Benutzeraktivitätserkennung konfigurieren

NetApp Ransomware Resilience

NetApp
April 13, 2026

Inhalt

Benutzeraktivitätserkennung konfigurieren

Erfahren Sie mehr über die Erkennung von Benutzeraktivitäten in NetApp Ransomware Resilience

Mit der Erkennung von Benutzeraktivitäten ermöglicht NetApp Ransomware Resilience Ihnen, Ransomware-Ereignisse auf Benutzerebene zu adressieren und Ereignisse wie Datenlecks und großflächige Löschungen zu stoppen.

NetApp Ransomware Resilience bietet eine KI-gestützte Erkennung von Datenschutzverletzungen durch Überwachung verdächtiger Benutzeraktivitäten. Deutliche Anstiege der Leseaktivität und Zugriffsmuster bei Lesezugriffen werden genutzt, um böswillige Absichten zu erkennen. Nach der Erkennung generiert Ransomware Resilience automatisch Warnmeldungen in der NetApp Console, per E-Mail und in jedem konfigurierten Sicherheitssystem (zum Beispiel SIEM).

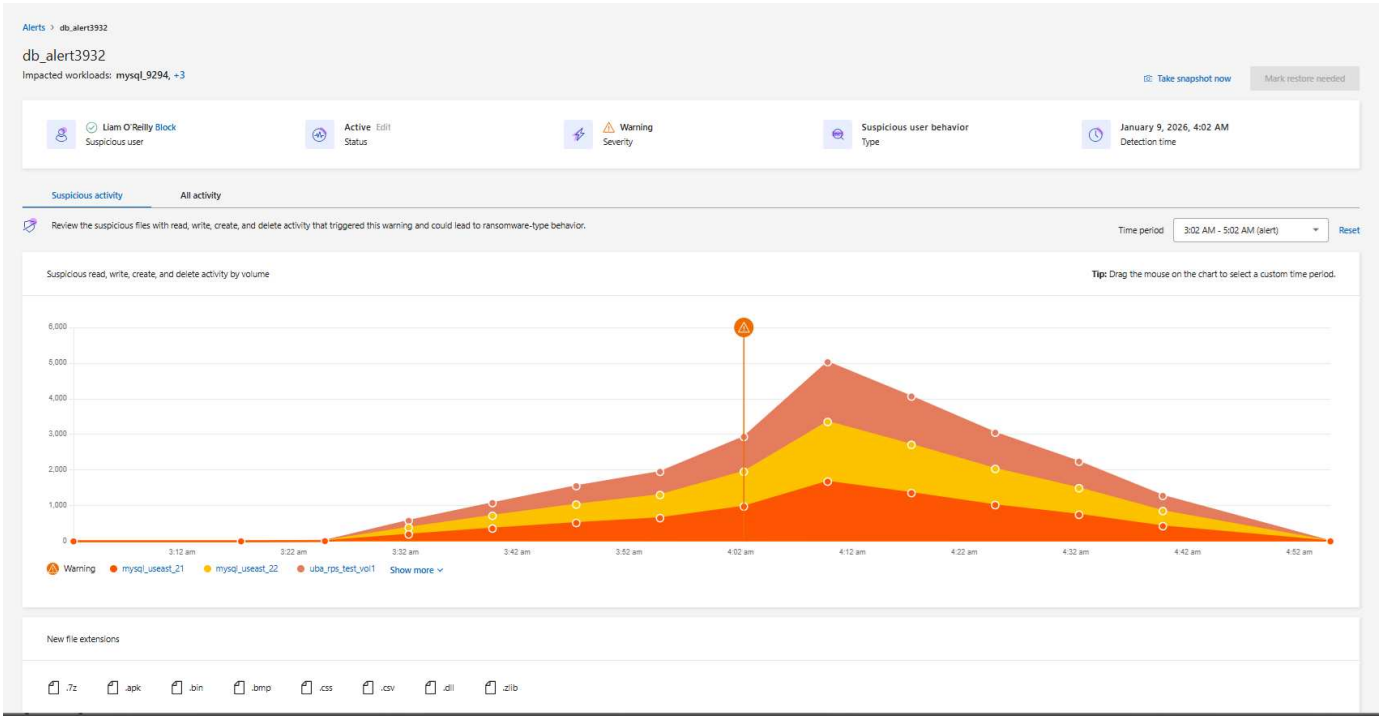
Durch die Erkennung und Benachrichtigung über verdächtiges Nutzerverhalten warnt Sie Ransomware Resilience vor Datenlecks und Datenzerstörungsversuchen sowie Mustern, die verdächtig erscheinen. In jeder Benachrichtigung identifiziert Ransomware Resilience einen Benutzer, den Sie sperren können.

Ransomware Resilience erkennt verdächtige Benutzeraktivitäten durch die Analyse von Benutzeraktivitätsereignissen, die von FPolicy in ONTAP generiert werden. Um Daten zur Benutzeraktivität zu erfassen, müssen Sie einen oder mehrere Benutzeraktivitätsagenten bereitstellen. Der Agent ist ein Linux-Server oder eine VM mit Konnektivität zu Geräten auf Ihrem Mandanten.

