Sicherheit

Data Infrastructure Insights

NetApp
December 19, 2024

Inhalt

Sicherheit

Einblicke In Die Dateninfrastruktur, Sicherheit

Die Datensicherheit bei Produkten und Kunden ist bei NetApp von größter Bedeutung. Data Infrastructure Insights befolgt während des gesamten Release-Lebenszyklus sicherheitstechnisch bewährte Verfahren, damit Kundeninformationen und -Daten bestmöglich geschützt werden.

Sicherheit – Überblick

Physische Sicherheit

Die Produktionsinfrastruktur von Data Infrastructure Insights wird auf Amazon Web Services (AWS) gehostet. Physische und umgebungsbezogene Sicherheitskontrollen für Data Infrastructure Insights Produktions-Server, einschließlich Gebäude sowie Schlösser oder Schlüssel, die an Türen verwendet werden, werden von AWS gemanagt. Gemäß AWS: „Der physische Zugang wird sowohl am Perimeter als auch an Einbruchstellen durch professionelles Sicherheitspersonal mithilfe von Videoüberwachung, Intrusion Detection Systemen und anderen elektronischen Mitteln gesteuert. Autorisierte Mitarbeiter nutzen Multi-Faktor-Authentifizierungsmechanismen für den Zugriff auf Datacenter-Stockwerke.“

Data Infrastructure Insights folgt den Best Practices"Modell der gemeinsamen Verantwortung", die von AWS beschrieben werden.

Produktsicherheit

Data Infrastructure Insights folgt einem Entwicklungslebenszyklus nach den Prinzipien von Agile. So können wir sicherheitsbezogene Softwarefehler im Vergleich zu Methoden zur Entwicklung eines längeren Release-Zyklus schneller beheben. Mithilfe von Methoden zur kontinuierlichen Integration sind wir in der Lage, schnell sowohl auf funktionale als auch auf Sicherheitsänderungen zu reagieren. Die Änderungsmanagementverfahren und -Richtlinien legen fest, wann und wie Änderungen vorgenommen werden, und tragen dazu bei, die Stabilität der Produktionsumgebung zu erhalten. Alle wirkungsvollen Änderungen werden formal kommuniziert, koordiniert, richtig überprüft und vor ihrer Veröffentlichung in der Produktionsumgebung genehmigt.

Netzwerksicherheit

Der Netzwerkzugriff auf Ressourcen in der Data Infrastructure Insights Umgebung wird über Host-basierte Firewalls gesteuert. Jede Ressource (wie z. B. ein Load Balancer oder eine virtuelle Maschineninstanz) verfügt über eine hostbasierte Firewall, die den eingehenden Datenverkehr auf nur die Ports beschränkt, die für die Ausführung ihrer Funktion benötigt werden.

Data Infrastructure Insights nutzt verschiedene Mechanismen wie Intrusion Detection Services, um die Produktionsumgebung auf Sicherheitsanomalien zu überwachen.

Risikoeinschätzung

Das Data Infrastructure Insights-Team folgt einem formalisierten Risikobewertungsprozess, um eine systematische, wiederholbare Methode zur Identifizierung und Bewertung der Risiken bereitzustellen, damit diese durch einen Risikobehandlungsplan angemessen gemanagt werden können.

Datensicherung

Die Produktionsumgebung von Data Infrastructure Insights wird in einer hochredundanten Infrastruktur eingerichtet, in der für alle Services und Komponenten mehrere Verfügbarkeitszonen genutzt werden. Neben einer hochverfügbaren und redundanten Computing-Infrastruktur werden wichtige Daten in regelmäßigen Abständen gesichert und Restores regelmäßig getestet. Formelle Backup-Richtlinien und -Verfahren minimieren die Auswirkungen von Unterbrechungen von Geschäftsaktivitäten und schützen Unternehmensprozesse gegen die Auswirkungen von Fehlern in Informationssystemen oder -Ausfällen und stellen einen zeitnahen und adäquaten Wiederaufnahme sicher.

Authentifizierung und Zugriffsmanagement

Der gesamte Zugriff von Kunden auf Data Infrastructure Insights erfolgt über Interaktionen auf der Browser-Benutzeroberfläche über HTTPS. Die Authentifizierung erfolgt über den Dienst Auth0 eines Drittanbieters. NetApp hat hier als Authentifizierungsebene für alle Cloud-Datenservices zentralisiert.

Data Infrastructure Insights befolgt branchenübliche Best Practices, einschließlich „Least Privilege“ und „rollenbasierte Zugriffssteuerung“ beim logischen Zugriff auf die Produktionsumgebung von Data Infrastructure Insights. Der Zugriff wird streng nach Anforderungen kontrolliert und nur ausgewählten autorisierten Mitarbeitern mit Multi-Faktor-Authentifizierungsmechanismen gewährt.

