Sicurezza

Data Infrastructure Insights

NetApp
February 03, 2026

Sommario

Sicurezza

Data Infrastructure Insights

Per NetApp la sicurezza dei dati dei prodotti e dei clienti è di fondamentale importanza. Data Infrastructure Insights segue le migliori pratiche di sicurezza durante l'intero ciclo di vita del rilascio per garantire che i dati e le informazioni dei clienti siano protetti nel miglior modo possibile.

Panoramica sulla sicurezza

Sicurezza fisica

L'infrastruttura di produzione Data Infrastructure Insights è ospitata in Amazon Web Services (AWS). I controlli relativi alla sicurezza fisica e ambientale per i server di produzione Data Infrastructure Insights , che includono edifici e serrature o chiavi utilizzate sulle porte, sono gestiti da AWS. Secondo AWS: "L'accesso fisico è controllato sia sul perimetro che nei punti di ingresso dell'edificio da personale di sicurezza professionale che utilizza videosorveglianza, sistemi di rilevamento delle intrusioni e altri mezzi elettronici. Il personale autorizzato utilizza meccanismi di autenticazione a più fattori per accedere ai piani del data center."

Data Infrastructure Insights segue le migliori pratiche del"Modello di responsabilità condivisa" descritto da AWS.

Sicurezza del prodotto

Data Infrastructure Insights segue un ciclo di sviluppo in linea con i principi Agile, consentendoci così di affrontare più rapidamente eventuali difetti software legati alla sicurezza, rispetto alle metodologie di sviluppo con cicli di rilascio più lunghi. Utilizzando metodologie di integrazione continua, siamo in grado di rispondere rapidamente ai cambiamenti sia funzionali che di sicurezza. Le procedure e le policy di gestione del cambiamento definiscono quando e come si verificano i cambiamenti e contribuiscono a mantenere la stabilità dell'ambiente di produzione. Tutte le modifiche significative vengono comunicate formalmente, coordinate, opportunamente esaminate e approvate prima di essere rilasciate nell'ambiente di produzione.

Sicurezza di rete

L'accesso di rete alle risorse nell'ambiente Data Infrastructure Insights è controllato da firewall basati su host. Ogni risorsa (ad esempio un bilanciatore del carico o un'istanza di macchina virtuale) dispone di un firewall basato su host che limita il traffico in entrata solo alle porte necessarie affinché la risorsa svolga la sua funzione.

Data Infrastructure Insights utilizza vari meccanismi, tra cui servizi di rilevamento delle intrusioni, per monitorare l'ambiente di produzione alla ricerca di anomalie di sicurezza.

Valutazione del rischio

Il team di Data Infrastructure Insights segue un processo formalizzato di valutazione del rischio per fornire un metodo sistematico e ripetibile per identificare e valutare i rischi, in modo che possano essere gestiti in modo appropriato tramite un piano di trattamento del rischio.

Protezione dei dati

L'ambiente di produzione Data Infrastructure Insights è configurato in un'infrastruttura altamente ridondante che utilizza più zone di disponibilità per tutti i servizi e i componenti. Oltre a utilizzare un'infrastruttura di elaborazione altamente disponibile e ridondante, i dati critici vengono sottoposti a backup a intervalli regolari e i ripristini vengono testati periodicamente. Le policy e le procedure di backup formali riducono al minimo l'impatto delle interruzioni delle attività aziendali e proteggono i processi aziendali dagli effetti di guasti dei sistemi informativi o disastri, garantendone la ripresa tempestiva e adeguata.

Autenticazione e gestione degli accessi

L'accesso dei clienti a Data Infrastructure Insights avviene tramite interazioni con l'interfaccia utente del browser tramite https. L'autenticazione viene effettuata tramite il servizio di terze parti Auth0. NetApp ha scelto questo come livello di autenticazione per tutti i servizi Cloud Data.

Data Infrastructure Insights segue le best practice del settore, tra cui "Privilegio minimo" e "Controllo degli accessi basato sui ruoli" per l'accesso logico all'ambiente di produzione di Data Infrastructure Insights . L'accesso è controllato in base alla stretta necessità e viene concesso solo a personale autorizzato selezionato mediante meccanismi di autenticazione a più fattori.