Die Erkennung von Benutzeraktivitäten wird derzeit für SAN-Workloads nicht unterstützt. Sie können die Erkennung von Benutzeraktivitäten mit NAS-Workloads in Amazon FSxN für ONTAP, Cloud Volumes ONTAP und ONTAP verwenden.

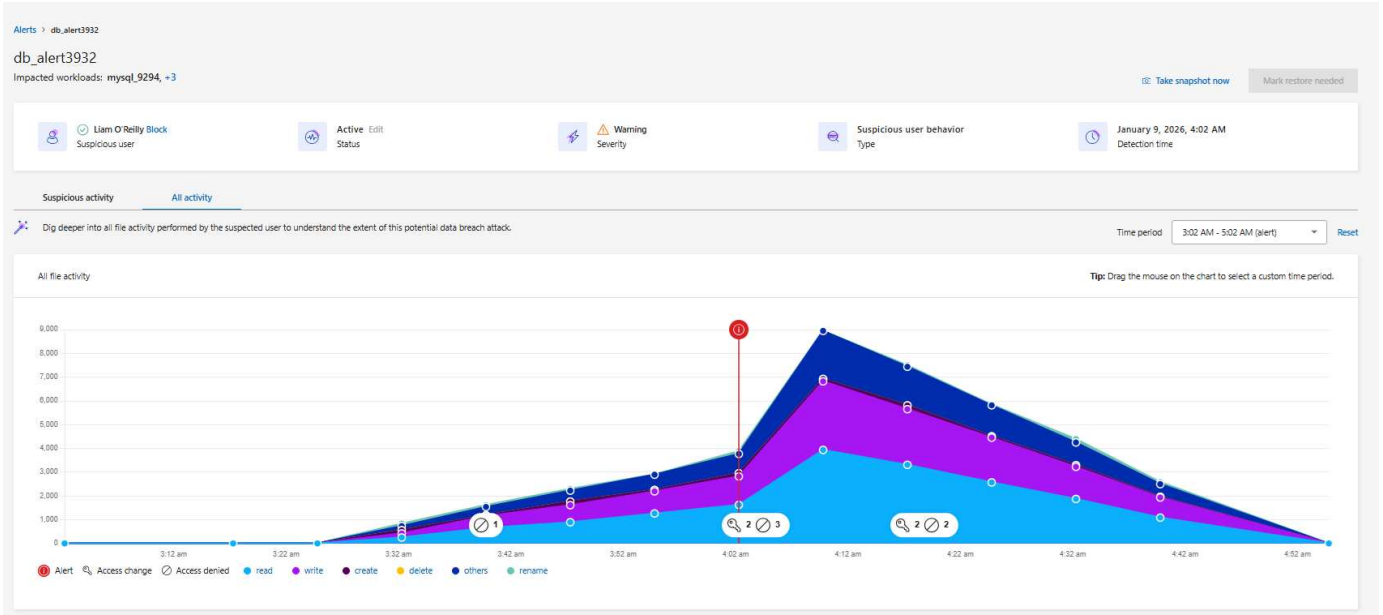
Forensik verdächtiger Benutzeraktivität

Ransomware Resilience bietet forensische Analysen des Nutzerverhaltens: Listen und Diagramme zeigen, wann verdächtige Aktivitäten auftraten und wann Benachrichtigungen versendet wurden. Diese zeigen die Häufigkeit verdächtiger Aktivitäten auf Dateien, Verzeichnissen, Volumes und Workloads im Zeitverlauf, um die Ereignisse zu veranschaulichen. Sie können auch das Auftreten neuer Dateierweiterungen beobachten.



.

Sie können verdächtige Aktivitäten mit einer Übersicht aller Aktivitäten vergleichen. In der Übersicht aller Aktivitäten können Sie neben Zugriffsänderungs- und Zugriffsverweigerungsereignissen auch Lese-, Schreib-, Umbenennungs-, Verschiebe-, Erstellungs- und Löschereignisse beobachten.



.

Komponenten

Es gibt drei Schlüsselkomponenten bei der Erkennung verdächtiger Benutzeraktivitäten in der Ransomware Resilience.

- Der **Benutzeraktivitätsagent** ist eine ausführbare Umgebung für Datensammler. Sie müssen den Benutzeraktivitätsagenten konfigurieren.

- Der **Datensammler** teilt Benutzeraktivitätsereignisse mit Ransomware Resilience. Der Datensammler wird automatisch erstellt, wenn Sie "Aktivieren Sie eine Ransomware-Schutzstrategie mit Erkennung verdächtiger Benutzeraktivität".
- Der **Benutzerverzeichnis-Connector** ermöglicht die Zuordnung von Benutzernamen und Benutzer-IDs und sorgt so für mehr Klarheit bei der Reaktion auf verdächtiges Benutzerverhalten. Sie müssen den Benutzerverzeichnis-Connector konfigurieren.

Ransomware Resilience und Data Infrastructure Insights

Die Erkennung verdächtigen Nutzerverhaltens in Ransomware Resilience ist eine Integration mit Data Infrastructure Insights (DII) Workload Security und verwendet "DII-Endpunkte". Sie benötigen keine DII-Konfiguration, um die Nutzerverhaltenserkennung in Ransomware Resilience zu aktivieren. Um die Nutzerverhaltenserkennung zu aktivieren, "Erstellen Sie die erforderlichen Agenten und Collector und aktivieren Sie die geeignete Ransomware-Schutzstrategie".