Erhebung und Schutz von Kundendaten

Alle Kundendaten werden während der Übertragung über öffentliche Netzwerke verschlüsselt und im Ruhezustand verschlüsselt. Data Infrastructure Insights nutzt Verschlüsselung an verschiedenen Stellen im System zum Schutz von Kundendaten. Dazu kommen Technologien wie Transport Layer Security (TLS) und der branchenübliche AES-256-Algorithmus.

Kundendeprovisionierung

E-Mail-Benachrichtigungen werden in verschiedenen Abständen versendet, um dem Kunden mitzuteilen, dass das Abonnement abläuft. Nach Ablauf des Abonnements wird die UI eingeschränkt und eine Kulanzzeit beginnt für die Datenerfassung. Der Kunde wird dann per E-Mail benachrichtigt. Bei Testabonnements besteht eine Frist von 14 Tagen. Im Rahmen der bezahlten Abonnements haben Sie eine Frist von 28 Tagen. Nach Ablauf der Kulanzzeit wird der Kunde per E-Mail darüber informiert, dass das Konto innerhalb von 2 Tagen gelöscht wird. Ein zahlter Kunde kann auch direkt beantragen, dass er nicht im Service ist.

Abgelaufene Mandanten und alle zugehörigen Kundendaten werden vom Data Infrastructure Insights Operations (SRE) Team am Ende der Gnadenfrist oder nach Bestätigung der Kontoersatzanfrage eines Kunden gelöscht. In beiden Fällen führt das SRE-Team einen API-Aufruf aus, um das Konto zu löschen. Der API-Aufruf löscht die Mandanteninstanz und alle Kundendaten. Die Löschung durch den Kunden wird durch den Aufruf derselben API überprüft und überprüft, ob der Kunde den Status „GELÖSCHT“ hat.

Management von Sicherheitsproblemen

Dateninfrastruktur Insights ist in den PSIRT-Prozess (Product Security Incident Response Team) von NetApp integriert, um bekannte Schwachstellen zu finden, zu bewerten und zu beheben. PSIRT nutzt Informationen zu Schwachstellen über mehrere Kanäle, darunter Kundenberichte, interne technische Informationen und allgemein anerkannte Quellen wie die CVE-Datenbank.

Wenn ein Problem vom Data Infrastructure Insights Engineering-Team erkannt wird, leitet das Team den PSIRT-Prozess ein, bewertet und Behebung des Problems.

Es ist auch möglich, dass ein Kunde oder Wissenschaftler bei Data Infrastructure Insights ein Sicherheitsproblem beim Data Infrastructure Insights Produkt identifiziert und das Problem dem technischen

Support oder direkt dem NetApp Incident Response-Team meldet. In diesen Fällen leitet das Team von Data Infrastructure Insights den PSIRT-Prozess ein, bewertet und beseitigt das Problem möglicherweise.

Schwachstellen- und Penetrationstests

Data Infrastructure Insights befolgt branchenübliche Best Practices und führt regelmäßig Schwachstellen- und Penetrationstests durch, bei denen sowohl interne als auch externe Sicherheitsexperten und Unternehmen zum Einsatz kommen.

Schulung zur Sensibilisierung für die Sicherheit

Alle Mitarbeiter von Data Infrastructure Insights werden gemäß dem Sicherheitstraining für individuelle Rollen entwickelt, um sicherzustellen, dass jeder Mitarbeiter in der Lage ist, mit den spezifischen sicherheitsorientierten Herausforderungen seiner Rolle umzugehen.

Compliance

Data Infrastructure Insights führt unabhängige Audits und Validierungen der Sicherheitsmaßnahmen, Prozesse und Services durch anerkannte externe Prüfer durch. Zu den Prüfungen zählen auch SOC 2-Audits.

NetApp-Sicherheitsempfehlungen

Sie können die verfügbaren Sicherheitsempfehlungen von NetApp anzeigen"Hier".

Informationen und Region

NetApp nimmt die Sicherheit von Kundeninformationen sehr ernst. Hier erfahren Sie, wie und wo Data Infrastructure Insights Ihre Informationen speichert.

Welche Informationen werden in Data Infrastructure Insights gespeichert?

Data Infrastructure Insights speichert folgende Informationen:

- Performance-Daten

  Performancedaten sind Zeitreihendaten, die Informationen zur Leistung des überwachten Geräts/der überwachten Quelle liefern. Dazu zählen beispielsweise die Anzahl der von einem Speichersystem bereitgestellten iOS, der Durchsatz eines FibreChannel-Ports, die Anzahl der von einem Webserver bereitgestellten Seiten, die Reaktionszeit einer Datenbank und vieles mehr.

