Sicherheit

Data Infrastructure Insights

NetApp
February 03, 2026

Inhalt

Sicherheit

Data Infrastructure Insights Sicherheit

Die Sicherheit von Produkt- und Kundendaten hat bei NetApp höchste Bedeutung. Data Infrastructure Insights befolgt während des gesamten Release-Lebenszyklus bewährte Sicherheitspraktiken, um sicherzustellen, dass Kundeninformationen und -daten bestmöglich geschützt sind.

Sicherheitsübersicht

Physische Sicherheit

Die Produktionsinfrastruktur von Data Infrastructure Insights wird in Amazon Web Services (AWS) gehostet. Physische und umweltbezogene sicherheitsrelevante Kontrollen für Data Infrastructure Insights Produktionsserver, zu denen Gebäude sowie an Türen verwendete Schlösser oder Schlüssel gehören, werden von AWS verwaltet. Laut AWS: „Der physische Zugang wird sowohl am Perimeter als auch an den Gebäudeeingängen von professionellem Sicherheitspersonal mithilfe von Videoüberwachung, Einbruchmeldeanlagen und anderen elektronischen Mitteln kontrolliert. Autorisierte Mitarbeiter nutzen Multi-Faktor-Authentifizierungsmechanismen, um auf die Etagen des Rechenzentrums zuzugreifen.“

Data Infrastructure Insights folgt den Best Practices der"Modell der geteilten Verantwortung" von AWS beschrieben.

Produktsicherheit

Data Infrastructure Insights folgt einem Entwicklungslebenszyklus im Einklang mit Agile-Prinzipien und ermöglicht uns so, sicherheitsrelevante Softwarefehler schneller zu beheben als bei Entwicklungsmethoden mit längeren Release-Zyklen. Durch den Einsatz kontinuierlicher Integrationsmethoden sind wir in der Lage, schnell auf funktionale und sicherheitsrelevante Änderungen zu reagieren. Die Verfahren und Richtlinien zum Änderungsmanagement definieren, wann und wie Änderungen erfolgen, und tragen dazu bei, die Stabilität der Produktionsumgebung aufrechtzuerhalten. Alle Änderungen mit Auswirkungen werden vor ihrer Veröffentlichung in der Produktionsumgebung formell kommuniziert, koordiniert, ordnungsgemäß überprüft und genehmigt.

Netzwerksicherheit

Der Netzwerkzugriff auf Ressourcen in der Data Infrastructure Insights Umgebung wird durch hostbasierte Firewalls gesteuert. Jede Ressource (z. B. ein Load Balancer oder eine Instanz einer virtuellen Maschine) verfügt über eine hostbasierte Firewall, die den eingehenden Datenverkehr auf die Ports beschränkt, die die Ressource zur Ausführung ihrer Funktion benötigt.

Data Infrastructure Insights verwendet verschiedene Mechanismen, darunter Intrusion Detection-Dienste, um die Produktionsumgebung auf Sicherheitsanomalien zu überwachen.

Risikobewertung

Das Data Infrastructure Insights -Team folgt einem formalisierten Risikobewertungsprozess, um eine systematische, wiederholbare Möglichkeit zur Identifizierung und Bewertung der Risiken bereitzustellen, sodass diese mithilfe eines Risikobehandlungsplans angemessen gemanagt werden können.

Datenschutz

Die Produktionsumgebung von Data Infrastructure Insights ist in einer hochredundanten Infrastruktur eingerichtet, die mehrere Verfügbarkeitszonen für alle Dienste und Komponenten nutzt. Neben der Nutzung einer hochverfügbaren und redundanten Computerinfrastruktur werden kritische Daten in regelmäßigen Abständen gesichert und Wiederherstellungen regelmäßig getestet. Formale Backup-Richtlinien und -Verfahren minimieren die Auswirkungen von Unterbrechungen der Geschäftstätigkeit, schützen Geschäftsprozesse vor den Auswirkungen von Ausfällen von Informationssystemen oder Katastrophen und gewährleisten ihre rechtzeitige und angemessene Wiederaufnahme.

