Sécurité

Data Infrastructure Insights

NetApp
January 17, 2025

Sommaire

Sécurité

Sécurité des informations exploitables de l'infrastructure de données

Chez NetApp, la sécurité des données des produits et des clients est au cœur de toute importance. Data Infrastructure Insights applique de bonnes pratiques de sécurité tout au long du cycle de vie des versions pour s'assurer que les informations et les données des clients bénéficient d'une sécurité optimale.

Présentation de la sécurité

Sécurité physique

L'infrastructure de production Data Infrastructure Insights est hébergée dans Amazon Web Services (AWS). Les contrôles de sécurité physiques et environnementaux des serveurs de production Data Infrastructure Insights, qui comprennent des bâtiments ainsi que des verrous ou des clés utilisés sur les portes, sont gérés par AWS. Conformément à AWS : « l'accès physique est contrôlé à la fois en périphérie et aux points d'entrée des bâtiments par du personnel de sécurité professionnel qui utilise la vidéosurveillance, les systèmes de détection d'intrusion et d'autres moyens électroniques. Le personnel autorisé utilise des mécanismes d'authentification multi-facteurs pour accéder aux sols des centres de données. »

Le service Data Infrastructure Insights respecte les bonnes pratiques de la "Modèle de responsabilité partagée" décrit par AWS.

Sécurité des produits

Data Infrastructure Insights suit un cycle de développement conforme aux principes agiles, ce qui nous permet de traiter plus rapidement tout défaut logiciel orienté sécurité, par rapport aux méthodologies de développement de cycle de lancement plus long. Grâce aux méthodologies d'intégration continue, nous sommes en mesure de répondre rapidement aux changements fonctionnels et de sécurité. Les procédures et les politiques de gestion du changement définissent le moment et la façon dont les changements se produisent et contribuent au maintien de la stabilité de l'environnement de production. Tout changement important est officiellement communiqué, coordonné, correctement examiné et approuvé avant leur libération dans l'environnement de production.

Sécurité réseau

L'accès réseau aux ressources dans l'environnement Data Infrastructure Insights est contrôlé par des pare-feu basés sur hôte. Chaque ressource (par exemple, un équilibreur de charge ou une instance de machine virtuelle) dispose d'un pare-feu basé sur l'hôte qui limite le trafic entrant aux ports nécessaires à cette ressource pour exécuter sa fonction.

Data Infrastructure Insights utilise divers mécanismes, notamment des services de détection des intrusions, pour surveiller l'environnement de production à la recherche d'anomalies de sécurité.

Évaluation des risques

L'équipe Data Infrastructure Insights suit un processus d'évaluation des risques formalisé afin de fournir un moyen systématique et reproductible d'identifier et d'évaluer les risques afin qu'ils puissent être gérés de manière appropriée par le biais d'un plan de traitement des risques.

Protection des données

L'environnement de production Data Infrastructure Insights est configuré dans une infrastructure hautement redondante utilisant plusieurs zones de disponibilité pour tous les services et composants. Outre l'utilisation d'une infrastructure de calcul extrêmement disponible et redondante, les données stratégiques sont sauvegardées à intervalles réguliers et les restaurations sont régulièrement testées. Des politiques et procédures de sauvegarde formelles minimisent l'impact des interruptions d'activités commerciales et protègent les processus de l'entreprise contre les défaillances des systèmes d'information ou des incidents et assurent leur reprise en temps voulu et adéquate.

Authentification et gestion des accès

Tout accès client à Data Infrastructure Insights se fait via des interactions de l'interface du navigateur via https. L'authentification s'effectue via le service tiers, Auth0. NetApp a centralisé cette démarche en tant que couche d'authentification pour l'ensemble des services de données cloud.

Data Infrastructure Insights suit de bonnes pratiques du secteur, notamment le « privilège minimal » et le « contrôle d'accès basé sur des rôles » concernant l'accès logique à l'environnement de production Data Infrastructure Insights. L'accès est contrôlé selon un besoin strict et ne peut être accordé que par du personnel autorisé grâce à des mécanismes d'authentification multifacteur.

Collecte et protection des données clients

Toutes les données des clients sont chiffrées en transit sur des réseaux publics et chiffrées au repos. Data Infrastructure Insights utilise le chiffrement à divers points du système pour protéger les données des clients à l'aide de technologies telles que TLS (transport Layer Security) et l'algorithme AES-256 standard.