- Bestandsdaten

  Bestandsdaten bestehen aus Metadaten, die das überwachte Gerät/die Quelle beschreiben und wie es konfiguriert wird. Dazu gehören beispielsweise installierte Hardware- und Softwareversionen, Festplatten und LUNs in einem Storage-System, CPU-Kerne, RAM und Festplatten einer Virtual Machine, die Tabellen einer Datenbank, die Anzahl und die Art der Ports auf einem SAN Switch, Verzeichnis-/Dateinamen (bei aktivierter Storage Workload Security) usw.

- Konfigurationsdaten

  Dies fasst vom Kunden bereitgestellte Konfigurationsdaten zusammen, die zur Verwaltung von Kundeninventar und -Vorgängen verwendet werden, z. B. Hostnamen oder IP-Adressen der überwachten Geräte, Abfrageintervalle, Zeitlimits usw.

- Secrets

  Geheimnisse umfassen die Anmeldeinformationen, die von der Data Infrastructure Insights Acquisition Unit für den Zugriff auf Kundengeräte und -Services verwendet werden. Diese Anmeldeinformationen werden mit einer starken asymmetrischen Verschlüsselung verschlüsselt, und die privaten Schlüssel werden nur auf den Akquisitionseinheiten gespeichert und verlassen nie die Kundenumgebung. Selbst privilegierte Data Infrastructure Insights SRES können aufgrund dieses Designs nicht auf Kundengeheimnisse im Klartext zugreifen.

- Funktionale Daten

  Diese Daten werden durch die Bereitstellung des Cloud Data Service durch NetApp generiert, der NetApp über die Entwicklung, Implementierung, den Betrieb, die Wartung und die Sicherung des Cloud Data Service informiert. Funktionale Daten enthalten weder Kundendaten noch personenbezogene Daten.

- Benutzerdaten

  Authentifizierungs- und Zugriffsinformationen, die es NetApp BlueXP ermöglichen, mit regionalen Dateninfrastrukturen Insights zu kommunizieren, einschließlich Daten zur Benutzerautorisierung.

- Sicherheitsdaten Des Benutzerverzeichnisses Für Storage-Workloads

  In Fällen, in denen die Workload-Sicherheitsfunktion aktiviert ist UND der Kunde den Benutzer-Directory-Collector aktivieren möchte, speichert das System Anzeigenamen, Unternehmens-E-Mail-Adressen und andere Informationen, die aus Active Directory gesammelt wurden.

Benutzerverzeichnisdaten beziehen sich auf Benutzerverzeichnisinformationen, die vom Datensammler Workload Security User Directory erfasst werden, nicht auf Daten über die Benutzer von Data Infrastructure Insights/Workload Security selbst.

Es werden keine expliziten personenbezogenen Daten aus Infrastruktur- und Dienstleistungsressourcen erhoben. Die erfassten Daten bestehen aus Performance-Kennzahlen, Konfigurationsdaten und Infrastrukturmetadaten, ähnlich wie viele Telefonanbieter mit NetApp Auto-Support und ActiveIQ. Abhängig von den Namenskonventionen des Kunden werden jedoch Daten für Shares, Volumes, VMs, qtrees, Anwendungen usw. können personenbezogene Informationen enthalten.

Wenn Workload Security aktiviert ist, untersucht das System außerdem Datei- und Verzeichnisnamen auf SMB- oder anderen Freigaben, die personenbezogene Informationen enthalten können. Wenn Kunden den Workload Security User Directory Collector aktivieren (der Windows SIDs im Wesentlichen über Active Directory Benutzernamen zuordnet), werden der Anzeigename, die Unternehmens-E-Mail-Adresse und alle zusätzlich ausgewählten Attribute von Data Infrastructure Insights erfasst und gespeichert.

Darüber hinaus werden Zugriffsprotokolle zu Data Infrastructure Insights verwaltet und enthalten die IP- und E-Mail-Adressen der Benutzer, die zur Anmeldung beim Service verwendet werden.

Wo werden meine Informationen gespeichert?

Data Infrastructure Insights speichert Informationen entsprechend der Region, in der Ihre Umgebung erstellt wird.

