Anzahl der SVMs erhöht wird.

Was passiert, wenn ich den Event Rate Checker mit einem vorhandenen Agenten ausführe?	Das Ausführen des Event Rate Checker für einen bereits vorhandenen Agenten kann zu einer Erhöhung der Latenz auf der SVM führen. Diese Erhöhung ist vorübergehender Natur, während der Event Rate Checker ausgeführt wird.

Warnmeldungen verstehen und untersuchen

Die Seite „Workload-Sicherheitswarnungen“ bietet eine umfassende Zeitleiste der erkannten Bedrohungen und Warnungen sowie detaillierte Untersuchungswerkzeuge. Alarmdetails einsehen, Statusaktualisierungen verwalten, nach Kriterien filtern und Benutzeraktivitäten verfolgen, um Sicherheitsvorfälle effizient zu untersuchen und darauf zu reagieren.



Alarm

Die Warnliste zeigt ein Diagramm mit der Gesamtzahl der potenziellen Angriffe und/oder Warnungen an, die im

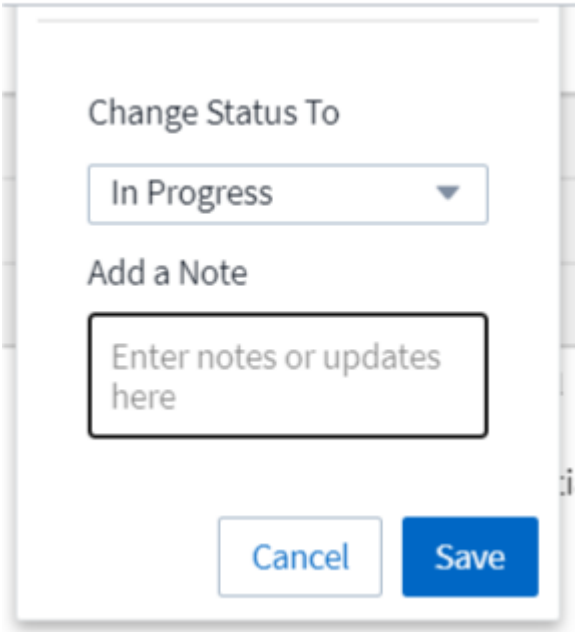
ausgewählten Zeitraum ausgelöst wurden, gefolgt von einer Liste der Angriffe und/oder Warnungen, die in diesem Zeitraum aufgetreten sind. Sie können den Zeitbereich ändern, indem Sie die Schieberegler für Start- und Endzeit im Diagramm anpassen.

Für jeden Alarm wird Folgendes angezeigt:

Potenzielle Angriffe:

- Die Art des *potenziellen Angriffs* (z. B. Dateimanipulation oder Sabotage)
- Datum und Uhrzeit der *Erkennung* des potenziellen Angriffs
- Der *Status* der Warnung:
  - **Neu**: Dies ist die Standardeinstellung für neue Warnungen.
  - **In Bearbeitung**: Die Warnung wird von einem oder mehreren Teammitgliedern untersucht.
  - **Gelöst**: Der Alarm wurde von einem Teammitglied als gelöst markiert.
  - **Abgelehnt**: Die Warnung wurde als falsch positiv oder als erwartetes Verhalten abgewiesen.

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



- Der *Benutzer*, dessen Verhalten den Alarm ausgelöst hat
- *Beweise* für den Angriff (z. B. wurde eine große Anzahl von Dateien verschlüsselt)
- Die *durchgeführte Aktion* (z. B. wurde ein Schnappschuss gemacht)

Warnungen:

- Das *Abnormale Verhalten*, das die Warnung ausgelöst hat
- Datum und Uhrzeit der *Erkennung* des Verhaltens
- Der *Status* der Warnung (Neu, In Bearbeitung usw.)
- Der *Benutzer*, dessen Verhalten den Alarm ausgelöst hat

- Eine Beschreibung der *Änderung* (z. B. ein ungewöhnlicher Anstieg der Dateizugriffe)
- Die *durchgeführte Aktion*

Filteroptionen

Sie können Warnungen nach Folgendem filtern:

- Der *Status* der Warnung
- Spezifischer Text in der *Anmerkung*
- Die Art der *Angriffe/Warnungen*
- Der *Benutzer*, dessen Aktionen den Alarm/die Warnung ausgelöst haben

Die Seite „Warnungsdetails“

Sie können auf der Seite „Warnungen“ auf einen Warnhinweis klicken, um eine Detailseite für die jeweilige Warnung zu öffnen. Die Details der Warnung können je nach Art des Angriffs oder der Warnung variieren. Eine Detailseite zu einem Dateimanipulationsangriff könnte beispielsweise folgende Informationen enthalten:

Abschnitt „Zusammenfassung“:

- Angriffsart (Dateimanipulation, Sabotage) und Warn-ID (vergeben von Workload Security)
- Datum und Uhrzeit der Erkennung des Angriffs
- Durchgeführte Aktion (z. B. wurde ein automatischer Schnappschuss erstellt). Die Uhrzeit des Schnappschusses wird direkt unter dem Abschnitt „Zusammenfassung“ angezeigt.))
- Status (Neu, In Bearbeitung usw.)

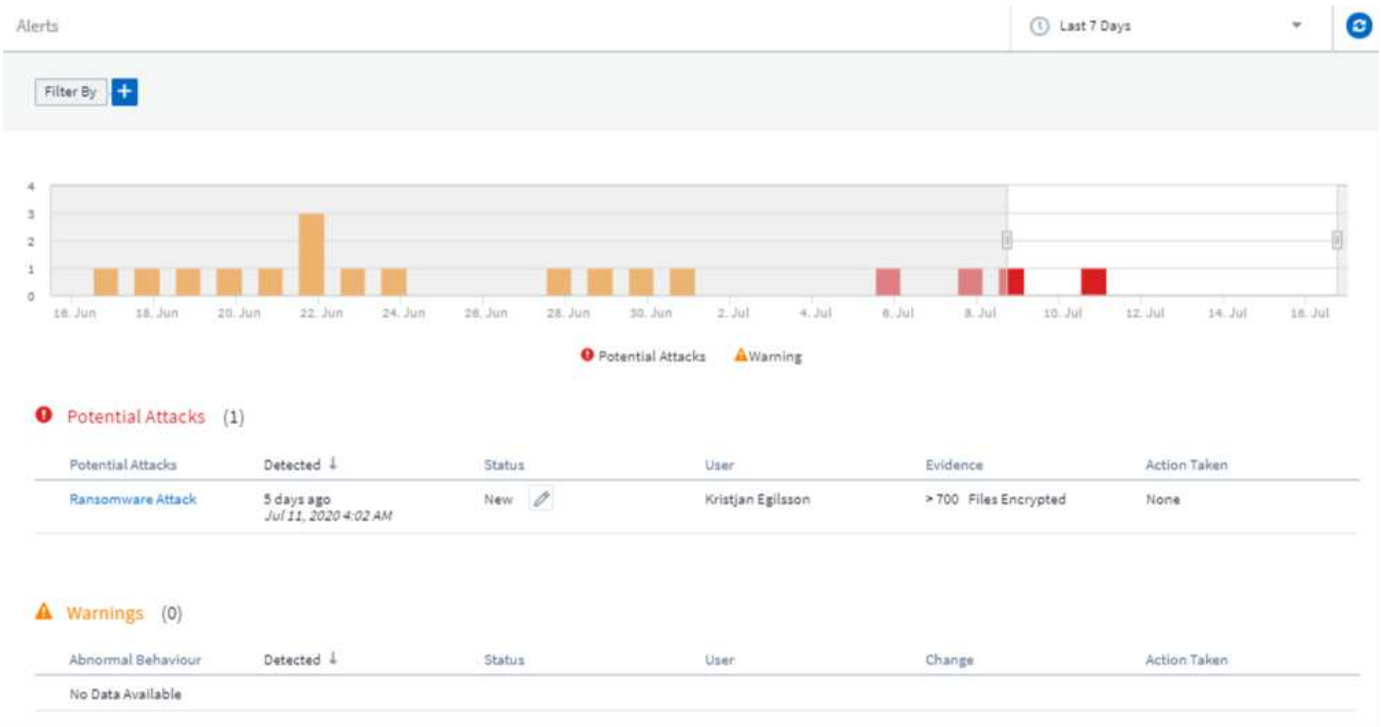
Abschnitt „Angriffsergebnisse“:

- Anzahl der betroffenen Volumes und Dateien
- Eine begleitende Zusammenfassung der Entdeckung
- Ein Diagramm, das die Dateiaktivität während des Angriffs zeigt

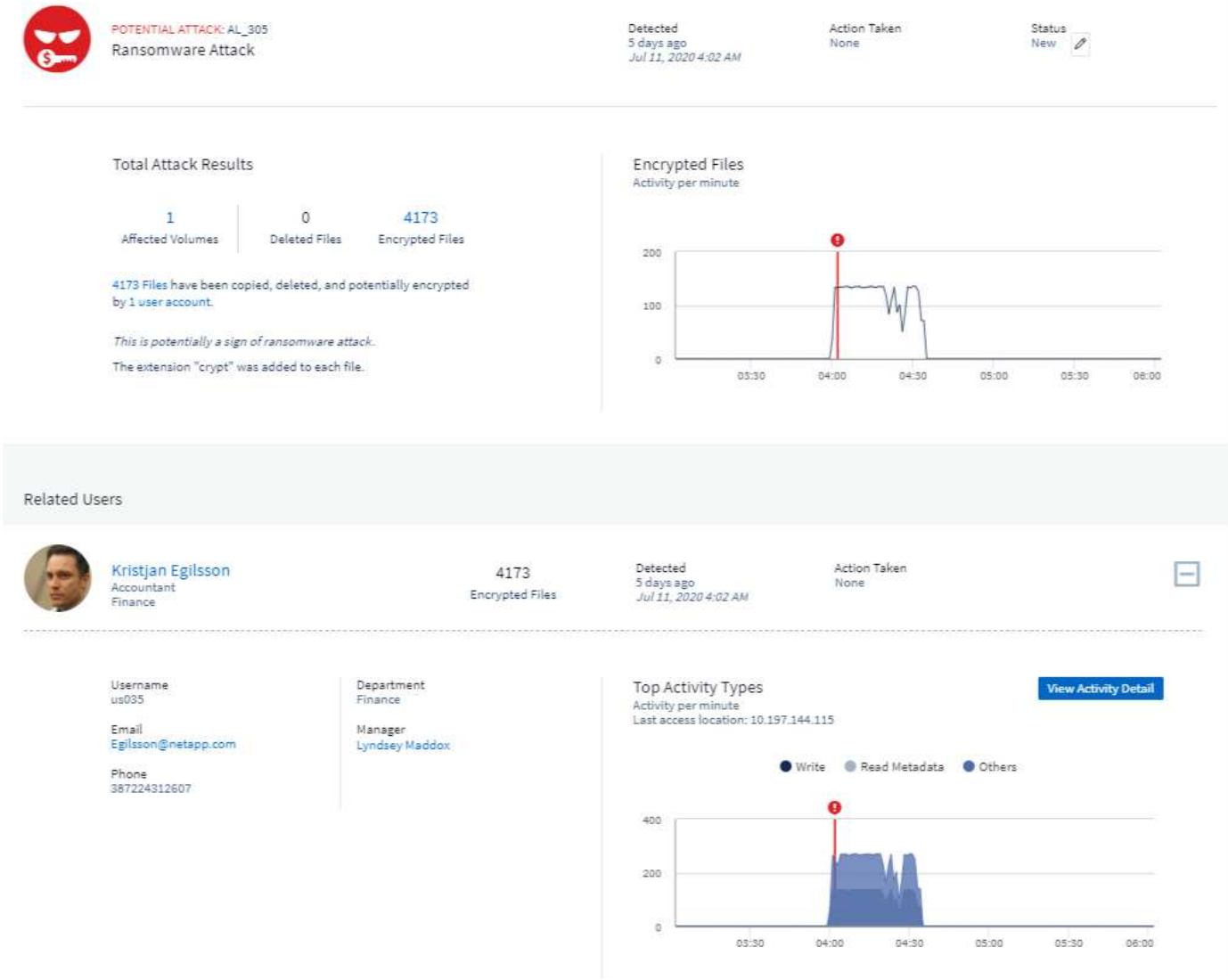
Abschnitt „Verwandte Benutzer“:

Dieser Abschnitt zeigt Details zum Benutzer, der an dem potenziellen Angriff beteiligt war, einschließlich eines Diagramms der Top-Aktivitäten des Benutzers.

Warnseite (dieses Beispiel zeigt einen möglichen Angriff zur Manipulation von Dateien):



Detailseite (dieses Beispiel zeigt einen möglichen Angriff zur Dateimanipulation):

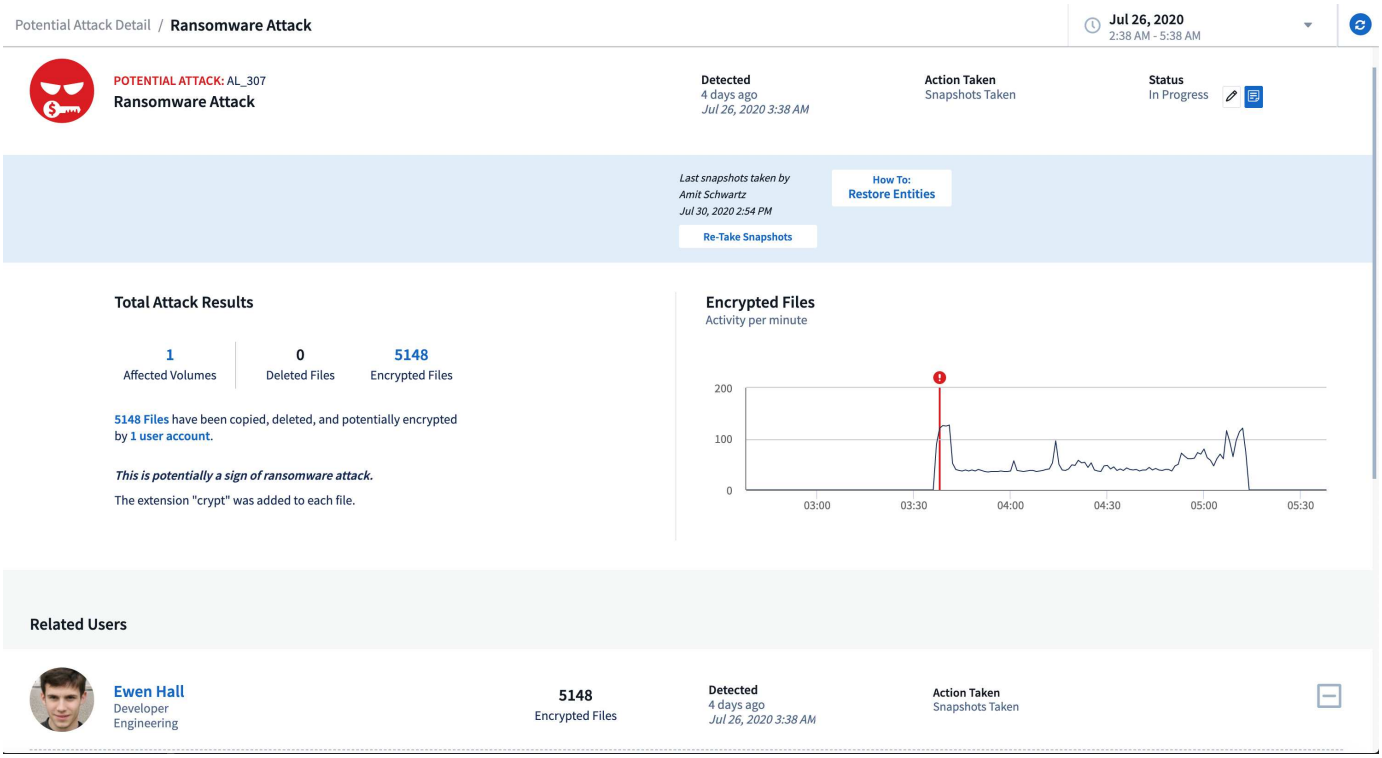


Aktion „Schnappschuss machen“

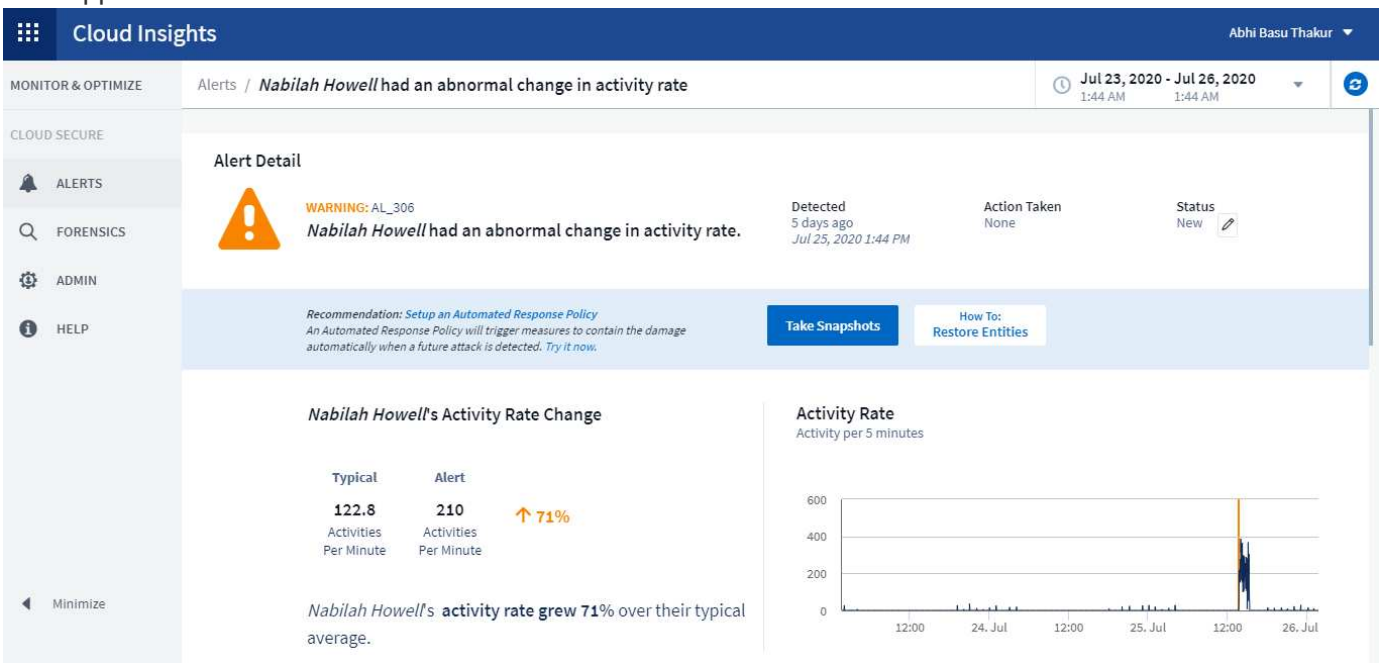
Workload Security schützt Ihre Daten, indem es automatisch einen Snapshot erstellt, wenn böswillige Aktivitäten erkannt werden, und so gewährleistet, dass Ihre Daten sicher gesichert werden.

Sie können definieren "Richtlinien für automatisierte Antworten" die einen Snapshot erstellen, wenn ein Dateimanipulationsangriff oder eine andere ungewöhnliche Benutzeraktivität erkannt wird. Sie können auch manuell einen Screenshot von der Benachrichtigungsseite erstellen.

Automatischer Schnappschuss
erstellt:



Manueller Schnappschuss:



Warnmeldungen

Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen zu Warnungen an eine Warnungsempfängerliste gesendet. Um die Empfänger der Benachrichtigungen zu konfigurieren, klicken Sie auf **Admin > Benachrichtigungen** und geben Sie für jeden Empfänger eine E-Mail-Adresse ein.

Aufbewahrungsrichtlinie

Alarme und Warnungen werden 13 Monate lang gespeichert. Alarme und Warnungen, die älter als 13 Monate

sind, werden gelöscht. Wenn die Workload Security-Umgebung gelöscht wird, werden auch alle mit der Umgebung verknüpften Daten gelöscht.

Fehlerbehebung

Problem:	Versuchen Sie Folgendes:
Es gibt eine Situation, in der ONTAP stündlich Snapshots pro Tag erstellt. Werden Workload Security (WS)-Snapshots dies beeinflussen? Wird der WS-Snapshot den Platz des stündlichen Snapshots einnehmen? Wird der standardmäßige stündliche Snapshot gestoppt?	Snapshots der Workload-Sicherheit haben keinen Einfluss auf die stündlichen Snapshots. WS-Snapshots belegen nicht den stündlichen Snapshot-Speicherplatz und das sollte auch so bleiben wie bisher. Der standardmäßige stündliche Snapshot wird nicht gestoppt.
Was passiert, wenn die maximale Snapshot-Anzahl in ONTAP erreicht wird?	Wenn die maximale Snapshot-Anzahl erreicht ist, schlägt die nachfolgende Snapshot-Erstellung fehl und Workload Security zeigt eine Fehlermeldung mit dem Hinweis an, dass der Snapshot voll ist. Der Benutzer muss Snapshot-Richtlinien definieren, um die ältesten Snapshots zu löschen, andernfalls werden keine Snapshots erstellt. In ONTAP 9.3 und früheren Versionen kann ein Volume bis zu 255 Snapshot-Kopien enthalten. In ONTAP 9.4 und höher kann ein Volume bis zu 1023 Snapshot-Kopien enthalten. Informationen zu"Festlegen der Richtlinie zum Löschen von Snapshots" .
Workload Security kann überhaupt keine Snapshots erstellen.	Stellen Sie sicher, dass die zum Erstellen von Snapshots verwendete Rolle über den Link: korrekte Rechte zugewiesen verfügt. Stellen Sie sicher, dass *csrole* mit den richtigen Zugriffsrechten zum Erstellen von Snapshots erstellt wird: security login role create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Snapshots schlagen für ältere Warnungen auf SVMs fehl, die aus Workload Security entfernt und anschließend wieder hinzugefügt wurden. Für neue Warnungen, die nach dem erneuten Hinzufügen von SVM auftreten, werden Snapshots erstellt.	Dies ist ein seltenes Szenario. Falls dies bei Ihnen der Fall ist, melden Sie sich bei ONTAP an und erstellen Sie die Snapshots für die älteren Warnungen manuell.
Auf der Seite „Alarmdetails“ wird unter der Schaltfläche „Snapshot erstellen“ die Fehlermeldung „Letzter Versuch fehlgeschlagen“ angezeigt. Wenn Sie mit der Maus über den Fehler fahren, wird „Zeitüberschreitung beim Aufrufen des API-Befehls für den Datensammler mit der ID“ angezeigt.	Dies kann passieren, wenn ein Datensammler über die SVM-Verwaltungs-IP zur Workload-Sicherheit hinzugefügt wird, wenn sich das LIF der SVM in ONTAP im Status *deaktiviert* befindet. Aktivieren Sie das jeweilige LIF in ONTAP und lösen Sie „Manuell Snapshot erstellen“ von Workload Security aus. Die Snapshot-Aktion wird dann erfolgreich sein.

Forensik

Forensik – Alle Aktivitäten

Auf der Seite „Alle Aktivitäten“ können Sie die Aktionen nachvollziehen, die an Entitäten

in der Workload Security-Umgebung ausgeführt werden.

Untersuchen aller Aktivitätsdaten

Klicken Sie auf **Forensik > Aktivitätsforensik** und dann auf die Registerkarte **Alle Aktivitäten**, um auf die Seite „Alle Aktivitäten“ zuzugreifen. Diese Seite bietet einen Überblick über die Aktivitäten Ihres Mandanten und hebt die folgenden Informationen hervor:

- Ein Diagramm, das den *Aktivitätsverlauf* zeigt (basierend auf einem ausgewählten globalen Zeitbereich)

  Sie können das Diagramm vergrößern, indem Sie ein Rechteck im Diagramm aufziehen. Die gesamte Seite wird geladen, um den gezoomten Zeitbereich anzuzeigen. Beim Vergrößern wird eine Schaltfläche angezeigt, mit der der Benutzer herauszoomen kann.

- Eine Liste aller Aktivitätsdaten.
- Ein Dropdown-Menü „Gruppieren nach“ bietet die Möglichkeit, die Aktivität nach Benutzern, Ordnern, Entitätstyp usw. zu gruppieren.
- Über der Tabelle ist eine Schaltfläche für den allgemeinen Pfad verfügbar, über die wir durch Anklicken ein ausziehbares Bedienfeld mit Details zum Entitätspfad erhalten.