Wenn Sie bereits NetApp Data Infrastructure Insights (DII) Workload Security verwenden, wird empfohlen, dieselben Workload Security Agents auch für Ransomware Resilience zu verwenden. Sie müssen keine separaten Workload Security Agents für Ransomware Resilience bereitstellen, jedoch erfordert die Verwendung derselben Workload Security Agents eine Kopplung zwischen der Ransomware Resilience Console Organization und dem DII Storage Workload Security Tenant. Wenden Sie sich an Ihren Account Representative, um diese Kopplung zu aktivieren.

Nächste Schritte

- "Anforderungen für die Erkennung von Benutzeraktivitäten"
- "Konfigurieren Sie Agenten und Detektoren für Benutzerverhaltensaktivitäten"

Anforderungen an die Erkennung von Benutzeraktivitäten für NetApp Ransomware Resilience

NetApp Ransomware Resilience Benutzerverhaltenserkennung ermöglicht es Ihnen, auf Ransomware-Ereignisse auf Benutzerebene zu reagieren. Sie müssen eine Gruppe von Agenten erstellen, um die Benutzerverhaltenserkennung zu aktivieren. Bevor Sie die Erkennung aktivieren, müssen Sie sicherstellen, dass Sie die beschriebenen Betriebssystem-, Server- und Netzwerkvoraussetzungen erfüllen, damit Ransomware Resilience Ereignisse korrekt erkennen und melden kann.

Cloud-Anbieter-Support

Verdächtige Benutzeraktivitätsdaten können in AWS und Azure in den folgenden Regionen gespeichert werden:

Cloud-Anbieter	Region
AWS	• Asien-Pazifik (Sydney) (ap-southeast-2) • Europa (Frankfurt) (eu-central-1) • US Ost (Nord-Virginia) (us-east-1)
Azurblau	Ostküste der USA

Betriebssystemanforderungen

Die Erkennung verdächtigen Benutzerverhaltens wird mit den folgenden Betriebssystemen unterstützt:

Betriebssystem	Unterstützte Versionen
AlmaLinux	9.4 (64 Bit) bis 9.5 (64 Bit) und 10 (64 Bit), einschließlich SELinux
CentOS	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) und 9.1 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux
Red Hat	8.10 (64 Bit), 9.1 (64 Bit) bis 9.6 (64 Bit) und 10 (64 Bit), einschließlich SELinux
Felsig	Rocky 9.4 (64 Bit) bis 9.6 (64 Bit), einschließlich SELinux
SUSE Enterprise Linux	15 SP4 (64 Bit) bis 15 SP6 (64 Bit), einschließlich SELinux
Ubuntu	20.04 LTS (64 Bit), 22.04 LTS (64 Bit) und 24.04 LTS (64 Bit)

Auf dem Computer, den Sie für den Benutzeraktivitätsagenten verwenden, sollte keine andere Software auf Anwendungsebene ausgeführt werden. Ein dedizierter Server wird empfohlen.

Der `unzip` Für die Installation wird ein Befehl benötigt. Der `sudo su -` Der Befehl wird für die Installation, die Ausführung von Skripten und die Deinstallation benötigt.

Serveranforderungen

Der Server muss die folgenden Mindestanforderungen erfüllen:

- **CPU**: 4 Kerne
- **RAM**: 16 GB RAM
- **Festplattenspeicher**: 36 GB freier Festplattenspeicher

Serverempfehlungen

- Weisen Sie zusätzlichen Speicherplatz zu, um die Erstellung des Dateisystems zu ermöglichen. Stellen Sie sicher, dass im Dateisystem mindestens 35 GB freier Speicherplatz vorhanden sind. + Wenn `/opt` Es handelt sich um einen eingebundenen Ordner von einem NAS-Speicher; lokale Benutzer müssen Zugriff auf diesen Ordner haben. Die Erstellung eines Benutzeraktivitätsagenten kann fehlschlagen, wenn lokale Benutzer nicht über die erforderlichen Berechtigungen verfügen.
- Es wird empfohlen, den Benutzeraktivitätsagenten auf einem separaten System zu installieren, das von Ihrer Ransomware Resilience-Umgebung getrennt ist. Wenn Sie sie dennoch auf demselben Rechner installieren, sollten Sie 50 bis 55 GB Festplattenspeicher einplanen. Für Linux sollten Sie 25–30 GB Speicherplatz für `/opt/netapp` und 25 GB für `var/log/netapp` reservieren.

- Es wird empfohlen, die Zeit sowohl auf dem ONTAP System als auch auf dem Rechner des Benutzeraktivitätsagenten mithilfe des Network Time Protocol (NTP) oder des Simple Network Time Protocol (SNTP) zu synchronisieren.

Cloud-Netzwerkzugriffsregeln

Prüfen Sie die Cloud-Netzwerkzugriffsregeln für Ihre jeweilige Region (Asien-Pazifik, Europa oder Vereinigte Staaten).

