Forensik

Data Infrastructure Insights

NetApp
February 03, 2026

Inhalt

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.

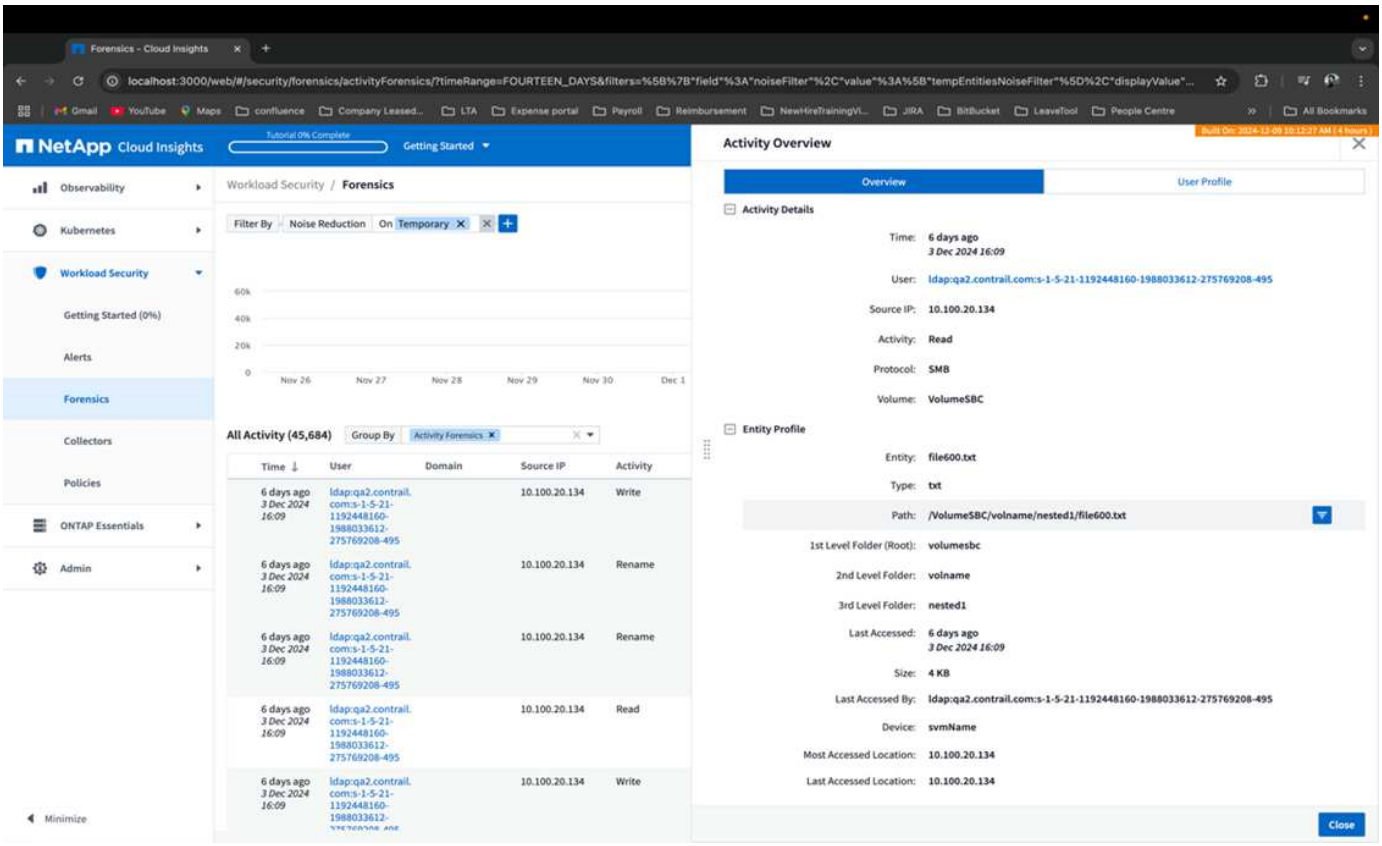
- Eine Liste aller Aktivitätsdaten.
- Ein Dropdown-Menü „Gruppieren nach“ bietet die Möglichkeit, die Aktivität nach Benutzern, Ordnern, Entitätstyp usw. zu gruppieren.
- Über der Tabelle ist eine Schaltfläche für den allgemeinen Pfad verfügbar, über die wir durch Anklicken ein ausziehbares Bedienfeld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