Raccolta e protezione dei dati dei clienti

Tutti i dati dei clienti vengono crittografati durante il transito sulle reti pubbliche e crittografati a riposo. Data Infrastructure Insights utilizza la crittografia in vari punti del sistema per proteggere i dati dei clienti tramite tecnologie che includono Transport Layer Security (TLS) e l'algoritmo standard del settore AES-256.

Deprovisioning del cliente

Le notifiche e-mail vengono inviate a intervalli diversi per informare il cliente che il suo abbonamento sta per scadere. Una volta scaduto l'abbonamento, l'interfaccia utente viene limitata e inizia un periodo di tolleranza per la raccolta dei dati. Il cliente viene quindi avvisato tramite e-mail. Gli abbonamenti di prova hanno un periodo di grazia di 14 giorni, mentre gli abbonamenti a pagamento hanno un periodo di grazia di 28 giorni. Una volta scaduto il periodo di tolleranza, il cliente verrà avvisato tramite e-mail che l'account verrà eliminato entro 2 giorni. Anche un cliente pagante può richiedere direttamente di uscire dal servizio.

I tenant scaduti e tutti i dati dei clienti associati vengono eliminati dal team Data Infrastructure Insights Operations (SRE) al termine del periodo di tolleranza o alla conferma della richiesta del cliente di chiudere il proprio account. In entrambi i casi, il team SRE esegue una chiamata API per eliminare l'account. La chiamata API elimina l'istanza del tenant e tutti i dati del cliente. L'eliminazione del cliente viene verificata chiamando la stessa API e verificando che lo stato del tenant del cliente sia "ELIMINATO".

Gestione degli incidenti di sicurezza

Data Infrastructure Insights è integrato con il processo Product Security Incident Response Team (PSIRT) di NetApp per individuare, valutare e risolvere le vulnerabilità note. PSIRT acquisisce informazioni sulle vulnerabilità da più canali, tra cui segnalazioni dei clienti, ingegneria interna e fonti ampiamente riconosciute come il database CVE.

Se il team di ingegneria Data Infrastructure Insights rileva un problema, avvierà il processo PSIRT, valuterà e potenzialmente risolverà il problema.

È anche possibile che un cliente o un ricercatore Data Infrastructure Insights identifichi un problema di sicurezza con il prodotto Data Infrastructure Insights e segnali il problema al supporto tecnico o direttamente al team di risposta agli incidenti di NetApp. In questi casi, il team Data Infrastructure Insights avvierà il processo PSIRT, valuterà e potenzialmente risolverà il problema.

Test di vulnerabilità e penetrazione

Data Infrastructure Insights segue le migliori pratiche del settore ed esegue regolarmente test di vulnerabilità e penetrazione avvalendosi di professionisti e aziende della sicurezza interne ed esterne.

Formazione sulla consapevolezza della sicurezza

Tutto il personale di Data Infrastructure Insights segue una formazione sulla sicurezza, sviluppata per i singoli ruoli, per garantire che ogni dipendente sia in grado di gestire le sfide specifiche in materia di sicurezza dei propri ruoli.

Conformità

Data Infrastructure Insights esegue audit indipendenti di terze parti e convalide da parte di società di revisione contabile autorizzate esterne sulla sua sicurezza, sui suoi processi e sui suoi servizi, incluso il completamento dell'audit SOC 2.

Avvisi di sicurezza NetApp

Puoi visualizzare gli avvisi di sicurezza disponibili di NetApp"Qui" .

Informazioni e Regione

NetApp prende molto seriamente la sicurezza delle informazioni dei clienti. Ecco come e dove Data Infrastructure Insights archivia le tue informazioni.

Quali informazioni memorizza Data Infrastructure Insights ?