Authentifizierung und Zugriffsverwaltung

Der gesamte Kundenzugriff auf Data Infrastructure Insights erfolgt über Browser-UI-Interaktionen über https. Die Authentifizierung erfolgt über den Drittanbieterdienst Auth0. NetApp hat dies als Authentifizierungsebene für alle Cloud-Datendienste zentralisiert.

Data Infrastructure Insights befolgt branchenübliche Best Practices, darunter „Least Privilege“ und „rollenbasierte Zugriffskontrolle“ für den logischen Zugriff auf die Data Infrastructure Insights -Produktionsumgebung. Der Zugriff wird streng nach Bedarf kontrolliert und nur ausgewählten autorisierten Mitarbeitern mithilfe von Multi-Faktor-Authentifizierungsmechanismen gewährt.

Erhebung und Schutz von Kundendaten

Alle Kundendaten werden während der Übertragung über öffentliche Netzwerke und im Ruhezustand verschlüsselt. Data Infrastructure Insights nutzt an verschiedenen Stellen im System Verschlüsselung, um Kundendaten mithilfe von Technologien wie Transport Layer Security (TLS) und dem Industriestandard-Algorithmus AES-256 zu schützen.

Kunden-Deprovisionierung

In unterschiedlichen Abständen werden E-Mail-Benachrichtigungen versendet, um den Kunden über den Ablauf seines Abonnements zu informieren. Nach Ablauf des Abonnements wird die Benutzeroberfläche eingeschränkt und es beginnt eine Schonfrist für die Datenerfassung. Der Kunde wird anschließend per E-Mail benachrichtigt. Für Testabonnements gilt eine Nachfrist von 14 Tagen und für kostenpflichtige Abonnementkonten eine Nachfrist von 28 Tagen. Nach Ablauf der Nachfrist wird der Kunde per E-Mail darüber informiert, dass das Konto in 2 Tagen gelöscht wird. Ein zahlender Kunde kann auch direkt die Abmeldung vom Dienst beantragen.

Abgelaufene Mandanten und alle zugehörigen Kundendaten werden vom Data Infrastructure Insights Operations (SRE)-Team am Ende der Nachfrist oder nach Bestätigung der Anfrage eines Kunden zur Kündigung seines Kontos 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 des Kunden wird durch Aufrufen derselben API und Überprüfen, ob der Mandantenstatus des Kunden „GELÖSCHT“ lautet, überprüft.

Sicherheitsvorfallmanagement

Data Infrastructure 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 bezieht Informationen zu Sicherheitslücken aus mehreren Kanälen, darunter Kundenberichte, interne Entwicklungsabteilungen und allgemein anerkannte Quellen wie die CVE-Datenbank.

Wenn das Data Infrastructure Insights Engineering-Team ein Problem erkennt, leitet das Team den PSIRT-Prozess ein, bewertet das Problem und behebt es möglicherweise.

Es ist auch möglich, dass ein Kunde oder Forscher von Data Infrastructure Insights ein Sicherheitsproblem mit dem Data Infrastructure Insights -Produkt erkennt und das Problem dem technischen Support oder direkt dem Incident Response Team von NetApp meldet. In diesen Fällen leitet das Data Infrastructure Insights -Team den PSIRT-Prozess ein, bewertet das Problem und behebt es möglicherweise.

Schwachstellen- und Penetrationstests

Data Infrastructure Insights befolgt die Best Practices der Branche und führt regelmäßig Schwachstellen- und Penetrationstests mithilfe interner und externer Sicherheitsexperten und -unternehmen durch.

Schulung zum Sicherheitsbewusstsein

Alle Mitarbeiter von Data Infrastructure Insights absolvieren ein Sicherheitstraining, das auf die jeweilige Rolle zugeschnitten ist, um sicherzustellen, dass jeder Mitarbeiter für die spezifischen sicherheitsbezogenen Herausforderungen seiner Rolle gerüstet ist.

Einhaltung

Data Infrastructure Insights führt unabhängige Audits und Validierungen seiner Sicherheit, Prozesse und Dienste durch externe lizenzierte CPA-Unternehmen durch, einschließlich der Durchführung des SOC 2-Audits.