Déprovisionnement du client

Des notifications par e-mail sont envoyées à divers intervalles pour informer le client que son abonnement arrive à expiration. Une fois l'abonnement expiré, l'interface utilisateur est limitée et la collecte des données commence. Le client est alors averti par e-mail. Les abonnements d'essai bénéficient d'une période de grâce de 14 jours et les comptes d'abonnement payant bénéficient d'un délai de grâce de 28 jours. Une fois le délai de grâce expiré, le client est averti par e-mail que le compte sera supprimé dans 2 jours. Un client payant peut également demander directement de ne pas bénéficier du service.

Les locataires arrivés à expiration et toutes les données client associées sont supprimés par l'équipe Data Infrastructure Insights Operations (SRE) à la fin du délai de grâce ou après confirmation de la demande de résiliation du compte d'un client. Dans les deux cas, l'équipe SRE effectue un appel d'API pour supprimer le compte. L'appel d'API supprime l'instance de tenant et toutes les données client. La suppression du client est vérifiée en appelant la même API et en vérifiant que le statut du locataire client est "SUPPRIMÉ".

Gestion des incidents de sécurité

Ces données sont intégrées au processus d'équipe d'intervention en cas d'incident de sécurité des produits (PSIRT) de NetApp afin de détecter, d'évaluer et de résoudre les vulnérabilités connues. PSIRT affiche les informations de vulnérabilité provenant de plusieurs canaux, notamment les rapports clients, l'ingénierie interne et des sources largement reconnues comme la base de données CVE.

Si un problème est détecté par l'équipe d'ingénierie Data Infrastructure Insights, l'équipe lance le processus PSIRT, évalue et peut éventuellement résoudre le problème.

Il est également possible qu'un client ou un chercheur Data Infrastructure Insights identifie un problème de sécurité avec le produit Data Infrastructure Insights et le signale au support technique ou directement à l'équipe de réponse aux incidents de NetApp. Dans ce cas, l'équipe Data Infrastructure Insights lancera le

processus PSIRT, évaluera le problème et pourra éventuellement le résoudre.

Tests de vulnérabilité et de pénétration

Data Infrastructure Insights applique les bonnes pratiques du secteur et procède régulièrement à des tests de vulnérabilité et d'intrusion auprès de professionnels et d'entreprises de sécurité internes et externes.

Formation à la sensibilisation à la sécurité

Tous les membres du personnel Data Infrastructure Insights suivent une formation sur la sécurité, développée pour chaque rôle, afin de s'assurer que chaque employé est équipé pour gérer les défis spécifiques liés à la sécurité de son poste.

La conformité

La solution Data Infrastructure Insights confie à une entreprise externe détenant une licence CPA la réalisation d'un audit et de validations tiers indépendants portant sur la sécurité, les processus et les services, notamment l'exécution de l'audit SOC 2.

Avis de sécurité NetApp

Vous pouvez afficher les conseils de sécurité disponibles "ici"deNetApp .

Information et région

NetApp prend très au sérieux la sécurité des informations client. Voici comment et où les informations relatives à l'infrastructure de données sont stockées.

Quelles sont les informations stockées par Data Infrastructure Insights ?

Data Infrastructure Insights stocke les informations suivantes :

- Les données de performance

  Les données de performances sont des données de séries chronologiques fournissant des informations sur les performances de l'appareil/source surveillé. Cela inclut, par exemple, le nombre d'E/S fournies par un système de stockage, le débit d'un port FiberChannel, le nombre de pages fournies par un serveur Web, le temps de réponse d'une base de données, etc.

