



Sicurezza

Data Infrastructure Insights

NetApp
January 17, 2025

Sommario

- Sicurezza 1
 - Sicurezza degli approfondimenti sull'infrastruttura dati 1
 - Informazioni e Regione 3
 - Strumento securityadmin 5

Sicurezza

Sicurezza degli approfondimenti sull'infrastruttura dati

La sicurezza dei dati di prodotti e clienti è di estrema importanza per NetApp. Data Infrastructure Insights segue le Best practice per la sicurezza durante tutto il ciclo di vita del rilascio per garantire che le informazioni e i dati dei clienti siano protetti nel modo migliore possibile.

Panoramica sulla sicurezza

Sicurezza fisica

L'infrastruttura di produzione Data Infrastructure Insights si trova in Amazon Web Services (AWS). Controlli fisici e ambientali relativi alla sicurezza per i server di produzione Data Infrastructure Insights, che includono edifici, nonché i blocchi o le chiavi utilizzati sulle porte, sono gestiti da AWS. Come da 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 data center".

Data Infrastructure Insights segue le Best practice "[Modello di responsabilità condivisa](#)" descritte da AWS.

Sicurezza del prodotto

Data Infrastructure Insights segue un ciclo di vita dello sviluppo in linea con i principi Agile, consentendoci così di risolvere più rapidamente qualsiasi difetto software orientato alla sicurezza, rispetto alle metodologie di sviluppo del ciclo di rilascio più lungo. Grazie a metodologie di integrazione continua, siamo in grado di rispondere rapidamente alle modifiche funzionali e di sicurezza. Le procedure e le policy di gestione delle modifiche definiscono quando e come si verificano le modifiche e contribuiscono a mantenere la stabilità dell'ambiente di produzione. Qualsiasi modifica di impatto viene formalmente comunicata, coordinata, correttamente esaminata e approvata prima del rilascio 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'istanza di bilanciamento del carico o di macchina virtuale) dispone di un firewall basato su host che limita il traffico in entrata solo alle porte necessarie per eseguire la funzione di tale risorsa.

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

Valutazione dei rischi

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

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 all'utilizzo di un'infrastruttura di calcolo ridondante e altamente disponibile, viene eseguito il backup dei dati critici a intervalli regolari e i

ripristini vengono periodicamente testati. Le policy e le procedure di backup formali riducono al minimo l'impatto delle interruzioni delle attività di business e proteggono i processi di business dagli effetti dei guasti dei sistemi informativi o dei disastri e ne garantiscono una ripresa tempestiva e adeguata.

Autenticazione e gestione degli accessi

Tutto l'accesso dei clienti a Data Infrastructure Insights avviene tramite interazioni dell'interfaccia utente del browser su https. L'autenticazione viene eseguita tramite il servizio di terze parti Auth0. NetApp si è centralizzata su questo come livello di autenticazione per tutti i servizi dati cloud.

Data Infrastructure Insights segue le Best practice del settore, tra cui "Least Privilege" e "role-based access control", riguardo all'accesso logico all'ambiente di produzione Data Infrastructure Insights. L'accesso è controllato in base a esigenze rigorose e viene concesso solo a personale autorizzato selezionato che utilizza meccanismi di autenticazione a più fattori.

Raccolta e protezione dei dati dei clienti

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

Deprovisioning del cliente

Le notifiche e-mail vengono inviate a vari intervalli per informare il cliente che l'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 in prova hanno un periodo di tolleranza di 14 giorni e gli account di abbonamento a pagamento hanno un periodo di tolleranza di 28 giorni. Una volta scaduto il periodo di tolleranza, il cliente riceve una notifica via e-mail che l'account verrà cancellato tra 2 giorni. Un cliente a pagamento può anche richiedere direttamente di non usufruire del servizio.

I tenant scaduti e tutti i dati del cliente associati vengono eliminati dal team Data Infrastructure Insights Operations (SRE) al termine del periodo di tolleranza o alla conferma della richiesta di chiusura dell'account da parte del cliente. 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 "CANCELLATO".

Gestione degli incidenti di sicurezza

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

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

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

Test di vulnerabilità e penetrazione

Data Infrastructure Insights segue le Best practice del settore ed esegue regolarmente test di vulnerabilità e penetrazione utilizzando professionisti e aziende della sicurezza interni ed esterni.

Training sulla consapevolezza della sicurezza

Tutto il personale di Data Infrastructure Insights è sottoposto a corsi di formazione sulla sicurezza, sviluppati per i singoli ruoli, per assicurarsi che ogni dipendente sia in grado di gestire le sfide specifiche orientate alla sicurezza dei propri ruoli.