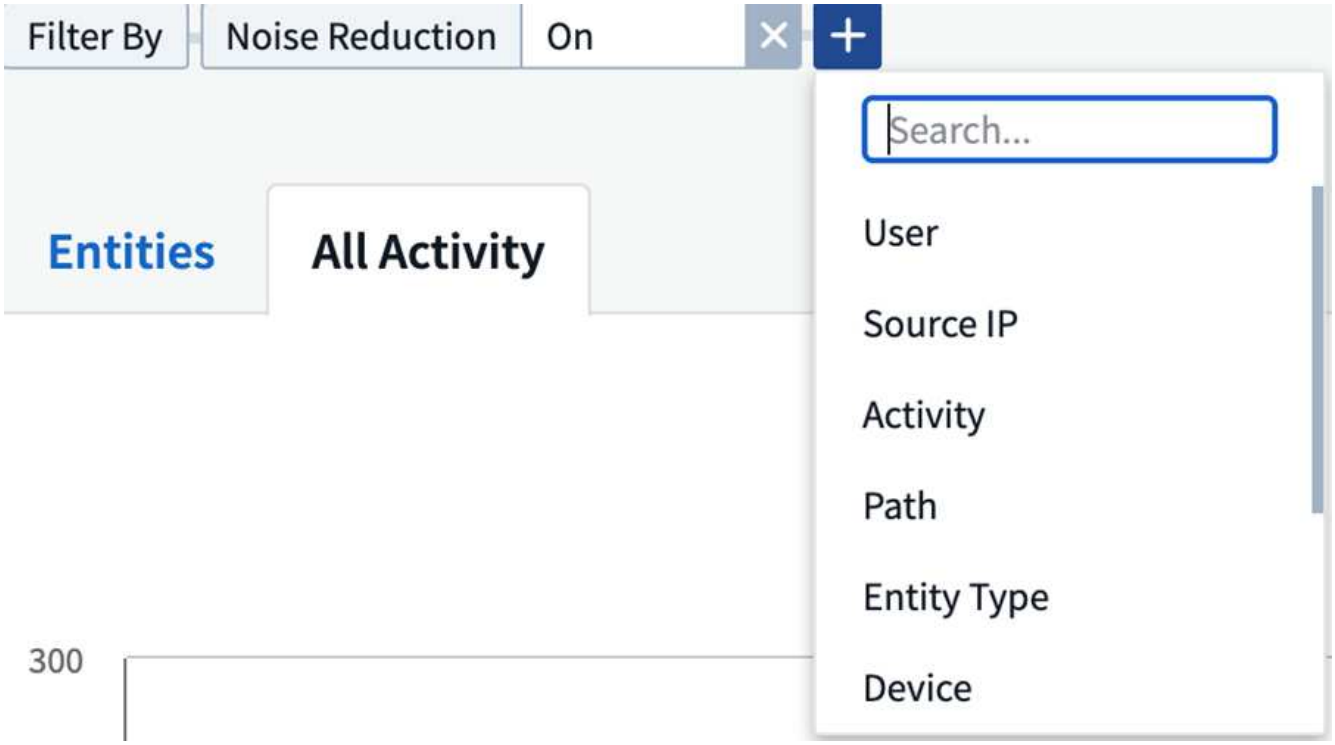
- Die Aktivitätsanzahl wird als Hyperlink angezeigt. Wenn Sie diesen auswählen, wird die ausgewählte Gruppierung als Filter hinzugefügt. Die Aktivitätstabelle wird basierend auf diesem Filter aktualisiert.
- Beachten Sie, dass Sie, wenn Sie den Filter ändern, den Zeitbereich ändern oder den Bildschirm 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.

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Leistungsbeurteilung	Kommentar
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.
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.