- Données d'inventaire

  Les données d'inventaire se composent de métadonnées décrivant l'appareil/la source surveillé et la façon dont il est configuré. Cela inclut, par exemple, les versions matérielles et logicielles installées, les disques et les LUN d'un système de stockage, les cœurs de CPU, la RAM et les disques d'une machine virtuelle, les espaces de stockage d'une base de données, le nombre et le type de ports d'un commutateur SAN, les noms de répertoire/fichier (si la sécurité des charges de travail de stockage est activée), etc

- Données de configuration

  Cette section récapitule les données de configuration fournies par le client utilisées pour gérer l'inventaire et les opérations du client, par exemple les noms d'hôtes ou les adresses IP des périphériques surveillés, les intervalles d'interrogation, les valeurs de délai d'attente, etc

- Secrets

  Les secrets sont les références utilisées par l'unité d'acquisition Data Infrastructure Insights pour accéder aux appareils et services du client. Ces informations d'identification sont chiffrées à l'aide d'un cryptage asymétrique puissant, et les clés privées sont stockées uniquement sur les unités d'acquisition et ne quittent jamais l'environnement du client. Même les SRE Privileged Data Infrastructure Insights ne peuvent pas accéder aux secrets des clients en texte brut en raison de cette conception.

- Données fonctionnelles

  Il s'agit de données générées par NetApp avec le service de données cloud qui informe NetApp dans le développement, le déploiement, les opérations, la maintenance et la sécurisation du service de données cloud. Les données fonctionnelles ne contiennent pas d'informations client ou de données personnelles.

- Données d'accès utilisateur

  Informations d'authentification et d'accès permettant à NetApp BlueXP de communiquer avec les sites régionaux d'informations sur l'infrastructure de données, y compris les données relatives aux autorisations des utilisateurs.

- Données du répertoire utilisateur pour la sécurité des charges de travail de stockage

  Lorsque la fonctionnalité de sécurité de la charge de travail est activée ET que le client choisit d'activer le collecteur d'annuaire de l'utilisateur, le système stocke les noms d'affichage des utilisateurs, les adresses e-mail de l'entreprise et d'autres informations collectées à partir d'Active Directory.

> ⓘ Les données de répertoire d'utilisateurs font référence aux informations de répertoire d'utilisateurs collectées par le collecteur de données de l'annuaire d'utilisateurs Workload Security, et non aux données relatives aux utilisateurs de Data Infrastructure Insights/Workload Security eux-mêmes.

Aucune donnée personnelle explicite n'est recueillie dans les ressources de l'infrastructure et des services. Les informations collectées concernent uniquement les mesures de performance, les informations de configuration et les métadonnées de l'infrastructure, comme bon nombre de fournisseurs de téléphonie, y compris le support automatique NetApp et ActiveIQ. Toutefois, en fonction des conventions de nom utilisées par le client, les données pour les partages, les volumes, les machines virtuelles, les qtrees, les applications, etc., peuvent contenir des informations personnelles identifiables.

Si la sécurité des charges de travail est activée, le système examine en outre les noms de fichiers et de répertoires sur SMB ou d'autres partages, qui peuvent contenir des informations personnellement identifiables. Lorsque les clients activent le collecteur d'annuaire d'utilisateurs Workload Security (qui mappe essentiellement les SID Windows aux noms d'utilisateurs via Active Directory), le nom d'affichage, l'adresse e-mail d'entreprise et tous les attributs supplémentaires sélectionnés seront collectés et stockés par Data Infrastructure Insights.

En outre, les journaux d'accès à Data Infrastructure Insights sont conservés et contiennent les adresses IP et e-mail des utilisateurs utilisés pour se connecter au service.

Où mes informations sont-elles stockées ?

Les informations d'infrastructure de données stockent les informations en fonction de la région dans laquelle votre environnement est créé.

Les informations suivantes sont stockées dans la région hôte :

- Données de télémétrie et de ressources/objet, notamment compteurs et mesures de performances
- Informations sur l'unité d'acquisition
- Données fonctionnelles
- Informations d'audit sur les activités des utilisateurs dans Data Infrastructure Insights
- Informations Active Directory de sécurité des charges de travail
- Informations sur l'audit de sécurité de la charge de travail

Quelle que soit la région hébergeant votre environnement Data Infrastructure Insights, les informations suivantes résident aux États-Unis :

- Informations sur le site de l'environnement (parfois appelées « locataire »), telles que le site ou le propriétaire du compte.
- Informations permettant à NetApp BlueXP de communiquer avec les sites d'informations stratégiques régionaux sur l'infrastructure de données, y compris tout ce qui a à voir avec les autorisations des utilisateurs.
- Informations relatives à la relation entre l'utilisateur Data Infrastructure Insights et le locataire.