NetApp Sicherheitshinweise

Sie können die verfügbaren Sicherheitshinweise von NetApp einsehen"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 speichert Data Infrastructure Insights ?

Data Infrastructure Insights speichert die folgenden Informationen:

- Leistungsdaten

  Leistungsdaten sind Zeitreihendaten, die Informationen über die Leistung des überwachten Geräts/der überwachten Quelle liefern. Hierzu zählen beispielsweise die Anzahl der von einem Speichersystem bereitgestellten E/A-Vorgänge, der Durchsatz eines FibreChannel-Ports, die Anzahl der von einem Webserver bereitgestellten Seiten, die Antwortzeit einer Datenbank und mehr.

- Bestandsdaten

  Inventardaten bestehen aus Metadaten, die das überwachte Gerät/die überwachte Quelle und deren Konfiguration beschreiben. Hierzu gehören beispielsweise installierte Hardware- und Softwareversionen, Festplatten und LUNs in einem Speichersystem, CPU-Kerne, RAM und Festplatten einer virtuellen Maschine, die Tablespaces einer Datenbank, die Anzahl und Art der Ports auf einem SAN-Switch, Verzeichnis-/Dateinamen (wenn Storage Workload Security aktiviert ist) usw.

- Konfigurationsdaten

  Dies fasst die vom Kunden bereitgestellten Konfigurationsdaten zusammen, die zur Verwaltung des Kundenbestands und der Vorgänge verwendet werden, z. B. Hostnamen oder IP-Adressen der

überwachten Geräte, Abfrageintervalle, Timeout-Werte usw.

- Geheimnisse

  Geheimnisse bestehen aus den Anmeldeinformationen, die von der Data Infrastructure Insights Acquisition Unit für den Zugriff auf Kundengeräte und -dienste verwendet werden. Diese Anmeldeinformationen werden mithilfe einer starken asymmetrischen Verschlüsselung verschlüsselt und die privaten Schlüssel werden nur auf den Erfassungseinheiten gespeichert und verlassen nie die Kundenumgebung. Aufgrund dieses Designs können selbst privilegierte Data Infrastructure Insights SREs nicht auf Kundengeheimnisse im Klartext zugreifen.

- Funktionale Daten

  Dabei handelt es sich um Daten, die durch die Bereitstellung des Cloud Data Service durch NetApp generiert werden und die NetApp bei der Entwicklung, Bereitstellung, dem Betrieb, der Wartung und der Sicherung des Cloud Data Service unterstützen. Funktionale Daten enthalten keine Kundeninformationen oder personenbezogenen Daten.

- Benutzerzugriffsdaten

  Authentifizierungs- und Zugriffsinformationen, die es der NetApp Console ermöglichen, mit regionalen Data Infrastructure Insights -Sites zu kommunizieren, einschließlich Daten zur Benutzerautorisierung.

- Speicher-Workload-Sicherheit Benutzerverzeichnisdaten

  In Fällen, in denen die Workload-Sicherheitsfunktion aktiviert ist UND der Kunde den Benutzerverzeichnis-Collector aktiviert, speichert das System Benutzeranzeigenamen, Unternehmens-E-Mail-Adressen und andere aus Active Directory gesammelte Informationen.

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

Es werden **keine expliziten personenbezogenen Daten** aus Infrastruktur- und Serviceressourcen erhoben. Die gesammelten Informationen bestehen nur aus Leistungsmesswerten, Konfigurationsinformationen und Infrastrukturmetadaten, ähnlich wie bei vielen Anbietern von Phone-Homes, einschließlich NetApp Auto-Support und ActiveIQ. Abhängig von den Namenskonventionen eines Kunden können Daten für Freigaben, Volumes, VMs, Qtrees, Anwendungen usw. jedoch personenbezogene Daten enthalten.

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

Darüber hinaus werden Zugriffsprotokolle für Data Infrastructure Insights geführt, die die IP- und E-Mail-Adressen der Benutzer enthalten, die sie zum Anmelden beim Dienst verwendet haben.

Wo werden meine Informationen gespeichert?