Data Infrastructure Insights memorizza le seguenti informazioni:

- Dati sulle prestazioni

  I dati sulle prestazioni sono dati di serie temporali che forniscono informazioni sulle prestazioni del dispositivo/sorgente monitorato. Ciò include, ad esempio, il numero di I/O forniti da un sistema di archiviazione, la capacità di elaborazione di una porta FibreChannel, il numero di pagine fornite da un server Web, il tempo di risposta di un database e altro ancora.

- dati di inventario

  I dati di inventario sono costituiti da metadati che descrivono il dispositivo/la sorgente monitorati e la loro configurazione. Ciò include, ad esempio, le versioni hardware e software installate, i dischi e le LUN in un sistema di archiviazione, i core della CPU, la RAM e i dischi di una macchina virtuale, gli spazi tabella di un database, il numero e il tipo di porte su uno switch SAN, i nomi di directory/file (se Storage Workload Security è abilitato), ecc.

- Dati di configurazione

  Riepiloga i dati di configurazione forniti dal cliente, utilizzati per gestire l'inventario e le operazioni del cliente, ad esempio nomi host o indirizzi IP dei dispositivi monitorati, intervalli di polling, valori di timeout, ecc.

- Segreti

  I segreti sono costituiti dalle credenziali utilizzate dalla Data Infrastructure Insights Acquisition Unit per

accedere ai dispositivi e ai servizi dei clienti. Queste credenziali vengono crittografate utilizzando una crittografia asimmetrica avanzata e le chiavi private vengono memorizzate solo sulle unità di acquisizione e non escono mai dall'ambiente del cliente. A causa di questa progettazione, anche gli SRE Data Infrastructure Insights privilegiati non sono in grado di accedere ai segreti dei clienti in testo normale.

- Dati funzionali

  Si tratta di dati generati in seguito alla fornitura del Cloud Data Service da parte di NetApp , che informano NetApp sullo sviluppo, l'implementazione, le operazioni, la manutenzione e la protezione del Cloud Data Service. I dati funzionali non contengono informazioni sul cliente o informazioni personali.

- Dati di accesso dell'utente

  Informazioni di autenticazione e accesso che consentono a NetApp Console di comunicare con i siti Data Infrastructure Insights regionali, inclusi i dati relativi all'autorizzazione dell'utente.

- Dati della directory utente della sicurezza del carico di lavoro di archiviazione

  Nei casi in cui la funzionalità Workload Security è abilitata E il cliente sceglie di abilitare il raccoglitore di directory utente, il sistema memorizzerà i nomi visualizzati degli utenti, gli indirizzi e-mail aziendali e altre informazioni raccolte da Active Directory.

> I dati della directory utente si riferiscono alle informazioni della directory utente raccolte dal raccoglitore dati della directory utente di Workload Security, non ai dati sugli utenti stessi di Data Infrastructure Insights/Workload Security.

Nessun dato personale esplicito viene raccolto dalle risorse infrastrutturali e dei servizi. Le informazioni raccolte sono costituite solo da parametri di prestazione, informazioni di configurazione e metadati dell'infrastruttura, in modo molto simile a quanto avviene con i servizi telefonici di molti fornitori, tra cui il supporto automatico NetApp e ActiveIQ. Tuttavia, a seconda delle convenzioni di denominazione del cliente, i dati per condivisioni, volumi, VM, qtree, applicazioni, ecc. possono contenere informazioni di identificazione personale.

Se Workload Security è abilitato, il sistema esamina anche i nomi di file e directory su SMB o altre condivisioni, che potrebbero contenere informazioni personali identificabili. Quando i clienti abilitano Workload Security User Directory Collector (che sostanzialmente mappa i SID di Windows ai nomi utente tramite Active Directory), il nome visualizzato, l'indirizzo e-mail aziendale e tutti gli attributi aggiuntivi selezionati verranno raccolti e archiviati da Data Infrastructure Insights.

Inoltre, vengono conservati i registri di accesso a Data Infrastructure Insights , che contengono gli indirizzi IP e gli indirizzi e-mail degli utenti utilizzati per accedere al servizio.

Dove vengono archiviate le mie informazioni?

Data Infrastructure Insights archivia le informazioni in base alla regione in cui è stato creato l'ambiente.