Régions hôtes

Les régions hôtes sont les suivantes :

- ÉTATS-Unis : US-est-1
- EMEA : Europe centrale 1
- APAC : ap-Sud-est-2

Plus d'informations

Pour en savoir plus sur la confidentialité et la sécurité de NetApp, consultez les liens suivants :

- "Centre de confiance"
- "Transferts de données hors des frontières"
- "Règles de société contraignantes"
- "Répondre aux demandes de données tierces"
- "Principes de confidentialité de NetApp"

Outil SecurityAdmin

Les informations d'infrastructure de données incluent des fonctionnalités de sécurité qui permettent à votre environnement de fonctionner avec une sécurité renforcée. Ces fonctionnalités comprennent des améliorations au cryptage, au hachage de mot de passe et à la possibilité de modifier les mots de passe des utilisateurs internes ainsi que les paires de clés qui chiffrent et décryptent les mots de passe.

Pour protéger les données sensibles, NetApp vous recommande de modifier les clés par défaut et le mot de passe utilisateur *acquisition* après une installation ou une mise à niveau.

Les mots de passe cryptés de la source de données sont stockés dans Data Infrastructure Insights, qui utilise

une clé publique pour chiffrer les mots de passe lorsqu'un utilisateur les saisit sur une page de configuration du collecteur de données. Data Infrastructure Insights ne dispose pas des clés privées requises pour décrypter les mots de passe du collecteur de données ; seules les unités d'acquisition (AUS) possèdent la clé privée du collecteur de données requise pour décrypter les mots de passe du collecteur de données.

Mise à niveau et installation

Si le système Insight contient des configurations de sécurité autres que celles par défaut (c'est-à-dire que vous avez des mots de passe avec clé de clés à clé), vous devez sauvegarder vos configurations de sécurité. L'installation de nouveaux logiciels ou, dans certains cas, la mise à niveau de logiciels restaure la configuration de sécurité par défaut de votre système. Lorsque votre système revient à la configuration par défaut, vous devez restaurer la configuration non par défaut pour que le système fonctionne correctement.

Gestion de la sécurité sur l'unité d'acquisition

L'outil SecurityAdmin vous permet de gérer les options de sécurité de Data Infrastructure Insights et est exécuté sur le système d'unités d'acquisition. La gestion de la sécurité inclut la gestion des clés et des mots de passe, l'enregistrement et la restauration des configurations de sécurité que vous créez ou restaurez aux paramètres par défaut.

Avant de commencer

- Vous devez disposer de privilèges d'administrateur sur le système au pour installer le logiciel de l'unité d'acquisition (qui inclut l'outil SecurityAdmin).
- Si vous avez des utilisateurs non-admin qui devront ensuite accéder à l'outil SecurityAdmin, ils doivent être ajoutés au groupe *cisys*. Le groupe *cisys* est créé lors de l'installation au.

Après l'installation de au, l'outil SecurityAdmin se trouve sur le système d'unités d'acquisition à l'un des emplacements suivants :