Folgende Informationen werden in der Host-Region gespeichert:

- Telemetrie- und Asset-/Objektdaten, einschließlich Zähler und Performance-Kennzahlen

- Informationen zu den Erfassungseinheiten
- Funktionale Daten
- Audit-Informationen zu Benutzeraktivitäten innerhalb von Data Infrastructure Insights
- Active Directory-Informationen zu Workload-Sicherheit
- Informationen zur Workload Security Audit

Die folgenden Informationen verbleiben in den USA, unabhängig von der Region, in der Ihre Data Infrastructure Insights Umgebung gehostet wird:

- Angaben zum Umgebungsstandort (manchmal auch „Mandant“ genannt), z. B. Standort-/Kontoinhaber.
- Informationen, die es NetApp BlueXP ermöglichen, mit regionalen Einsichten zu Dateninfrastrukturen zu kommunizieren, einschließlich aller Vorgänge, die mit der Benutzerautorisierung ausgeführt werden.
- Informationen im Zusammenhang mit der Beziehung zwischen dem Benutzer Data Infrastructure Insights und dem Mandanten.

Host-Regionen

Host-Regionen sind:

- USA: USA-Osten-1
- EMEA: EU-Mitte-1
- APAC: ap-Südost-2

Weitere Informationen

Weitere Informationen zu Datenschutz und Sicherheit von NetApp finden Sie unter folgenden Links:

- "Trust Center"
- "Grenzüberschreitende Datenübertragungen"
- "Binding Corporate Rules"
- "Reaktion auf Datenanfragen von Drittanbietern"
- "NetApp Datenschutzgrundsätze"

Sicherheitstool

Dateninfrastruktur Insights umfasst Sicherheitsfunktionen, mit denen Ihre Umgebung sicherer betrieben werden kann. Die Funktionen umfassen Verbesserungen bei der Verschlüsselung, Passwort-Hashing und die Fähigkeit, interne Benutzerpasswörter zu ändern sowie Schlüsselpaare, die Kennwörter verschlüsseln und entschlüsseln.

Zum Schutz sensibler Daten empfiehlt NetApp, nach einer Installation oder einem Upgrade die Standardschlüssel und das Benutzerpasswort „*Acquisition*“ zu ändern.

Verschlüsselte Passwörter der Datenquelle werden in Data Infrastructure Insights gespeichert, das einen öffentlichen Schlüssel verwendet, um Passwörter zu verschlüsseln, wenn ein Benutzer sie auf einer Konfigurationsseite für den Datensammler eingibt. Data Infrastructure Insights verfügt nicht über die privaten Schlüssel, die zum Entschlüsseln der Datensammlerkennwörter erforderlich sind. Nur Acquisition Units (aus)

verfügen über den privaten Datensammlerschlüssel, der zum Entschlüsseln der Datensammlerkennwörter erforderlich ist.

Überlegungen zu Upgrades und Installationen

Wenn Ihr Insight-System nicht standardmäßige Sicherheitskonfigurationen enthält (d. h. Sie haben ein rekeyed Kennwort), müssen Sie Ihre Sicherheitskonfigurationen sichern. Durch die Installation neuer Software oder in einigen Fällen eines Software-Upgrades wird das System auf eine Standardsicherheitskonfiguration zurückgesetzt. Wenn Ihr System auf die Standardkonfiguration zurückgesetzt wird, müssen Sie die nicht voreingestellte Konfiguration wiederherstellen, damit das System ordnungsgemäß funktioniert.

Sicherheitsverwaltung auf der Akquisitionseinheit

Mit dem SecurityAdmin-Tool können Sie die Sicherheitsoptionen für Data Infrastructure Insights verwalten und wird auf dem Erfassungssystem ausgeführt. Die Sicherheitsverwaltung umfasst das Verwalten von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen von Sicherheitskonfigurationen, die Sie erstellen oder auf die Standardeinstellungen wiederherstellen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte auf dem AU-System verfügen, um die Acquisition Unit-Software (die das SecurityAdmin-Tool enthält) installieren zu können.
- Wenn Sie nicht-Admin-Benutzer haben, die anschließend auf das SecurityAdmin-Tool zugreifen müssen, müssen diese zur *cisys*-Gruppe hinzugefügt werden. Die *cisys*-Gruppe wird während der AU-Installation erstellt.

Nach der AU-Installation befindet sich das SecurityAdmin-Tool auf dem Erfassungseinheitssystem an einem der folgenden Standorte:

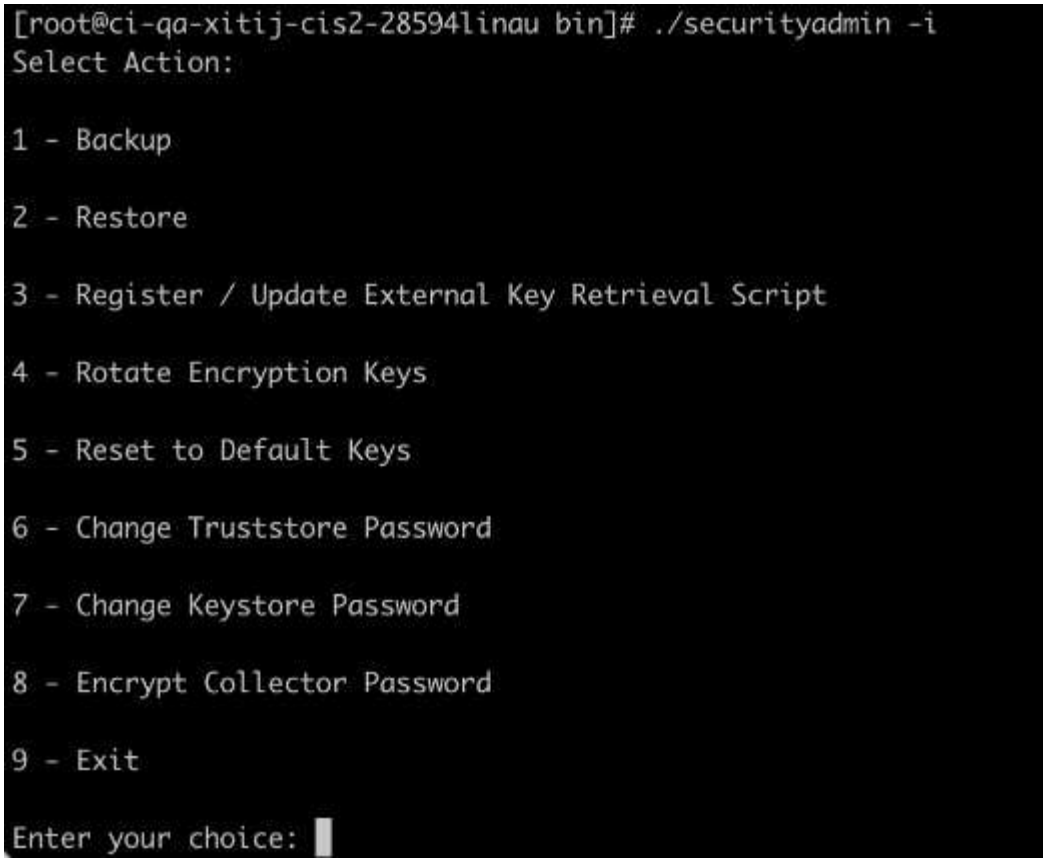
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Verwenden des SecurityAdmin-Tools

Starten Sie das SecurityAdmin-Tool im interaktiven Modus (-i).

> Es wird empfohlen, das SecurityAdmin-Tool im interaktiven Modus zu verwenden, um das Übergeben von Geheimnissen in der Befehlszeile zu vermeiden, die in Protokollen erfasst werden können.

Folgende Optionen werden angezeigt:



1. **Backup**

   Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

   ```
   Windows - C:\Program Files\SANscreen\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Es wird empfohlen, Vault-Backups sicher zu halten, da sie vertrauliche Informationen enthalten.

2. **Wiederherstellen**

   Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

   Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel mit den folgenden Schritten: 1) Ändern der Verschlüsselungsschlüssel auf der AU. 2) Erstellen Sie eine Sicherung des Tresors. 3) Stellen Sie die Vault-Sicherung auf jedem der aus wieder her.

3. **Skript Zum Abrufen Des Externen Schlüssels Registrieren/Aktualisieren**

   Verwenden Sie ein externes Skript, um die AU-Verschlüsselungsschlüssel zu registrieren oder zu ändern, die zum Verschlüsseln oder Entschlüsseln von Gerätekennwörtern verwendet werden.

   Wenn Sie Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

Beachten Sie, dass diese Option nur unter Linux verfügbar ist.

Wenn Sie Ihr eigenes Schlüsselabruf-Skript mit dem SecurityAdmin-Tool verwenden, beachten Sie Folgendes:

- Der aktuell unterstützte Algorithmus ist RSA mit mindestens 2048 Bit.
- Das Skript muss die privaten und öffentlichen Schlüssel im Klartext zurückgeben. Das Skript darf keine verschlüsselten privaten und öffentlichen Schlüssel zurückgeben.
- Das Skript sollte rohe, codierte Inhalte zurückgeben (nur PEM-Format).
- Das externe Skript muss über *execute* Berechtigungen verfügen.

4. **Verschlüsselungstasten Drehen**

   Drehen Sie die Verschlüsselungsschlüssel (heben Sie die Registrierung der aktuellen Schlüssel auf und registrieren Sie neue Schlüssel). Um einen Schlüssel aus einem externen Schlüsselverwaltungssystem zu verwenden, müssen Sie die ID des öffentlichen Schlüssels und die ID des privaten Schlüssels angeben.

5. **Auf Standardschlüssel zurücksetzen**

   Setzt das Erfassungs-Benutzerpasswort und die Erfassungs-Benutzerverschlüsselungsschlüssel auf die Standardwerte zurück. Bei der Installation werden die Standardwerte angegeben.

6. **Passwort Des Truststore Ändern**

   Ändern Sie das Passwort des Truststore.

7. **Passwort Des Keystore Ändern**

   Ändern Sie das Passwort des Keystore.

8. **Passwort Des Verschlüsselten Collectors**

   Kennwort für den Datensammler verschlüsseln.

9. **Ausgang**

   Beenden Sie das SecurityAdmin-Tool.

Wählen Sie die Option, die Sie konfigurieren möchten, und befolgen Sie die Anweisungen.

Festlegen eines Benutzers, der das Tool ausführen soll

Wenn Sie sich in einer kontrollierten, sicherheitsbewussten Umgebung befinden, verfügen Sie möglicherweise nicht über die *cisys*-Gruppe, möchten aber möglicherweise, dass bestimmte Benutzer das SecurityAdmin-Tool ausführen.

Sie können dies erreichen, indem Sie die AU-Software manuell installieren und den Benutzer/die Gruppe angeben, für den Sie Zugriff haben möchten.

- Laden Sie den CI Installer mithilfe der API auf das AU-System herunter, und entpacken Sie ihn.
  - Sie benötigen ein einmaliger Autorisierungstoken. Siehe API Swagger Dokumentation (*Admin > API Access* und wählen Sie den Link *API Documentation*) und finden Sie den Abschnitt *GET /au/oneTimeToken* API.

    - Sobald Sie das Token haben, verwenden Sie die *GET /au/Installers/{Platform}/{Version}* API, um die Installer-Datei herunterzuladen. Sie müssen sowohl die Plattform (Linux oder Windows) als auch die Installer-Version bereitstellen.
- Kopieren Sie die heruntergeladene Installationsdatei auf das AU-System, und entpacken Sie sie.
- Navigieren Sie zu dem Ordner, der die Dateien enthält, und führen Sie das Installationsprogramm als root aus. Geben Sie dabei den Benutzer und die Gruppe an:

```
./cloudinsights-install.sh <User> <Group>
```

Wenn der angegebene Benutzer und/oder die angegebene Gruppe nicht vorhanden ist, werden diese erstellt. Der Benutzer hat Zugriff auf das SecurityAdmin-Tool.

Proxy wird aktualisiert oder entfernt

Mit dem SecurityAdmin-Tool können Proxy-Informationen für die Acquisition Unit festgelegt oder entfernt werden, indem das Tool mit dem Parameter *-PR* ausgeführt wird:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Um den Proxy beispielsweise zu entfernen, führen Sie folgenden Befehl aus:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Sie müssen die Erfassungseinheit neu starten, nachdem Sie den Befehl
ausgeführt haben.
```

Um einen Proxy zu aktualisieren, lautet der Befehl

```
./securityadmin -pr -upr <arg>
```

Externer Schlüsselabruf

Wenn Sie ein UNIX-Shell-Skript bereitstellen, kann es von der Erfassungseinheit ausgeführt werden, um den **privaten Schlüssel** und den **öffentlichen Schlüssel** von Ihrem Schlüsselverwaltungssystem abzurufen.

Um den Schlüssel abzurufen, führt Data Infrastructure Insights das Skript aus und gibt zwei Parameter an: *Key id* und *key type*. *Key id* kann verwendet werden, um den Schlüssel in Ihrem Key Management System zu identifizieren. *Schlüsseltyp* ist entweder "öffentlich" oder "privat". Wenn der Schlüsseltyp „public“ ist, muss das Skript den öffentlichen Schlüssel zurückgeben. Wenn der Schlüsseltyp „privat“ ist, muss der private Schlüssel zurückgegeben werden.

Um den Schlüssel an die Erfassungseinheit zurücksenden zu können, muss das Skript den Schlüssel auf die Standardausgabe drucken. Das Skript muss *only* den Schlüssel zur Standardausgabe drucken; kein anderer Text muss in der Standardausgabe gedruckt werden. Sobald der angeforderte Schlüssel in die Standardausgabe gedruckt wurde, muss das Skript mit einem Exit-Code von 0 beendet werden. Jeder andere Rückgabewert wird als Fehler angesehen.

Das Skript muss mit der Erfassungseinheit mit dem SecurityAdmin-Tool registriert werden, das das Skript zusammen mit der Erfassungseinheit ausführt. Das Skript muss über *read* und *execute* Berechtigungen für den Root- und „cisys“-Benutzer verfügen. Wenn das Shell-Skript nach der Registrierung geändert wird, muss das geänderte Shell-Skript erneut bei der Erfassungseinheit registriert werden.