Nella regione host vengono memorizzate le seguenti informazioni:

- Telemetria e informazioni su asset/oggetti, inclusi contatori e metriche delle prestazioni
- Informazioni sull'unità di acquisizione
- Dati funzionali
- Informazioni di audit sulle attività degli utenti all'interno di Data Infrastructure Insights

- Informazioni sulla sicurezza del carico di lavoro di Active Directory
- Informazioni sull'audit di sicurezza del carico di lavoro

Le seguenti informazioni risiedono negli Stati Uniti, indipendentemente dalla regione che ospita l'ambiente Data Infrastructure Insights :

- Informazioni sul sito ambientale (talvolta denominato "inquilino"), come il proprietario del sito/account.
- Informazioni che consentono a NetApp Console di comunicare con i siti Data Infrastructure Insights regionali, incluso tutto ciò che riguarda l'autorizzazione dell'utente.
- Informazioni relative alla relazione tra l'utente Data Infrastructure Insights e il tenant.

Regioni ospitanti

Le regioni ospitanti includono:

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

Ulteriori informazioni

Per maggiori informazioni sulla privacy e la sicurezza di NetApp, consulta i seguenti xref:{relative_path}*
"Centro di fiducia"
* "Trasferimenti transfrontalieri di dati"
* "Regole aziendali vincolanti"
* "Rispondere alle richieste di dati di terze parti"
* "Principi sulla privacy NetApp"

Strumento SecurityAdmin

Data Infrastructure Insights include funzionalità di sicurezza che consentono al tuo ambiente di funzionare con maggiore sicurezza. Le funzionalità includono miglioramenti alla crittografia, all'hashing delle password e alla possibilità di modificare le password utente interne, nonché coppie di chiavi che crittografano e decrittografano le password.

Per proteggere i dati sensibili, NetApp consiglia di modificare le chiavi predefinite e la password utente *Acquisition* dopo un'installazione o un aggiornamento.

Le password crittografate dell'origine dati vengono archiviate in Data Infrastructure Insights, che utilizza una chiave pubblica per crittografare le password quando un utente le immette in una pagina di configurazione del raccoglitore dati. Data Infrastructure Insights non dispone delle chiavi private necessarie per decrittografare le password del data collector; solo le Acquisition Unit (AU) dispongono della chiave privata del data collector necessaria per decrittografare le password del data collector.

Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (ad esempio se sono state modificate le password), è necessario eseguire il backup delle configurazioni di sicurezza. L'installazione di un nuovo software o, in alcuni casi, l'aggiornamento del software, ripristina la configurazione di sicurezza predefinita del sistema. Quando il sistema torna alla configurazione predefinita, è necessario ripristinare la configurazione non

predefinita affinché il sistema funzioni correttamente.

Gestione della sicurezza sull'unità di acquisizione

Lo strumento SecurityAdmin consente di gestire le opzioni di sicurezza per Data Infrastructure Insights e viene eseguito sul sistema dell'unità di acquisizione. La gestione della sicurezza include la gestione di chiavi e password, il salvataggio e il ripristino delle configurazioni di sicurezza create o il ripristino delle configurazioni alle impostazioni predefinite.

Prima di iniziare

- Per installare il software Acquisition Unit (che include lo strumento SecurityAdmin), è necessario disporre dei privilegi di amministratore sul sistema AU.
- Se in seguito sono presenti utenti non amministratori che dovranno accedere allo strumento SecurityAdmin, è necessario aggiungerli al gruppo *cisys*. Il gruppo *cisys* viene creato durante l'installazione di AU.

Dopo l'installazione di AU, lo strumento SecurityAdmin si trova sul sistema dell'unità di acquisizione in una di queste posizioni:

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Utilizzo dello strumento SecurityAdmin

Avviare lo strumento SecurityAdmin in modalità interattiva (-i).

> Si consiglia di utilizzare lo strumento SecurityAdmin in modalità interattiva, per evitare di passare segreti sulla riga di comando, che potrebbero essere catturati nei log.