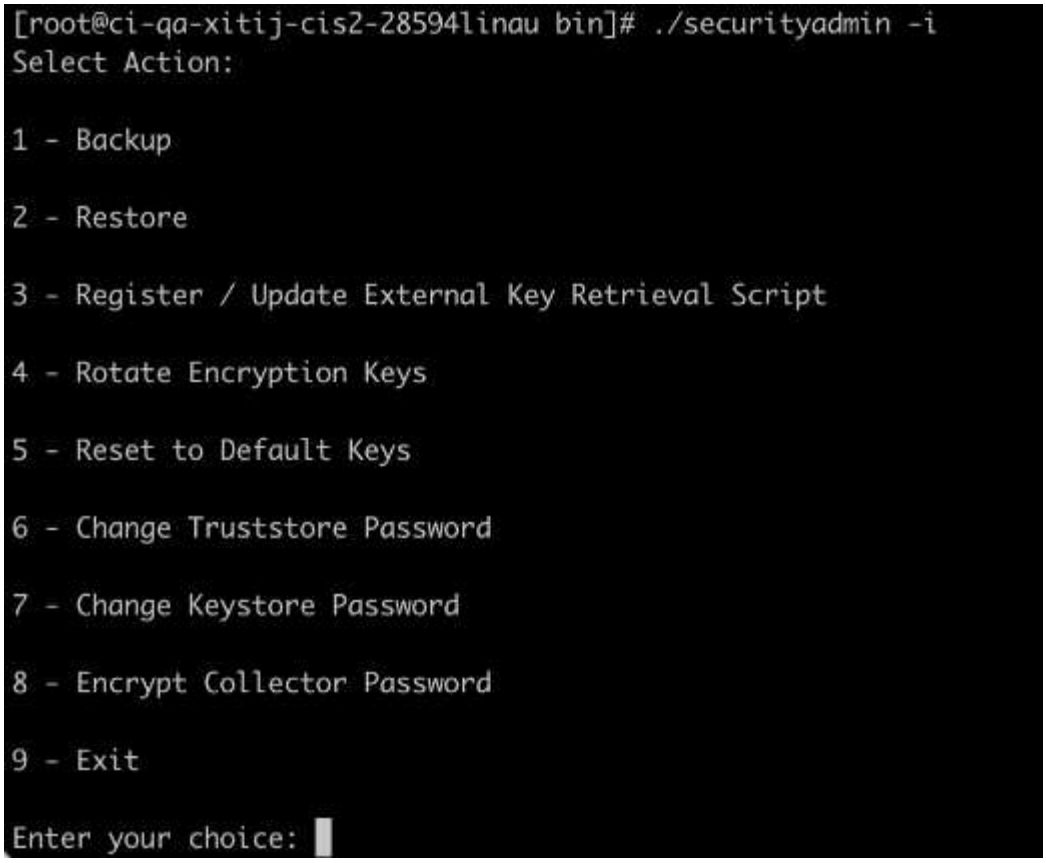
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Utilisation de l'outil SecurityAdmin

Démarrez l'outil SecurityAdmin en mode interactif (-i).

Il est recommandé d'utiliser l'outil SecurityAdmin en mode interactif, afin d'éviter de transmettre des secrets sur la ligne de commande, qui peuvent être capturés dans les journaux.

Les options suivantes sont affichées :



1. **Sauvegarde**

   Crée un fichier zip de sauvegarde du coffre-fort contenant tous les mots de passe et clés et place le fichier à un emplacement spécifié par l'utilisateur ou aux emplacements par défaut suivants :

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

   Il est recommandé de préserver la sécurité des sauvegardes de coffre-fort, car elles contiennent des informations sensibles.

2. **Restaurer**

   Restaure la sauvegarde zip du coffre-fort créé. Une fois restaurées, tous les mots de passe et clés sont rétablis dans les valeurs existantes au moment de la création de la sauvegarde.

   Restore peut être utilisé pour synchroniser les mots de passe et les clés sur plusieurs serveurs, par exemple en procédant comme suit : 1) modifiez les clés de cryptage sur l'au. 2) Créez une sauvegarde du coffre-fort. 3) restaurez la sauvegarde du coffre-fort sur chacun des États-Unis.

3. **Enregistrer / mettre à jour le script de récupération de clé externe**

   Utilisez un script externe pour enregistrer ou modifier les clés de cryptage au utilisées pour crypter ou décrypter les mots de passe du terminal.

   Lorsque vous modifiez des clés de cryptage, sauvegardez votre nouvelle configuration de sécurité afin de pouvoir la restaurer après une mise à niveau ou une installation.

Remarque cette option est uniquement disponible sous Linux.

Lorsque vous utilisez votre propre script de récupération de clé avec l'outil SecurityAdmin, gardez à l'esprit les points suivants :

- L'algorithme actuellement pris en charge est RSA avec un minimum de 2048 bits.
- Le script doit renvoyer les clés privées et publiques en texte brut. Le script ne doit pas renvoyer de clés publiques et privées cryptées.
- Le script doit renvoyer un contenu brut et codé (format PEM uniquement).
- Le script externe doit avoir des autorisations *execute*.

4. **Rotation des clés de cryptage**

   Faites pivoter vos clés de cryptage (désenregistre les clés actuelles et enregistre les nouvelles clés). Pour utiliser une clé d'un système de gestion externe des clés, vous devez spécifier l'ID de clé publique et l'ID de clé privée

5. **Réinitialiser les touches par défaut**

   Réinitialise le mot de passe de l'utilisateur d'acquisition et les clés de cryptage de l'utilisateur d'acquisition sur les valeurs par défaut. Les valeurs par défaut sont celles fournies lors de l'installation.