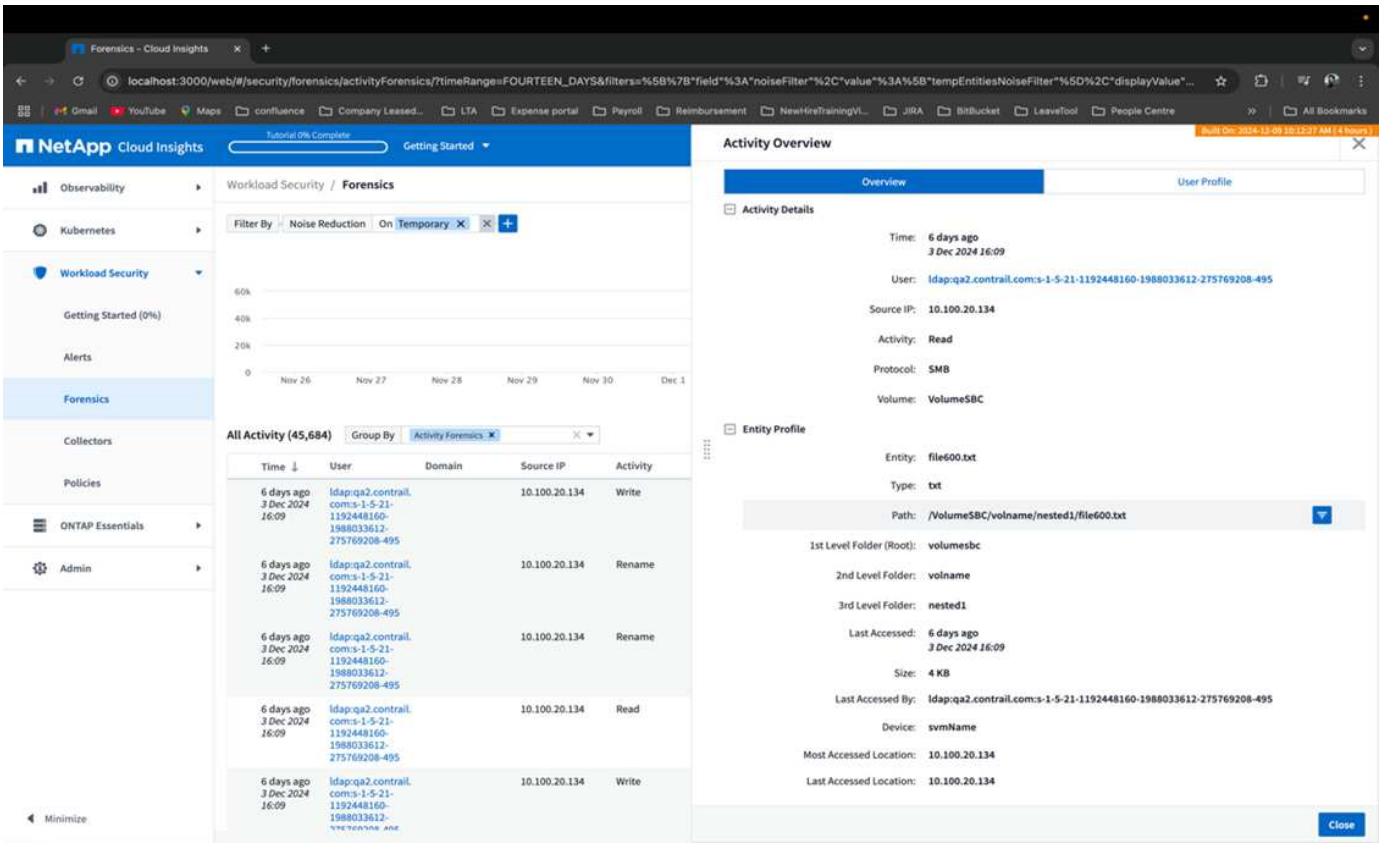
Die Tabelle **Alle Aktivitäten** zeigt die folgenden Informationen. Beachten Sie, dass nicht alle dieser Spalten standardmäßig angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das Zahnradsymbol klicken.

- Die **Zeit**, zu der auf eine Entität zugegriffen wurde, einschließlich Jahr, Monat, Tag und Uhrzeit des letzten Zugriffs.
- Der **Benutzer**, der auf die Entität mit einem Link zugegriffen hat"Benutzerinformationen" als ausziehbare Platte.
- Die **Aktivität**, die der Benutzer ausgeführt hat. Unterstützte Typen sind:
  - **Gruppeneigentum ändern** – Der Gruppeneigentum einer Datei oder eines Ordners wird geändert. Weitere Einzelheiten zum Gruppeneigentum finden Sie unter"dieser Link."
  - **Eigentümer ändern** – Der Besitz einer Datei oder eines Ordners wird auf einen anderen Benutzer geändert.
  - **Berechtigung ändern** – Die Datei- oder Ordnerberechtigung wurde geändert.
  - **Erstellen** – Datei oder Ordner erstellen.
  - **Löschen** – Datei oder Ordner löschen. Wenn ein Ordner gelöscht wird, werden *delete*-Ereignisse für alle Dateien in diesem Ordner und den Unterordnern abgerufen.
  - **Lesen** – Datei wird gelesen.
  - **Metadaten lesen** – Nur beim Aktivieren der Ordnerüberwachungsoption. Wird beim Öffnen eines Ordners unter Windows oder beim Ausführen von „ls“ in einem Ordner unter Linux generiert.
  - **Umbenennen** – Datei oder Ordner umbenennen.
  - **Schreiben** – Daten werden in eine Datei geschrieben.
  - **Metadaten schreiben** – Dateimetadaten werden geschrieben, z. B. geänderte Berechtigungen.
  - **Andere Änderung** – Alle anderen Ereignisse, die oben nicht beschrieben sind. Alle nicht zugeordneten Ereignisse werden dem Aktivitätstyp „Andere Änderung“ zugeordnet. Gilt für Dateien und Ordner.
- Der **Pfad** ist der *Entitätspfad. Dies sollte entweder der genaue Entitätspfad (z. B.*

„/home/userX/nested1/nested2/abc.txt_“) ODER der Verzeichnisteil des Pfads für die rekursive Suche (z. B. „*/home/userX/nested1/nested2/*“) sein. HINWEIS: Regex-Pfadmuster (z. B. *verschachtelt*) sind hier NICHT zulässig. Alternativ können für die Pfadfilterung auch einzelne Filter auf Pfadordnerebene wie unten erwähnt angegeben werden.

- Der **Ordner der 1. Ebene (Stammverzeichnis)** ist das Stammverzeichnis des Entitätspfads in Kleinbuchstaben.
- Der **Ordner der zweiten Ebene** ist das Verzeichnis der zweiten Ebene des Entitätspfads in Kleinbuchstaben.
- Der **Ordner der 3. Ebene** ist das Verzeichnis der dritten Ebene des Entitätspfads in Kleinbuchstaben.
- Der **Ordner der 4. Ebene** ist das Verzeichnis der vierten Ebene des Entitätspfads in Kleinbuchstaben.
- Der **Entitätstyp**, einschließlich der Entitätserweiterung (d. h. Dateierweiterung) (.doc, .docx, .tmp usw.).
- Das **Gerät**, auf dem sich die Entitäten befinden.
- Das zum Abrufen von Ereignissen verwendete **Protokoll**.
- Der **Ursprüngliche Pfad**, der für Umbenennungsereignisse verwendet wurde, als die Originaldatei umbenannt wurde. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie den Spaltenselektor, um diese Spalte zur Tabelle hinzuzufügen.
- Das **Volume**, in dem sich die Entitäten befinden. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie den Spaltenselektor, um diese Spalte zur Tabelle hinzuzufügen.
- Der **Entitätsname** ist die letzte Komponente des Entitätspfads; beim Entitätstyp als Datei ist es der Dateiname.

Durch Auswählen einer Tabellenzeile wird ein ausziehbares Fenster mit dem Benutzerprofil auf einer Registerkarte und der Aktivitäts- und Entitätsübersicht auf einer anderen Registerkarte geöffnet.



Die Standardmethode „Gruppieren nach“ ist „Aktivitätsforensik“. Wenn Sie eine andere *Gruppieren nach*

-Methode auswählen, beispielsweise Entitätstyp, wird die Entitäts-*Gruppieren nach*-Tabelle angezeigt. Wenn keine Auswahl getroffen wird, wird *Gruppieren nach* **alle** angezeigt.

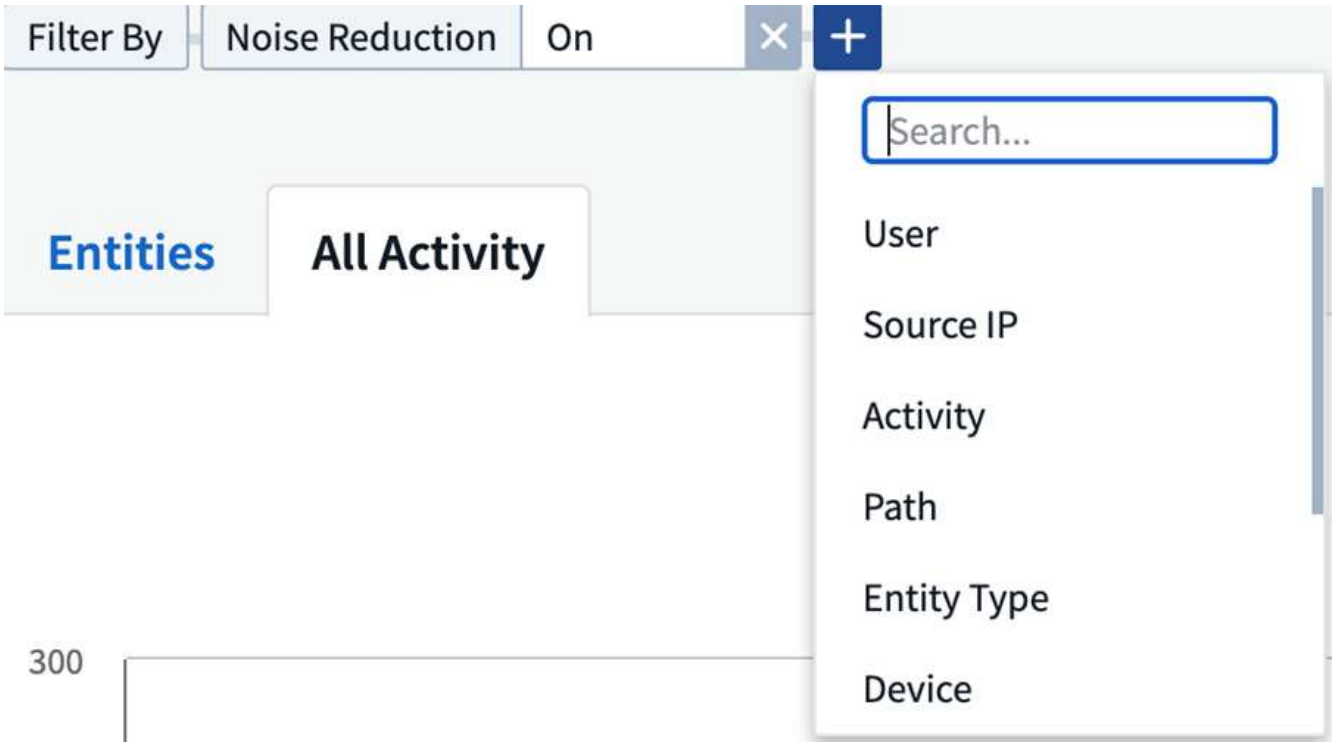
- Die Aktivitätsanzahl wird als Hyperlink angezeigt. Wenn Sie diesen auswählen, wird die ausgewählte Gruppierung als Filter hinzugefügt. Die Aktivitätstabelle wird basierend auf diesem Filter aktualisiert.
- Beachten Sie, dass Sie, wenn Sie den Filter ändern, den Zeitbereich ändern oder den Bildschirm aktualisieren, nicht zu den gefilterten Ergebnissen zurückkehren können, ohne den Filter erneut einzustellen.
- Bitte beachten Sie, dass das Dropdown-Menü „Gruppieren nach“ deaktiviert wird, wenn „Entitätsname“ als Filter ausgewählt ist. Wenn sich der Benutzer bereits auf dem Bildschirm „Gruppieren nach“ befindet, wird der Entitätsname als Filter deaktiviert.

Filtern von Daten zum forensischen Aktivitätsverlauf

Zum Filtern von Daten können Sie zwei Methoden verwenden.

- Der Filter kann über das ausziehbare Bedienfeld hinzugefügt werden. Der Wert wird den entsprechenden Filtern in der oberen Liste „Filtern nach“ hinzugefügt.
- Filtern Sie Daten, indem Sie in das Feld *Filtern nach* Folgendes eingeben:

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



  Geben Sie den Suchtext ein

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

Sie können Daten zur forensischen Aktivität nach den folgenden Feldern filtern:

- Der *Aktivitäts*typ.

- **Protokoll** zum Abrufen protokollspezifischer Aktivitäten.
- **Benutzername** des Benutzers, der die Aktivität ausführt. Sie müssen den genauen Benutzernamen zum Filtern angeben. Die Suche mit einem teilweisen Benutzernamen oder einem teilweisen Benutzernamen mit dem Präfix oder Suffix „*“ funktioniert nicht.
- **Rauschunterdrückung** zum Filtern von Dateien, die in den letzten 2 Stunden vom Benutzer erstellt wurden. Es wird auch zum Filtern temporärer Dateien (z. B. .tmp-Dateien) verwendet, auf die der Benutzer zugreift.
- **Domäne** des Benutzers, der die Aktivität ausführt. Sie müssen die **genaue Domäne** zum Filtern angeben. Die Suche nach Teildomänen oder Teildomänen mit einem Platzhalter ('*') als Präfix oder Suffix funktioniert nicht. *None* kann angegeben werden, um nach fehlenden Domänen zu suchen.

Für die folgenden Felder gelten besondere Filterregeln:

- **Entitätstyp**, unter Verwendung der Entitäts-(Datei-)Erweiterung – es ist vorzuziehen, den genauen Entitätstyp in Anführungszeichen anzugeben. Zum Beispiel *"txt"*.
- **Pfad** der Entität – Dies sollte entweder der genaue Entitätspfad (z. B. *„/home/userX/nested1/nested2/abc.txt*“) ODER der Verzeichnisteil des Pfads für die rekursive Suche (z. B. *„/home/userX/nested1/nested2/*“) sein. HINWEIS: Regex-Pfadmuster (z. B. *verschachtelt*) sind hier NICHT zulässig. Für schnellere Ergebnisse werden Verzeichnispfadfilter (Pfadzeichenfolge endet mit /) mit einer Tiefe von bis zu 4 Verzeichnissen empfohlen. Beispiel: *„/home/userX/nested1/nested2/*“. Weitere Einzelheiten finden Sie in der folgenden Tabelle.
- Ordner der 1. Ebene (Stammverzeichnis) – Stammverzeichnis des Entitätspfads als Filter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann home ODER „home“ verwendet werden.
- Ordner der 2. Ebene – Verzeichnis der 2. Ebene der Entitätspfadfilter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann userX ODER „userX“ verwendet werden.
- Ordner der 3. Ebene – Verzeichnis der 3. Ebene der Entitätspfadfilter.
- Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann nested1 ODER „nested1“ verwendet werden.
- Ordner der 4. Ebene – Verzeichnis Verzeichnis der 4. Ebene der Entitätspfadfilter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/nested2/ ist, kann nested2 ODER „nested2“ verwendet werden.
- **Benutzer**, der die Aktivität ausführt – es ist vorzuziehen, den genauen Benutzer in Anführungszeichen anzugeben. Beispiel: *"Administrator"*.
- **Gerät** (SVM), auf dem sich Entitäten befinden
- **Volume**, in dem sich Entitäten befinden
- Der **Ursprüngliche Pfad**, der für Umbenennungsereignisse verwendet wurde, als die Originaldatei umbenannt wurde.
- **Quell-IP**, von der aus auf die Entität zugegriffen wurde.
  - Sie können die Platzhalter * und ? verwenden. Zum Beispiel: 10.0.0.**, 10.0?.0.10, 10.10**
  - Wenn eine exakte Übereinstimmung erforderlich ist, müssen Sie eine gültige Quell-IP-Adresse in Anführungszeichen angeben, beispielsweise „10.1.1.1.“. Unvollständige IPs mit Anführungszeichen wie „10.1.1.“, „10.1..*“ usw. funktionieren nicht.
- Der **Entitätsname** – der Dateiname des Entitätspfads als Filter. Wenn der Entitätspfad beispielsweise /home/userX/nested1/testfile.txt lautet, ist der Entitätsname testfile.txt. Bitte beachten Sie, dass es empfohlen wird, den genauen Dateinamen in Anführungszeichen anzugeben. Versuchen Sie, die Suche mit Platzhaltern zu vermeiden. Beispiel: „testfile.txt“. Beachten Sie außerdem, dass dieser Entitätsnamenfilter für kürzere Zeiträume (bis zu 3 Tage) empfohlen wird.

Für die vorangehenden Felder gelten beim Filtern folgende Punkte:

- Der genaue Wert sollte in Anführungszeichen stehen: Beispiel: „Suchtext“
- Platzhalterzeichenfolgen dürfen keine Anführungszeichen enthalten: Beispiel: Suchtext, *Suchtext*, filtert nach allen Zeichenfolgen, die „Suchtext“ enthalten.
- Zeichenfolgen mit einem Präfix, Beispiel: Suchtext*, suchen nach allen Zeichenfolgen, die mit „Suchtext“ beginnen.

Bitte beachten Sie, dass bei allen Filterfeldern die Groß- und Kleinschreibung beachtet wird. Beispiel: Wenn der angewendete Filter „Entitätstyp“ mit dem Wert „Suchtext“ ist, werden Ergebnisse mit dem Entitätstyp „Suchtext“, „Suchtext“ oder „SUCHTEXT“ zurückgegeben.

Beispiele für Aktivitätsforensikfilter:

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Leistungsbeurteilung	Kommentar
Pfad = "/home/userX/nested1/nested2/"	Rekursive Suche aller Dateien und Ordner unter einem bestimmten Verzeichnis	Schnell	Verzeichnissuchen in bis zu 4 Verzeichnissen sind schnell.
Pfad = "/home/userX/nested1/"	Rekursive Suche aller Dateien und Ordner unter einem bestimmten Verzeichnis	Schnell	Verzeichnissuchen in bis zu 4 Verzeichnissen sind schnell.
Pfad = "/home/userX/nested1/test"	Exakte Übereinstimmung, wenn der Pfadwert mit /home/userX/nested1/test übereinstimmt	Langsamer	Die exakte Suche ist im Vergleich zur Verzeichnissuche langsamer.
Pfad = "/home/userX/nested1/nested2/nested3/"	Rekursive Suche aller Dateien und Ordner unter einem bestimmten Verzeichnis	Langsamer	Die Suche in mehr als 4 Verzeichnissen ist langsamer.
Alle anderen nicht pfadbasierten Filter. Es wird empfohlen, Benutzer- und Entitätstypfilter in Anführungszeichen zu setzen, z. B. „Benutzer="Administrator" Entitätstyp="txt"		Schnell	
Entitätsname = "test.log"	Genaue Übereinstimmung, wenn der Dateiname „test.log“ lautet	Schnell	Da es sich um eine exakte Übereinstimmung handelt
Entitätsname = *test.log	Dateinamen, die mit test.log enden	Langsam	Aufgrund von Platzhaltern kann es langsam sein.

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Leistungsbeurteilung	Kommentar
Entitätsname = test*.log	Dateinamen, die mit „test“ beginnen und mit „.log“ enden	Langsam	Aufgrund von Platzhaltern kann es langsam sein.
Entitätsname = test.lo	Dateinamen, die mit test.lo beginnen. Beispiel: Es entspricht test.log, test.log.1, test.log1	Langsamer	Aufgrund des Platzhalters am Ende kann es langsam sein.
Entitätsname = Test	Dateinamen, die mit „test“ beginnen	Am langsamsten	Aufgrund des Platzhalters am Ende und der Verwendung allgemeinerer Werte kann es langsam sein.

NOTIZ:

1. Die neben dem Symbol „Alle Aktivitäten“ angezeigte Aktivitätsanzahl wird auf 30 Minuten gerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst. Beispielsweise zeigt ein Zeitraum vom 1. September, 10:15 Uhr bis 7. September, 10:15 Uhr die Aktivitätsanzahl vom 1. September, 10:00 Uhr bis 7. September, 10:30 Uhr an.
2. Ebenso werden die im Diagramm „Aktivitätsverlauf“ angezeigten Zählmetriken auf 30 Minuten gerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst.

Sortieren von Daten zum forensischen Aktivitätsverlauf

Sie können die Aktivitätsverlaufsdaten nach *Zeit, Benutzer, Quell-IP, Aktivität*, *Entitätstyp*, Ordner der 1. Ebene (Stamm), Ordner der 2. Ebene, Ordner der 3. Ebene und Ordner der 4. Ebene sortieren. Standardmäßig ist die Tabelle in absteigender Zeitreihenfolge sortiert, d. h. die neuesten Daten werden zuerst angezeigt. Die Sortierung ist für die Felder *Gerät* und *Protokoll* deaktiviert.

Benutzerhandbuch für asynchrone Exporte

Überblick

Die Funktion „Asynchrone Exporte“ in Storage Workload Security ist für die Verarbeitung großer Datenexporte konzipiert.

Schritt-für-Schritt-Anleitung: Daten mit asynchronen Exporten exportieren

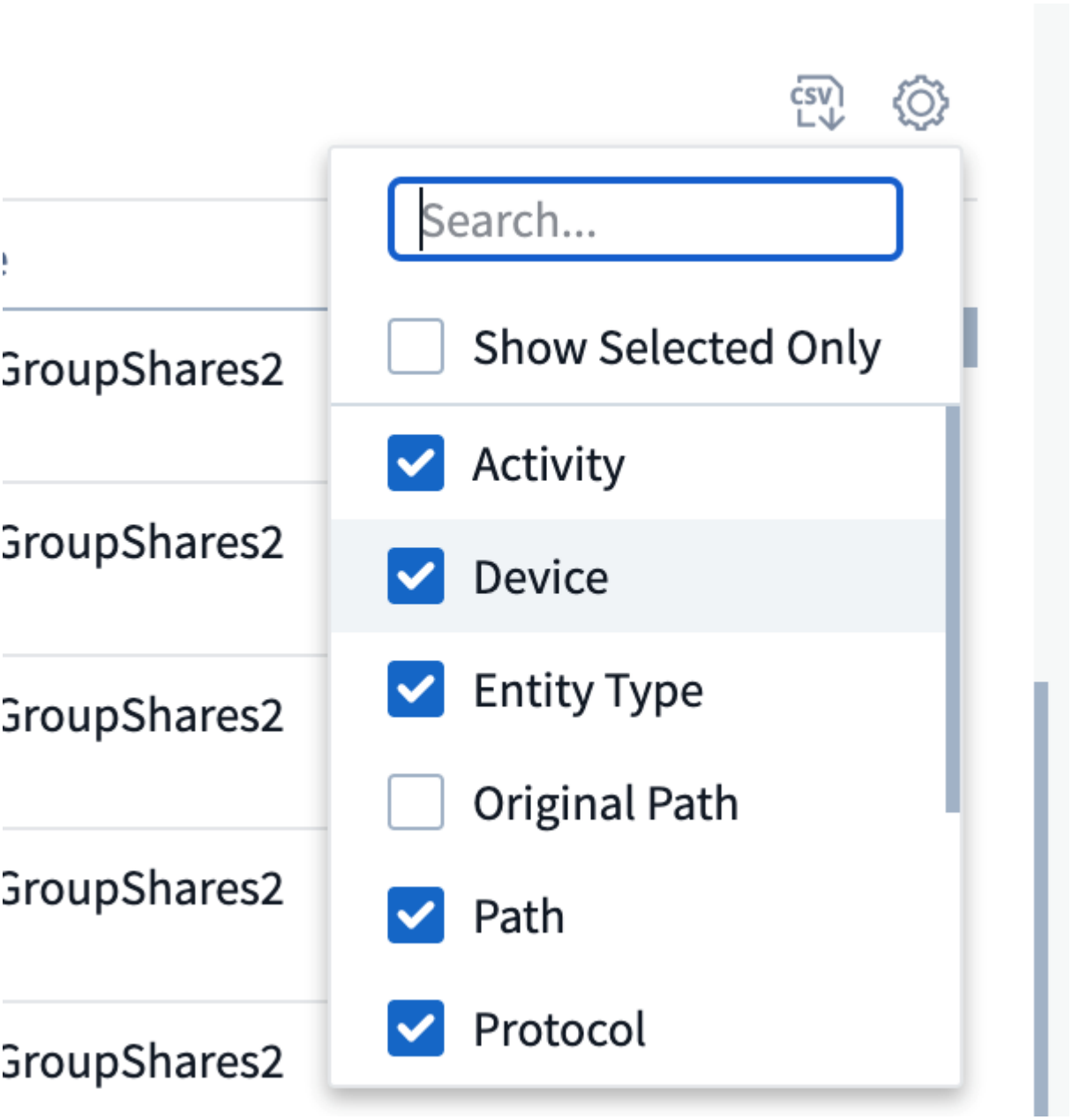
1. **Export starten**: Wählen Sie die gewünschte Zeitdauer und Filter für den Export aus und klicken Sie auf die Schaltfläche „Exportieren“.
2. **Warten Sie, bis der Export abgeschlossen ist**: Die Verarbeitungszeit kann zwischen einigen Minuten und einigen Stunden liegen. Möglicherweise müssen Sie die Forensikseite einige Male aktualisieren. Sobald der Exportauftrag abgeschlossen ist, wird die Schaltfläche „Letzte CSV-Exportdatei herunterladen“ aktiviert.
3. **Herunterladen**: Klicken Sie auf die Schaltfläche „Zuletzt erstellte Exportdatei herunterladen“, um die exportierten Daten im ZIP-Format zu erhalten. Diese Daten stehen zum Download zur Verfügung, bis der Benutzer einen weiteren asynchronen Export initiiert oder drei Tage vergangen sind, je nachdem, was zuerst eintritt. Die Schaltfläche bleibt aktiviert, bis ein weiterer asynchroner Export gestartet wird.

4. **Einschränkungen**:
    - Die Anzahl der asynchronen Downloads ist derzeit auf 1 pro Benutzer für jede Aktivitäts- und Aktivitätsanalysetabelle und 3 pro Mandant begrenzt.
    - Die exportierten Daten sind für die Aktivitätentabelle auf maximal 1 Million Datensätze begrenzt, während für „Gruppieren nach“ die Begrenzung auf eine halbe Million Datensätze liegt.

Ein Beispielskript zum Extrahieren forensischer Daten über die API befindet sich unter */opt/netapp/cloudsecure/agent/export-script/* auf dem Agenten. Weitere Einzelheiten zum Skript finden Sie in der Readme-Datei an dieser Stelle.

Spaltenauswahl für alle Aktivitäten

Die Tabelle „Alle Aktivitäten“ zeigt standardmäßig ausgewählte Spalten an. Um 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.



Aufbewahrung des Aktivitätsverlaufs

Der Aktivitätsverlauf wird für aktive Workload Security-Umgebungen 13 Monate lang aufbewahrt.