Ersetzen Sie während der Erstinstallation die `<site_name>` durch eine Platzhalter-(`*` -Berechtigung. Nachdem der Agent aktiviert und voll funktionsfähig ist, können Sie die Berechtigung durch den Standortnamen ersetzen. Wenden Sie sich an Ihren NetApp-Ansprechpartner, um den Standortnamen zu erhalten.

Der Benutzeraktivitätsagent nutzt NetApp Data Insights Infrastructure-Technologie, daher die Verwendung von `cloudinsights` Endpunkten. Weitere Informationen finden Sie unter

Bereitstellungen von Benutzeraktivitätsagenten mit Sitz in APAC

Protokoll	Hafen	Quelle	Ziel	Beschreibung
HTTPS (TCP)	443	Benutzeraktivitätsagent	• <site_name>.cs01-ap-1.cloudinsights.netapp.com • <site_name>.c01-ap-1.cloudinsights.netapp.com • <site_name>.c02-ap-1.cloudinsights.netapp.com • gentlogin.cs01-ap-1.cloudinsights.netapp.com	Zugang zu Ransomware-Resilienz

Benutzeraktivitätsagenten-Bereitstellungen mit Sitz in Europa

Protokoll	Hafen	Quelle	Ziel	Beschreibung
HTTPS (TCP)	443	Benutzeraktivitätsagent	• <site_name>.cs01-eu-1.cloudinsights.netapp.com • <site_name>.c01-eu-1.cloudinsights.netapp.com • <site_name>.c02-eu-1.cloudinsights.netapp.com • agentlogin.cs01-eu-1.cloudinsights.netapp.com	Zugang zu Ransomware-Resilienz

US-basierte Bereitstellungen von Benutzeraktivitätsagenten

Protokoll	Hafen	Quelle	Ziel	Beschreibung
HTTPS (TCP)	443	Benutzeraktivitätsagent	• <site_name>.cs01.cloudinsights.netapp.com • <site_name>.c01.cloudinsights.netapp.com • <site_name>.c02.cloudinsights.netapp.com • agentlogin.cs01.cloudinsights.netapp.com	Zugang zu Ransomware-Resilienz

Netzwerkinterne Regeln

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	389 (LDAP) 636 (LDAPs / Start-TLS)	Benutzeraktivitätsagent	LDAP-Server-URL	Mit LDAP verbinden
HTTPS (TCP)	443	Benutzeraktivitätsagent	Cluster- oder SVM-Management-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	Benutzeraktivitätsagent	Kommunikation von ONTAP an den Benutzeraktivitätsagenten für Fpolicy-Ereignisse. Diese Ports müssen zum Benutzeraktivitätsagenten hin geöffnet werden, damit ONTAP Ereignisse an ihn senden kann, einschließlich etwaiger Firewall-Anforderungen auf dem Benutzeraktivitätsagenten selbst (falls vorhanden). + **HINWEIS:** Sie müssen nicht **alle** dieser Ports reservieren, aber die Ports, die Sie hierfür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, mit der Reservierung von 100 Ports zu beginnen und diese bei Bedarf zu erhöhen.

Protokoll	Hafen	Quelle	Ziel	Beschreibung
TCP	35000-55000	Cluster-Verwaltungs-IP	Benutzeraktivitätsagent	Kommunikation von der ONTAP Clusterverwaltungs-IP zum Benutzeraktivitätsagenten für **EMS-Ereignisse**. Diese Ports müssen zum Benutzeraktivitätsagenten hin geöffnet werden, damit ONTAP EMS-Ereignisse an ihn senden kann, einschließlich etwaiger Firewall-Anforderungen auf dem Benutzeraktivitätsagenten selbst. + **HINWEIS:** Sie müssen nicht **alle** dieser Ports reservieren, aber die Ports, die Sie hierfür reservieren, müssen innerhalb dieses Bereichs liegen. Es wird empfohlen, mit der Reservierung von 100 Ports zu beginnen und diese bei Bedarf zu erhöhen.
SSH	22	Benutzeraktivitätsagent	Clusterverwaltung	Wird für die CIFS/SMB-Benutzerblockierung benötigt.

Nächster Schritt

- "Benutzeraktivitätsagenten und -sammler konfigurieren"

Konfigurieren der Benutzeraktivitätserkennung in NetApp Ransomware Resilience

NetApp Ransomware Resilience Benutzeraktivitätserkennung hilft Ihnen, Ransomware-Ereignisse auf Benutzerebene zu verhindern. Um die Erkennung verdächtigen Benutzerverhaltens in Ransomware Resilience zu aktivieren, müssen Sie mindestens

einen Benutzeraktivitätsagenten installieren, der eine Datenerfassungsumgebung erstellt, um das Benutzerverhalten auf abweichende Muster zu überwachen, die Ransomware-Ereignissen ähneln.

Ein Benutzeraktivitätsagent hostet einen Datensammler und einen Benutzerverzeichnis-Connector, die beide Daten zur Analyse an einen SaaS-Standort senden.