Vengono visualizzate le seguenti opzioni:

[Opzioni per SecurityAdmin Tool (Linux)]

1. **Backup**

   Crea un file zip di backup del vault contenente tutte le password e le chiavi e posiziona il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

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

   Si consiglia di mantenere sicuri i backup del vault, poiché contengono informazioni sensibili.

2. **Ripristinare**

   Ripristina il backup zip del vault creato. Una volta ripristinate, tutte le password e le chiavi vengono

riportate ai valori esistenti al momento della creazione del backup.

È possibile utilizzare Restore per sincronizzare password e chiavi su più server, ad esempio seguendo questi passaggi: 1) Modificare le chiavi di crittografia sull'AU. 2) Creare un backup del vault. 3) Ripristinare il backup del vault su ciascuna delle AU.

3. **Registra/Aggiorna lo script di recupero delle chiavi esterne**

   Utilizzare uno script esterno per registrare o modificare le chiavi di crittografia AU utilizzate per crittografare o decrittografare le password dei dispositivi.

   Quando si modificano le chiavi di crittografia, è opportuno eseguire il backup della nuova configurazione di sicurezza in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

   Nota che questa opzione è disponibile solo su Linux.

   Quando si utilizza uno script di recupero delle chiavi personalizzato con lo strumento SecurityAdmin, tenere presente quanto segue:

   - L'algoritmo attualmente supportato è RSA con un minimo di 2048 bit.
   - Lo script deve restituire le chiavi privata e pubblica in testo normale. Lo script non deve restituire chiavi private e pubbliche crittografate.
   - Lo script dovrebbe restituire contenuti grezzi e codificati (solo formato PEM).
   - Lo script esterno deve avere i permessi *execute*.
4. **Ruota le chiavi di crittografia**

   Ruota le chiavi di crittografia (annulla la registrazione delle chiavi correnti e registra nuove chiavi). Per utilizzare una chiave da un sistema di gestione delle chiavi esterno, è necessario specificare l'ID della chiave pubblica e l'ID della chiave privata.

5. **Ripristina i tasti predefiniti**

   Reimposta la password dell'utente di acquisizione e le chiavi di crittografia dell'utente di acquisizione ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

6. **Cambia password Truststore**

   Cambia la password del truststore.

7. **Cambia password archivio chiavi**

   Cambia la password del keystore.

8. **Crittografa la password del collezionista**

   Crittografa la password del raccoglitore dati.

9. **Uscita**

   Uscire dallo strumento SecurityAdmin.

Scegli l'opzione che vuoi configurare e segui le istruzioni.

Specificare un utente per eseguire lo strumento

Se ti trovi in un ambiente controllato e attento alla sicurezza, potresti non disporre del gruppo *cisys* ma potresti comunque voler consentire a utenti specifici di eseguire lo strumento SecurityAdmin.

È possibile ottenere questo risultato installando manualmente il software AU e specificando l'utente/gruppo per il quale si desidera l'accesso.

- Utilizzando l'API, scaricare il CI Installer sul sistema AU e decomprimerlo.
  - Sarà necessario un token di autorizzazione monouso. Consulta la documentazione API Swagger (*Admin > Accesso API* e seleziona il link *Documentazione API*) e trova la sezione API *GET /au/oneTimeToken*.
  - Una volta ottenuto il token, utilizza l'API *GET /au/installers/{platform}/{version}* per scaricare il file di installazione. Sarà necessario fornire la piattaforma (Linux o Windows) e la versione del programma di installazione.
- Copiare il file di installazione scaricato sul sistema AU e decomprimerlo.
- Passare alla cartella contenente i file ed eseguire il programma di installazione come root, specificando l'utente e il gruppo:

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

Se l'utente e/o il gruppo specificato non esistono, verranno creati. L'utente avrà accesso allo strumento SecurityAdmin.