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

Die folgenden Informationen werden in der Hostregion gespeichert:

- Telemetrie- und Asset-/Objektinformationen, einschließlich Zähler und Leistungsmetriken
- Informationen zur Erfassungseinheit
- Funktionale Daten
- Prüfinformationen zu Benutzeraktivitäten in Data Infrastructure Insights
- Informationen zur Workload-Sicherheit in Active Directory
- Informationen zum Workload-Sicherheitsaudit

Die folgenden Informationen befinden sich in den Vereinigten Staaten, unabhängig von der Region, in der Ihre Data Infrastructure Insights Umgebung gehostet wird:

- Informationen zur Umgebungssite (manchmal auch „Mandant“ genannt), z. B. Site-/Kontoinhaber.
- Informationen, die es der NetApp Console ermöglichen, mit regionalen Data Infrastructure Insights -Sites zu kommunizieren, einschließlich aller Informationen, die mit der Benutzerautorisierung zu tun haben.
- Informationen zur Beziehung zwischen dem Data Infrastructure Insights Benutzer und dem Mandanten.

Gastgeberregionen

Zu den Gastgeberregionen gehören:

- USA: us-east-1
- EMEA: eu-central-1
- APAC: ap-southeast-2

Weitere Informationen

Weitere Informationen zum Datenschutz und zur Sicherheit von NetApp finden Sie unter den folgenden Links:

- "Vertrauenszentrum"
- "Grenzüberschreitende Datenübertragungen"
- "Verbindliche Unternehmensregeln"
- "Antworten auf Datenanfragen von Drittanbietern"
- "NetApp Datenschutzgrundsätze"

SecurityAdmin-Tool

Data Infrastructure Insights umfasst Sicherheitsfunktionen, die einen Betrieb Ihrer Umgebung mit erhöhter Sicherheit ermöglichen. Zu den Funktionen gehören Verbesserungen bei der Verschlüsselung, beim Passwort-Hashing und die Möglichkeit, interne Benutzerpasswörter sowie Schlüsselpaare zum Ver- und Entschlüsseln von Passwörtern zu ändern.

Zum Schutz vertraulicher Daten empfiehlt NetApp , die Standardschlüssel und das *Acquisition* -Benutzerkennwort nach einer Installation oder einem Upgrade zu ändern.

Verschlüsselte Passwörter von Datenquellen werden in Data Infrastructure Insights gespeichert. Dabei wird ein öffentlicher Schlüssel zum Verschlüsseln von Passwörtern verwendet, wenn ein Benutzer sie auf einer Konfigurationsseite eines Datensammlers eingibt. Data Infrastructure Insights verfügt nicht über die privaten

Schlüssel, die zum Entschlüsseln der Kennwörter des Datensammlers erforderlich sind. Nur Acquisition Units (AUs) verfügen über den privaten Schlüssel des Datensammlers, der zum Entschlüsseln der Kennwörter des Datensammlers erforderlich ist.

Überlegungen zu Upgrades und Installationen

Wenn Ihr Insight-System nicht standardmäßige Sicherheitskonfigurationen enthält (d. h. Sie haben Passwörter neu verschlüsselt), müssen Sie Ihre Sicherheitskonfigurationen sichern. Durch die Installation neuer Software oder in einigen Fällen durch ein Software-Upgrade wird Ihr System auf die Standardsicherheitskonfiguration zurückgesetzt. Wenn Ihr System zur Standardkonfiguration zurückkehrt, müssen Sie die nicht standardmäßige Konfiguration wiederherstellen, damit das System ordnungsgemäß funktioniert.

Verwalten der Sicherheit auf der Erfassungseinheit

Mit dem Tool SecurityAdmin können Sie Sicherheitsoptionen für Data Infrastructure Insights verwalten. Es wird auf dem System der Erfassungseinheit ausgeführt. Zur Sicherheitsverwaltung gehört die Verwaltung von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen der von Ihnen erstellten Sicherheitskonfigurationen oder das Zurücksetzen der Konfigurationen auf die Standardeinstellungen.