6. **Modifier le mot de passe de la banque de confiance**

   Modifiez le mot de passe du magasin de confiance.

7. **Changer le mot de passe de la base de stockage**

   Modifiez le mot de passe de la base de stockage de clés.

8. **Crypter le mot de passe du collecteur**

   Crypter le mot de passe du collecteur de données.

9. **Quitter**

   Quittez l'outil SecurityAdmin.

Choisissez l'option que vous souhaitez configurer et suivez les invites.

Spécification d'un utilisateur pour exécuter l'outil

Si vous vous trouvez dans un environnement contrôlé et soucieux de la sécurité, vous ne disposez peut-être pas du groupe *cisys* mais vous pouvez toujours demander à des utilisateurs spécifiques d'exécuter l'outil SecurityAdmin.

Pour ce faire, vous pouvez installer manuellement le logiciel au et spécifier l'utilisateur/le groupe auquel vous souhaitez accéder.

- À l'aide de l'API, téléchargez le programme d'installation d'EC sur le système au et décompressez-le.
  - Vous aurez besoin d'un jeton d'autorisation unique. Reportez-vous à la documentation API swagger (*Admin > API Access* et sélectionnez le lien *API Documentation*) et recherchez la section *GET /au/oneTimeToken* API.

    - Une fois que vous avez le jeton, utilisez l'API *GET /au/installateurs/{Platform}/{version}* pour télécharger le fichier d'installation. Vous devrez fournir une plate-forme (Linux ou Windows) ainsi qu'une version du programme d'installation.
- Copiez le fichier d'installation téléchargé sur le système au et décompressez-le.
- Accédez au dossier contenant les fichiers et exécutez le programme d'installation en tant que racine, en spécifiant l'utilisateur et le groupe :

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

Si l'utilisateur et/ou le groupe spécifié n'existe pas, ils seront créés. L'utilisateur aura accès à l'outil SecurityAdmin.

Mise à jour ou suppression du proxy

L'outil SecurityAdmin peut être utilisé pour définir ou supprimer des informations de proxy pour l'unité d'acquisition en exécutant l'outil avec le paramètre *-pr* :

```
[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.)
```

Par exemple, pour supprimer le proxy, exécutez la commande suivante :