Aggiornamento o rimozione del proxy

Lo strumento SecurityAdmin può essere utilizzato per impostare o rimuovere le informazioni proxy per l'unità di acquisizione eseguendo lo strumento con il parametro *-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.)
```

Ad esempio, per rimuovere il proxy, eseguire questo comando:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Dopo aver eseguito il comando, è necessario riavviare l'unità di
acquisizione.
```

Per aggiornare un proxy, il comando è

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

Recupero della chiave esterna

Se si fornisce uno script shell UNIX, questo può essere eseguito dall'unità di acquisizione per recuperare la **chiave privata** e la **chiave pubblica** dal sistema di gestione delle chiavi.

Per recuperare la chiave, Data Infrastructure Insights eseguirà lo script, passando due parametri: *key id* e *key type*. *Key id* può essere utilizzato per identificare la chiave nel sistema di gestione delle chiavi. Il *tipo di chiave* è "pubblico" o "privato". Quando il tipo di chiave è "pubblico", lo script deve restituire la chiave pubblica. Quando il tipo di chiave è "privato", è necessario restituire la chiave privata.

Per inviare la chiave all'unità di acquisizione, lo script deve stamparla sull'output standard. Lo script deve stampare *solo* la chiave sull'output standard; nessun altro testo deve essere stampato sull'output standard. Una volta che la chiave richiesta viene stampata sull'output standard, lo script deve uscire con un codice di uscita pari a 0; qualsiasi altro codice di ritorno è considerato un errore.

Lo script deve essere registrato con l'unità di acquisizione tramite lo strumento SecurityAdmin, che eseguirà lo script insieme all'unità di acquisizione. Lo script deve avere i permessi di *lettura* ed *esecuzione* per l'utente root e "cisys". Se lo script shell viene modificato dopo la registrazione, lo script shell modificato deve essere nuovamente registrato nell'unità di acquisizione.

parametro di input: ID chiave	Identificatore chiave utilizzato per identificare la chiave nel sistema di gestione delle chiavi del cliente.
parametro di input: tipo di chiave	pubblico o privato.
produzione	La chiave richiesta deve essere stampata sull'output standard. Attualmente è supportata la chiave RSA a 2048 bit. Le chiavi devono essere codificate e stampate nel seguente formato: formato chiave privata: PEM, codificato DER PKCS8 PrivateKeyInfo RFC 5958 formato chiave pubblica: PEM, codificato DER X.509 SubjectPublicKeyInfo RFC 5280
codice di uscita	Codice di uscita zero in caso di successo. Tutti gli altri valori di uscita sono considerati fallimentari.
permessi di script	Lo script deve avere i permessi di lettura ed esecuzione per l'utente root e "cisys".
registri	Le esecuzioni degli script vengono registrate. I log possono essere trovati in - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Crittografia di una password per l'uso nell'API

L'opzione 8 consente di crittografare una password, che può poi essere passata a un raccoglitore di dati tramite API.

Avviare lo strumento SecurityAdmin in modalità interattiva e selezionare l'opzione 8: *Crittografa password*.

```
 securityadmin.sh -i
Ti verrà chiesto di inserire la password che desideri crittografare.
Tieni presente che i caratteri digitati non vengono visualizzati sullo
schermo.  Reinserire la password quando richiesto.
```

In alternativa, se si desidera utilizzare il comando in uno script, su una riga di comando utilizzare *securityadmin.sh* con il parametro "-enc", passando la password non crittografata:

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

La password crittografata viene visualizzata sullo schermo. Copia l'intera stringa, compresi eventuali simboli iniziali o finali.

[Modalità interattiva Crittografa password, larghezza=640]

Per inviare la password crittografata a un raccoglitore di dati, è possibile utilizzare l'API di raccolta dati. È possibile trovare lo swagger per questa API in **Amministrazione > Accesso API** e fare clic sul collegamento "Documentazione API". Selezionare il tipo di API "Raccolta dati". Sotto l'intestazione *data_collection.data_collector*, seleziona l'API POST */collector/datasources* per questo esempio.

[API per la raccolta dati]

Se si imposta l'opzione *preEncrypted* su *True*, qualsiasi password passata tramite il comando API verrà trattata come **già crittografata**; l'API non crittograferà nuovamente la/le password. Quando crei la tua API, incolla semplicemente la password precedentemente crittografata nella posizione appropriata.

[Esempio API, larghezza=600]