Anwendbarkeit von Filtern in der Forensik-Seite

Filter	Was es bewirkt	Beispiel	Anwendbar für diese Filter	Gilt nicht für diese Filter	Ergebnis
* (Sternchen)	ermöglicht Ihnen die Suche nach allem	Auto*03172022 Wenn der Suchtext Bindestriche oder Unterstriche enthält, geben Sie den Ausdruck in Klammern ein. zB (svm*) für die Suche nach svm-123	Benutzer, Entitätstyp, Gerät, Volume, Originalpfad, Ordner der 1. Ebene, Ordner der 2. Ebene, Ordner der 3. Ebene, Ordner der 4. Ebene, Entitätsname, Quell-IP		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, Entitätstyp, Gerät, Volume, Ordner der 1. Ebene, Ordner der 2. Ebene, Ordner der 3. Ebene, Ordner der 4. Ebene, Entitätsname, Quell-IP		gibt AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 usw. zurück
ODER	ermöglicht Ihnen die Angabe mehrerer Entitäten	AutoSabotageUser1_03172022 ODER AutoRansomUser4_03162022	Benutzer, Domäne, Entitätstyp, ursprünglicher Pfad, Entitätsname, Quell-IP		gibt entweder AutoSabotageUser1_03172022 oder AutoRansomUser4_03162022 zurück.
NICHT	ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen	NOT AutoRansomUser4_03162022	Benutzer, Domäne, Entitätstyp, Originalpfad, Ordner der 1. Ebene, Ordner der 2. Ebene, Ordner der 3. Ebene, Ordner der 4. Ebene, Entitätsname, Quell-IP	Gerät	gibt alles zurück, was nicht mit „AutoRansomUser4_03162022“ beginnt

Filter	Was es bewirkt	Beispiel	Anwendbar für diese Filter	Gilt nicht für diese Filter	Ergebnis
Keine	sucht in allen Feldern nach NULL-Werten	Keine	Domain		gibt Ergebnisse zurück, bei denen das Zielfeld leer ist

Pfadsuche

Suchergebnisse mit und ohne / werden unterschiedlich sein

"/AutoDir1/AutoFile03242022"	Nur die exakte Suche funktioniert; gibt alle Aktivitäten mit dem exakten Pfad als /AutoDir1/AutoFile03242022 zurück (ohne Berücksichtigung der Groß-/Kleinschreibung).
"/AutoDir1/ "	Funktioniert; gibt alle Aktivitäten mit Verzeichnis der 1. Ebene zurück, das mit AutoDir1 übereinstimmt (ohne Berücksichtigung der Groß-/Kleinschreibung)
"/AutoDir1/AutoFile03242022/"	Funktioniert; gibt alle Aktivitäten zurück, bei denen das Verzeichnis der 1. Ebene mit AutoDir1 übereinstimmt und das Verzeichnis der 2. Ebene mit AutoFile03242022 übereinstimmt (ohne Berücksichtigung der Groß-/Kleinschreibung).
/AutoDir1/AutoFile03242022 ODER /AutoDir1/AutoFile03242022	Funktioniert nicht
NICHT /AutoDir1/AutoFile03242022	Funktioniert nicht
NICHT /AutoDir1	Funktioniert nicht
NICHT /AutoFile03242022	Funktioniert nicht
*	Funktioniert nicht

Änderungen der Aktivität des lokalen Root-SVM-Benutzers

Wenn ein lokaler Root-SVM-Benutzer eine Aktivität ausführt, wird jetzt die IP des Clients, auf dem die NFS-Freigabe gemountet ist, im Benutzernamen berücksichtigt. Dieser wird sowohl auf der Seite mit der forensischen Aktivität als auch auf der Seite mit der Benutzeraktivität als root@<IP-Adresse des Clients> angezeigt.

Beispiel:

- Wenn SVM-1 von Workload Security überwacht wird und der Root-Benutzer dieses SVM die Freigabe auf einem Client mit der IP-Adresse 10.197.12.40 bereitstellt, lautet der auf der Seite mit der forensischen Aktivität angezeigte Benutzername *root@10.197.12.40*.
- Wenn derselbe SVM-1 in einen anderen Client mit der IP-Adresse 10.197.12.41 eingebunden wird, lautet der auf der forensischen Aktivitätsseite angezeigte Benutzername *root@10.197.12.41*.

*• Dies geschieht, um die NFS-Root-Benutzeraktivität nach IP-Adresse zu trennen. Zuvor wurde davon ausgegangen, dass alle Aktivitäten nur vom Root-Benutzer ohne IP-Unterscheidung ausgeführt werden konnten.

Fehlerbehebung

Problem	Versuchen Sie Folgendes
In der Tabelle „Alle Aktivitäten“ wird der Benutzername in der Spalte „Benutzer“ wie folgt angezeigt: „ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817“ oder „ldap:default:80038003“.	Mögliche Gründe könnten sein: 1. Es wurden noch keine Benutzerverzeichnis-Sammler konfiguriert. Um einen hinzuzufügen, gehen Sie zu **Workload Security > Collectors > User Directory Collectors** und klicken Sie auf **+User Directory Collector**. Wählen Sie *Active Directory* oder *LDAP-Verzeichnisserver*. 2. Ein User Directory Collector wurde konfiguriert, wurde jedoch gestoppt oder befindet sich in einem Fehlerzustand. Gehen Sie bitte zu **Sammler > Benutzerverzeichnissammler** und überprüfen Sie den Status. Weitere Informationen finden Sie im"Fehlerbehebung beim User Directory Collector" Tipps zur Fehlerbehebung finden Sie im Abschnitt der Dokumentation. Nach der ordnungsgemäßen Konfiguration wird der Name innerhalb von 24 Stunden automatisch aufgelöst. Wenn das Problem immer noch nicht behoben ist, überprüfen Sie, ob Sie den richtigen Benutzerdatensammler hinzugefügt haben. Stellen Sie sicher, dass der Benutzer tatsächlich Teil des hinzugefügten Active Directory/LDAP-Verzeichnisservers ist.
Einige NFS-Ereignisse werden in der Benutzeroberfläche nicht angezeigt.	Überprüfen Sie Folgendes: 1. Ein Benutzerverzeichnis-Collector für AD-Server mit festgelegten POSIX-Attributen sollte mit dem über die Benutzeroberfläche aktivierten UnixID-Attribut ausgeführt werden. 2. Jeder Benutzer mit NFS-Zugriff sollte bei der Suche auf der Benutzerseite von UI 3 angezeigt werden. Rohereignisse (Ereignisse, bei denen der Benutzer noch nicht erkannt wurde) werden für NFS 4 nicht unterstützt. Anonyme Zugriffe auf den NFS-Export werden nicht überwacht. 5. Stellen Sie sicher, dass die verwendete NFS-Version 4.1 oder niedriger ist. (Beachten Sie, dass NFS 4.1 mit ONTAP 9.15 oder höher unterstützt wird.)

Nachdem ich in den Filtern auf den Seiten „Alle Aktivitäten“ oder „Entitäten“ der Forensik einige Buchstaben mit Platzhalterzeichen wie einem Sternchen (*) eingegeben habe, werden die Seiten sehr langsam geladen.	Ein Sternchen (*) im Suchstring sucht nach allem. Führende Platzhalterzeichenfolgen wie *<*Suchbegriff*> oder *<*Suchbegriff*>* führen jedoch zu einer langsamen Abfrage. Um eine bessere Leistung zu erzielen, verwenden Sie stattdessen Präfixzeichenfolgen im Format <*Suchbegriff*>* (mit anderen Worten: Fügen Sie das Sternchen (*) *nach* einem Suchbegriff an). Beispiel: Verwenden Sie die Zeichenfolge *testvolume** anstelle von **testvolume* oder **test*volume*. Verwenden Sie eine Verzeichnissuche, um alle Aktivitäten unter einem bestimmten Ordner rekursiv anzuzeigen (hierarchische Suche). Beispielsweise listet „/Pfad1/Pfad2/Pfad3/“ alle Aktivitäten unter /Pfad1/Pfad2/Pfad3 rekursiv auf. Alternativ können Sie die Option „Zum Filter hinzufügen“ unter der Registerkarte „Alle Aktivitäten“ verwenden.
Beim Verwenden eines Pfadfilters tritt die Fehlermeldung „Anforderung fehlgeschlagen mit Statuscode 500/503“ auf.	Versuchen Sie, zum Filtern der Datensätze einen kleineren Datumsbereich zu verwenden.
Die forensische Benutzeroberfläche lädt Daten langsam, wenn der *Pfad*-Filter verwendet wird.	Für schnellere Ergebnisse werden Verzeichnispfadfilter (Pfadzeichenfolge endet mit /) mit einer Tiefe von bis zu 4 Verzeichnissen empfohlen. Wenn der Verzeichnispfad beispielsweise /Aaa/Bbb/Ccc/Ddd lautet, versuchen Sie, nach „/Aaa/Bbb/Ccc/Ddd/“ zu suchen, um die Daten schneller zu laden.
Die Forensics-Benutzeroberfläche lädt Daten langsam und weist Fehler auf, wenn der Entitätsnamenfilter verwendet wird.	Bitte versuchen Sie es mit kleineren Zeiträumen und mit einer genauen Wertesuche mit Anführungszeichen. Wenn der EntityPath beispielsweise „/home/userX/nested1/nested2/nested3/testfile.txt“ ist, versuchen Sie es mit „testfile.txt“ als Entity-Namensfilter.

Forensische Benutzerübersicht

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

Benutzerprofil

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

- Name des Benutzers
- E-Mail-Adresse des Nutzers
- Benutzermanager

- Telefonkontakt für den Benutzer
- Standort des Benutzers

Nutzerverhalten

Die Informationen zum Benutzerverhalten identifizieren die letzten Aktivitäten und Vorgänge, die der Benutzer durchgeführt hat. Zu diesen Informationen gehören:

- Letzte Aktivität
  - Letzter Zugriffsort
  - Aktivitätsdiagramm
  - Warnungen
- Operationen der letzten sieben Tage
  - Anzahl der Operationen

Aktualisierungsintervall

Die Benutzerliste wird alle 12 Stunden aktualisiert.

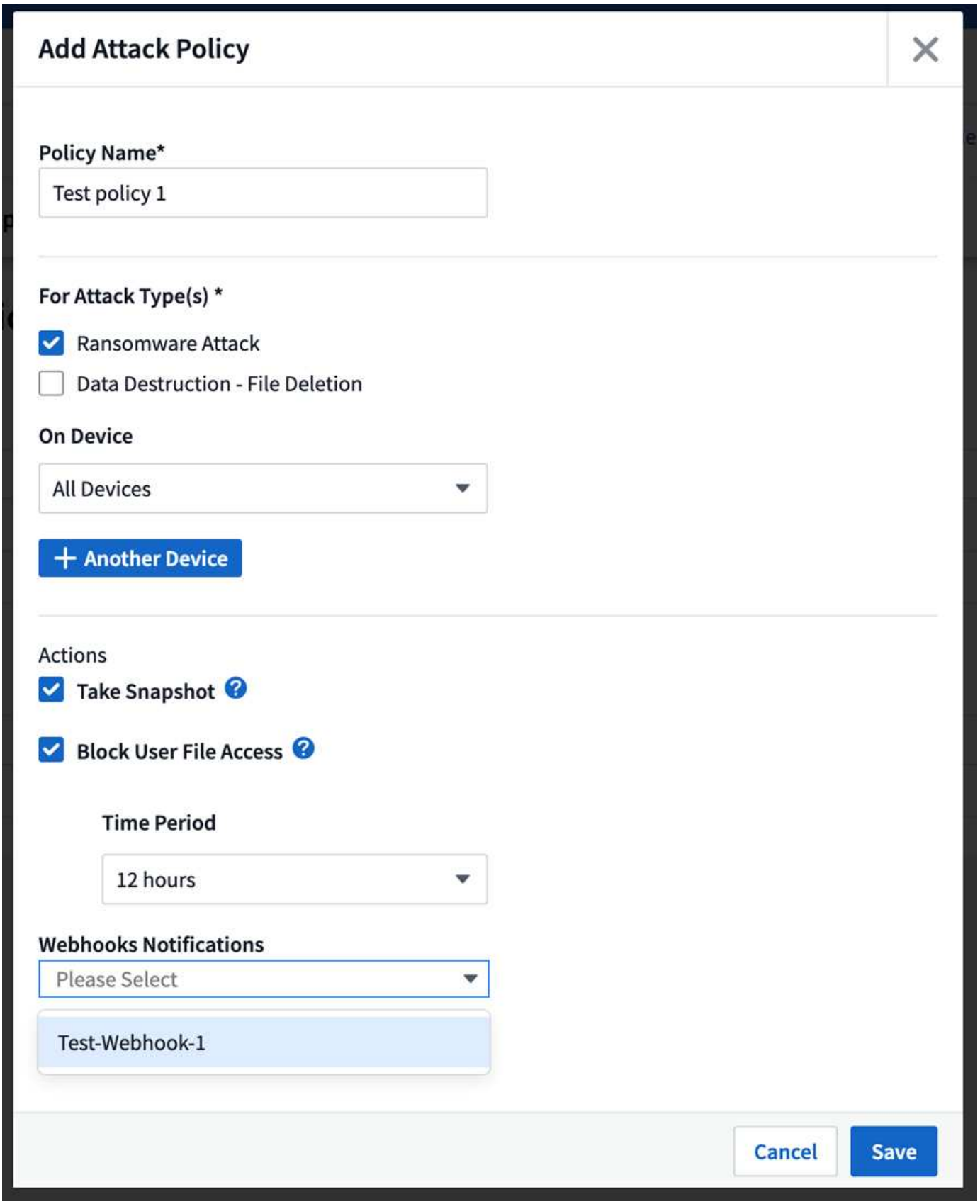
Aufbewahrungsrichtlinie

Wenn die Benutzerliste nicht erneut aktualisiert wird, bleibt sie 13 Monate lang erhalten. Nach 13 Monaten werden die Daten gelöscht. Wenn Ihre Workload Security-Umgebung gelöscht wird, werden alle mit der Umgebung verknüpften Daten gelöscht.

Richtlinien für automatisierte Antworten

Reaktionsrichtlinien lösen im Falle eines Angriffs oder abnormalen Benutzerverhaltens Aktionen aus, beispielsweise das Erstellen eines Snapshots oder die Einschränkung des Benutzerzugriffs.

Sie können Richtlinien für bestimmte oder alle Geräte festlegen. Um eine Antwortrichtlinie festzulegen, wählen Sie **Admin > Automatisierte Antwortrichtlinien** und klicken Sie auf die entsprechende Schaltfläche **+Richtlinie**. Sie können Richtlinien für Angriffe oder Warnungen erstellen.



Sie müssen die Richtlinie unter einem eindeutigen Namen speichern.

Um eine automatisierte Antwortaktion (z. B. „Snapshot erstellen“) zu deaktivieren, deaktivieren Sie einfach die Aktion und speichern Sie die Richtlinie.

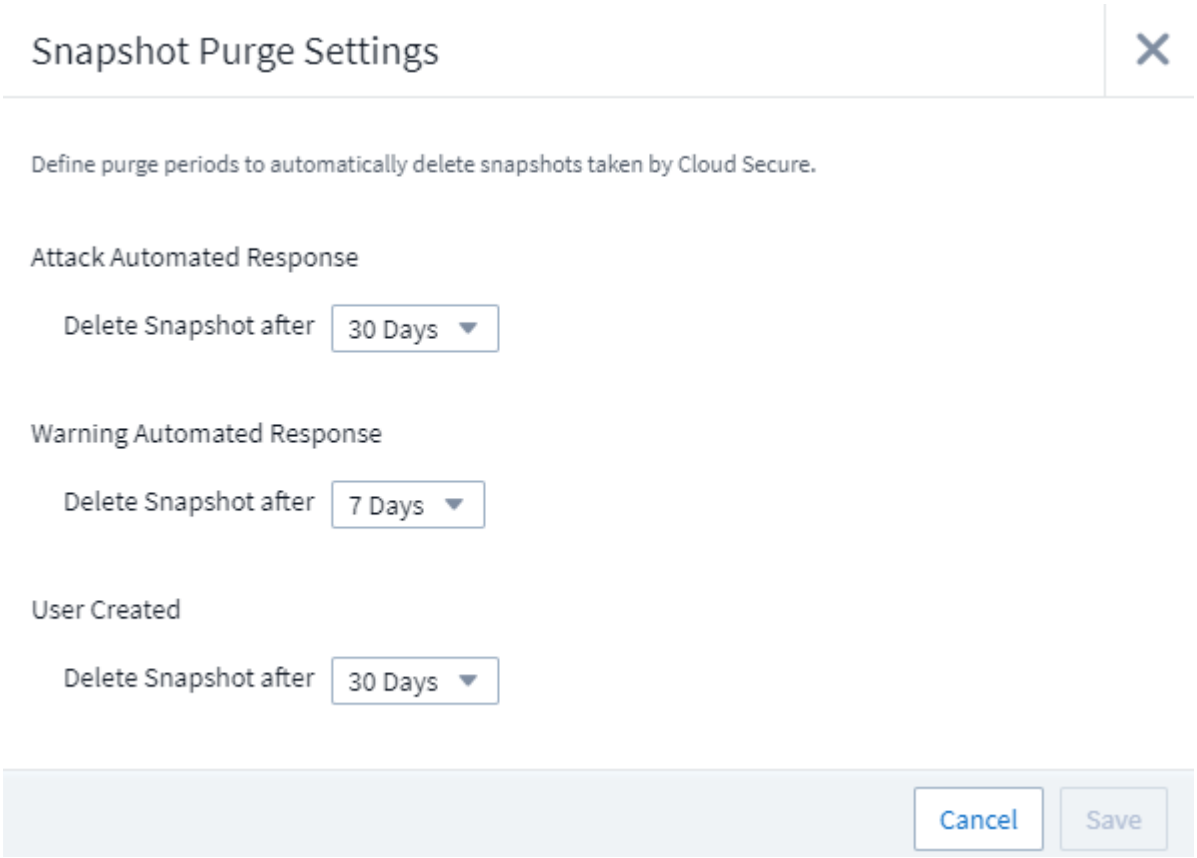
Wenn für die angegebenen Geräte (oder alle Geräte, falls ausgewählt) eine Warnung ausgelöst wird, erstellt die Richtlinie für automatisierte Antworten einen Snapshot Ihrer Daten. Sie können den Snapshot-Status auf der"Seite mit den Alarmdetails" .

Siehe die"Benutzerzugriff einschränken" Weitere Informationen zum Einschränken des Benutzerzugriffs per IP finden Sie auf der Seite.

Sie können einer Richtlinie einen oder mehrere Webhooks hinzufügen, um benachrichtigt zu werden, wenn eine Warnung erstellt und eine Aktion ausgeführt wird. Es wird empfohlen, einer Richtlinie nicht mehr als 10 Webhooks hinzuzufügen. Beachten Sie, dass keine Webhook-Benachrichtigungen ausgelöst werden, wenn eine Richtlinie angehalten wird.

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

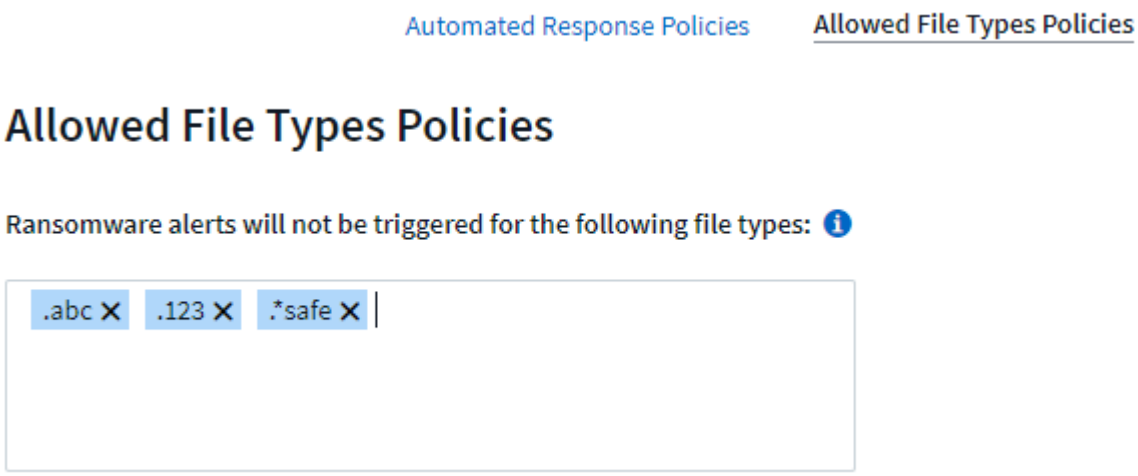
Workload Security löscht Snapshots basierend auf den Snapshot-Bereinigungseinstellungen automatisch einmal pro Tag.



Richtlinien für zulässige Dateitypen

Wird ein Angriff auf eine Dateimanipulation bei einer bekannten Dateierweiterung festgestellt und werden Warnungen auf dem Warnbildschirm generiert, kann diese Dateierweiterung einer Liste *zulässiger Dateitypen* hinzugefügt werden, um unnötige Warnungen zu vermeiden.

Navigieren Sie zu **Workload-Sicherheit > Richtlinien** und wechseln Sie zur Registerkarte *Richtlinien für zulässige Dateitypen*.



Sobald ein Dateityp zur Liste der zulässigen Dateitypen hinzugefügt wurde, wird für diesen zulässigen Dateityp keine Warnung vor Dateimanipulationsangriffen mehr generiert. Beachten Sie, dass die Richtlinie *Zulässige Dateitypen* nur für die Erkennung von Dateimanipulationen gilt.

Wenn beispielsweise eine Datei mit dem Namen *test.txt* in *test.txt.abc* umbenannt wird und Workload Security aufgrund der Dateiendung *.abc* einen Angriff auf Dateimanipulation feststellt, kann die Dateiendung *.abc* zur Liste der *zulässigen Dateitypen* hinzugefügt werden. Nach der Aufnahme in die Liste werden keine Dateimanipulationsangriffe mehr gegen Dateien mit der Erweiterung *.abc* generiert.

Zulässige Dateitypen können exakte Übereinstimmungen (z. B. „.abc“) oder Ausdrücke (z. B. „.**Typ“, „.Typ**“ oder „**Typ**“) sein. Ausdrücke der Typen „.a*c“, „.p*f“ werden nicht unterstützt.

Integration mit ONTAP Autonomous Ransomware Protection

Die ONTAP Funktion Autonomous Protection nutzt die Workload-Analyse in NAS-Umgebungen (NFS und SMB), um proaktiv ungewöhnliche Aktivitäten in Dateien zu erkennen und davor zu warnen, die auf böswillige Angriffe oder unautorisierte Datenänderungen hindeuten könnten.

Weitere Details und Lizenzanforderungen zu ARP finden Sie"hier," .

Workload Security lässt sich in ONTAP integrieren, um ARP-Ereignisse zu empfangen und eine zusätzliche Analyse- und automatische Antwortebene bereitzustellen.

Workload Security empfängt die ARP-Ereignisse von ONTAP und führt die folgenden Aktionen aus:

1. Korreliert Volume-Verschlüsselungsereignisse mit der Benutzeraktivität, um zu ermitteln, wer den Schaden verursacht.
2. Implementiert automatische Antwortrichtlinien (falls definiert)
3. Bietet forensische Funktionen:
    - Ermöglichen Sie Kunden die Durchführung von Untersuchungen zu Datenschutzverletzungen.
    - Ermitteln Sie, welche Dateien betroffen waren, und beschleunigen Sie so die Wiederherstellung und die Durchführung von Untersuchungen zu Datenschutzverletzungen.

Voraussetzungen

1. Mindestversion von ONTAP : 9.11.1
2. ARP-fähige Volumes. Details zur Aktivierung von ARP finden Sie"hier," . ARP muss über OnCommand System Manager aktiviert werden. Workload Security kann ARP nicht aktivieren.
3. Der Workload Security Collector sollte über die Cluster-IP hinzugefügt werden.
4. Damit diese Funktion funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich. Mit anderen Worten: Beim Hinzufügen der SVM müssen Anmeldeinformationen auf Clusterebene verwendet werden.