- Der **Datensammler** erfasst Benutzeraktivitätsdaten von ONTAP. Der Datensammler wird automatisch erstellt, wenn Sie eine Schutzstrategie mit Benutzerverhaltenserkennung erstellen.
- Der **Benutzerverzeichnis-Connector** stellt eine Verbindung zu Ihrem Verzeichnis her, um Benutzer-IDs Benutzernamen zuzuordnen. Sie müssen den Benutzerverzeichnis-Connector konfigurieren.

Der Benutzeraktivitätsagent, der Datensammler und der Benutzerverzeichnis-Connector können alle über das Dashboard der Ransomware Resilience-Einstellungen verwaltet werden.

> Wenn Sie bereits NetApp Data Infrastructure Insights (DII) Workload Security verwenden, wird empfohlen, dieselben Workload Security Agents auch für Ransomware Resilience zu verwenden. Sie müssen keine separaten Workload Security Agents für Ransomware Resilience bereitstellen, jedoch erfordert die Verwendung derselben Workload Security Agents eine Kopplung zwischen der Ransomware Resilience Console Organization und dem DII Storage Workload Security Tenant. Wenden Sie sich an Ihren Account Representative, um diese Kopplung zu aktivieren.

+ Falls Sie *nicht* DII verwenden, fahren Sie mit den Konfigurationsanweisungen hier fort.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie die "Anforderungen an Betriebssystem, Server und Netzwerk" erfüllen.

Erforderliche Konsolenrolle Um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren, benötigen Sie die **Organization admin role**. Für nachfolgende Konfigurationen verdächtiger Benutzeraktivitäten benötigen Sie die **Ransomware Resilience user behavior admin role**. "Erfahren Sie mehr über Ransomware Resilience-Rollen für die NetApp Console".

Stellen Sie sicher, dass jede Rolle auf Organisationsebene angewendet wird.

Erstellen Sie einen Benutzeraktivitätsagenten

Benutzeraktivitätsagenten sind ausführbare Umgebungen für "Datensammler"; Datensammler teilen Benutzeraktivitätsereignisse mit Ransomware Resilience. Sie müssen mindestens einen Benutzeraktivitätsagenten erstellen, um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren.

Schritte

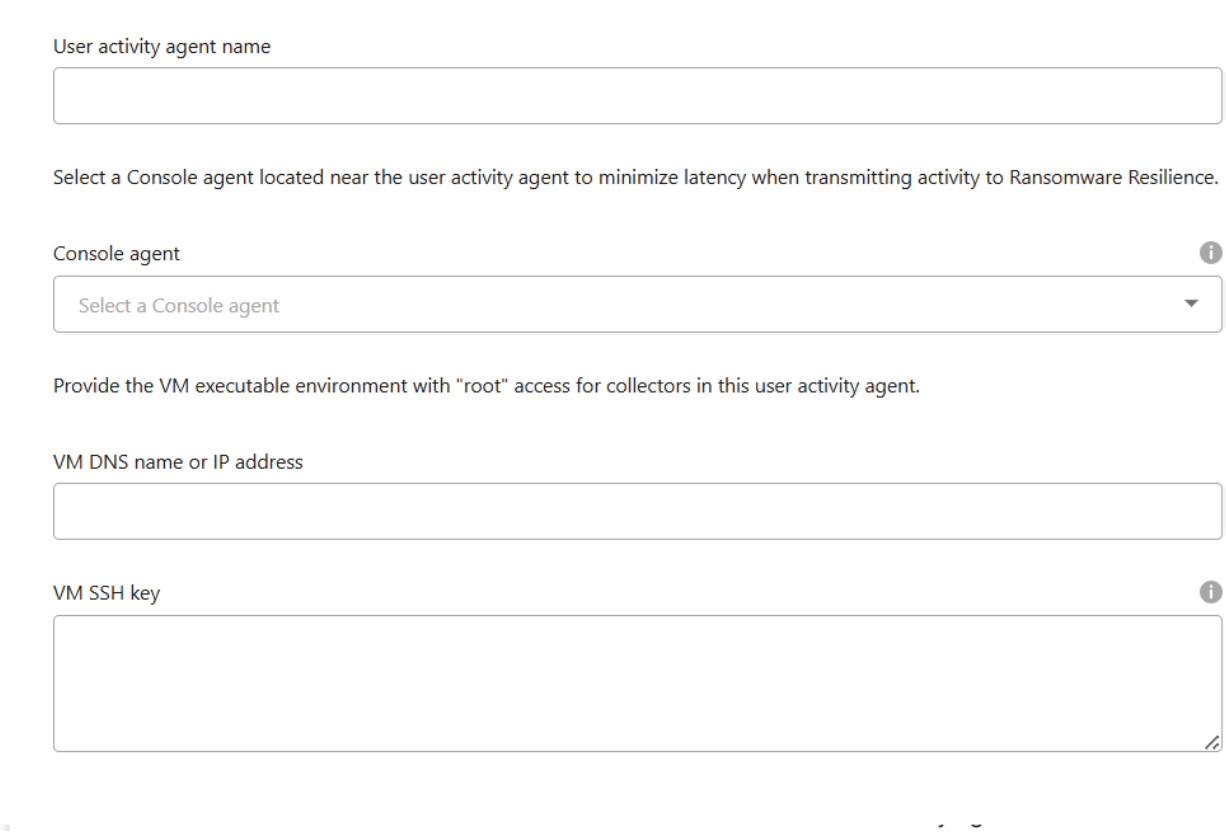
1. Wenn Sie zum ersten Mal einen Benutzeraktivitätsagenten erstellen, gehen Sie zum **Dashboard**. Wählen Sie in der Kachel **Benutzeraktivität** die Option **Aktivieren** aus.