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Vous devez redémarrer l'unité d'acquisition après avoir exécuté la
commande.
```

Pour mettre à jour un proxy, la commande est

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

Récupération de clé externe

Si vous fournissez un script shell UNIX, il peut être exécuté par l'unité d'acquisition pour récupérer la **clé privée** et la **clé publique** de votre système de gestion des clés.

Pour récupérer la clé, Data Infrastructure Insights exécute le script en passant deux paramètres : *Key ID* et *Key type*. *Key ID* peut être utilisé pour identifier la clé dans votre système de gestion des clés. *Key type* est "public" ou "privé". Lorsque le type de clé est « public », le script doit renvoyer la clé publique. Lorsque le type de clé est "privé", la clé privée doit être renvoyée.

Pour renvoyer la clé à l'unité d'acquisition, le script doit imprimer la clé sur la sortie standard. Le script doit imprimer *uniquement* la clé de la sortie standard ; aucun autre texte ne doit être imprimé sur la sortie standard. Une fois la clé demandée imprimée sur la sortie standard, le script doit se fermer avec un code de sortie de 0 ; tout autre code de retour est considéré comme une erreur.

Le script doit être enregistré avec l'unité d'acquisition à l'aide de l'outil SecurityAdmin, qui exécutera le script avec l'unité d'acquisition. Le script doit disposer des autorisations *read* et *execute* pour l'utilisateur root et "cisys". Si le script shell est modifié après l'enregistrement, le script shell modifié doit être réenregistré avec l'unité d'acquisition.

paramètre d'entrée : id de clé	Identificateur de clé utilisé pour identifier la clé dans le système de gestion des clés du client.
paramètre d'entrée : type de clé	public ou privé.
sortie	La clé demandée doit être imprimée sur la sortie standard. La clé RSA 2048 bits est actuellement prise en charge. Les clés doivent être codées et imprimées au format suivant - format de clé privée - PEM, format de clé publique PKCS8 PrivateKeyInfo RFC 5958 codé DER - PEM, X.509 PublictsubjecKeyInfo RFC 5280
code de sortie	Code de sortie de zéro pour réussir. Toutes les autres valeurs de sortie sont considérées comme ayant échoué.
autorisations de script	Le script doit disposer d'une autorisation de lecture et d'exécution pour l'utilisateur root et cisys.
journaux	Les exécutions de script sont consignées. Les journaux sont disponibles dans - /var/log/NetApp/cloudInsights/securityadmin/securityadmin.log /var/log/NetApp/cloudInsights/acq/acq.log

Cryptage d'un mot de passe à utiliser dans l'API

L'option 8 vous permet de crypter un mot de passe que vous pouvez ensuite transmettre à un collecteur de données via l'API.

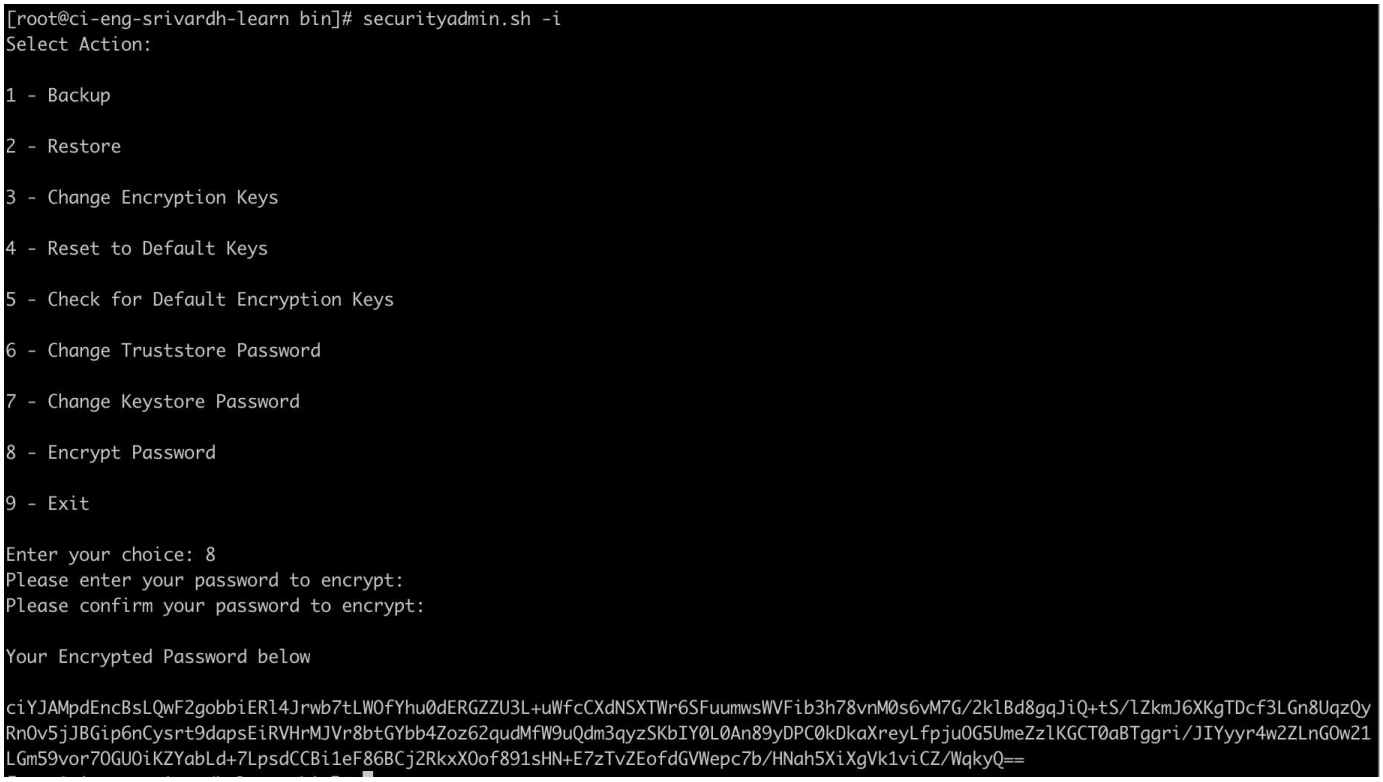
Démarrez l'outil SecurityAdmin en mode interactif et sélectionnez l'option 8 : *crypter le mot de passe*.