Conformità

Data Infrastructure Insights esegue verifiche e convalide indipendenti di terze parti da parte di un'azienda CPA esterna con licenza per la sicurezza, i processi e i servizi, compreso il completamento dell'audit SOC 2.

Avvisi di sicurezza NetApp

È possibile visualizzare gli avvisi di protezione disponibili in NetApp ["qui"](#).

Informazioni e Regione

NetApp prende molto sul serio la sicurezza delle informazioni dei clienti. Ecco come e dove Data Infrastructure Insights memorizza le tue informazioni.

Quali informazioni vengono memorizzate da Data Infrastructure Insights?

Data Infrastructure Insights memorizza le seguenti informazioni:

- Dati sulle performance

I dati sulle performance sono dati Time-Series che forniscono informazioni sulle performance del dispositivo/origine monitorato. Ad esempio, il numero di iOS forniti da un sistema di storage, il throughput di una porta FibreChannel, il numero di pagine inviate da un server Web, il tempo di risposta di un database e molto altro ancora.

- Dati di inventario

I dati di inventario sono costituiti da metadati che descrivono il dispositivo/origine monitorato e il modo in cui sono configurati. Ad esempio, le versioni hardware e software installate, i dischi e le LUN in un sistema di storage, i core della CPU, la RAM e i dischi di una macchina virtuale, gli spazi delle tabelle di un database, il numero e il tipo di porte su uno switch SAN, i nomi di directory/file (se la protezione del carico di lavoro dello storage è attivata) e così via

- Dati di configurazione

In questo modo vengono riepilogati 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 dall'unità di acquisizione di Data Infrastructure Insights per accedere ai dispositivi e ai servizi del cliente. 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. Anche gli SRE privilegiati di Data Infrastructure Insights non sono in grado di accedere ai segreti dei clienti in testo normale a causa di questa progettazione.

- Dati funzionali

Si tratta di dati generati in seguito alla fornitura da parte di NetApp del Cloud Data Service, che informa 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 sull'autenticazione e sull'accesso che consentono a NetApp BlueXP di comunicare con i siti regionali di Data Infrastructure Insights, inclusi i dati relativi all'autorizzazione dell'utente.

- Storage workload Security User Directory Data

Nei casi in cui la funzionalità workload Security è attivata E il cliente sceglie di attivare User Directory Collector, il sistema memorizza i nomi 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 collettore di dati della directory utente di sicurezza del carico di lavoro, non ai dati sugli utenti di Data Infrastructure Insights/workload Security.

Nessun dato personale esplicito viene raccolto dalle risorse dell'infrastruttura e dei servizi. Le informazioni raccolte comprendono solo metriche delle performance, informazioni di configurazione e metadati dell'infrastruttura, come molti case telefoniche dei vendor, tra cui il supporto automatico di NetApp e ActiveIQ. Tuttavia, a seconda delle convenzioni di denominazione di un cliente, i dati per condivisioni, volumi, macchine virtuali, qtree, le applicazioni, ecc. possono contenere informazioni di identificazione personale.

Se la sicurezza del carico di lavoro è attivata, il sistema esamina inoltre i nomi di file e directory su SMB o altre condivisioni, che potrebbero contenere informazioni di identificazione personale. Se i clienti abilitano il servizio di raccolta directory utente per la protezione del workload (che essenzialmente mappa i SID di Windows ai nomi utente tramite Active Directory), il nome visualizzato, l'indirizzo e-mail aziendale e gli eventuali attributi aggiuntivi selezionati verranno raccolti e memorizzati da Data Infrastructure Insights.

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

Dove sono memorizzate le mie informazioni?

Data Infrastructure Insights memorizza le informazioni in base all'area in cui viene creato l'ambiente.

Nella regione host vengono memorizzate le seguenti informazioni:

- Telemetria e informazioni su asset/oggetti, inclusi contatori e metriche delle performance
- Informazioni sull'unità di acquisizione
- Dati funzionali
- Informazioni di controllo sulle attività degli utenti all'interno di Data Infrastructure Insights
- Sicurezza del carico di lavoro informazioni su Active Directory
- Informazioni sulla verifica della sicurezza del carico di lavoro

Le seguenti informazioni risiedono negli Stati Uniti, indipendentemente dalla regione in cui risiede l'ambiente Data Infrastructure Insights:

- Informazioni sul sito dell'ambiente (talvolta chiamate "tenant"), come il proprietario del sito o dell'account.