Erforderliche Benutzerberechtigungen

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

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

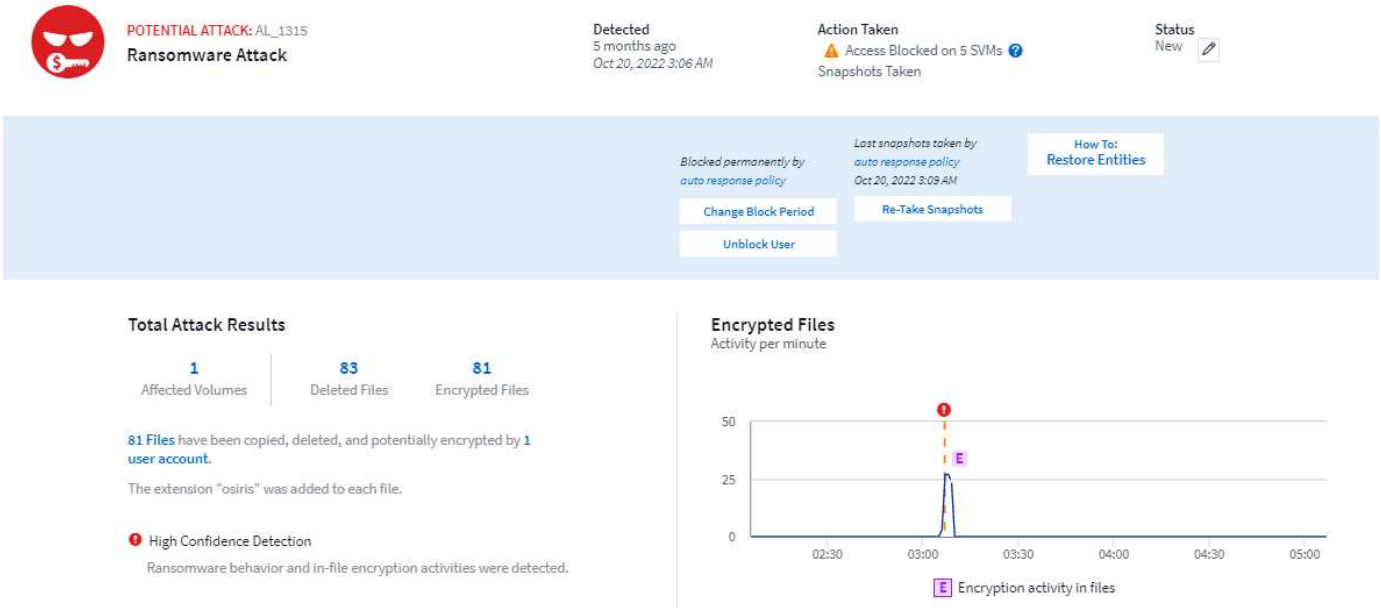
Führen Sie für *csuser* mit Cluster-Anmeldeinformationen Folgendes über die ONTAP Befehlszeile aus:

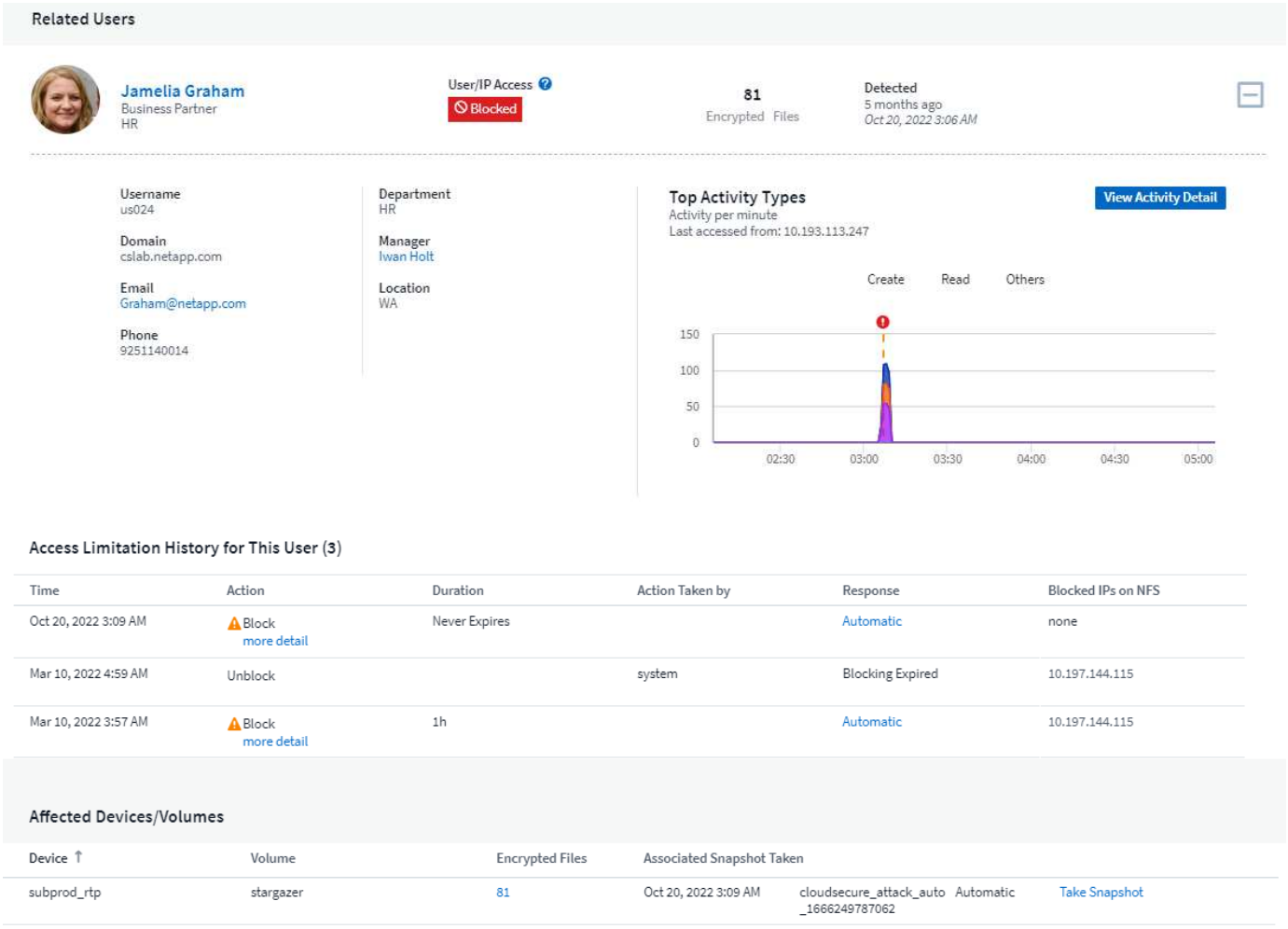
```
security login role create -role csrole -cmddirname "volume" -access
readonly
security login role create -role csrole -cmddirname "security anti-
ransomware volume" -access readonly
```

Lesen Sie mehr über die Konfiguration anderer"ONTAP-Berechtigungen" .

Beispielwarnung

Nachfolgend sehen Sie ein Beispiel für eine Warnung, die aufgrund eines ARP-Ereignisses generiert wurde:





Ein Banner mit hoher Konfidenz kennzeichnet Aktivitäten, bei denen der Angriff neben Dateiverschlüsselung auch Dateimanipulationen aufwies. Die Grafik der verschlüsselten Dateien zeigt den Zeitstempel an, zu dem die Aktivität der Datenträgerverschlüsselung von der ARP-Lösung erkannt wurde.

Einschränkungen

Falls eine SVM nicht von Workload Security überwacht wird, aber von ONTAP ARP-Ereignisse generiert werden, werden die Ereignisse dennoch von Workload Security empfangen und angezeigt. Forensische Informationen im Zusammenhang mit der Warnung sowie die Benutzerzuordnung werden jedoch nicht erfasst oder angezeigt.

Fehlerbehebung

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

Problem:	Auflösung:
E-Mail-Benachrichtigungen werden 24 Stunden nach Erkennung eines Angriffs empfangen. In der Benutzeroberfläche werden die Warnungen 24 Stunden vorher angezeigt, wenn die E-Mails von Data Infrastructure Insights Workload Security empfangen werden.	Wenn ONTAP das Ereignis *Ransomware erkannt* an Data Infrastructure Insights Workload Security (d. h. Workload Security) sendet, wird die E-Mail gesendet. Das Ereignis enthält eine Liste der Angriffe und deren Zeitstempel. Die Workload Security-Benutzeroberfläche zeigt den Alarmzeitstempel der ersten angegriffenen Datei an. ONTAP sendet das Ereignis *Ransomware erkannt* an Data Infrastructure Insights, wenn eine bestimmte Anzahl von Dateien verschlüsselt ist. Daher kann es zu einer Differenz zwischen dem Zeitpunkt, zu dem die Warnung in der Benutzeroberfläche angezeigt wird, und dem Zeitpunkt, zu dem die E-Mail gesendet wird, kommen.

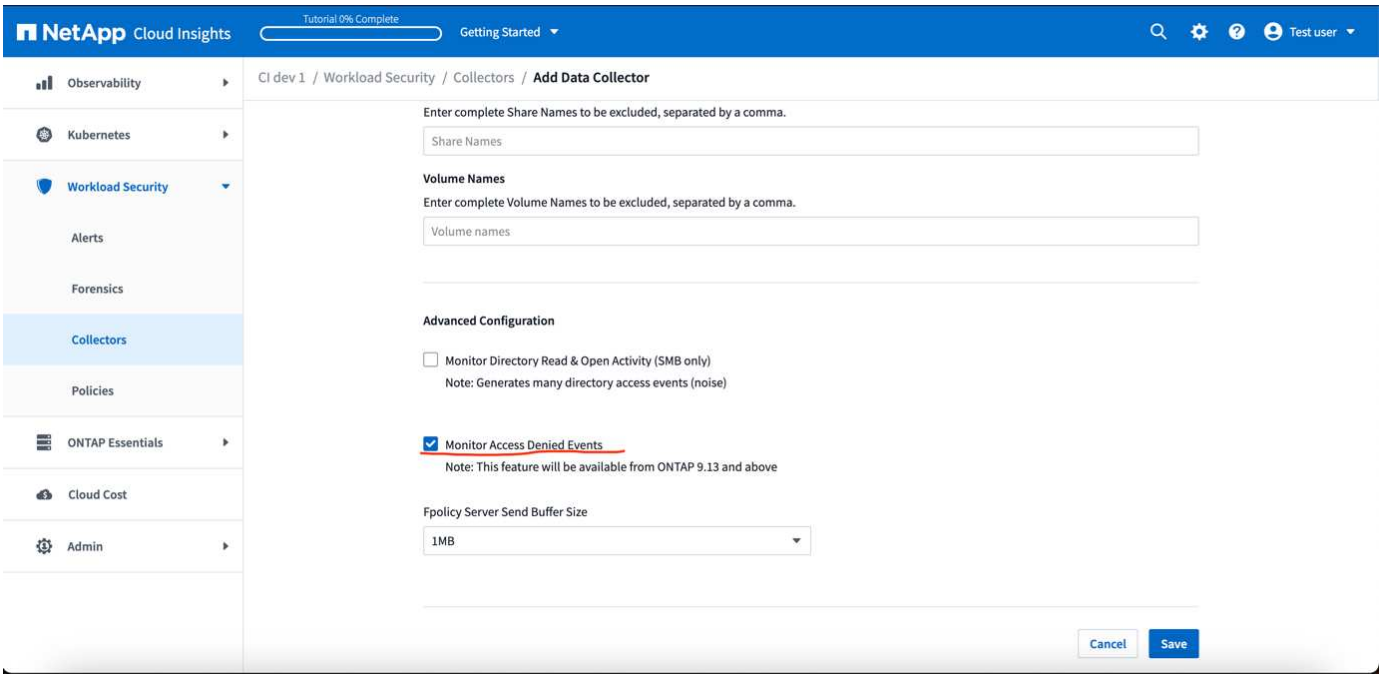
Integration mit ONTAP Access Denied

Die ONTAP Access Denied-Funktion verwendet eine Workload-Analyse in NAS-Umgebungen (NFS und SMB), um fehlgeschlagene Dateivorgänge (z. B. wenn ein Benutzer versucht, einen Vorgang auszuführen, für den er keine Berechtigung hat) proaktiv zu erkennen und davor zu warnen. Diese Benachrichtigungen über fehlgeschlagene Dateivorgänge – insbesondere bei sicherheitsrelevanten Fehlern – tragen zusätzlich dazu bei, Insider-Angriffe bereits im Frühstadium zu blockieren.

Data Infrastructure Insights Workload Security lässt sich in ONTAP integrieren, um Zugriffsverweigerungsereignisse zu empfangen und eine zusätzliche Analyse- und automatische Reaktionsebene bereitzustellen.

Voraussetzungen

- Mindestversion von ONTAP : 9.13.0.
- Ein Workload-Sicherheitsadministrator muss die Funktion „Zugriff verweigert“ aktivieren, wenn er einen neuen Collector hinzufügt oder einen vorhandenen Collector bearbeitet, indem er unter „Erweiterte Konfiguration“ das Kontrollkästchen „Ereignisse „Zugriff verweigert“ überwachen“ aktiviert.



Erforderliche Benutzerberechtigungen

Wenn der Datensammler mithilfe der Clusteradministrationsanmeldeinformationen hinzugefügt wird, sind keine neuen Berechtigungen erforderlich.

Wenn der Collector mithilfe eines benutzerdefinierten Benutzers (z. B. *csuser*) mit dem Benutzer erteilten Berechtigungen hinzugefügt wird, führen Sie die folgenden Schritte aus, um Workload Security die erforderliche Berechtigung zum Registrieren für Zugriffsverweigerungsereignisse bei ONTAP zu erteilen.

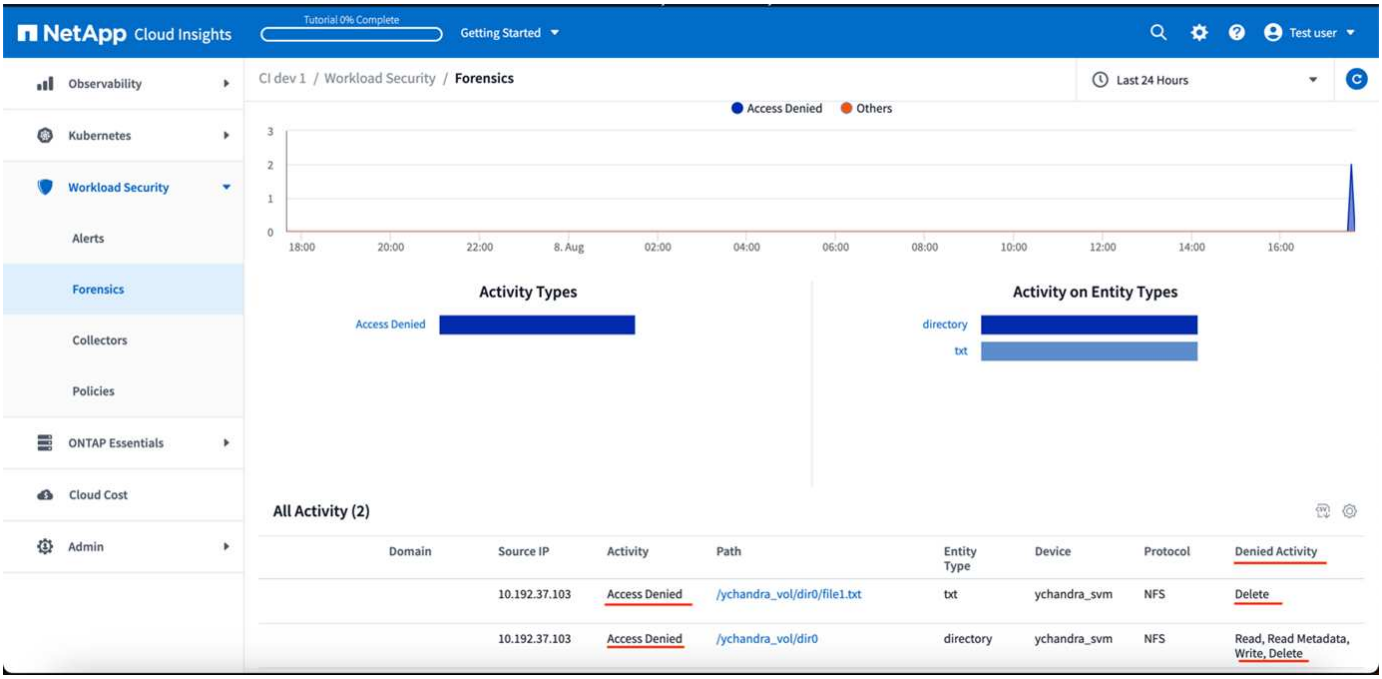
Führen Sie für csuser mit *cluster*-Anmeldeinformationen die folgenden Befehle über die ONTAP -Befehlszeile aus. Beachten Sie, dass diese Berechtigung möglicherweise bereits vorhanden ist.

```
 security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
Führen Sie für csuser mit _SVM_-Anmeldeinformationen die folgenden Befehle
über die ONTAP -Befehlszeile aus.  Beachten Sie, dass diese Berechtigung
möglicherweise bereits vorhanden ist.
```

```
 security login role create -vserver <vservername> -role csrole
-cmddirname "vserver fpolicy" -access all
Lesen Sie mehr über die Konfiguration
andererlink:task_add_collector_svm.html["ONTAP-Berechtigungen"] .
```

Ereignisse vom Typ „Zugriff verweigert“

Sobald Ereignisse vom ONTAP System abgerufen wurden, werden auf der Seite „Workload Security Forensics“ Ereignisse mit dem Status „Zugriff verweigert“ angezeigt. Zusätzlich zu den angezeigten Informationen können Sie die fehlenden Benutzerberechtigungen für einen bestimmten Vorgang anzeigen, indem Sie der Tabelle über das Zahnradsymbol die Spalte *Gewünschte Aktivität* hinzufügen.



Sperrung des Benutzerzugriffs zur Verhinderung von Angriffen

Um weitere Datenbeschädigung oder Datenexfiltration zu verhindern, müssen erkannte Angriffe umgehend gestoppt werden, indem der Zugriff kompromittierter Benutzer gesperrt wird. Die Workload-Sicherheit ermöglicht sowohl die automatische Blockierung durch automatisierte Reaktionsrichtlinien als auch das manuelle Eingreifen über Warnmeldungs- oder Benutzerdetailseiten und gibt Ihnen so eine flexible Kontrolle über Ihre Sicherheitsreaktion. Zugriffsbeschränkungen gelten automatisch für alle überwachten Speichervolumes und sind zeitlich begrenzt für die automatische Wiederherstellung.

Der Benutzer wird direkt für SMB blockiert und die IP-Adresse der Host-Computer, die den Angriff verursachen, wird für NFS blockiert. Den IP-Adressen dieser Maschinen wird der Zugriff auf alle von Workload Security überwachten Storage Virtual Machines (SVMs) verweigert.

Nehmen wir beispielsweise an, dass Workload Security 10 SVMs verwaltet und die Richtlinie für automatische Antworten für vier dieser SVMs konfiguriert ist. Wenn der Angriff von einer der vier SVMs ausgeht, wird der Zugriff des Benutzers auf allen 10 SVMs blockiert. Auf der ursprünglichen SVM wird weiterhin ein Snapshot erstellt.

Wenn vier SVMs vorhanden sind und eine SVM für SMB, eine für NFS und die beiden anderen sowohl für NFS als auch für SMB konfiguriert sind, werden alle SVMs blockiert, wenn der Angriff von einer der vier SVMs ausgeht.

Voraussetzungen für die Benutzerzugriffssperre

Damit diese Funktion funktioniert, sind Anmeldeinformationen auf Clusterebene erforderlich.

Wenn Sie Anmeldeinformationen für die Clusterverwaltung verwenden, sind keine neuen Berechtigungen erforderlich.

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

Führen Sie für csuser mit Cluster-Anmeldeinformationen Folgendes über die 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
```

Lesen Sie unbedingt den Abschnitt „Berechtigungen“ der"Konfigurieren des ONTAP SVM-Datenkollektors" Seite auch.

Wie aktiviere ich die Funktion?

- Navigieren Sie in Workload Security zu **Workload Security > Richtlinien > Richtlinien für automatisierte Antworten**. Wählen Sie **+Angriffsrichtlinie**.
- Wählen (aktivieren) Sie „Dateizugriff des Benutzers blockieren“.

Wie richte ich 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 „Dateizugriff des Benutzers blockieren“. Die Funktion wird aktiviert, wenn diese Option ausgewählt ist.
- Wählen Sie unter „Zeitraum“ den Zeitraum aus, bis zu dem die Sperre gelten soll.
- Um die automatische Benutzerblockierung zu testen, können Sie einen Angriff über eine"simuliertes Skript" .

Wie kann ich feststellen, ob es im System blockierte Benutzer gibt?

- Auf der Seite mit den Warnlisten wird oben auf dem Bildschirm ein Banner angezeigt, falls ein Benutzer blockiert wird.
- Durch Klicken auf das Banner gelangen Sie zur Seite „Benutzer“, auf der die Liste der blockierten Benutzer angezeigt wird.
- Auf der Seite „Benutzer“ gibt es eine Spalte mit der Bezeichnung „Benutzer-/IP-Zugriff“. In dieser Spalte wird der aktuelle Status der Benutzerblockierung angezeigt.

Manuelles Einschränken und Verwalten des Benutzerzugriffs

- Sie können zum Bildschirm mit den Alarmdetails oder Benutzerdetails gehen und dann von diesen

Bildschirmen aus einen Benutzer manuell sperren oder wiederherstellen.

Verlauf der Benutzerzugriffsbeschränkungen

Auf der Seite mit den Alarmdetails und Benutzerdetails im Benutzerbereich können Sie eine Prüfung des Zugriffsbeschränkungsverlaufs des Benutzers anzeigen: Zeit, Aktion (Blockieren, Entsperren), Dauer, durchgeführte Aktion, manuell/automatisch und betroffene IPs für NFS.

Wie deaktiviere ich die Funktion?

Sie können die Funktion jederzeit deaktivieren. Wenn im System eingeschränkte Benutzer vorhanden sind, müssen Sie deren Zugriff zuerst wiederherstellen.

- Navigieren Sie in Workload Security zu **Workload Security > Richtlinien > Richtlinien für automatisierte Antworten**. Wählen Sie **+Angriffsrichtlinie**.
- Deaktivieren Sie „Benutzerdateizugriff blockieren“.

Die Funktion wird auf allen Seiten ausgeblendet.

Manuelles Wiederherstellen von IPs für NFS

Führen Sie die folgenden Schritte aus, um alle IPs von ONTAP manuell wiederherzustellen, wenn Ihre Workload Security-Testversion abläuft oder der Agent/Collector ausgefallen 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
                                     nfs4,    10.11.12.13
                                     cifs
svm1         default         4       cifs,    0.0.0.0/0             any
                                     nfs
svm2         test            1       nfs3,    cloudsecure_rule,     never
                                     nfs4,    10.11.12.13
                                     cifs
svm3         test            3       cifs,    0.0.0.0/0             any
                                     nfs,
                                     flexcache
4 entries were displayed.
```

2. Löschen Sie die Regeln für alle Richtlinien auf der SVM, die „cloudsecure_rule“ als Client-Übereinstimmung haben, indem Sie den entsprechenden RuleIndex angeben. Die Workload-Sicherheitsregel steht normalerweise auf 1.

```
 contrail-qa-fas8020:*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Stellen Sie sicher, dass die Workload-Sicherheitsregel gelöscht ist
(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.
```

Manuelles Wiederherstellen von Benutzern für SMB

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

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

1. Melden Sie sich mit den Cluster-Admin-Anmeldeinformationen beim ONTAP -Cluster an (wo Sie die Blockierung der Benutzer aufheben möchten). (Melden Sie sich bei Amazon FSx mit Ihren FSx-Anmeldeinformationen an.)
2. Führen Sie den folgenden Befehl aus, um alle von Workload Security für SMB blockierten Benutzer in allen SVMs aufzulisten:

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

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

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

1. Sobald wir die Position anhand der obigen Ausgabe identifiziert haben, führen Sie den folgenden Befehl aus, um die Blockierung des Benutzers aufzuheben:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Bestätigen Sie die Blockierung der Benutzer, indem Sie den folgenden
Befehl ausführen:
```

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

Für die zuvor gesperrten Benutzer sollen keine Einträge mehr angezeigt werden.

Fehlerbehebung

Problem	Versuchen Sie Folgendes
Einige Benutzer werden nicht eingeschränkt, obwohl es einen Angriff gibt.	1. Stellen Sie sicher, dass sich der Datensammler und der Agent für die SVMs im Status „Ausführen“ befinden. Workload Security kann keine Befehle senden, wenn der Datensammler und der Agent gestoppt sind. 2. Dies liegt daran, dass der Benutzer möglicherweise von einem Computer mit einer neuen IP 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. Suchen Sie in der Benutzeroberfläche (Alarmdetails > Zugriffsbeschränkungsverlauf für diesen Benutzer > Betroffene IPs) nach der Liste der eingeschränkten IP-Adressen. Wenn der Benutzer auf den Speicher von einem Host aus zugreift, dessen IP-Adresse sich von den eingeschränkten IP-Adressen unterscheidet, kann der Benutzer dennoch über die nicht eingeschränkte IP-Adresse auf den Speicher zugreifen. Wenn der Benutzer versucht, von Hosts aus zuzugreifen, deren IPs eingeschränkt sind, ist der Speicher nicht zugänglich.
Wenn Sie manuell auf „Zugriff einschränken“ klicken, wird die Meldung „Die IP-Adressen dieses Benutzers wurden bereits eingeschränkt“ angezeigt.	Die einzuschränkende IP wird bereits von einem anderen Benutzer eingeschränkt.
Die Richtlinie konnte nicht geändert werden. Grund: Für diesen Befehl nicht autorisiert.	Überprüfen Sie, ob bei Verwendung von csuser dem Benutzer die oben genannten Berechtigungen erteilt wurden.

Problem	Versuchen Sie Folgendes
Die Benutzerblockierung (IP-Adresse) für NFS funktioniert, aber für SMB/CIFS wird eine Fehlermeldung angezeigt: „Die Umwandlung von SID in Domänenname ist fehlgeschlagen.“ Grund für Timeout: Socket ist nicht eingerichtet“	Dies kann passieren, wenn *csuser* keine Berechtigung zum Ausführen von SSH hat. (Stellen Sie die Verbindung auf Clusterebene sicher und stellen Sie dann sicher, dass der Benutzer SSH ausführen kann.) Die Rolle *csuser* erfordert diese Berechtigungen. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking Für *csuser* mit Cluster-Anmeldeinformationen führen Sie Folgendes von 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 Wenn *csuser* nicht verwendet wird und der Administratorbenutzer auf Clusterebene verwendet wird, stellen Sie sicher, dass der Administratorbenutzer über SSH-Berechtigungen für ONTAP verfügt.
Ich erhalte die Fehlermeldung *SID-Übersetzung fehlgeschlagen. Grund:255:Fehler: Befehl fehlgeschlagen: für diesen Befehl nicht autorisiert.Fehler: „access-check“ ist kein erkannter Befehl*, obwohl ein Benutzer hätte gesperrt werden sollen.	Dies kann passieren, wenn *csuser* nicht über die richtigen Berechtigungen verfügt. Sehen "Voraussetzungen für die Benutzerzugriffssperre" für weitere Informationen. Nach dem Anwenden der Berechtigungen wird empfohlen, den ONTAP Datensammler und den Benutzerverzeichnis-Datensammler neu zu starten. Die erforderlichen Berechtigungsbefehle sind unten aufgeführt. ---- Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-Exportrichtlinienregel" -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname festlegen -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-CIFS-Sitzung" -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-Dienste-Zugriffsprüfung, Authentifizierungsübersetzung" -alles zugreifen Sicherheits-Login-Rolle erstellen -role csrole -cmddirname "vServer-Namenszuordnung" -alles zugreifen ----

Workload-Sicherheit: Simulation von Dateimanipulationen

Mithilfe der Anweisungen auf dieser Seite können Sie die Manipulation von Dateien simulieren, um die Sicherheit von Arbeitslasten mithilfe des beigefügten Skripts zur Simulation der Dateimanipulation zu testen oder zu demonstrieren.

Dinge, die Sie vor dem Beginn beachten sollten

- Das Skript zur Simulation von Dateimanipulationen funktioniert nur unter Linux. Das Simulationsskript sollte außerdem Warnmeldungen mit hoher Zuverlässigkeit generieren, falls der Benutzer ONTAP ARP in die Workload-Sicherheit integriert hat.
- Workload Security erkennt mit NFS 4.1 generierte Ereignisse und Warnungen nur, wenn die ONTAP Version 9.15 oder höher ist.
- Das Skript wird mit den Installationsdateien des Workload Security-Agenten bereitgestellt. Es ist auf jedem Computer verfügbar, auf dem ein Workload Security-Agent installiert ist.
- Sie können das Skript auf der Workload Security-Agent-Maschine selbst ausführen. Es ist nicht erforderlich, eine weitere Linux-Maschine vorzubereiten. Wenn Sie das Skript jedoch lieber auf einem anderen System ausführen möchten, kopieren Sie das Skript einfach und führen Sie es dort aus.
- Benutzer können sich je nach ihren Präferenzen und Systemanforderungen entweder für das Python- oder das Shell-Skript entscheiden.
- Für das Python-Skript sind Installationen erforderlich. Wenn Sie Python nicht verwenden möchten, verwenden Sie das Shell-Skript.

Richtlinien:

Dieses Skript sollte auf einer SVM ausgeführt werden, die einen Ordner mit einer beträchtlichen Anzahl zu verschlüsselnder Dateien enthält, idealerweise 100 oder mehr, einschließlich Dateien in Unterordnern. Stellen Sie sicher, dass die Dateien nicht leer sind.

Um die Warnung zu generieren, halten Sie den Collector vor der Erstellung der Testdaten vorübergehend an. Sobald die Beispieldateien generiert sind, setzen Sie den Collector fort und starten Sie den Verschlüsselungsprozess.

Schritte:

Bereiten Sie das System vor:

Mounten Sie zunächst das Zielvolume auf der Maschine. Sie können entweder einen NFS- oder einen CIFS-Export mounten.

So mounten Sie den NFS-Export unter Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Mounten Sie NFS Version 4.1 nicht, da es von Fpolicy nicht unterstützt wird.

So mounten Sie CIFS unter Linux:

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
```

ONTAP Autonomous Ransomware Protection aktivieren (Optional):

Wenn Ihre ONTAP Clusterversion 9.11.1 oder höher ist, können Sie den ONTAP Ransomware Protection-Dienst aktivieren, indem Sie den folgenden Befehl auf der ONTAP Befehlskonsole ausführen.

```
 security anti-ransomware volume enable -volume [volume_name] -vserver
[svm_name]
Richten Sie als Nächstes einen Datensammler ein:
```

1. Konfigurieren Sie den Workload Security-Agenten, falls dies noch nicht geschehen ist.
2. Konfigurieren Sie einen SVM-Datensammler, falls dies noch nicht geschehen ist.
3. Stellen Sie sicher, dass beim Konfigurieren des Datensammlers das Mount-Protokoll ausgewählt ist.