   Wenn Sie einen zusätzlichen Benutzeraktivitätsagenten hinzufügen, gehen Sie zu **Einstellungen**, suchen Sie die Kachel **Benutzeraktivität** und wählen Sie dann **Verwalten**. Wählen Sie auf dem Bildschirm „Benutzeraktivität“ die Registerkarte **Benutzeraktivitätsagenten** und dann **Hinzufügen**.

2. Wählen Sie einen **Cloud-Anbieter** und dann eine **Region** aus. Wählen Sie **Weiter**.
3. Geben Sie die Details des Benutzeraktivitätsagenten an:

- **Name des Benutzeraktivitätsagenten**
- **Konsolenagent** - Der Konsolenagent sollte sich im selben Netzwerk wie der Benutzeraktivitätsagent befinden und über eine SSH-Verbindung zur IP-Adresse des Benutzeraktivitätsagenten verfügen.
- **VM-DNS-Name oder IP-Adresse**
- **VM SSH Key** - Geben Sie den SSH-Schlüssel in diesem Format ein:

```
-----BEGIN OPENSSH PRIVATE KEY-----
private-key-contents
-----END OPENSSH PRIVATE KEY-----
```



4. Wählen Sie **Weiter**.
5. Überprüfen Sie Ihre Einstellungen. Wählen Sie **Aktivieren**, um das Hinzufügen des Benutzeraktivitätsagenten abzuschließen.
6. Bestätigen Sie, dass der Benutzeraktivitätsagent erfolgreich erstellt wurde. In der Kachel „Benutzeraktivität“ wird eine erfolgreiche Bereitstellung als **Wird ausgeführt** angezeigt.

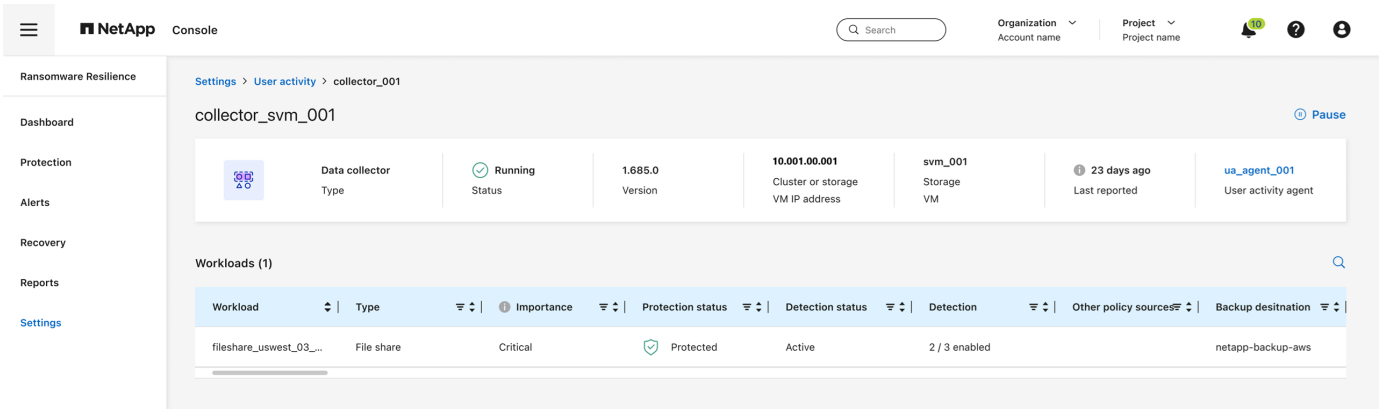
Ergebnis

Nachdem der Benutzeraktivitätsagent erfolgreich erstellt wurde, kehren Sie zum Menü **Einstellungen** zurück und wählen Sie dann **Verwalten** im Bereich Benutzeraktivität. Wählen Sie den Tab **Benutzeraktivitätsagenten** und dann den Benutzeraktivitätsagenten aus, um Details dazu anzuzeigen, einschließlich Datensammler und Benutzerverzeichnis-Konnektoren.

Hinzufügen eines Datensammlers

Datensammler werden automatisch erstellt, wenn Sie eine Ransomware-Schutzstrategie mit Erkennung verdächtiger Benutzeraktivitäten aktivieren. Weitere Informationen finden Sie unter "Hinzufügen einer Erkennungsrichtlinie".

Sie können die Details des Datensammlers anzeigen. Wählen Sie in den Einstellungen in der Kachel „Benutzeraktivität“ die Option **Verwalten** aus. Wählen Sie die Registerkarte **Datensammler** und dann den Datensammler aus, um seine Details anzuzeigen oder ihn anzuhalten.