- Informazioni che consentono a NetApp BlueXP di comunicare con i siti regionali di approfondimento sull'infrastruttura dati, incluso qualsiasi cosa fare con l'autorizzazione dell'utente.
- Informazioni relative alla relazione tra l'utente di Data Infrastructure Insights e il tenant.

Regioni host

Le regioni host includono:

- USA: US-est-1
- EMEA: eu-Central-1
- APAC: ap-sud-est-2

Ulteriori informazioni

Per ulteriori informazioni sulla privacy e la sicurezza di NetApp, consultare i seguenti xref:./* ["Trust Center"](#)

* ["Trasferimenti di dati transfrontalieri"](#)

* ["Regole aziendali vincolanti"](#)

* ["Risposta a richieste di dati di terze parti"](#)

* ["Principi di privacy di NetApp"](#)

Strumento securityadmin

Data Infrastructure Insights include funzionalità di sicurezza che consentono al tuo ambiente di operare con una 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 decrittare 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 delle origini dati sono memorizzate in Data Infrastructure Insights, che utilizza una chiave pubblica per crittografare le password quando un utente le inserisce in una pagina di configurazione di raccolta dati. Data Infrastructure Insights non dispone delle chiavi private necessarie per decrittografare le password di raccolta dati; solo le unità di acquisizione (AUS) dispongono della chiave privata di raccolta dati necessaria per decrittografare le password di raccolta dati.

Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (ad esempio, password ridgettate), 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 per il corretto funzionamento del sistema.

Gestione della sicurezza sull'unità di acquisizione

Lo strumento securityadmin consente di gestire le opzioni di sicurezza per Data Infrastructure Insights, 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 impostazioni predefinite delle configurazioni.

Prima di iniziare

- Per installare il software dell'unità di acquisizione (che include lo strumento securityadmin), è necessario disporre dei privilegi di amministratore sul sistema AU.
- Se in seguito si dispone di utenti non amministratori che dovranno accedere allo strumento securityadmin, questi devono essere aggiunti al gruppo *cisys*. Il gruppo *cisys* viene creato durante l'installazione dell'AU.

Dopo l'installazione di AU, lo strumento securityadmin si trova nel sistema dell'unità di acquisizione in una delle seguenti posizioni:

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

Utilizzando lo strumento securityadmin

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



Si consiglia di utilizzare lo strumento securityadmin in modalità interattiva, per evitare di trasmettere segreti sulla riga di comando, che possono essere acquisiti nei registri.

Vengono visualizzate le seguenti opzioni:

```
[root@ci-qa-xitij-cis2-285941linau bin]# ./securityadmin -i
Select Action:

1 - Backup
2 - Restore
3 - Register / Update External Key Retrieval Script
4 - Rotate Encryption Keys
5 - Reset to Default Keys
6 - Change Truststore Password
7 - Change Keystore Password
8 - Encrypt Collector Password
9 - Exit

Enter your choice: █
```

1. Backup

Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione

specificata dall'utente o nelle seguenti posizioni predefinite:

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

Si consiglia di mantenere al sicuro i backup del vault, poiché includono informazioni riservate.

2. Ripristina

Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio utilizzando i seguenti passaggi: 1) modificare le chiavi di crittografia sull'AU. 2) creare un backup del vault. 3) ripristinare il backup del vault in ciascuna delle aus.

3. Registra / Aggiorna script di recupero chiave esterna

Utilizzare uno script esterno per registrare o modificare le chiavi di crittografia AU utilizzate per crittografare o decrittare le password del dispositivo.

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

Nota questa opzione è disponibile solo su Linux.

Quando si utilizza il proprio script di recupero delle chiavi 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 private e pubbliche in testo normale. Lo script non deve restituire chiavi private e pubbliche crittografate.
- Lo script deve restituire contenuti codificati raw (solo formato PEM).
- Lo script esterno deve disporre delle autorizzazioni *execute*.

4. Ruota chiavi di crittografia

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

5. Ripristina chiavi predefinite

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

6. Modifica password Truststore

Modificare la password del truststore.

7. Modifica password keystore

Modificare la password del keystore.

8. Encrypt Collector Password

Crittografare la password del data collector.

9. Esci

Uscire dallo strumento securityadmin.

Scegliere l'opzione che si desidera configurare e seguire le istruzioni.