Generieren Sie die Beispieldateien programmgesteuert:

Bevor Sie die Dateien erstellen, müssen Sie zuerst stoppen oder"den Datensammler anhalten" Verarbeitung.

Bevor Sie die Simulation ausführen, müssen Sie zunächst zu verschlüsselnde Dateien hinzufügen. Sie können die zu verschlüsselnden Dateien entweder manuell in den Zielordner kopieren oder eines der enthaltenen Skripte verwenden, um die Dateien programmgesteuert zu erstellen. Unabhängig davon, welche Methode Sie verwenden, stellen Sie sicher, dass mindestens 100 Dateien zum Verschlüsseln vorhanden sind.

Wenn Sie die Dateien programmgesteuert erstellen möchten, können Sie die Shell oder Python verwenden:

Hülse:

1. Melden Sie sich beim Agentenfeld an.
2. Mounten Sie eine NFS- oder CIFS-Freigabe vom SVM des Filers auf der Agent-Maschine. Wechseln Sie mit CD in diesen Ordner.
3. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/create_dataset.sh) an den Ziel-Mount-Speicherort.
4. Führen Sie den folgenden Befehl mithilfe der Skripts im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Ordner und die Dateien des Testdatensatzes zu erstellen:

   ```
    './create_dataset.sh'
   . Dadurch werden 100 nicht leere Dateien mit verschiedenen Erweiterungen
   im Mount-Ordner unter einem Verzeichnis namens „test_dataset“ erstellt.
   ```

Python:

Python-Skript Voraussetzung:

- Installieren Sie Python (falls noch nicht installiert).
  - Laden Sie Python 3.5.2 oder höher herunter von https://www.python.org/ .
  - Um die Python-Installation zu überprüfen, führen Sie `python --version` .
  - Das Python-Skript wurde bereits in Versionen ab 3.5.2 getestet.

- Installieren Sie pip, falls es noch nicht installiert ist:
  - Laden Sie das Skript get-pip.py herunter von https://bootstrap.pypa.io/ .
  - Installieren Sie pip mit `python get-pip.py` .
  - Überprüfen Sie die Pip-Installation mit `pip --version` .
- PyCryptodome-Bibliothek:
  - Das Skript verwendet die PyCryptodome-Bibliothek.
  - Installieren Sie PyCryptodome mit `pip install pycryptodome` .
  - Bestätigen Sie die Installation von PyCryptodome durch Ausführen `pip show pycryptodome` .

Python-Skript zum Erstellen von Dateien:

1. Melden Sie sich beim Agentenfeld an.
2. Mounten Sie eine NFS- oder CIFS-Freigabe vom SVM des Filers auf der Agent-Maschine. Wechseln Sie mit CD in diesen Ordner.
3. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/create_dataset.py) an den Ziel-Mount-Speicherort.
4. Führen Sie den folgenden Befehl mithilfe der Skripts im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Ordner und die Dateien für den Testdatensatz zu erstellen:

```
 'python create_dataset.py'
. Dadurch werden 100 nicht leere Dateien mit verschiedenen Erweiterungen
im Mount-Ordner unter einem Verzeichnis namens „test_dataset“ erstellt.
```

Fortsetzen des Collectors

Wenn Sie den Collector vor dem Ausführen dieser Schritte angehalten haben, denken Sie bitte daran, den Collector wieder aufzunehmen, sobald die Beispieldateien erstellt wurden.

Generieren Sie die Beispieldateien programmgesteuert:

Bevor Sie die Dateien erstellen, müssen Sie zuerst stoppen oder"den Datensammler anhalten" Verarbeitung.

Um eine Warnung wegen Dateimanipulation zu generieren, können Sie das beigefügte Skript ausführen, das eine solche Warnung in Workload Security simuliert.

Hülse:

1. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/shell/simulate_attack.sh) an den Ziel-Mount-Speicherort.
2. Führen Sie den folgenden Befehl mithilfe der Skripte im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Testdatensatz zu verschlüsseln:

```
 './simulate_attack.sh'
. Dadurch werden die im Verzeichnis „test_dataset“ erstellten
Beispieldateien verschlüsselt.
```

Python:

1. Kopieren Sie das Skript aus dem Agent-Installationsverzeichnis (%AGENT_INSTALL_DIR/agent/install/ransomware_simulation/python/simulate_attack.py) an den Ziel-Mount-Speicherort.
2. Bitte beachten Sie, dass die Python-Voraussetzungen gemäß dem Abschnitt „Voraussetzungen für Python-Skripte“ installiert werden.
3. Führen Sie den folgenden Befehl mithilfe der Skripte im bereitgestellten Verzeichnis (z. B. /root/demo) aus, um den Testdatensatz zu verschlüsseln:

```
 'python simulate_attack.py'
. Dadurch werden die im Verzeichnis „test_dataset“ erstellten
Beispieldateien verschlüsselt.
```

Generieren einer Warnung in Workload Security

Sobald die Ausführung des Simulatorskripts abgeschlossen ist, wird innerhalb weniger Minuten eine Warnung auf der Web-Benutzeroberfläche angezeigt.

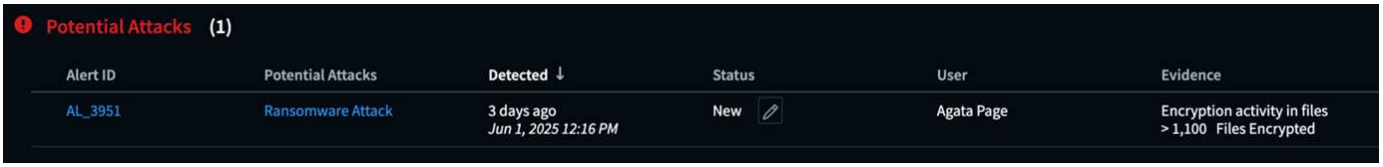
Hinweis: Falls alle der folgenden Bedingungen erfüllt sind, wird eine Warnung mit hoher Zuverlässigkeit generiert.

1. Überwachte SVM- ONTAP Version höher als 9.11.1
2. ONTAP Autonomous Ransomware Protection konfiguriert
3. Der Workload Security Data Collector wird im Clustermodus hinzugefügt.

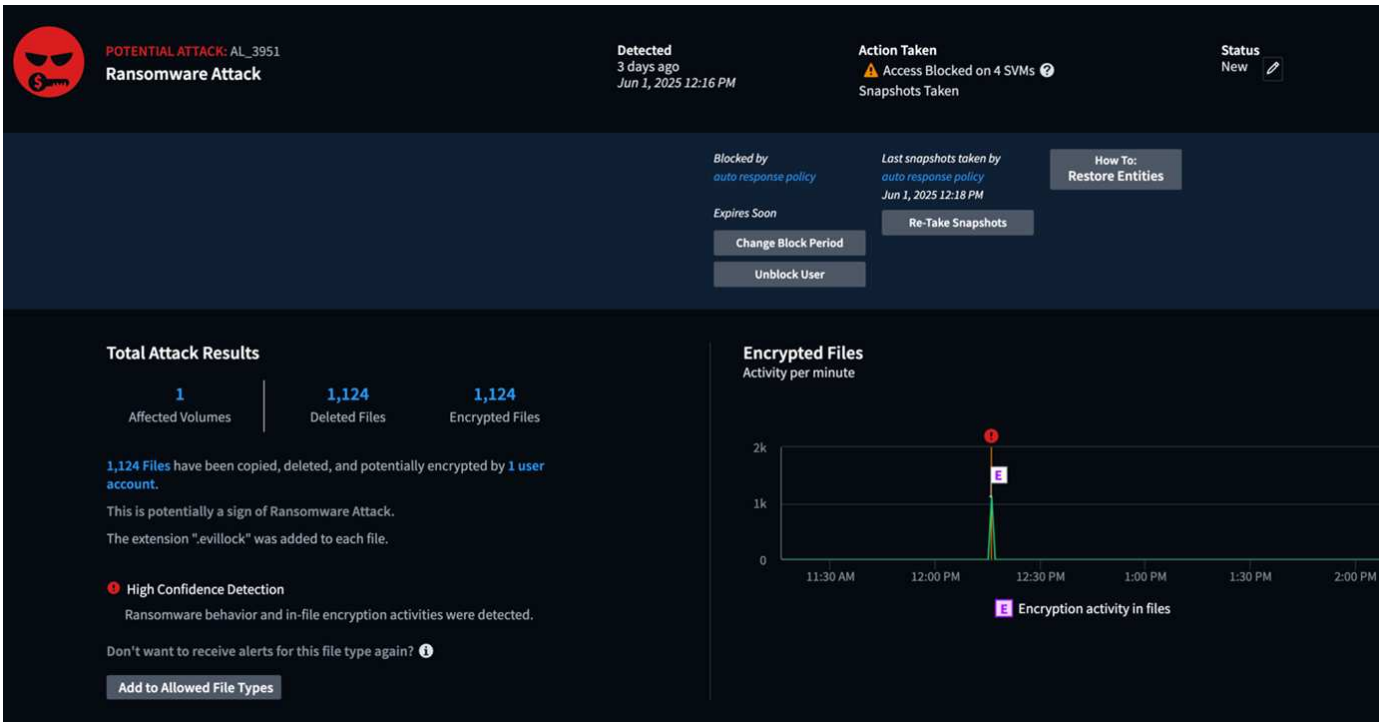
Workload Security erkennt Dateimanipulationsmuster anhand des Benutzerverhaltens, während ONTAP ARP Dateimanipulationsaktivitäten anhand von Verschlüsselungsaktivitäten in Dateien erkennt.

Wenn die Bedingungen erfüllt sind, kennzeichnet Workload Security die Warnungen als Warnungen mit hoher Zuverlässigkeit.

Beispiel für eine Warnung mit hoher Zuverlässigkeit auf der Seite mit der Warnungsliste:



Beispiel für Details einer Warnung mit hoher Zuverlässigkeit:



Alarm wird mehrmals ausgelöst

Workload Security lernt das Benutzerverhalten und generiert keine Warnmeldungen bei wiederholten Dateimanipulationsangriffen innerhalb von 24 Stunden für denselben Benutzer.

Um einen neuen Alarm mit einem anderen Benutzer zu generieren, führen Sie bitte dieselben Schritte erneut aus (Erstellen von Testdaten und anschließendes Verschlüsseln der Testdaten).

Konfigurieren von E-Mail-Benachrichtigungen für Alarme, Warnungen und den Zustand von Agenten/Datenquellen-Sammlern

E-Mail-Benachrichtigungen ermöglichen es Ihnen, über potenzielle Angriffe, Sicherheitswarnungen und Probleme mit der Infrastruktur auf dem Laufenden zu bleiben, sobald diese auftreten. Konfigurieren Sie die E-Mail-Adressen der Empfänger unter Admin > Benachrichtigungen, um Echtzeit-Benachrichtigungen zu erhalten, die auf die jeweiligen Verantwortlichkeiten der Empfänger zugeschnitten sind.

Alarme und Warnungen vor potenziellen Angriffen

Um Warnmeldungen zu *potenziellen Angriffen* zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt *Warnmeldungen zu potenziellen Angriffen senden* ein. Für jede Aktion im Zusammenhang mit der Warnung werden E-Mail-Benachrichtigungen an die Empfängerliste der Warnung gesendet.

Um *Warnbenachrichtigungen* zu senden, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt *Warnmeldungen senden* ein.

Integritätsüberwachung für Agenten und Datensammler

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

Um Benachrichtigungen zu erhalten, falls ein Agent oder Datenquellensammler nicht funktioniert, geben Sie die E-Mail-Adressen der Empfänger im Abschnitt „Warnungen zum Zustand der Datensammlung“ ein.

Beachten Sie Folgendes:

- Gesundheitswarnungen werden erst gesendet, wenn der Agent/Sammler mindestens eine Stunde lang keine Berichte mehr sendet.
- Innerhalb eines Zeitraums von 24 Stunden wird nur eine E-Mail-Benachrichtigung an die vorgesehenen Empfänger gesendet, selbst wenn die Verbindung zum Agenten oder Datensammler für einen längeren Zeitraum unterbrochen ist.
- Im Falle eines Agentenfehlers wird eine Warnung gesendet (nicht eine pro Collector). Die E-Mail enthält eine Liste aller betroffenen SVMs.
- Ein Fehler bei der Active Directory-Datenerfassung wird als Warnung gemeldet; er hat keinen Einfluss auf die Bedrohungserkennung.
- Die Setup-Liste „Erste Schritte“ enthält jetzt eine neue Phase „E-Mail-Benachrichtigungen konfigurieren“.

Empfangen von Agent- und Data Collector-Upgrade-Benachrichtigungen

- Geben Sie die E-Mail-ID(s) in den „Health Alerts zur Datenerfassung“ ein.
- Das Kontrollkästchen „Upgrade-Benachrichtigungen aktivieren“ wird aktiviert.
- E-Mail-Benachrichtigungen zu Agent- und Data Collector-Upgrades werden einen Tag vor dem geplanten Upgrade an die E-Mail-IDs gesendet.

Fehlerbehebung

Problem:	Versuchen Sie Folgendes:
In den „Data Collector Health Alerts“ sind E-Mail-IDs vorhanden, ich erhalte jedoch keine Benachrichtigungen.	Benachrichtigungs-E-Mails werden von der NetApp Data Infrastructure Insights Domäne gesendet, d. h. von *accounts@service.cloudinsights.netapp.com*. Einige Unternehmen blockieren eingehende E-Mails, wenn diese von einer externen Domäne stammen. Stellen Sie sicher, dass externe Benachrichtigungen von NetApp Data Infrastructure Insights -Domänen auf die Whitelist gesetzt werden.

Webhook-Benachrichtigungen

Workload-Sicherheitsbenachrichtigungen mithilfe von Webhooks

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal kritische Warnmeldungen oder Warnmeldungen an verschiedene Anwendungen senden.

Viele kommerzielle Anwendungen unterstützen Webhooks als Standardeingabeschnittstelle, zum Beispiel: Slack, PagerDuty, Teams und Discord. Durch die Unterstützung eines generischen, anpassbaren Webhook-Kanals kann Workload Security viele dieser Bereitstellungskanäle unterstützen. Informationen zur

Konfiguration der Webhooks finden Sie auf den Webseiten der jeweiligen Anwendungen. Slack bietet beispielsweise"dieser nützliche Leitfaden" .

Sie können mehrere Webhook-Kanäle erstellen, wobei jeder Kanal einem anderen Zweck, separaten Anwendungen, verschiedenen Empfängern usw. dient.

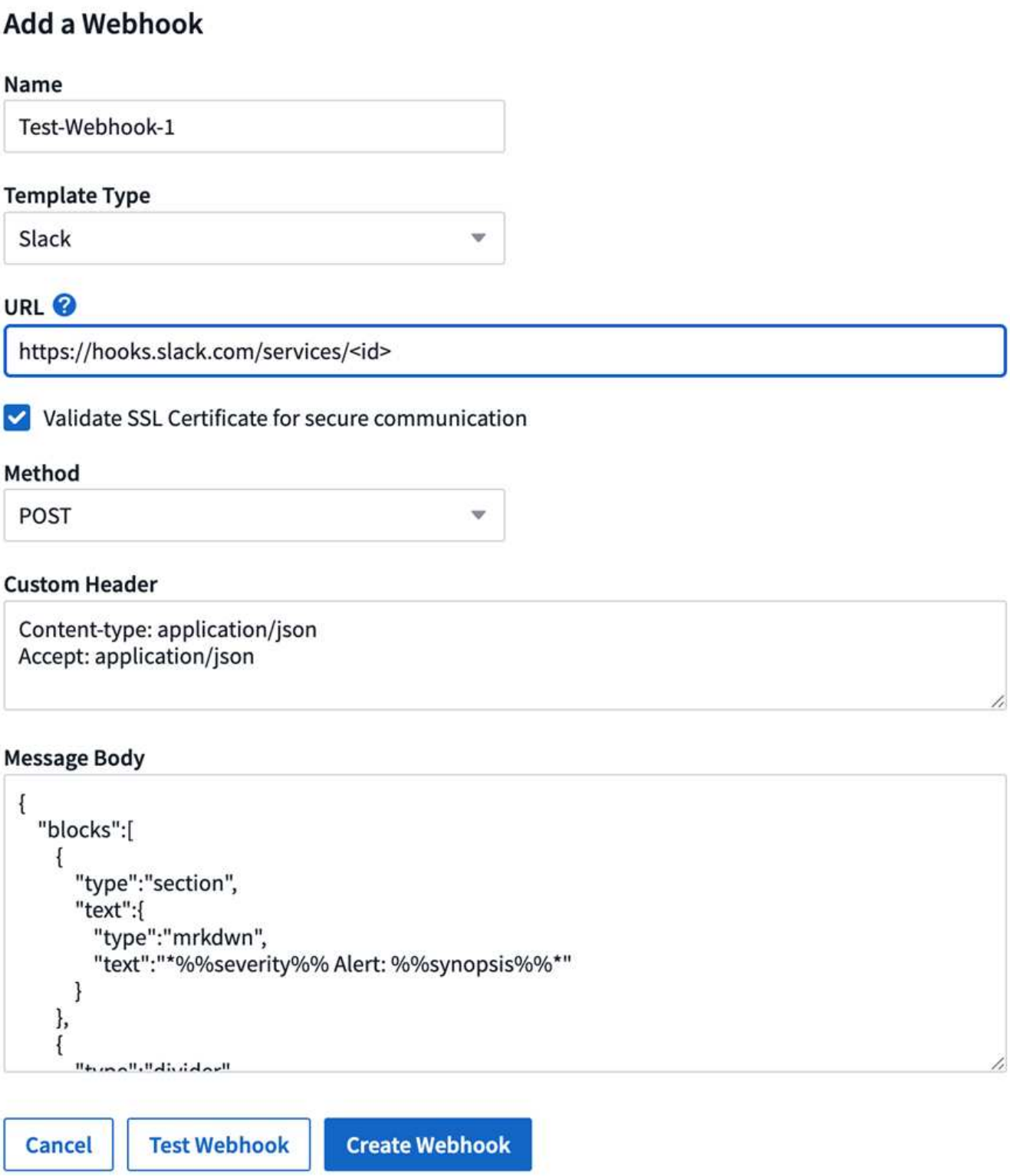
Die Webhook-Kanalinstanz besteht aus den folgenden Elementen

Name	Beschreibung
URL	Webhook-Ziel-URL, einschließlich des Präfixes http:// oder https:// zusammen mit den URL-Parametern
Verfahren	GET/POST – Standard ist POST
Benutzerdefinierter Header	Geben Sie hier alle benutzerdefinierten Header an
Nachrichtentext	Geben Sie hier den Text Ihrer Nachricht ein
Standard-Alarmparameter	Listet die Standardparameter für den Webhook auf
Benutzerdefinierte Parameter und Geheimnisse	Benutzerdefinierte Parameter und Geheimnisse ermöglichen Ihnen das Hinzufügen einzigartiger Parameter und sicherer Elemente wie Passwörter

Erstellen eines Webhooks

Um einen Workload Security Webhook zu erstellen, gehen Sie zu Admin > Benachrichtigungen und wählen Sie die Registerkarte „Workload Security Webhooks“. Das folgende Bild zeigt einen Beispielbildschirm zum Erstellen eines Slack-Webhooks.

Hinweis: Der Benutzer muss ein Workload Security-Administrator sein, um Workload Security-Webhooks erstellen und verwalten zu können.



- Geben Sie in jedes Feld die entsprechenden Informationen ein und klicken Sie auf „Speichern“.
- Sie können auch auf die Schaltfläche „Webhook testen“ klicken, um die Verbindung zu testen. Beachten Sie, dass dadurch der „Nachrichtentext“ (ohne Ersetzungen) gemäß der ausgewählten Methode an die definierte URL gesendet wird.
- SWS-Webhooks umfassen eine Reihe von Standardparametern. Darüber hinaus können Sie Ihre eigenen benutzerdefinierten Parameter oder Geheimnisse erstellen.

Parameter: Was sind sie und wie werden sie verwendet?

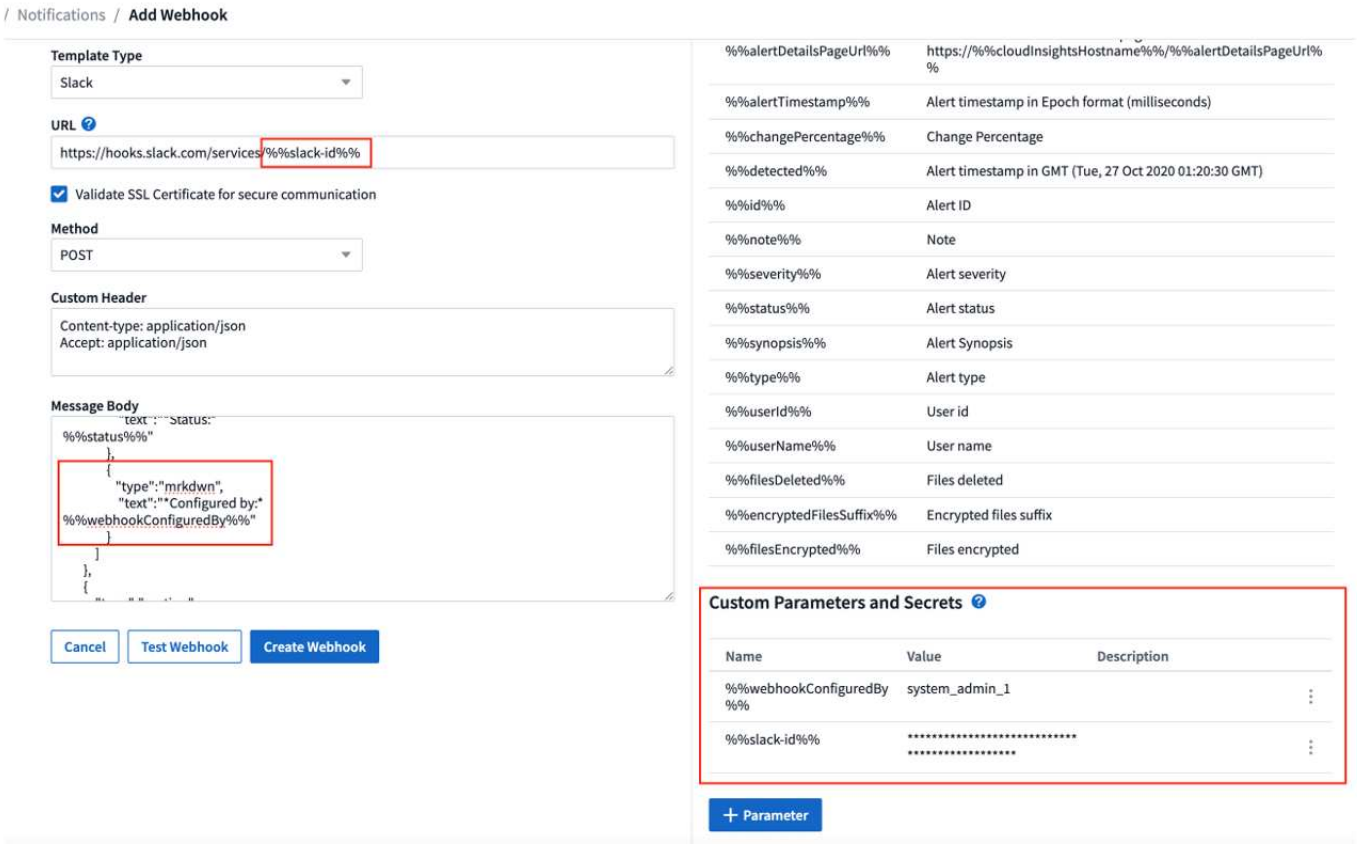
Alarmparameter sind dynamische Werte, die pro Alarm ausgefüllt werden. Beispielsweise wird der Parameter *%%severity%%* durch den Schweregradtyp der Warnung ersetzt.