```
 securityadmin.sh -i
Vous êtes invité à saisir le mot de passe que vous souhaitez crypter.
Notez que les caractères que vous saisissez ne s'affichent pas à l'écran.
Saisissez à nouveau le mot de passe lorsque vous y êtes invité.
```

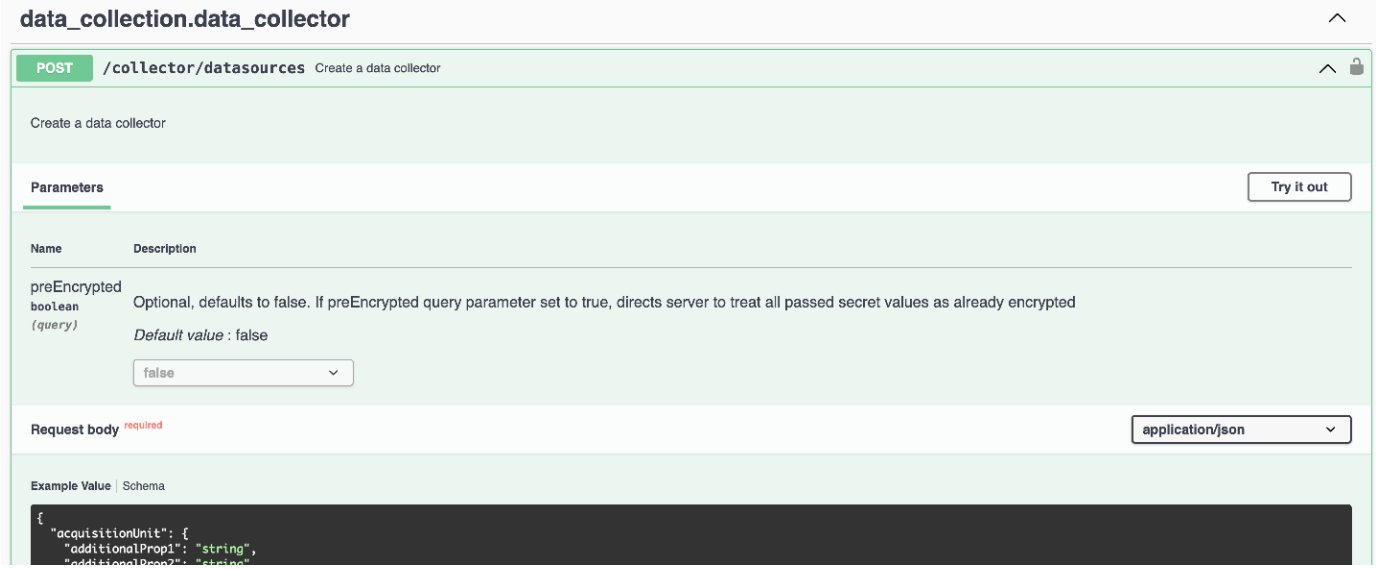
Sinon, si vous utilisez la commande dans un script, sur une ligne de commande, utilisez *securityadmin.sh* avec le paramètre "-enc", en transmettant votre mot de passe non chiffré :

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

Le mot de passe chiffré s'affiche à l'écran. Copiez la chaîne entière, y compris les symboles de début ou de fin.



Pour envoyer le mot de passe crypté à un collecteur de données, vous pouvez utiliser l'API de collecte de données. Le swagger pour cette API se trouve à l'adresse **Admin > API Access** et cliquez sur le lien « Documentation API ». Sélectionnez le type d'API « collecte de données ». Sous l'en-tête *data_collection.data_Collector*, choisissez l'API */Collector/datasources* POST pour cet exemple.



Si vous définissez l'option *preEncrypted* sur *True*, tout mot de passe que vous passez par la commande API sera traité comme **déjà crypté**; l'API ne recryptera pas le(s) mot(s) de passe. Lors de la création de votre API, il vous suffit de coller le mot de passe précédemment chiffré à l'emplacement approprié.

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"
  }
}
```