Eingabeparameter: Schlüssel-id	Schlüsselkennung zur Identifizierung des Schlüssels im Verschlüsselungsmanagement-System des Kunden
Eingabeparameter: Schlüsseltyp	Public oder Private Cloud.
Ausgang	Die angeforderte Taste muss in der Standardausgabe ausgedruckt werden. 2048-Bit RSA-Schlüssel wird derzeit unterstützt. Schlüssel müssen im folgenden Format kodiert und gedruckt werden - privates Schlüsselformat - PEM, DER-encoded PKCS8 PrivateKeyInfo RFC 5958 public key Format - PEM, DER-encoded X.509 SubjectPublicKeyInfo RFC 5280
Exit-Code	Der Exit-Code von Null wird erfolgreich ausgeführt. Alle anderen Exit-Werte gelten als fehlgeschlagen.
Skriptberechtigungen	Das Skript muss über Lese- und Ausführungsberechtigungen für den Root- und „cisys“-Benutzer verfügen.
Protokolle	Skriptausführungen werden protokolliert. Protokolle finden Sie unter - /var/log/NetApp/cloudinsights/securityadmin/securityadmin.log /var/log/NetApp/cloudinsights/acq/acq.log

Verschlüsseln eines Kennworts für die Verwendung in API

Mit Option 8 können Sie ein Passwort verschlüsseln, das Sie dann per API an einen Datensammler weiterleiten können.

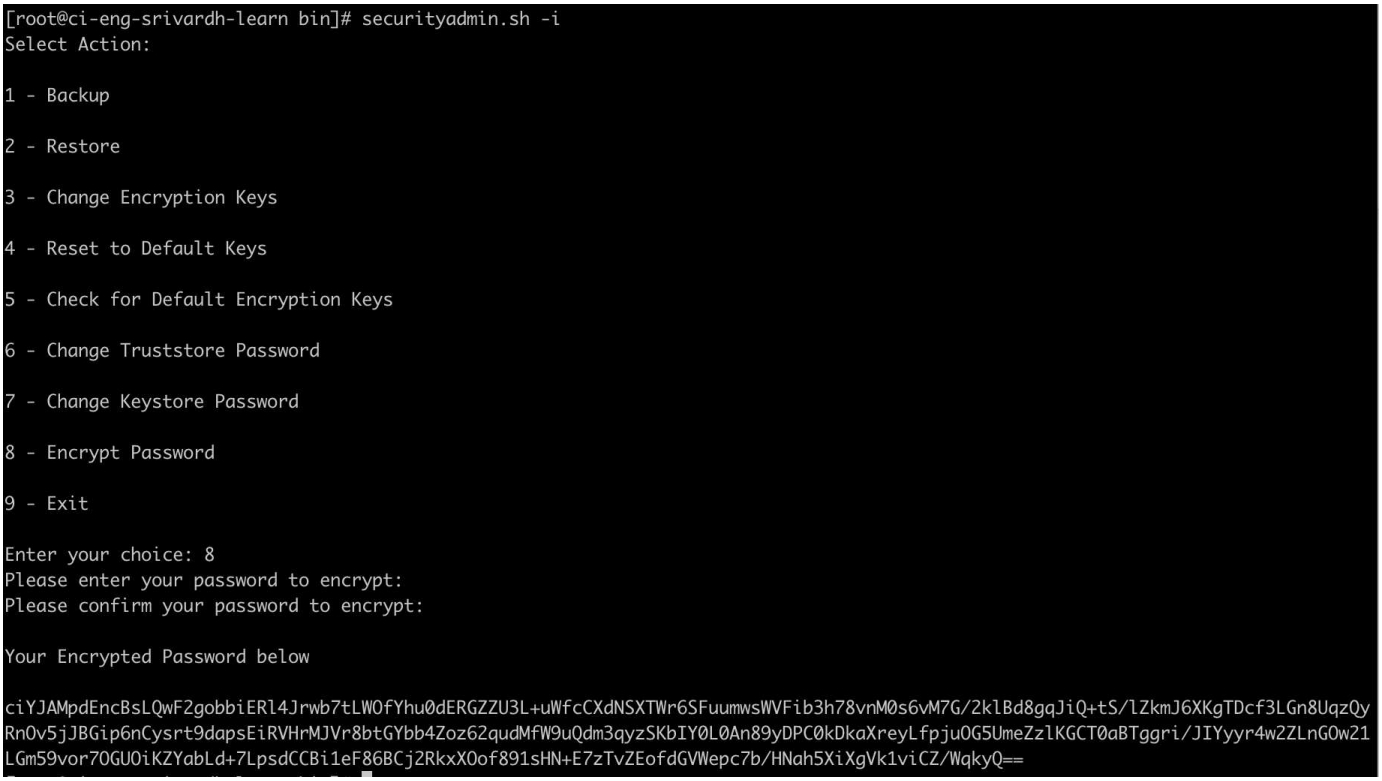
Starten Sie das SecurityAdmin-Tool im interaktiven Modus und wählen Sie Option 8: *Encrypt Password*.

```
 securityadmin.sh -i
Sie werden aufgefordert, das Kennwort einzugeben, das Sie verschlüsseln
möchten. Beachten Sie, dass die von Ihnen eingegebenen Zeichen nicht auf
dem Bildschirm angezeigt werden. Geben Sie das Passwort erneut ein, wenn
Sie dazu aufgefordert werden.
```