Beachten Sie, dass beim Klicken auf die Schaltfläche „Webhook testen“ keine Ersetzungen durchgeführt werden. Der Test sendet eine Nutzlast, die die Platzhalter des Parameters (*%%<param-name>%%*) anzeigt, diese jedoch nicht durch Daten ersetzt.

Benutzerdefinierte Parameter und Geheimnisse

In diesem Abschnitt können Sie beliebige benutzerdefinierte Parameter und/oder Geheimnisse hinzufügen. Ein benutzerdefinierter Parameter oder ein Geheimnis kann in der URL oder im Nachrichtentext enthalten sein. Mithilfe von Geheimnissen können Benutzer sichere benutzerdefinierte Parameter wie Kennwort, API-Schlüssel usw. konfigurieren.

Das folgende Beispielbild zeigt, wie benutzerdefinierte Parameter bei der Webhook-Erstellung verwendet werden.



Seite „Workload Security Webhooks – Liste“

Auf der Webhook-Listenseite werden die Felder „Name“, „Erstellt von“, „Erstellt am“, „Status“, „Sicher“ und „Zuletzt gemeldet“ angezeigt. Hinweis: Der Wert der Spalte „Status“ ändert sich ständig basierend auf dem Ergebnis des letzten Webhook-Triggers. Nachfolgend finden Sie Beispiele für Statusergebnisse.

Status	Beschreibung
OK	Benachrichtigung erfolgreich gesendet.

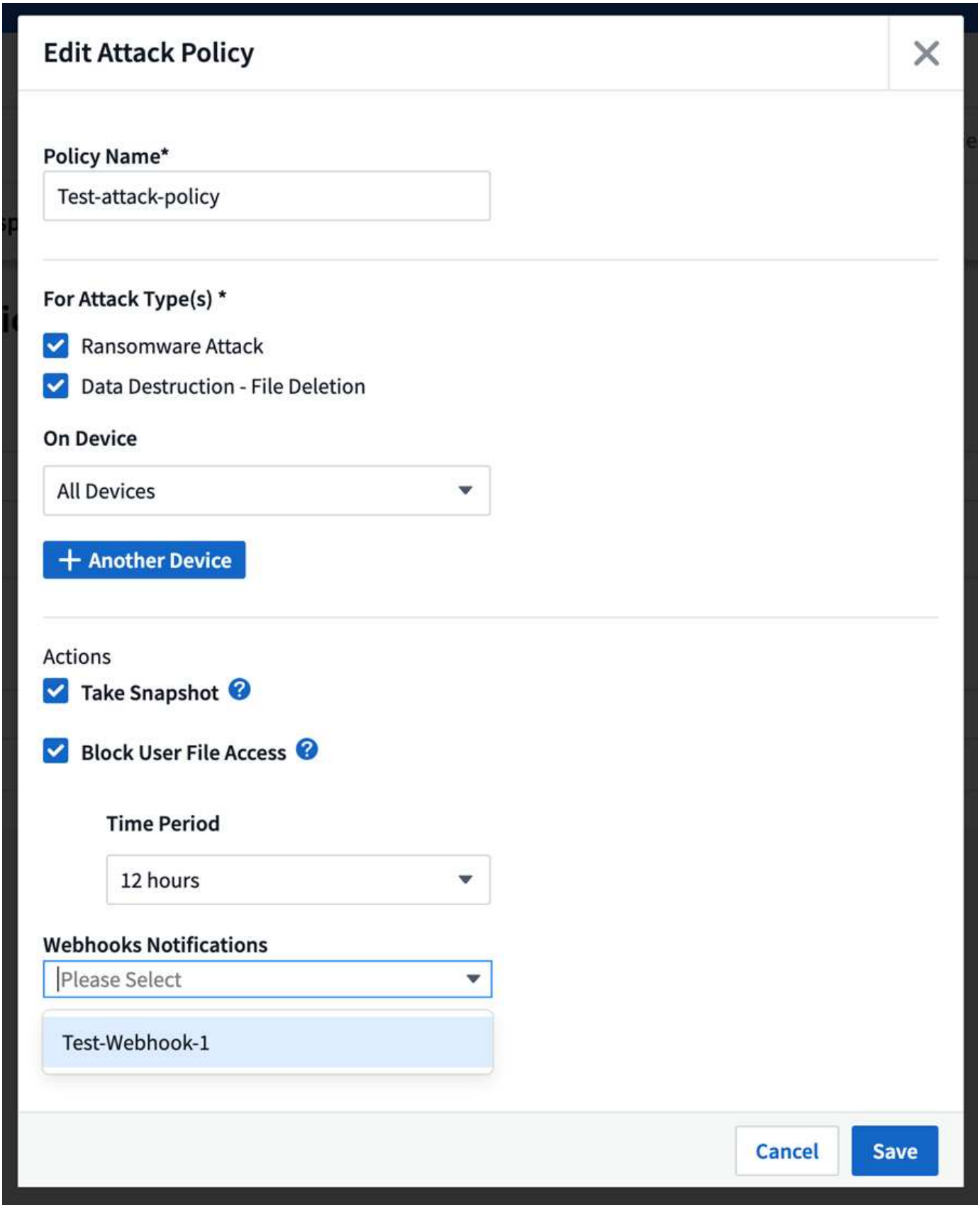
403	Verboten.
404	URL nicht gefunden.
400	Ungültige Anforderung. Dieser Status wird möglicherweise angezeigt, wenn im Nachrichtentext ein Fehler vorliegt, beispielsweise: • Schlecht formatiertes JSON. • Bereitstellung eines ungültigen Werts für reservierte Schlüssel. Beispielsweise akzeptiert PagerDuty für „Schweregrad“ nur „kritisch“/„Warnung“/„Fehler“/„Info“. Jedes andere Ergebnis kann zu einem 400-Status führen. • Anwendungsspezifische Validierungsfehler. Beispielsweise erlaubt Slack maximal 10 Felder innerhalb eines Abschnitts. Wenn Sie mehr als 10 angeben, kann dies zu einem 400-Status führen.
410	Ressource ist nicht mehr verfügbar

Die Spalte „Zuletzt gemeldet“ gibt den Zeitpunkt an, zu dem der Webhook zuletzt ausgelöst wurde.

Auf der Webhook-Listenseite können Benutzer Webhooks auch bearbeiten/duplizieren/löschen.

Konfigurieren der Webhook-Benachrichtigung in der Warnrichtlinie

Um einer Warnrichtlinie eine Webhook-Benachrichtigung hinzuzufügen, gehen Sie zu -Workload-Sicherheit > Richtlinien- und wählen Sie eine vorhandene Richtlinie aus oder fügen Sie eine neue Richtlinie hinzu. Wählen Sie im Abschnitt „Aktionen“ > Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus.



Webhook-Benachrichtigungen sind an Richtlinien gebunden. Wenn der Angriff (RW/DD/WARN) stattfindet, wird die konfigurierte Aktion (Snapshot erstellen/Benutzer blockieren) ausgeführt und anschließend die zugehörige Webhook-Benachrichtigung ausgelöst.

Hinweis: E-Mail-Benachrichtigungen sind unabhängig von Richtlinien und werden wie gewohnt ausgelöst.

- Wenn eine Richtlinie angehalten wird, werden keine Webhook-Benachrichtigungen ausgelöst.
- An eine einzelne Richtlinie können mehrere Webhooks angehängt werden. Es wird jedoch empfohlen, nicht mehr als 5 Webhooks an eine Richtlinie anzuhängen.

Beispiele für Workload-Sicherheits-Webhooks

Webhooks für"Locker"

Webhooks für"PagerDuty" Webhooks für"Teams" Webhooks für"Zwietracht"

Workload Security Webhook-Beispiel für Discord

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Discord.

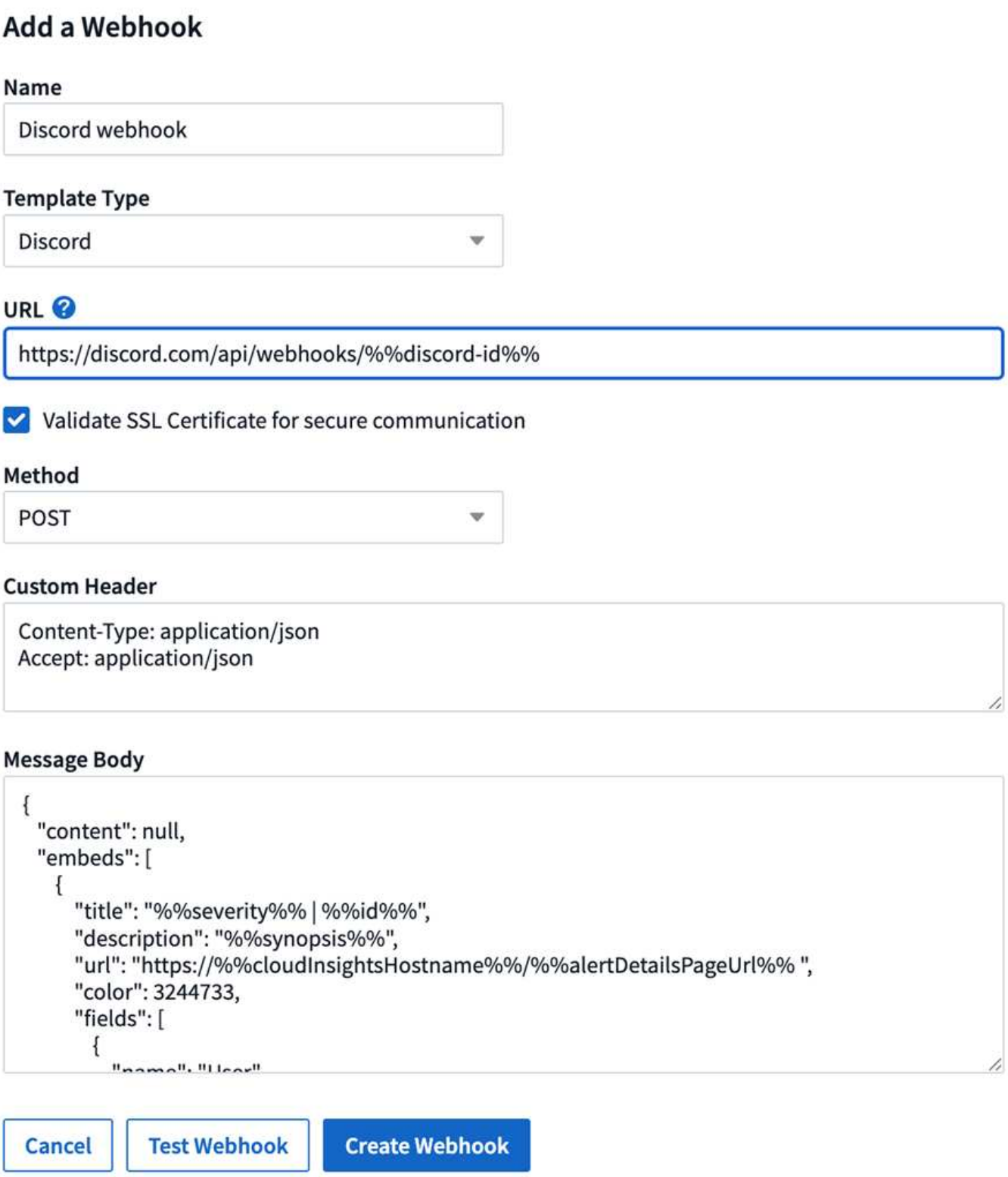
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"Discord-Dokumentation" für die aktuellsten Informationen.

Discord-Setup:

- Wählen Sie in Discord den Server aus und wählen Sie unter „Textkanäle“ die Option „Kanal bearbeiten“ (Zahnradsymbol).
- Wählen Sie **Integrationen > Webhooks anzeigen** und klicken Sie auf **Neuer Webhook**
- Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload-Sicherheits-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Klicken Sie auf „+ Webhook“, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ **Discord** aus.
4. Fügen Sie die Discord-URL von oben in das Feld *URL* ein.



Um den Webhook zu testen, ersetzen Sie den URL-Wert im Nachrichtentext vorübergehend durch eine beliebige gültige URL (z. B. *https://netapp.com*) und klicken Sie dann auf die Schaltfläche *Webhook testen*. Discord erfordert die Angabe einer gültigen URL, damit die Test-Webhook-Funktionalität funktioniert.

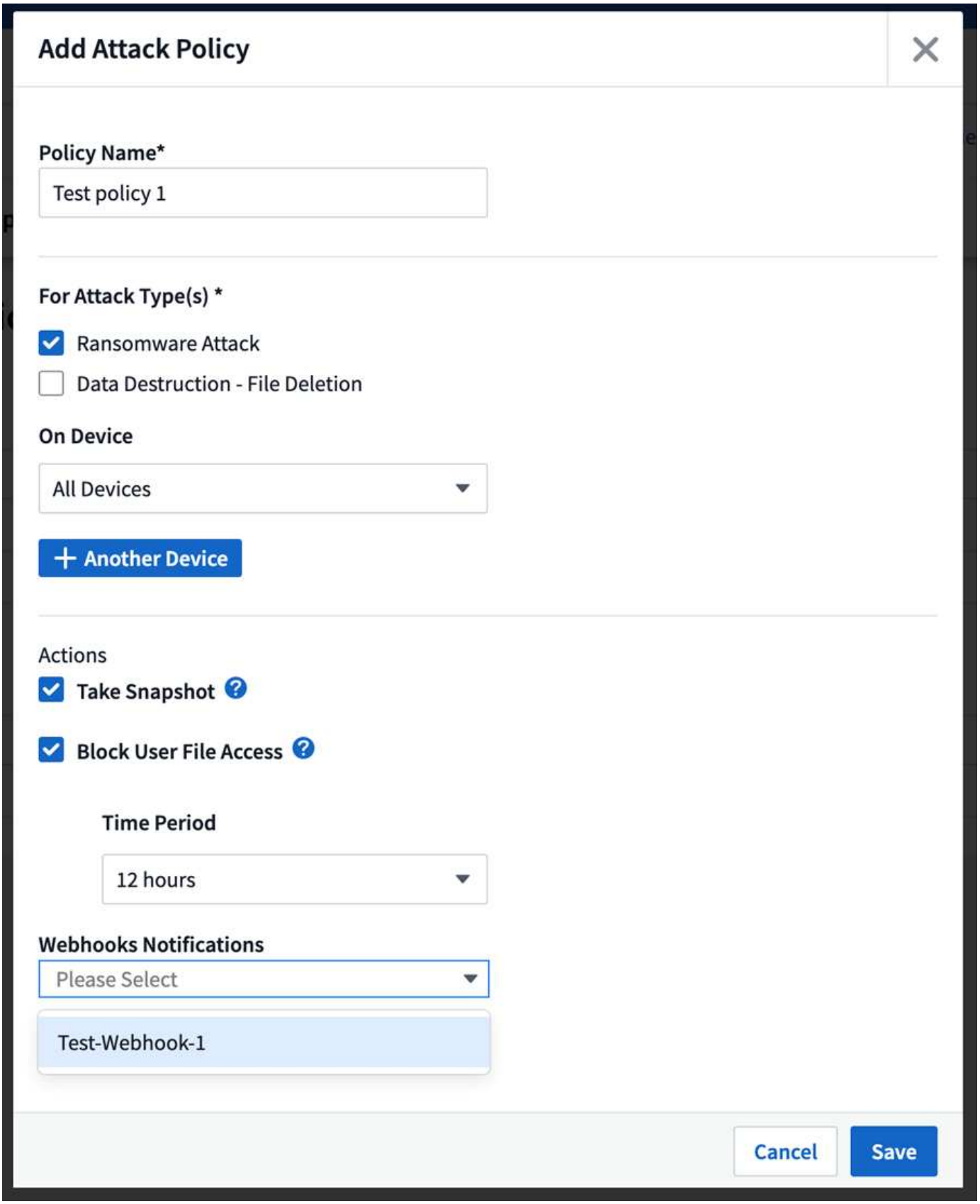
Denken Sie daran, den Nachrichtentext nach Abschluss des Tests wiederherzustellen.

Benachrichtigungen per Webhook

Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, denen die Richtlinie zugeordnet werden soll, und erforderliche Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die gewünschten Discord-Webhooks aus und speichern Sie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload Security Webhook-Beispiel für PagerDuty

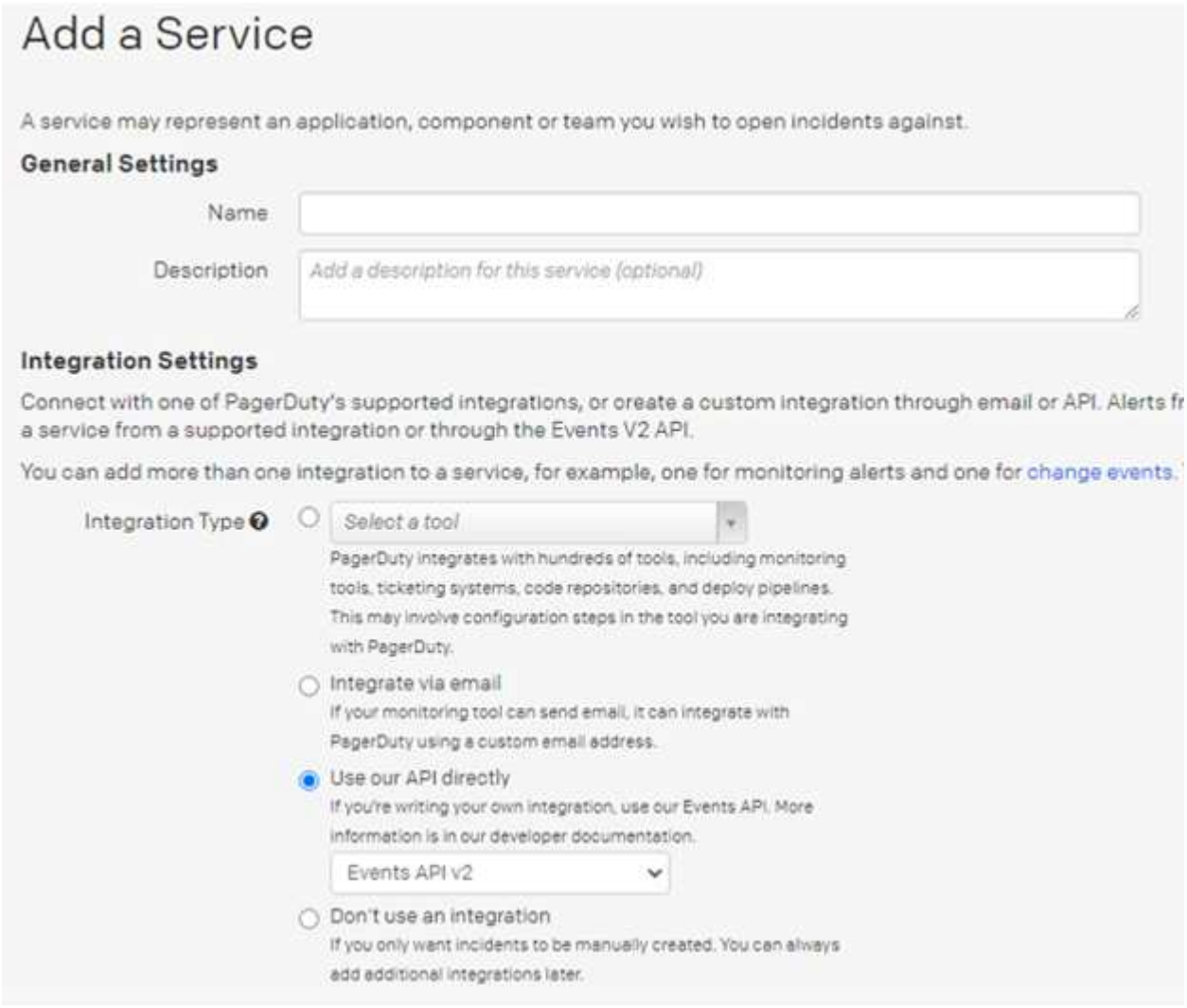
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein

Beispiel zum Einrichten von Webhooks für PagerDuty.

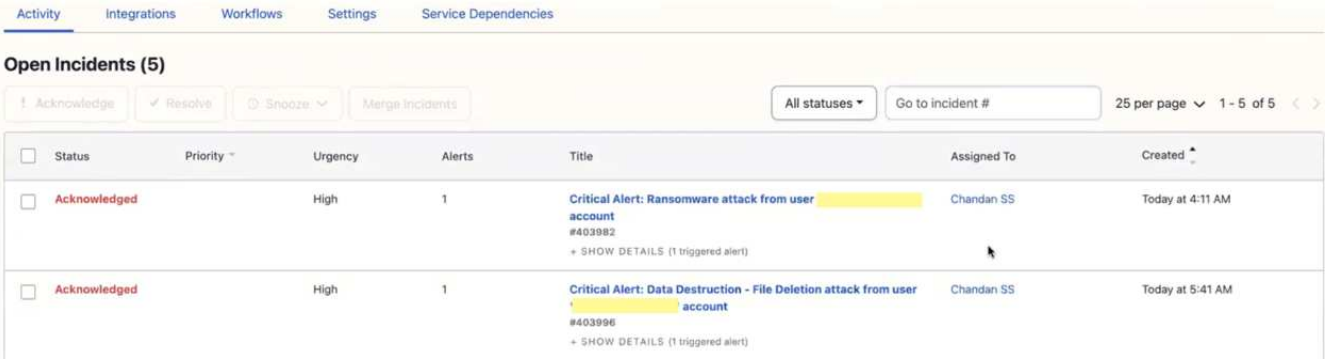
Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"PagerDuty-Dokumentation" für die aktuellsten Informationen.

PagerDuty-Setup:

1. Navigieren Sie in PagerDuty zu **Dienste > Dienstverzeichnis** und klicken Sie auf die Schaltfläche **+Neuer Dienst**.
2. Geben Sie einen *Namen* ein und wählen Sie *Unsere API direkt verwenden*. Wählen Sie *Dienst hinzufügen*.