Erstellen Sie einen Benutzerverzeichnis-Connector

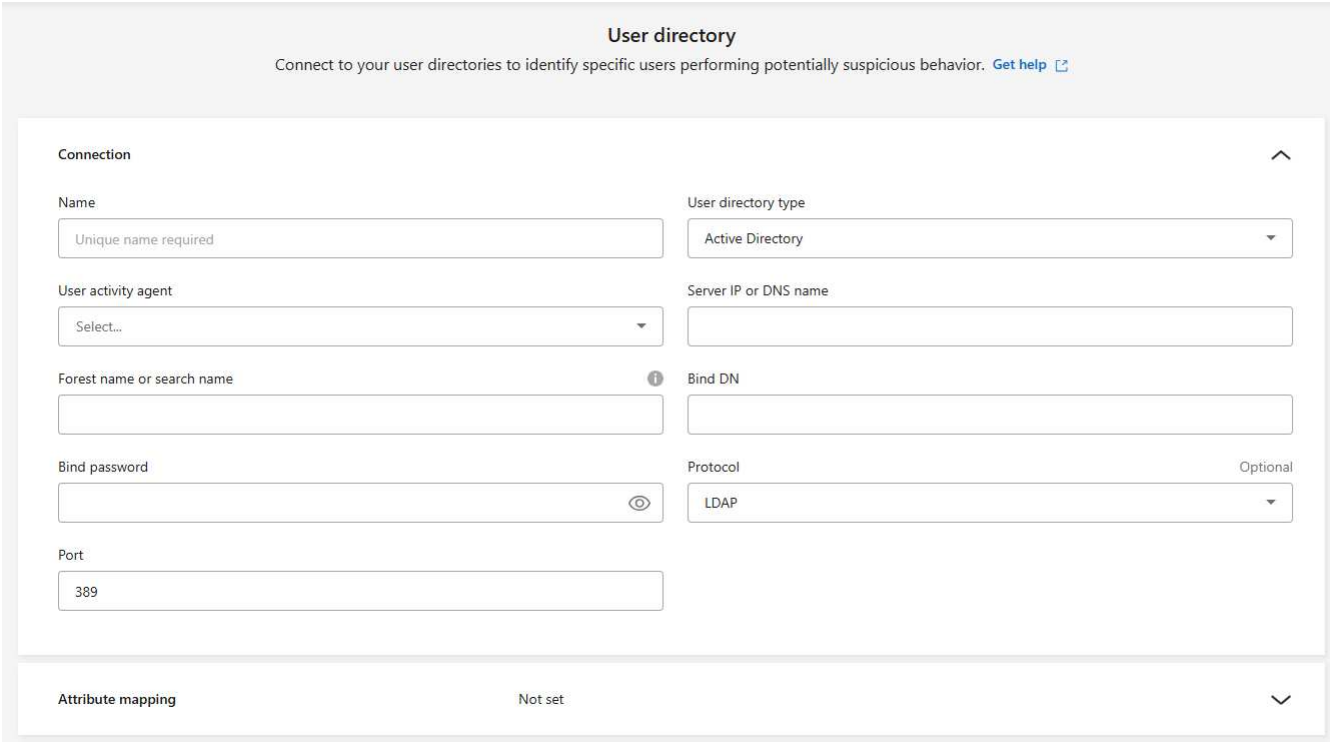
Um Benutzer-IDs Benutzernamen zuzuordnen, müssen Sie einen Benutzerverzeichnis-Connector erstellen.

Schritte

1. Gehen Sie in Ransomware Resilience zu **Einstellungen**.
2. Wählen Sie in der Kachel „Benutzeraktivität“ **Verwalten** aus.
3. Wählen Sie die Registerkarte **Benutzerverzeichnis-Konnektoren** und dann **Hinzufügen**.
4. Konfigurieren Sie die Verbindung. Geben Sie die erforderlichen Informationen für jedes Feld ein.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Benutzerverzeichnis-Connector ein.
Benutzerverzeichnistyp	Der Verzeichnistyp
Server-IP-Adresse oder Domänenname	Die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des Servers, der die Verbindung hostet
Waldname oder Suchname	Sie können die Gesamtstrukturebene der Verzeichnisstruktur als direkten Domänennamen angeben (zum Beispiel `unit.company.com`) oder eine Reihe relativer, angesehener Namen (zum Beispiel: `DC=unit,DC=company,DC=com`). Sie können auch einen Eintrag eingeben `OU` um nach einer Organisationseinheit oder einem `CN` auf einen bestimmten Benutzer beschränken (zum Beispiel: `CN=user,OU=engineering,DC=unit,DC=company,DC=com`).

Feld	Beschreibung
BIND DN	Der BIND DN ist ein Benutzerkonto, das berechtigt ist, das Verzeichnis zu durchsuchen, z. B. user@domain.com. Der Benutzer benötigt die Berechtigung „Domänenlesbar“.
BIND-Passwort	Das Passwort für den in BIND DN angegebenen Benutzer.
Protokoll	Das Feld „Protokoll“ ist optional. Sie können LDAP, LDAPS oder LDAP over StartTLS verwenden.
Hafen	Geben Sie die von Ihnen gewählte Portnummer ein.