Bevor Sie beginnen

- Sie müssen über Administratorrechte auf dem AU-System verfügen, um die Acquisition Unit-Software (einschließlich des SecurityAdmin-Tools) zu installieren.
- Wenn Sie Benutzer ohne Administratorrechte haben, die später auf das SecurityAdmin-Tool zugreifen müssen, müssen diese der Gruppe *cisys* hinzugefügt werden. Die Gruppe *cisys* wird während der AU-Installation erstellt.

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

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\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 die Weitergabe von Geheimnissen über die Befehlszeile zu vermeiden, die in Protokollen erfasst werden können.

Die folgenden Optionen werden angezeigt:

[Optionen für das SecurityAdmin-Tool (Linux)]

1. **Sicherung**

   Erstellt eine ZIP-Sicherungsdatei des Tresors mit allen Passwörtern und Schlüsseln und speichert die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardspeicherorten:

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\backup\vault
Linux - /var/log/netapp/oci/backup/vault
```

Es wird empfohlen, Tresor-Backups sicher aufzubewahren, da sie vertrauliche Informationen enthalten.

2. **Wiederherstellen**

   Stellt die erstellte ZIP-Sicherung des Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel auf die Werte zurückgesetzt, die zum Zeitpunkt der Sicherungserstellung gültig waren.

   Mit „Wiederherstellen“ können Sie Passwörter und Schlüssel auf mehreren Servern synchronisieren, beispielsweise mit diesen Schritten: 1) Ändern Sie die Verschlüsselungsschlüssel auf der AU. 2) Erstellen Sie eine Sicherungskopie des Tresors. 3) Stellen Sie die Tresorsicherung auf jeder der AUs wieder her.

3. **Skript zum Abrufen externer Schlüssel 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 Schlüsselabrufskript mit dem SecurityAdmin-Tool verwenden, beachten Sie Folgendes:

   - Der derzeit unterstützte Algorithmus ist RSA mit mindestens 2048 Bit.
   - Das Skript muss den privaten und öffentlichen Schlüssel im Klartext zurückgeben. Das Skript darf keine verschlüsselten privaten und öffentlichen Schlüssel zurückgeben.
   - Das Skript sollte unverarbeitete, codierte Inhalte zurückgeben (nur PEM-Format).
   - Das externe Skript muss über Ausführungsberechtigungen verfügen.

4. **Rotierende Verschlüsselungsschlüssel**

   Rotieren Sie Ihre Verschlüsselungsschlüssel (melden Sie aktuelle Schlüssel ab und registrieren Sie neue Schlüssel). Um einen Schlüssel aus einem externen Schlüsselverwaltungssystem zu verwenden, müssen Sie die öffentliche und die private Schlüssel-ID angeben.

5. **Auf Standardtasten zurücksetzen**

   Setzt das Kennwort und die Verschlüsselungsschlüssel des Erwerbsbenutzers auf die Standardwerte zurück. Die Standardwerte sind diejenigen, die während der Installation bereitgestellt werden.

6. **Truststore-Passwort ändern**

   Ändern Sie das Passwort des Truststores.

7. **Keystore-Passwort ändern**

Ändern Sie das Passwort des Schlüsselspeichers.

8. **Collector-Passwort verschlüsseln**

   Datensammlerkennwort verschlüsseln.

9. **Ausfahrt**

   Beenden Sie das SecurityAdmin-Tool.

Wählen Sie die Option, die Sie konfigurieren möchten, und folgen Sie den Anweisungen.

Festlegen eines Benutzers zum Ausführen des Tools

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

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

- Laden Sie mithilfe der API das CI-Installationsprogramm auf das AU-System herunter und entpacken Sie es.
  - Sie benötigen ein einmaliges Autorisierungstoken. Sehen Sie sich die API Swagger-Dokumentation an (*Admin > API-Zugriff* und wählen Sie den Link *API-Dokumentation*) und suchen Sie den API-Abschnitt *GET /au/oneTimeToken*.
  - Sobald Sie das Token haben, verwenden Sie die API *GET /au/installers/{platform}/{version}*, um die Installationsdatei herunterzuladen. Sie müssen die Plattform (Linux oder Windows) sowie die Installationsversion angeben.
- 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, wobei Sie den Benutzer und die Gruppe angeben:

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

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

Aktualisieren oder Entfernen des Proxys

Mit dem Tool SecurityAdmin können Sie Proxy-Informationen für die Erfassungseinheit festlegen oder entfernen, indem Sie das Tool mit dem Parameter *-pr* ausführen:

```
[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 beispielsweise den Proxy zu entfernen, führen Sie diesen Befehl aus:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Sie müssen die Erfassungseinheit nach der Ausführung des Befehls neu
starten.
```

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** aus Ihrem Schlüsselverwaltungssystem abzurufen.

Um den Schlüssel abzurufen, führt Data Infrastructure Insights das Skript aus und übergibt zwei Parameter: *Schlüssel-ID* und *Schlüsseltyp*. Mit der *Schlüssel-ID* können Sie den Schlüssel in Ihrem Schlüsselverwaltungssystem identifizieren. *Schlüsseltyp* ist entweder „öffentlich“ oder „privat“. Wenn der Schlüsseltyp „öffentlich“ 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 zurückzusenden, muss das Skript den Schlüssel in der Standardausgabe drucken. Das Skript darf *nur* den Schlüssel in die Standardausgabe drucken. Es darf kein anderer Text in die Standardausgabe gedruckt werden. Sobald der angeforderte Schlüssel in der Standardausgabe gedruckt wird, muss das Skript mit einem Exitcode von 0 beendet werden; jeder andere Rückgabecode wird als Fehler betrachtet.

Das Skript muss mithilfe des SecurityAdmin-Tools bei der Erfassungseinheit registriert werden, das das Skript zusammen mit der Erfassungseinheit ausführt. Das Skript muss über Lese- und Ausführungsberechtigungen 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, die zur Identifizierung des Schlüssels im Schlüsselverwaltungssystem des Kunden verwendet wird.
Eingabeparameter: Schlüsseltyp	öffentlich oder privat.
Ausgabe	Der angeforderte Schlüssel muss auf der Standardausgabe ausgegeben werden. Derzeit wird ein 2048-Bit-RSA-Schlüssel unterstützt. Schlüssel müssen im folgenden Format codiert und gedruckt werden: Privates Schlüsselformat – PEM, DER-codiert PKCS8 PrivateKeyInfo RFC 5958 Öffentliches Schlüsselformat – PEM, DER-codiert X.509 SubjectPublicKeyInfo RFC 5280
Exitcode	Bei Erfolg ist der Exitcode Null. Alle anderen Exit-Werte gelten als Fehlschlag.
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 Passworts zur Verwendung in der API

Option 8 ermöglicht Ihnen die Verschlüsselung eines Passworts, welches Sie dann per API an einen Datensammler weitergeben können.

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

```
 securityadmin.sh -i
Sie werden aufgefordert, das zu verschlüsselnde Kennwort einzugeben.
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 alternativ in einem Skript verwenden möchten, verwenden Sie in einer Befehlszeile *securityadmin.sh* mit dem Parameter „-enc“ und übergeben Sie Ihr unverschlüsseltes Kennwort:

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

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

[Interaktiver Modus, Passwort verschlüsseln, Breite=640]

Um das verschlüsselte Passwort an einen Datensammler zu senden, können Sie die Datensammlungs-API verwenden. Den Swagger für diese API finden Sie unter **Admin > API-Zugriff**. Klicken Sie auf den Link „API-Dokumentation“. Wählen Sie den API-Typ „Datenerfassung“ aus. Wählen Sie unter der Überschrift *data_collection.data_collector* die POST-API */collector/datasources* für dieses Beispiel aus.

[API zur Datenerfassung]

Wenn Sie die Option *preEncrypted* auf *True* setzen, wird jedes Kennwort, das Sie über den API-Befehl übergeben, als **bereits verschlüsselt** behandelt. Die API verschlüsselt das/die Kennwort(e) nicht erneut. Fügen Sie beim Erstellen Ihrer API einfach das zuvor verschlüsselte Passwort an der entsprechenden Stelle ein.

[API-Beispiel, Breite=600]