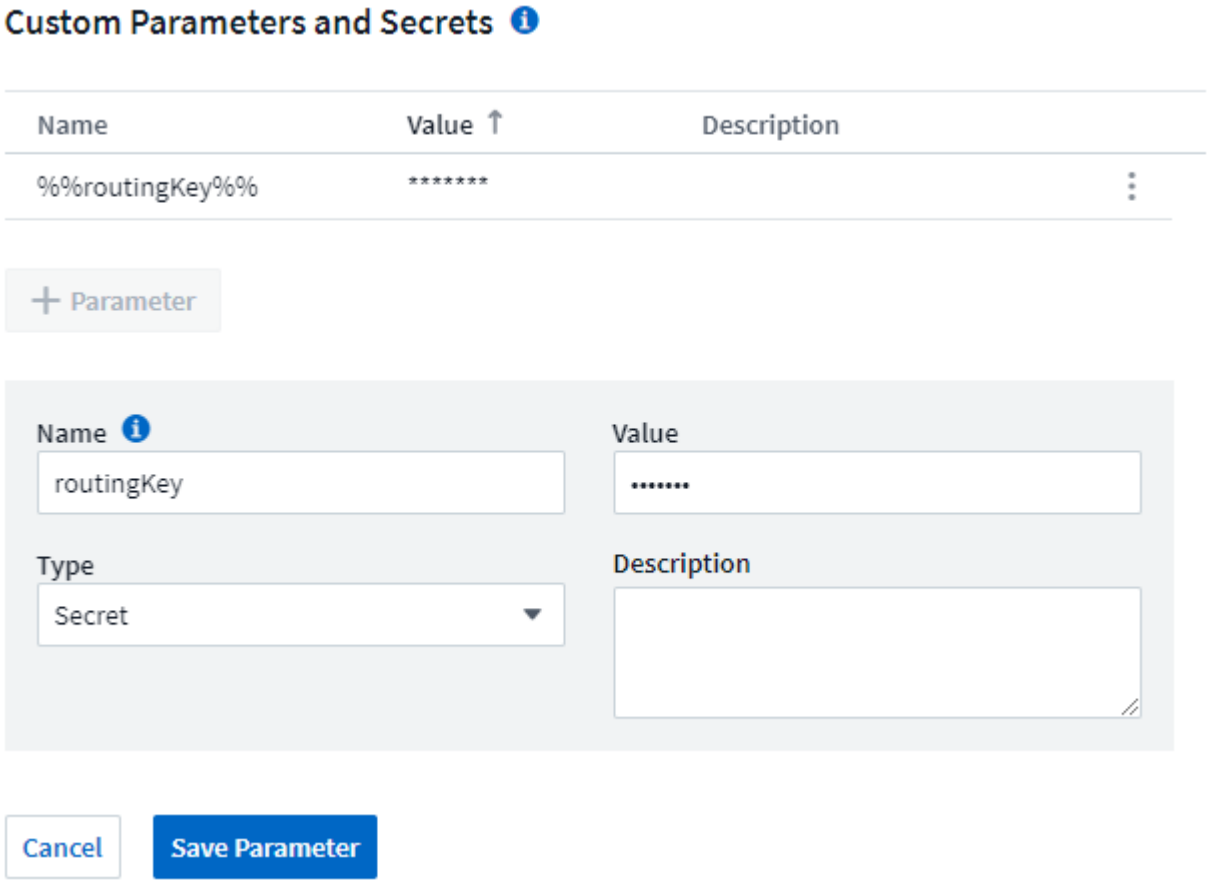


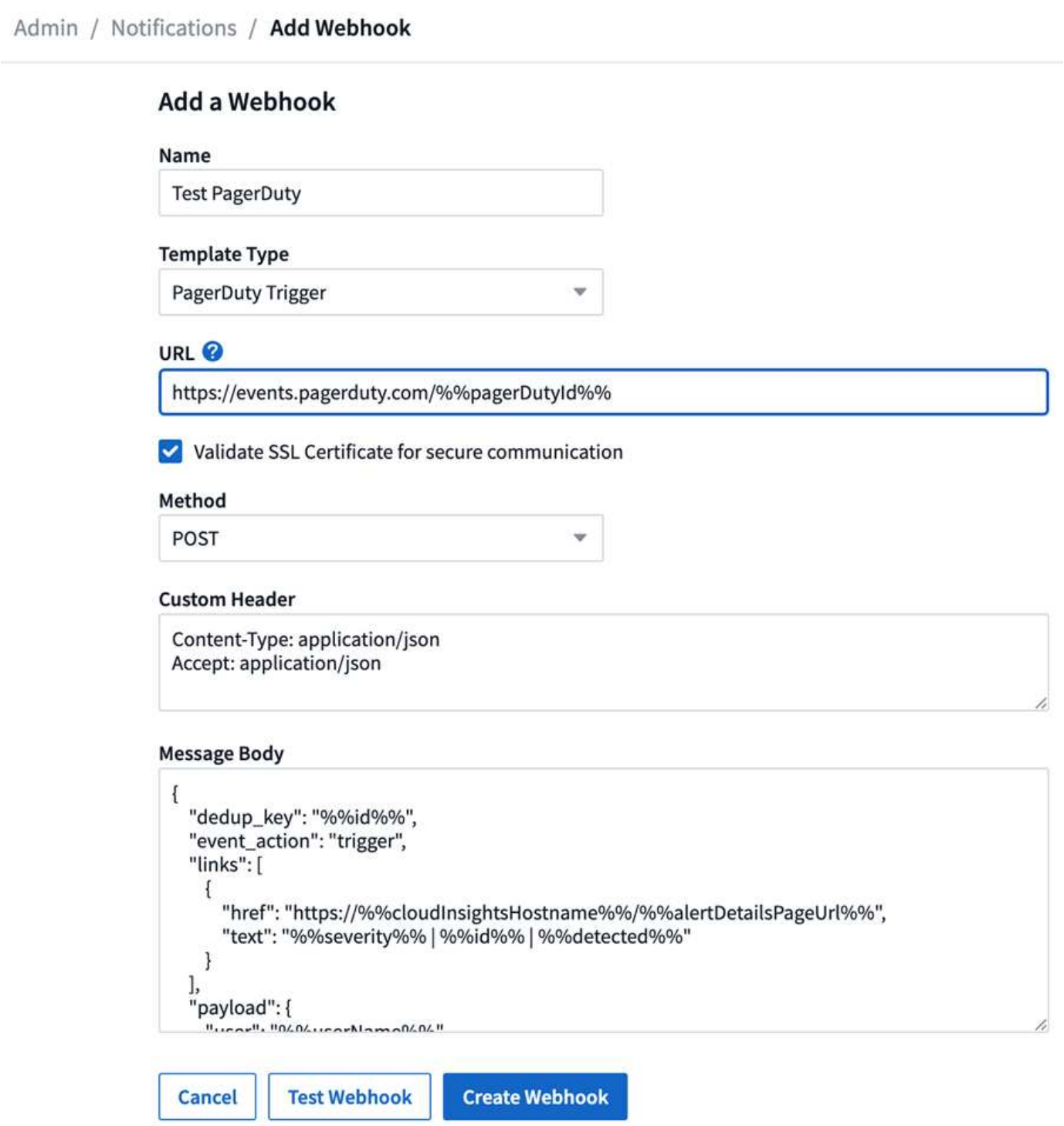
3. Wählen Sie die Registerkarte *Integrationen*, um den **Integrationsschlüssel** anzuzeigen. Sie benötigen diesen Schlüssel, wenn Sie unten den Workload Security-Webhook erstellen.
4. Gehen Sie zu **Vorfälle** oder **Dienste**, um Warnungen anzuzeigen.



Erstellen Sie einen Workload Security PagerDuty-Webhook:

- Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie „+ Webhook“, um einen neuen Webhook zu erstellen.
- Geben Sie dem Webhook einen aussagekräftigen Namen.
- Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *PagerDuty-Trigger* aus.
- Erstellen Sie ein benutzerdefiniertes Parametergeheimnis mit dem Namen *routingKey* und legen Sie den Wert auf den oben erstellten PagerDuty-*Integrationsschlüssel* fest.

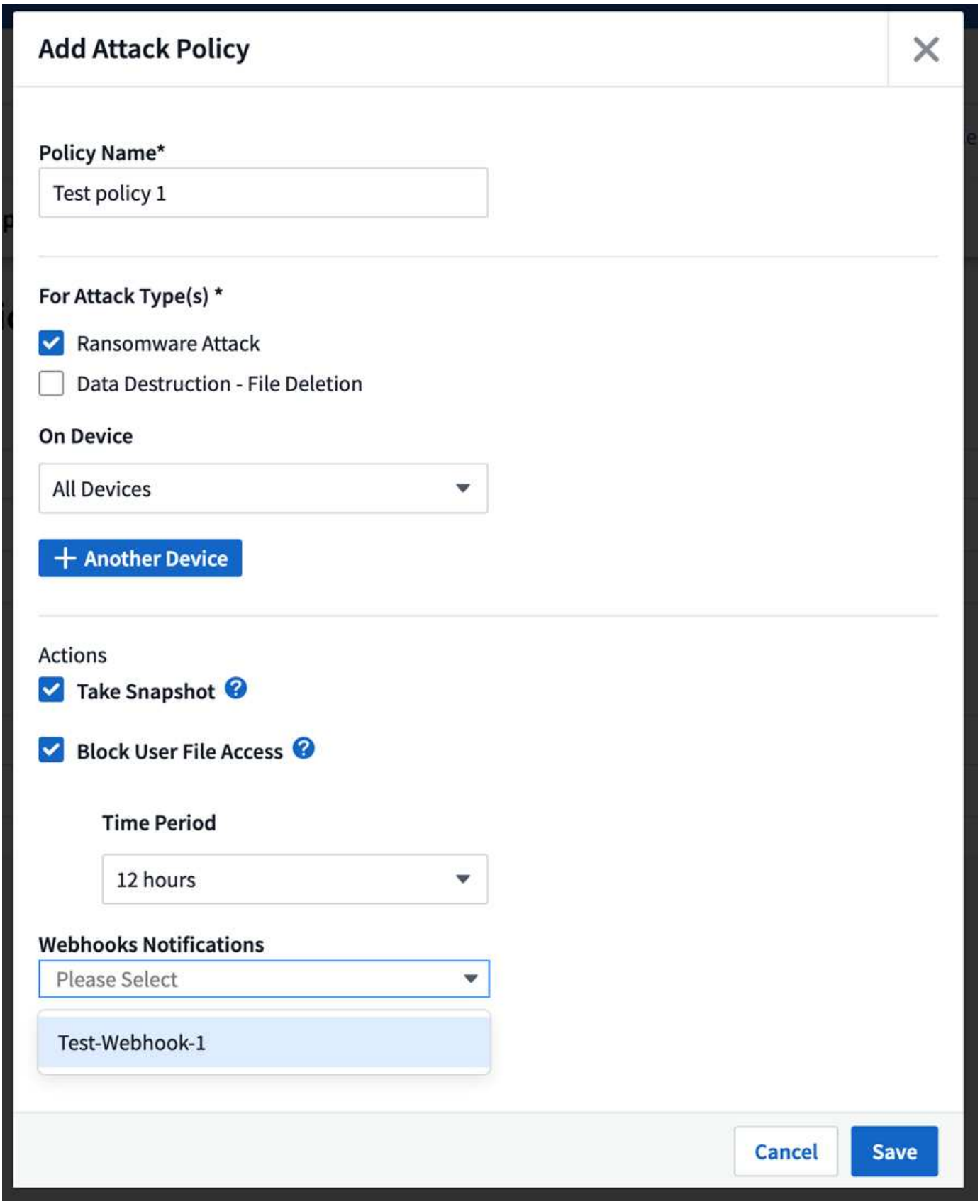




Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Wählen Sie *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die erforderlichen Aktionen aus.
- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen PagerDuty-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload Security Webhook-Beispiel für Slack

Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein Beispiel zum Einrichten von Webhooks für Slack.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Die aktuellsten Informationen finden Sie in der Slack-Dokumentation.

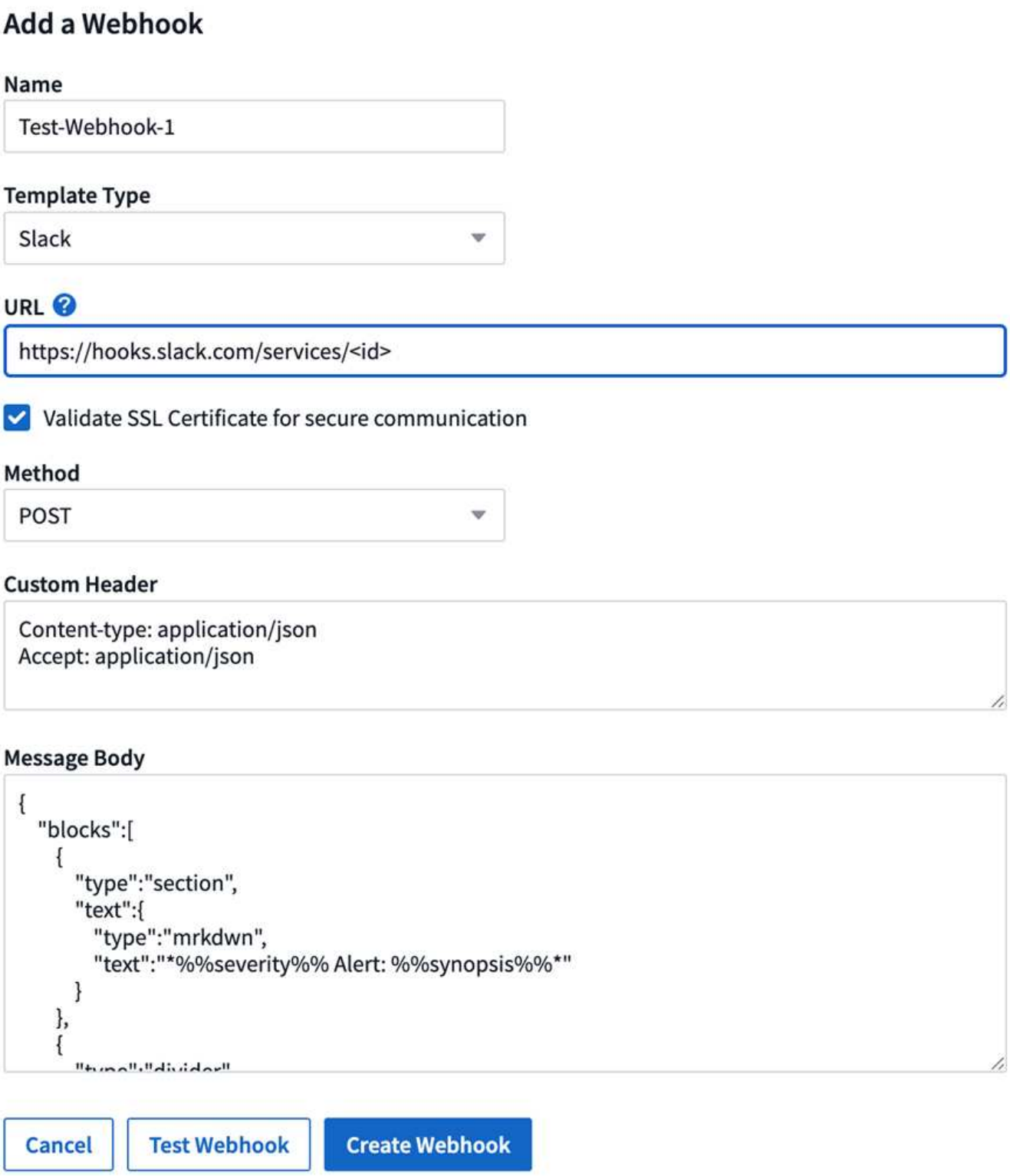
Slack-Beispiel

- Gehe zu https://api.slack.com/apps und erstellen Sie eine neue App. Geben Sie ihm einen aussagekräftigen Namen und wählen Sie einen Arbeitsbereich aus.

- Gehen Sie zu „Eingehende Webhooks“, klicken Sie auf „Eingehende Webhooks aktivieren“, wählen Sie „Neuen Webhook hinzufügen“ und wählen Sie den Kanal aus, auf dem gepostet werden soll.
- Kopieren Sie die Webhook-URL. Diese URL wird beim Erstellen eines Workload Security-Webhooks angegeben.

Erstellen Sie einen Slack-Webhook für die Workload-Sicherheit

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + *Webhook*, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü *Vorlagentyp* die Option *Slack* aus.
4. Fügen Sie die oben kopierte URL ein.

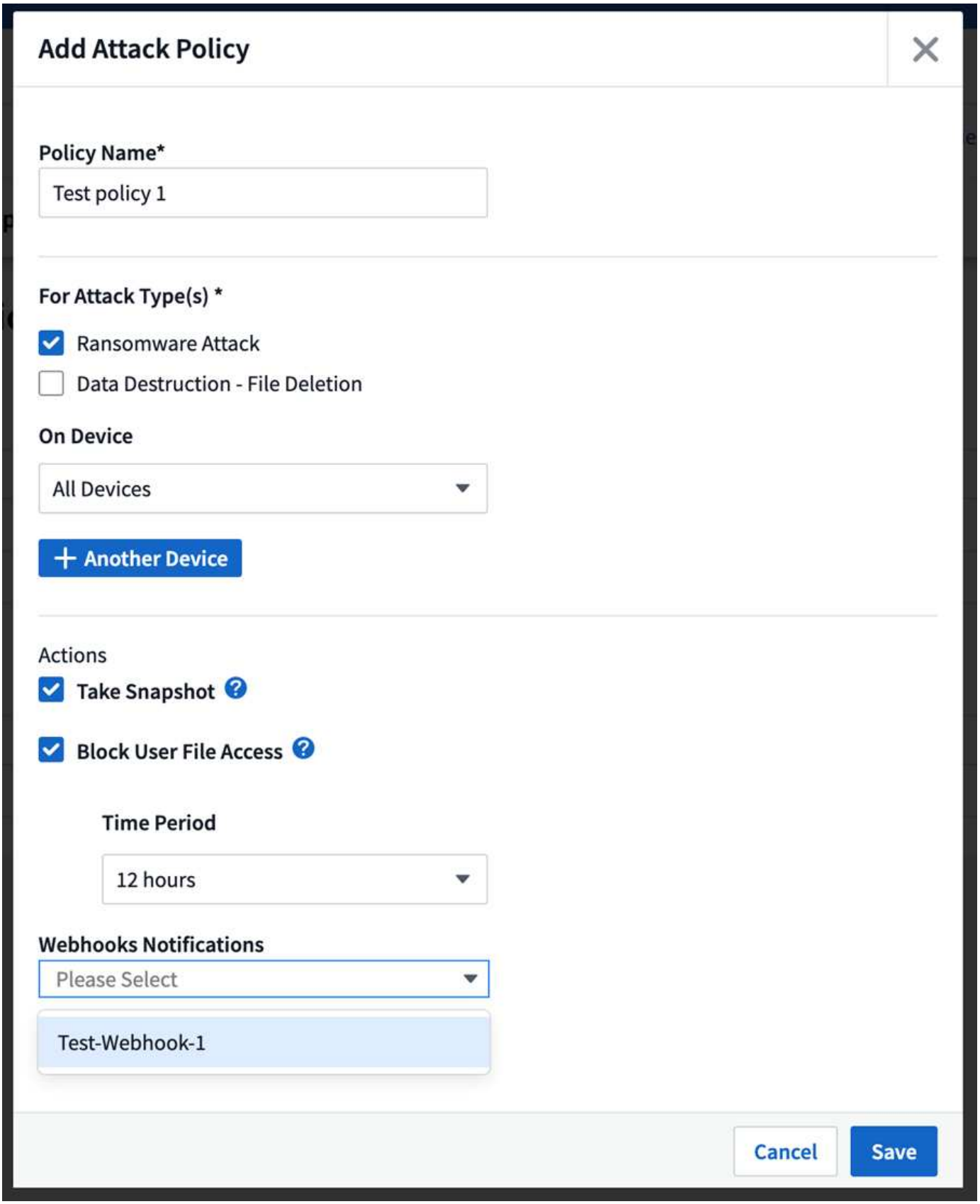


Benachrichtigungen per Webhook

- Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit > Richtlinien*. Klicken Sie auf *+Angriffsrichtlinie* oder *+Warnrichtlinie*.
- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und erforderliche Aktionen aus.

- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Beispiel für einen Workload-Sicherheits-Webhook für Microsoft Teams

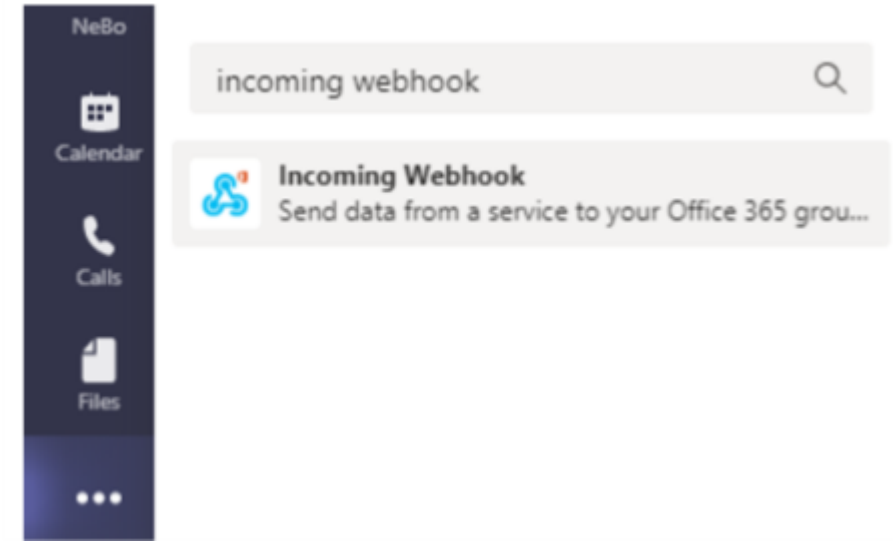
Mithilfe von Webhooks können Benutzer über einen benutzerdefinierten Webhook-Kanal Warnbenachrichtigungen an verschiedene Anwendungen senden. Diese Seite bietet ein

Beispiel zum Einrichten von Webhooks für Teams.

Diese Seite verweist auf Anweisungen von Drittanbietern, die Änderungen unterliegen. Weitere Informationen finden Sie im"Teams-Dokumentation" für die aktuellsten Informationen.

Teams-Setup:

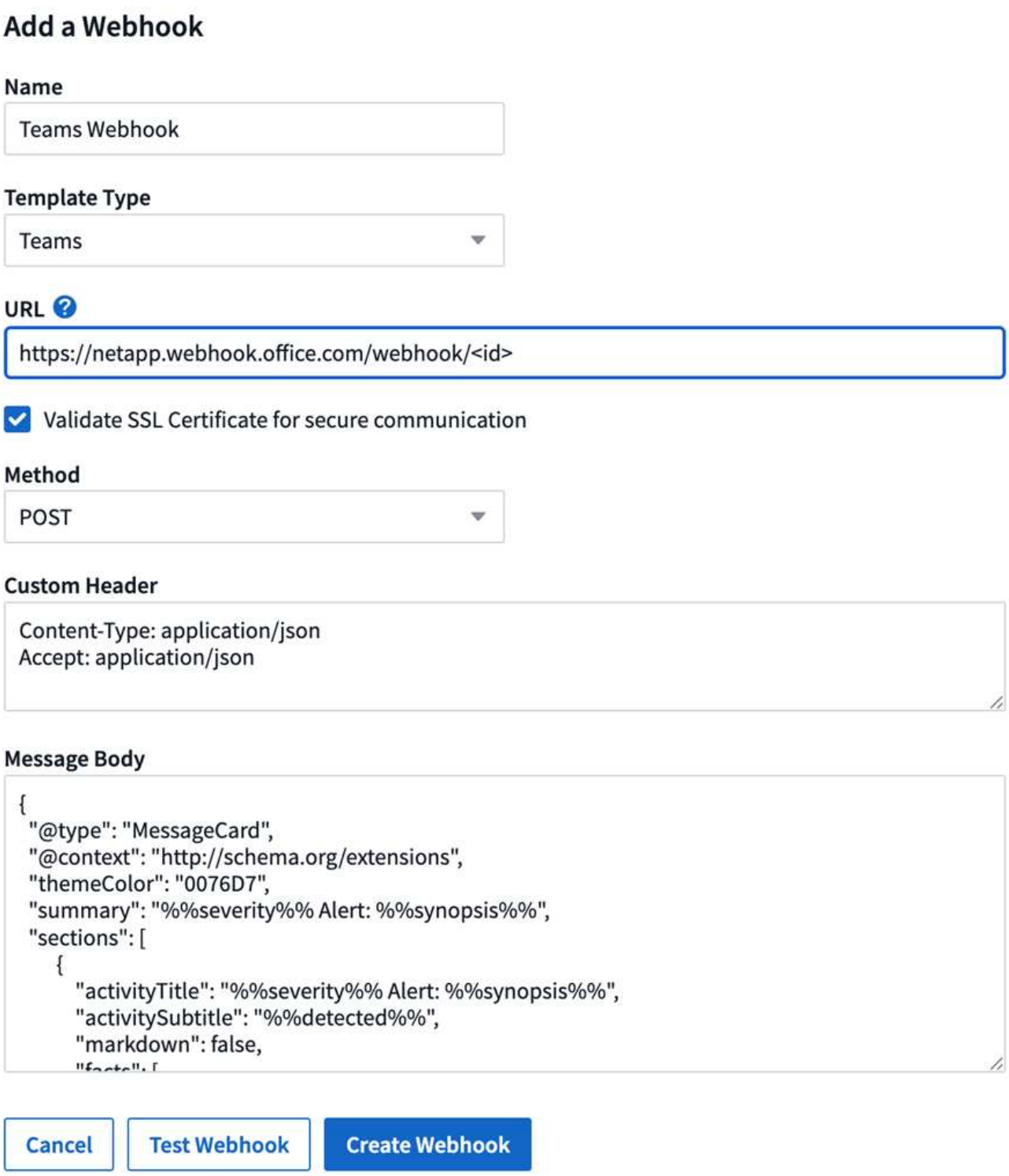
1. Wählen Sie in Teams den Kebab aus und suchen Sie nach „Eingehender Webhook“.



2. Wählen Sie **Zu einem Team hinzufügen > Ein Team auswählen > Einen Connector einrichten**.
3. Kopieren Sie die Webhook-URL. Sie müssen dies in die Workload Security-Webhook-Konfiguration einfügen.

Erstellen Sie einen Workload Security Teams-Webhook:

1. Navigieren Sie zu „Admin > Benachrichtigungen“ und wählen Sie die Registerkarte „Workload Security Webhooks“ aus. Wählen Sie + *Webhook*, um einen neuen Webhook zu erstellen.
2. Geben Sie dem Webhook einen aussagekräftigen Namen.
3. Wählen Sie im Dropdown-Menü „Vorlagentyp“ die Option „Teams“ aus.