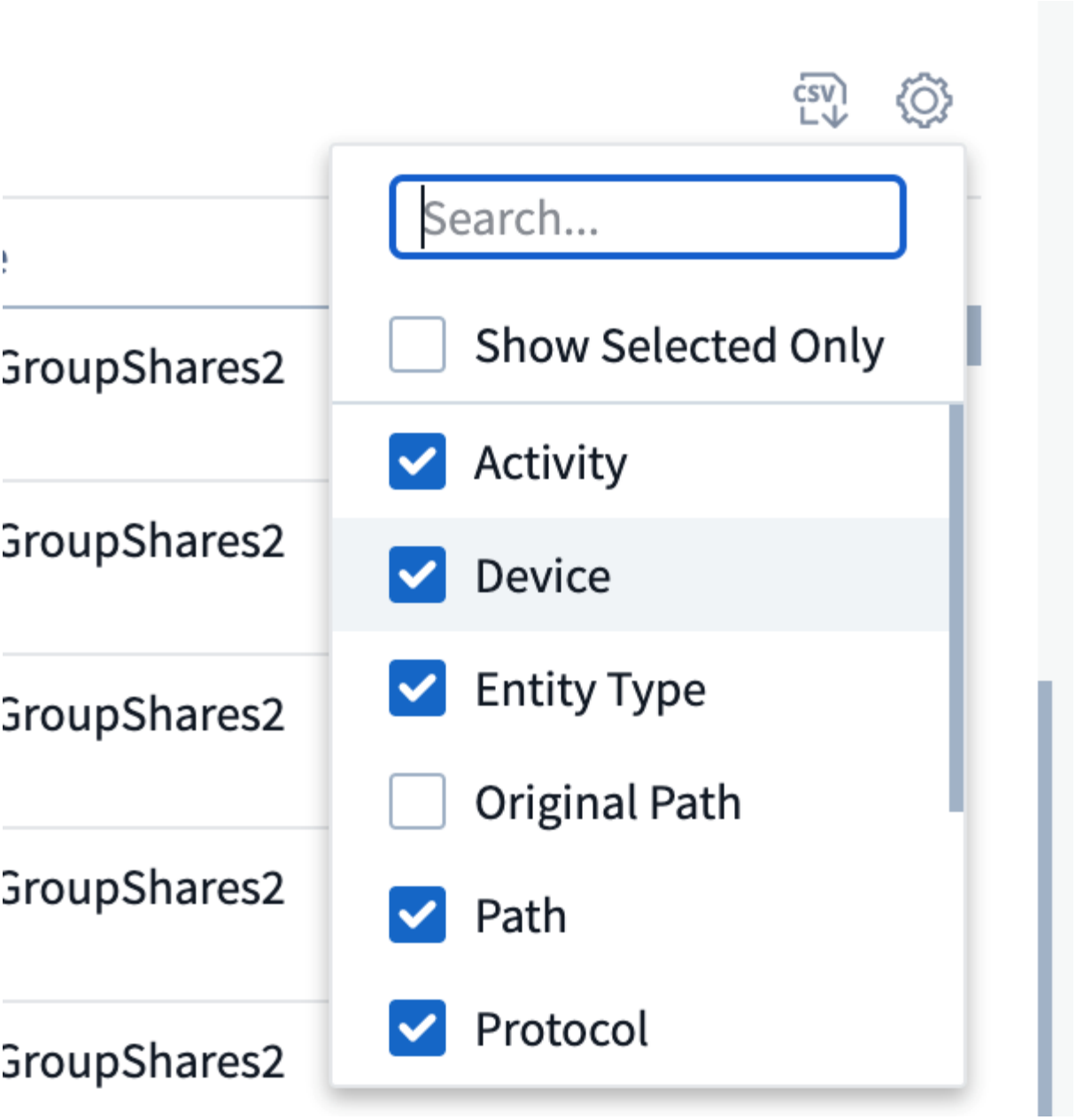
Schritt-für-Schritt-Anleitung: Daten mit asynchronen Exporten exportieren

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
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.