Geben Sie die Details zur Attributzuordnung an:

- **Anzeigename**
- **SID** (wenn Sie LDAP verwenden)
- **Benutzername**
- **Unix-ID** (wenn Sie NFS verwenden)
- Wenn Sie **Optionale Attribute einbeziehen** auswählen, können Sie auch eine E-Mail-Adresse, eine Telefonnummer, eine Rolle, ein Bundesland, ein Land, eine Abteilung, ein Foto, den Vorgesetzten-DN oder Gruppen hinzufügen. Wählen Sie **Erweitert**, um eine optionale Suchanfrage hinzuzufügen.

5. Wählen Sie **Hinzufügen**.
6. Kehren Sie zur Registerkarte „Benutzerverzeichnis-Konnektoren“ zurück, um den Status Ihres Benutzerverzeichnis-Konnektors zu überprüfen. Bei erfolgreicher Erstellung wird der Status des Benutzerverzeichnis-Connectors als **Wird ausgeführt** angezeigt.

Löschen eines Benutzerverzeichnis-Connectors

Schritte

1. Gehen Sie in Ransomware Resilience zu **Einstellungen**.
2. Suchen Sie die Kachel „Benutzeraktivität“ und wählen Sie **Verwalten** aus.
3. Wählen Sie die Registerkarte **Benutzerverzeichnis-Connector**.
4. Identifizieren Sie den Benutzerverzeichnis-Connector, den Sie löschen möchten. Wählen Sie im Aktionsmenü am Ende der Zeile die drei Punkte aus … dann **Löschen**.
5. Wählen Sie im Popup-Dialogfeld **Löschen** aus, um zu bestätigen.

Benutzer von Warnmeldungen ausschließen

Wenn es bestimmte vertrauenswürdige Benutzer gibt, deren Verhalten möglicherweise Warnmeldungen zum Benutzerverhalten auslöst, können Sie sie von Warnmeldungen ausschließen.

Schritte

1. Unter Ransomware Resilience wählen Sie **Einstellungen**.
2. Suchen Sie im Dashboard „Einstellungen“ die Karte „Benutzeraktivität“ und wählen Sie dann **Manage** aus.
3. Wählen Sie die Registerkarte **Excluded users** aus.
4. Um einzelne Benutzer in der Benutzeroberfläche zu überprüfen, wählen Sie **Manuell auswählen**. Um eine Liste ausgeschlossener Benutzer hochzuladen, wählen Sie **Hochladen**.

    a. Wenn Sie **Manuell auswählen** gewählt haben, aktivieren Sie das Kontrollkästchen neben den Namen der spezifischen Benutzer, die Sie ausschließen möchten.

    b. Wenn Sie **Hochladen** auswählen, laden Sie die CSV- oder JSON-Datei mit der Liste aller Benutzer herunter. Wählen Sie **Herunterladen**, um auf die Liste zuzugreifen.

    Überprüfen Sie die Datei auf Ihrem lokalen Rechner. Entfernen Sie die Namen aller Benutzer, für die Sie die Erkennung beibehalten möchten. Wenn die Liste nur noch die Namen der Benutzer enthält, die Sie von der Erkennung ausschließen möchten, speichern Sie sie.

    Wählen Sie in Ransomware Resilience **Hochladen** aus. Suchen Sie die Datei und laden Sie sie hoch.

5. Wählen Sie **Hinzufügen** aus, um das Hinzufügen der Benutzer zur Ausschlussliste abzuschließen.
6. Auf der Registerkarte **Ausgeschlossene Benutzer** werden nun die Namen der Benutzer angezeigt, die aus den Warnmeldungen zur Benutzerverhaltenserkennung entfernt wurden.

Sie können einen Benutzer auch direkt von einer Benachrichtigung ausschließen. Weitere Informationen finden Sie unter "Auf Ransomware-Warnungen reagieren".

Benutzer aus der Liste der ausgeschlossenen Benutzer entfernen

Sie können einen Benutzer anschließend wieder zur Erkennung hinzufügen.

Schritte

1. Suchen Sie im Dashboard „Einstellungen“ die Karte „Benutzeraktivität“ und wählen Sie dann **Manage** aus.
2. Wählen Sie die Registerkarte **Excluded users** aus.
3. Wählen Sie **Hinzufügen**.
4. Um einzelne Benutzer von der UI auszuschließen, wählen Sie **Select manually**.
5. Suchen Sie den Namen des Benutzers, den Sie aus der Liste der ausgeschlossenen Benutzer entfernen möchten. Wählen Sie das Aktionsmenü (…) in der Zeile mit dem Benutzernamen und dann **Entfernen**.

6. Wählen Sie im Dialogfeld **Entfernen** aus, um zu bestätigen, dass Sie die ausgewählten Benutzer entfernen möchten.

Reagieren Sie auf Warnungen zu verdächtigen Benutzeraktivitäten

Nachdem Sie die Erkennung verdächtiger Benutzeraktivitäten konfiguriert haben, können Sie Ereignisse auf der Warnseite überwachen. Weitere Informationen finden Sie unter "Erkennen Sie bösartige Aktivitäten und verdächtiges Nutzerverhalten".