4. Fügen Sie die URL von oben in das Feld *URL* ein.

Benachrichtigungen per Webhook

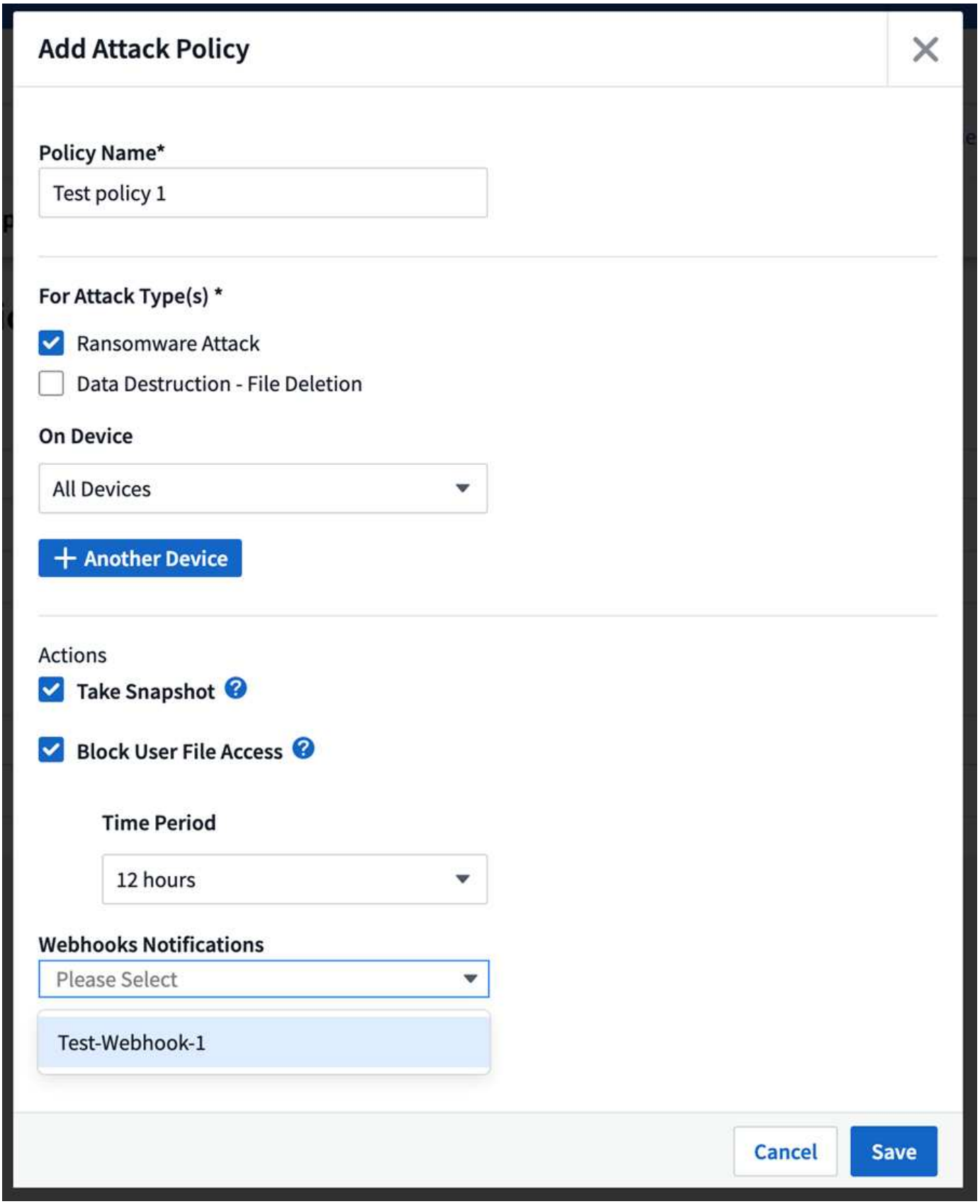
Um über Ereignisse per Webhook benachrichtigt zu werden, navigieren Sie zu *Workload-Sicherheit* > *Richtlinien*. Wählen Sie *+Angriffsrichtlinie* oder *+Warnrichtlinie*.

- Geben Sie einen aussagekräftigen Richtliniennamen ein.
- Wählen Sie die erforderlichen Angriffstypen, Geräte, an die die Richtlinie angehängt werden soll, und die

erforderlichen Aktionen aus.

- Wählen Sie im Dropdown-Menü „Webhook-Benachrichtigungen“ die erforderlichen Teams-Webhooks aus. Speichern Sie die Richtlinie.

Hinweis: Webhooks können auch an vorhandene Richtlinien angehängt werden, indem diese bearbeitet werden.



Workload-Sicherheits-API

Integrieren Sie Workload Security in Ihr Unternehmensökosystem mithilfe einer REST-

API, die durch sichere tokenbasierte Authentifizierung geschützt ist. Rufen Sie forensische Aktivitätsdaten ab, verwalten Sie API-Zugriffstoken und entwickeln Sie benutzerdefinierte Integrationen mit CMDBs, Ticketing-Systemen und anderen Anwendungen. Interaktive Swagger-Dokumentation bietet vollständige API-Spezifikationen und ermöglicht es Ihnen, Endpunkte direkt zu testen.

Voraussetzungen für den API-Zugriff:

- Zum Gewähren des Zugriffs wird ein API-Zugriffstokenmodell verwendet.
- Die API-Token-Verwaltung 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-Zugriff** navigieren. Klicken Sie auf den Link **API-Dokumentation**. Die API-Dokumentation basiert auf Swagger und bietet eine kurze Beschreibung und Nutzungsinformationen für die API. Sie können sie auch auf Ihrem Mandanten ausprobieren.

Wenn Sie die Forensics Activity API aufrufen, verwenden Sie die API cloudsecure_forensics.activities.**v2**. Wenn Sie diese API mehrfach aufrufen, stellen Sie sicher, dass die Aufrufe nacheinander und nicht parallel erfolgen. Mehrere parallele Aufrufe können zu einem Timeout der API führen.

API-Zugriffstoken

Bevor Sie die Workload Security API verwenden, müssen Sie ein oder mehrere **API-Zugriffstoken** erstellen. Zugriffstoken gewähren Leseberechtigungen. Sie können auch das Ablaufdatum für jedes Zugriffstoken festlegen.

So erstellen Sie ein Zugriffstoken:

- Klicken Sie auf **Admin > API-Zugriff**
- Klicken Sie auf **+API-Zugriffstoken**
- Geben Sie **Token-Name** ein
- Geben Sie **Token-Ablauf** an

Ihr Token steht Ihnen während des Erstellungsprozesses nur zum Kopieren in die Zwischenablage und zum Speichern zur Verfügung. Token können nach ihrer Erstellung nicht abgerufen werden. Es wird daher 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.

Token gewähren aus Kundensicht allgemeinen Zugriff auf APIs und verwalten den Zugriff auf APIs im Rahmen ihres eigenen Mandanten.

Die Anwendung erhält ein Zugriffstoken, nachdem ein Benutzer den Zugriff erfolgreich authentifiziert und autorisiert hat, und übergibt das Zugriffstoken dann als Anmeldeinformation, wenn sie die Ziel-API aufruft. Das übergebene Token informiert die API darüber, dass der Inhaber des Tokens autorisiert wurde, auf die API

zuzugreifen und basierend auf dem bei der Autorisierung gewährten Umfang bestimmte Aktionen auszuführen.

Der HTTP-Header, an den das Zugriffstoken übergeben wird, lautet **X-CloudInsights-ApiKey:**

Verwenden Sie beispielsweise Folgendes, um Speicherressourcen abzurufen:

```
 curl https://<Workload Security tenant>/rest/v1/cloudsecure/activities -H
'X-CloudInsights-ApiKey: <API_Access_Token>'
Dabei ist _<API_Access_Token>_ das Token, das Sie während der Erstellung
des API-Zugriffsschlüssels gespeichert haben, und _<Workload Security
Tenant>_ die Tenant-URL Ihrer Workload Security-Umgebung.
```

Detaillierte Informationen finden Sie im Link *API-Dokumentation* unter **Admin > API-Zugriff**.

Skript zum Extrahieren von Daten über die API

Workload Security-Agenten enthalten ein Exportskript, um parallele Aufrufe der v2-API zu ermöglichen, indem der angeforderte Zeitbereich in kleinere Stapel aufgeteilt wird.

Das Skript befindet sich unter */opt/netapp/cloudsecure/agent/export-script*. Eine README-Datei im selben Verzeichnis enthält Verwendungsanweisungen.

Hier ist ein Beispielbefehl zum Aufrufen des Skripts:

```
python3 data-export.py --tenant_url <Workload Security tenant>
--access_key %ACCESS_KEY% --path_filter "<dir path>" --user_name "<user>"
--from_time "01-08-2024 00:00:00" --to_time "31-08-2024 23:59:59"
--iteration_interval 12 --num_workers 3
```

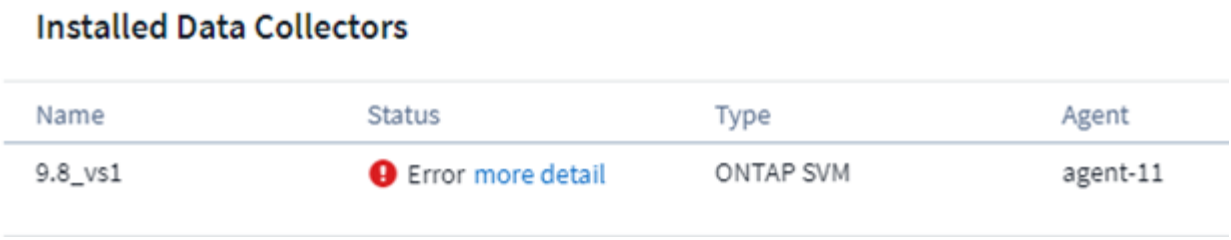
Schlüsselparameter: - `--iteration_interval 12` : Teilt den angeforderten Zeitbereich in Intervalle von 12 Stunden auf. - `--num_workers 3` : Ruft diese Intervalle parallel mithilfe von 3 Threads ab.

Fehlerbehebung beim ONTAP SVM Data Collector

Workload Security verwendet Datensammler, um Datei- und Benutzerzugriffsdaten von Geräten zu erfassen. Hier finden Sie Tipps zur Behebung von Problemen mit diesem Collector.

Siehe die"Konfigurieren des SVM-Collectors" Seite für Anweisungen zum Konfigurieren dieses Collectors.

Im Falle eines Fehlers können Sie auf der Seite „Installierte Datensammler“ in der Spalte „Status“ auf „Weitere Details“ klicken, um Einzelheiten zum Fehler anzuzeigen.



Bekannte Probleme und deren Lösungen werden unten beschrieben.

Problem: Der Datensammler läuft eine Zeit lang und stoppt nach einer zufälligen Zeit mit der Fehlermeldung: „Fehlermeldung: Connector befindet sich im Fehlerzustand.“ Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server überlastet." **Versuchen Sie Folgendes:** Die Ereignisrate von ONTAP war viel höher als das, was die Agent-Box verarbeiten kann. Daher wurde die Verbindung beendet.

Überprüfen Sie den Spitzenverkehr in CloudSecure, als die Verbindung getrennt wurde. Dies können Sie auf der Seite **CloudSecure > Aktivitätsforensik > Alle Aktivitäten** überprüfen.

Wenn der aggregierte Spitzenverkehr höher ist als das, was die Agent Box verarbeiten kann, lesen Sie auf der Seite „Event Rate Checker“ nach, wie Sie die Größe für die Collector-Bereitstellung in einer Agent Box festlegen.

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
```

Starten Sie den Collector nach der Größenänderung über die Benutzeroberfläche neu.

{leer}

Problem: Der Collector meldet die Fehlermeldung: „Auf dem Connector wurde keine lokale IP-Adresse gefunden, die die Datenschnittstellen der SVM erreichen kann.“ **Versuchen Sie Folgendes:** Dies liegt höchstwahrscheinlich an einem Netzwerkproblem auf der ONTAP Seite. Bitte befolgen Sie diese Schritte:

1. Stellen Sie sicher, dass auf der SVM-Daten- oder Verwaltungsebene keine Firewalls vorhanden sind, die die Verbindung von der SVM blockieren.
2. Wenn Sie eine SVM über eine Cluster-Management-IP hinzufügen, stellen Sie sicher, dass die Datenlebensdauer und die Managementlebensdauer der SVM von der Agent-VM aus pingbar sind. Überprüfen Sie bei Problemen das Gateway, die Netzmaske und die Routen für das Leben.

   Sie können auch versuchen, sich über SSH mit der Cluster-Verwaltungs-IP beim Cluster anzumelden und die Agent-IP anzupingen. Stellen Sie sicher, dass die Agent-IP pingbar ist:

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

Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.

3. Wenn Sie versucht haben, eine Verbindung über die Cluster-IP herzustellen, und dies nicht funktioniert hat, versuchen Sie, eine direkte Verbindung über die SVM-IP herzustellen. Die Schritte zum Herstellen einer Verbindung über die SVM-IP finden Sie oben.
4. Überprüfen Sie beim Hinzufügen des Collectors über die SVM-IP und die VSadmin-Anmeldeinformationen, ob für SVM Lif die Rolle „Data plus Mgmt“ aktiviert ist. In diesem Fall funktioniert ein Ping zum SVM Lif, ein SSH zum SVM Lif funktioniert jedoch nicht. Wenn ja, erstellen Sie ein SVM Mgmt Only Lif und versuchen Sie, über dieses SVM Management Only Lif eine Verbindung herzustellen.
5. Wenn es immer noch nicht funktioniert, erstellen Sie ein neues SVM-Lif und versuchen Sie, über dieses Lif eine Verbindung herzustellen. Stellen Sie sicher, dass die Subnetzmaske richtig eingestellt ist.
6. Erweitertes Debuggen:
   a. Starten Sie eine Paketverfolgung in ONTAP.
   b. Versuchen Sie, einen Datensammler über die CloudSecure-Benutzeroberfläche mit dem SVM zu verbinden.
   c. Warten Sie, bis der Fehler auftritt. Stoppen Sie die Paketverfolgung in ONTAP.
   d. Öffnen Sie die Paketverfolgung von ONTAP. Es ist an diesem Standort verfügbar

```
 https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/packet_traces/
.. Stellen Sie sicher, dass ein SYN von ONTAP zur Agent-Box vorhanden
ist.
.. Wenn kein SYN von ONTAP vorhanden ist, liegt ein Problem mit der
Firewall in ONTAP vor.
.. Öffnen Sie die Firewall in ONTAP, damit ONTAP eine Verbindung zur
Agent-Box herstellen kann.
```

7. Wenn es immer 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 keine der oben genannten Maßnahmen das Problem löst, eröffnen Sie einen Fall bei"Netapp-Support" für weitere Unterstützung.

{leer}

Problem: Meldung: „ ONTAP -Typ für [Hostname: <IP-Adresse>] konnte nicht ermittelt werden. Grund: Verbindungsfehler zum Speichersystem <IP-Adresse>: Host ist nicht erreichbar (Host nicht erreichbar)"
Versuchen Sie Folgendes:

1. Überprüfen Sie, ob die richtige SVM-IP-Verwaltungsadresse oder Cluster-Verwaltungs-IP angegeben wurde.
2. Stellen Sie per SSH eine Verbindung zum SVM oder Cluster her, zu dem Sie eine Verbindung herstellen

möchten. Sobald Sie verbunden sind, stellen Sie sicher, dass der SVM- oder Clustername korrekt ist.

{leer}

Problem: Fehlermeldung: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Externer fpolicy-Server beendet." **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich blockiert eine Firewall die erforderlichen Ports auf dem Agent-Computer. Überprüfen Sie, ob der Portbereich 35000–55000/TCP für die Agent-Maschine geöffnet ist, damit sie eine Verbindung vom SVM herstellen kann. Stellen Sie außerdem sicher, dass auf der ONTAP -Seite keine Firewalls aktiviert sind, die die Kommunikation mit dem Agent-Computer blockieren.
2. Geben Sie den folgenden Befehl in das Agent-Feld ein und stellen Sie sicher, dass der Portbereich geöffnet ist.

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

   Die Beispielausgabe sollte folgendermaßen aussehen:

   ```
    -A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate
   NEW -j ACCEPT
   . Melden Sie sich bei SVM an, geben Sie die folgenden Befehle ein und
   überprüfen Sie, dass keine Firewall eingerichtet ist, die die
   Kommunikation mit ONTAP blockiert.
   ```

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

   "Firewall-Befehle prüfen"auf der ONTAP -Seite.

3. Stellen Sie per SSH eine Verbindung zum SVM/Cluster her, den Sie überwachen möchten. Pingen Sie die Agent-Box vom SVM-Datenlebenszyklus aus (mit Unterstützung für CIFS- und NFS-Protokolle) und stellen Sie sicher, dass der Ping funktioniert:

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

   Wenn kein Ping möglich ist, stellen Sie sicher, dass die Netzwerkeinstellungen in ONTAP korrekt sind, sodass der Agent-Computer pingbar ist.

4. Wenn ein einzelner SVM über zwei Datensammler zweimal zu einem Mandanten hinzugefügt wird, wird dieser Fehler angezeigt. Löschen Sie einen der Datensammler über die Benutzeroberfläche. Starten Sie dann den anderen Datensammler über die Benutzeroberfläche neu. Anschließend zeigt der Datensammler den Status „RUNNING“ an und beginnt mit dem Empfang von Ereignissen vom SVM.

   Grundsätzlich sollte in einem Mandanten 1 SVM nur einmal über 1 Datensammler hinzugefügt werden. 1

SVM sollte nicht zweimal über 2 Datensammler hinzugefügt werden.

5. In Fällen, in denen dieselbe SVM in zwei verschiedenen Workload Security-Umgebungen (Mandanten) hinzugefügt wurde, ist die letzte immer erfolgreich. Der zweite Collector konfiguriert fpolicy mit seiner eigenen IP-Adresse und wirft den ersten raus. Der Collector im ersten empfängt also keine Ereignisse mehr und sein „Audit"-Dienst wechselt in einen Fehlerzustand. Um dies zu verhindern, konfigurieren Sie jede SVM in einer einzelnen Umgebung.
6. Dieser Fehler kann auch auftreten, wenn die Servicerichtlinien nicht richtig konfiguriert sind. Um bei ONTAP 9.8 oder höher eine Verbindung zum Data Source Collector herzustellen, ist der Dienst data-fpolicy-client zusammen mit dem Datendienst data-nfs und/oder data-cifs erforderlich. Darüber hinaus muss der Dienst „data-fpolicy-client" mit den Datenlebensdauern für die überwachte SVM verknüpft werden.

{leer}

Problem: Auf der Aktivitätsseite wurden keine Ereignisse angezeigt. **Versuchen Sie Folgendes:**

1. Überprüfen Sie, ob sich der ONTAP Collector im Status „RUNNING" befindet. Wenn ja, stellen Sie sicher, dass einige CIFS-Ereignisse auf den CIFS-Client-VMs generiert werden, indem Sie einige Dateien öffnen.
2. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an und geben Sie den folgenden Befehl ein.

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

   Bitte stellen Sie sicher, dass keine Fehler im Zusammenhang mit fpolicy vorliegen.
3. Wenn keine Aktivitäten angezeigt werden, melden Sie sich bitte beim SVM an. Geben Sie den folgenden Befehl ein:

   ```
   <SVM>fpolicy show
   ```

   Überprüfen Sie, ob die fpolicy-Richtlinie mit dem Präfix „cloudsecure_" festgelegt wurde und der Status „Ein" ist. Wenn nicht festgelegt, kann der Agent die Befehle im SVM höchstwahrscheinlich nicht ausführen. Bitte stellen Sie sicher, dass alle Voraussetzungen, wie am Anfang der Seite beschrieben, erfüllt sind.

{leer}

Problem: Der SVM-Datensammler befindet sich im Fehlerzustand und die Fehlermeldung lautet „Der Agent konnte keine Verbindung zum Sammler herstellen." **Versuchen Sie Folgendes:**

1. Höchstwahrscheinlich ist der Agent überlastet und kann keine Verbindung zu den Datenquellen-Sammlern 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 Benutzeroberfläche.
4. Wenn die Anzahl der Aktivitäten pro Sekunde sehr hoch ist, installieren Sie einen anderen Agenten und

verschieben Sie einige der Datenquellensammler auf den neuen Agenten.

{leer}

Problem: SVM Data Collector zeigt die Fehlermeldung „fpolicy.server.connectError: Knoten konnte keine Verbindung mit dem FPolicy-Server „12.195.15.146“ herstellen (Grund: „Select Timed out“)“ an. **Versuchen Sie Folgendes:** Die Firewall ist in SVM/Cluster aktiviert. Daher kann die fpolicy-Engine keine Verbindung zum fpolicy-Server herstellen. CLIs in ONTAP , die zum Abrufen weiterer Informationen verwendet werden können, sind:

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

"Firewall-Befehle prüfen"auf der ONTAP -Seite.

{leer}

Problem: Fehlermeldung: „Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Auf der SVM wurde keine gültige Datenschnittstelle (Rolle: Daten, Datenprotokolle: NFS oder CIFS oder beide, Status: aktiv) gefunden.“ **Versuchen Sie Folgendes:** Stellen Sie sicher, dass eine funktionsfähige Schnittstelle vorhanden ist (mit der Rolle „Daten“ und dem Datenprotokoll „CIFS/NFS“).

{leer}

Problem: Der Datensammler wechselt in den Fehlerzustand und nach einiger Zeit in den RUNNING-Zustand und dann wieder zurück in den Fehlerzustand. Dieser Zyklus wiederholt sich. **Versuchen Sie Folgendes:** Dies geschieht normalerweise im folgenden Szenario:

1. Es wurden mehrere Datensammler hinzugefügt.
2. Den Datensammlern, die dieses Verhalten zeigen, wird 1 SVM hinzugefügt. Das bedeutet, dass zwei oder mehr Datensammler mit einem SVM verbunden sind.
3. Stellen Sie sicher, dass 1 Datensammler nur mit 1 SVM verbunden ist.
4. Löschen Sie die anderen Datensammler, die mit derselben SVM verbunden sind.

{leer}

Problem: Der Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren (Richtlinie auf SVM svmname). Grund: Ungültiger Wert für das Element „shares-to-include“ in „fpolicy.policy.scope-modify: „Federal“ angegeben. **Versuchen Sie Folgendes:** *Die Freigabenamen müssen ohne Anführungszeichen angegeben werden. Bearbeiten Sie die ONTAP SVM DSC-Konfiguration, um die Freigabenamen zu korrigieren.

Freigaben einschließen und ausschließen ist nicht für eine lange Liste von Freigabenamen vorgesehen.

Verwenden Sie stattdessen die Filterung nach Volumen, wenn Sie eine große Anzahl von Aktien ein- oder ausschließen möchten.

{leer}

Problem: Es gibt im Cluster vorhandene fpolicies, die nicht verwendet werden. Was sollte vor der Installation von Workload Security damit geschehen? **Versuchen Sie Folgendes:** Es wird empfohlen, alle vorhandenen, nicht verwendeten fpolicy-Einstellungen zu löschen, auch wenn sie getrennt sind. Workload Security erstellt fpolicy mit dem Präfix „cloudsecure_“. Alle anderen nicht verwendeten fpolicy-Konfigurationen können gelöscht werden.

CLI-Befehl zum Anzeigen der fpolicy-Liste:

```
 fpolicy show
Schritte zum Löschen von fpolicy-Konfigurationen:
```

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

{leer}

Problem: Nach Aktivierung der Workload-Sicherheit wird die ONTAP Performance beeinträchtigt: Die Latenz steigt sporadisch stark an, die IOPS sinken sporadisch stark ab. **Probieren Sie Folgendes aus:** Bei der Verwendung von ONTAP mit Workload Security können gelegentlich Latenzprobleme in ONTAP auftreten. Dafür gibt es eine Reihe möglicher Gründe, wie im Folgenden erläutert wird:"1372994" , "1415152" , "1438207" , "1479704" , "1354659" Die Alle diese Probleme wurden in ONTAP 9.13.1 und höher behoben. Es wird dringend empfohlen, eine dieser neueren Versionen zu verwenden.

{leer}

Problem: Der Datensammler zeigt die Fehlermeldung an: „Fehler: Der Zustand des Sammlers konnte innerhalb von 2 Versuchen nicht ermittelt werden. Versuchen Sie, den Sammler erneut neu zu starten (Fehlercode: AGENT008)“. **Versuchen Sie Folgendes:**

1. Scrollen Sie auf der Seite „Datensammler“ nach rechts neben den Datensammler, der den Fehler ausgibt, und klicken Sie auf das Menü mit den drei Punkten. Wählen Sie *Bearbeiten*. Geben Sie das Passwort des Datensammlers erneut ein. Speichern Sie den Datensammler, indem Sie auf die Schaltfläche *Speichern* klicken. Data Collector wird neu gestartet und der Fehler sollte behoben sein.
2. Die Agent-Maschine verfügt möglicherweise nicht über genügend CPU- oder RAM-Reserve, weshalb die DSCs ausfallen. Bitte überprüfen Sie die Anzahl der Datensammler, die dem Agenten auf der Maschine

hinzugefügt wurden. Wenn es mehr als 20 sind, erhöhen Sie bitte die CPU- und RAM-Kapazität der Agent-Maschine. Sobald die CPU und der RAM erhöht werden, wechseln die DSCs automatisch in den Initialisierungs- und dann in den Ausführungszustand. Schauen Sie in die Größentabelle auf"diese Seite" .

{leer}

Problem: Der Datensammler gibt einen Fehler aus, wenn der SVM-Modus ausgewählt ist. **Versuchen Sie Folgendes:** Wenn beim Verbinden im SVM-Modus die Cluster-Management-IP anstelle der SVM-Management-IP zum Verbinden verwendet wird, tritt ein Verbindungsfehler auf. Stellen Sie sicher, dass die richtige SVM-IP verwendet wird.

{leer}

Problem: Der Datensammler zeigt eine Fehlermeldung an, wenn die Funktion „Zugriff verweigert“ aktiviert ist: „Connector befindet sich im Fehlerzustand. Dienstname: Audit. Grund für den Fehler: Fehler beim Konfigurieren von fpolicy auf SVM test_svm. Grund: Der Benutzer ist nicht autorisiert." **Versuchen Sie Folgendes:** Dem Benutzer fehlen möglicherweise die REST-Berechtigungen, die für die Funktion „Zugriff verweigert“ erforderlich sind. Bitte folgen Sie den Anweisungen auf"diese Seite" um die Berechtigungen festzulegen.

Starten Sie den Collector neu, sobald die Berechtigungen festgelegt sind.

{leer}

Problem: Der Collector befindet sich im Fehlerzustand mit der Meldung: Connector befindet sich im Fehlerzustand. Grund für den Fehler: Konfiguration des persistenten Speichers auf SVM <SVM-Name> fehlgeschlagen. Grund: Es konnte kein geeignetes Aggregat für das Volumen "<volumeName>" in der SVM "<SVM Name>" gefunden werden. Grund: Leistungsdaten für das Aggregat "<aggregateName>" sind derzeit nicht verfügbar. Warten Sie ein paar Minuten und versuchen Sie den Befehl erneut. Dienstname: Audit. Fehlergrund: Fehler beim Konfigurieren des persistenten Speichers auf der SVM <SVM name="">.</SVM> Ursache: Es konnte kein passendes Aggregat für Volume "<volumeName>" in der SVM "<SVM name=""></SVM></volumeName>gefunden werden". Ursache: Performance-Informationen für das Aggregat "<aggregateName>" sind derzeit nicht verfügbar.</aggregateName> Warten Sie einige Minuten, und versuchen Sie es erneut.

Versuchen Sie Folgendes: Warten Sie einige Minuten und starten Sie dann den Collector neu.

{leer}

Wenn weiterhin Probleme auftreten, verwenden Sie die Support-Links auf der Seite **Hilfe > Support**.