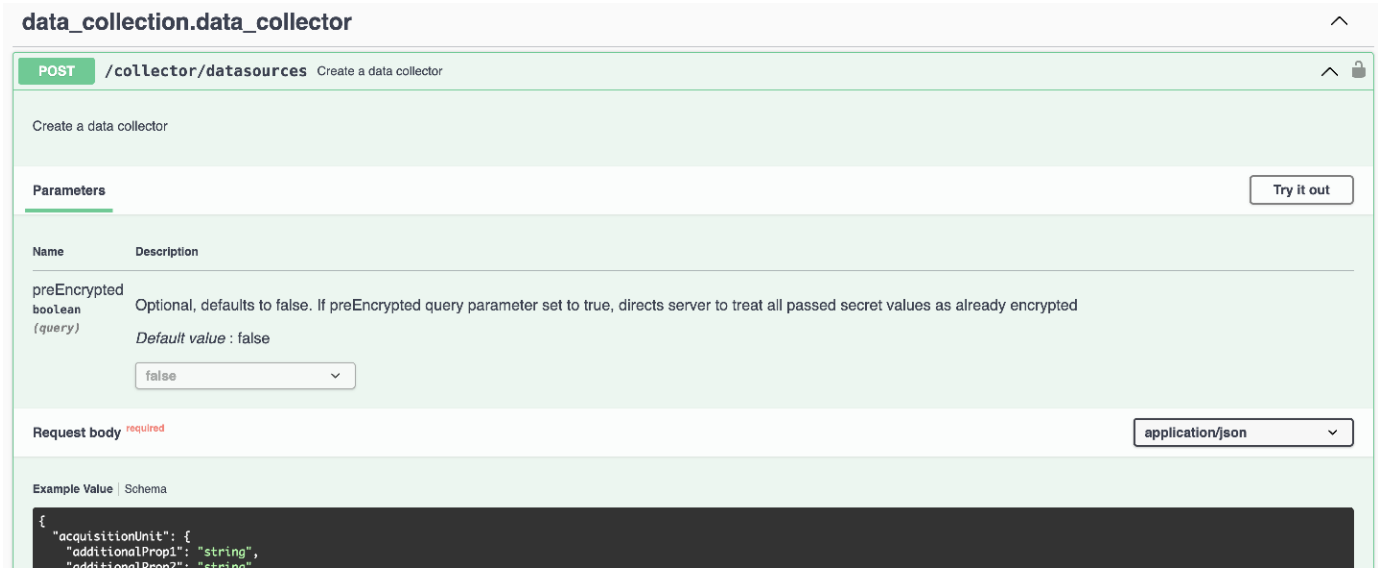
Wenn Sie den Befehl in einem Skript verwenden, verwenden Sie alternativ auf einer Befehlszeile *securityadmin.sh* mit dem Parameter "-enc" und geben Ihr unverschlüsseltes Passwort ein:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Beispiel für CLI"]
```

Das verschlüsselte Passwort wird auf dem Bildschirm angezeigt. Kopieren Sie die gesamte Zeichenfolge einschließlich aller führenden oder nachgestellten Symbole.



Um das verschlüsselte Passwort an einen Datensammler zu senden, können Sie die Data Collection API verwenden. Der Swagger für diese API ist unter **Admin > API Access** zu finden und auf den Link "API Documentation" zu klicken. Wählen Sie den API-Typ „Data Collection“ aus. Wählen Sie unter der Überschrift *Data_Collection.Data_Collector* die API */Collector/Datasources* POST für dieses Beispiel aus.



Wenn Sie die Option *preEncrypted* auf *true* setzen, wird jedes Passwort, das Sie über den API-Befehl übergeben, als **bereits verschlüsselt** behandelt; die API verschlüsselt das/die Passwort(e) nicht neu. Wenn Sie Ihre API erstellen, fügen Sie einfach das zuvor verschlüsselte Passwort an der entsprechenden Stelle ein.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```