Specificare un utente per eseguire lo strumento

Se ci si trova in un ambiente controllato e consapevole della sicurezza, è possibile che non si disponga del gruppo *cisys*, ma che si desideri comunque che utenti specifici eseguano lo strumento securityadmin.

Per ottenere questo risultato, installare manualmente il software AU e specificare l'utente/gruppo a cui si desidera accedere.

- Utilizzando l'API, scaricare il programma di installazione nel sistema AU e decomprimerlo.
 - È necessario un token di autorizzazione una tantum. Consultare la documentazione API Swagger (*Admin > API Access* e selezionare il link *API Documentation*) e individuare la sezione *GET /au/oneTimeToken* API.
 - Una volta ottenuto il token, utilizzare l'API *GET /au/installers/{platform}/{version}* per scaricare il file di installazione. È necessario fornire la versione della piattaforma (Linux o Windows) e dell'installatore.
- Copiare il file di installazione scaricato nel sistema AU e decomprimerlo.
- Accedere 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 specificati 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 il seguente comando:

```
[root@ci-eng-linau bin]# ./securityadmin -pr -rp
Dopo aver eseguito il comando, 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 di shell UNIX, 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. *Key type* è "public" o "private". Quando il tipo di chiave è "public", lo script deve restituire la chiave pubblica. Quando il tipo di chiave è "privata", la chiave privata deve essere restituita.

Per inviare nuovamente il tasto all'unità di acquisizione, lo script deve stampare il tasto sull'output standard. Lo script deve stampare *solo* la chiave per l'output standard; nessun altro testo deve essere stampato su output standard. Una volta che la chiave richiesta viene stampata nell'output standard, lo script deve uscire con un codice di uscita di 0; qualsiasi altro codice di ritorno viene considerato un errore.

Lo script deve essere registrato con l'unità di acquisizione utilizzando lo strumento securityadmin, che eseguirà lo script insieme all'unità di acquisizione. Lo script deve avere l'autorizzazione *Read* e *execute* per l'utente root e "cisys". Se lo script della shell viene modificato dopo la registrazione, lo script della shell modificato deve essere nuovamente registrato con l'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 immissione: tipo di chiave	pubblico o privato.
uscita	La chiave richiesta deve essere stampata sull'output standard. La chiave RSA a 2048 bit è attualmente supportata. Le chiavi devono essere codificate e stampate nel seguente formato - formato chiave privata - PEM, DER-encoded PKCS8 PrivateKeyInfo RFC 5958 formato chiave pubblica - PEM, DER-encoded X.509 SubjectPublicKeyInfo RFC 5280
codice di uscita	Codice di uscita zero per successo. Tutti gli altri valori di uscita sono considerati falliti.
autorizzazioni script	Lo script deve disporre dell'autorizzazione di lettura ed esecuzione per l'utente root e "cisys".
registri	Vengono registrate le esecuzioni degli script. I log si trovano in - /var/log/NetApp/cloudinsigives/securityadmin/securityadmin.log /var/log/NetApp/cloudinsigives/acq/acq.log

Crittografia di una password per l'utilizzo in API

L'opzione 8 consente di crittografare una password, che è quindi possibile passare a un agente di raccolta dati tramite API.

Avviare lo strumento securityadmin in modalità interattiva e selezionare l'opzione 8: *Encrypt Password*.

```
securityadmin.sh -i
```

Viene richiesto di immettere la password che si desidera crittografare. I caratteri digitati non vengono visualizzati sullo schermo. Inserire nuovamente la password quando richiesto.

In alternativa, se si utilizza il comando in uno script, sulla 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. Copiare l'intera stringa, inclusi i simboli iniziali o finali.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i  
Select Action:  
  
1 - Backup  
2 - Restore  
3 - Change Encryption Keys  
4 - Reset to Default Keys  
5 - Check for Default Encryption Keys  
6 - Change Truststore Password  
7 - Change Keystore Password  
8 - Encrypt Password  
9 - Exit  
  
Enter your choice: 8  
Please enter your password to encrypt:  
Please confirm your password to encrypt:  
  
Your Encrypted Password below  
  
ciYJAMPdEncBsLQwF2gobbiERl4Jrwb7tLW0fYhu0dERGZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8ggJiQ+tS/LZkmJ6XKgTDcf3LGn8UqzQy  
Rn0v5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSkbIY0L0An89yDPC0kDkaXreyLfpju0G5UmeZz1KGCT0aBTggri/JIYypr4wZLNG0w21  
LGm59vor70GU0iKZYabLd+7LpsdCCBi1eF86BCj2RkxX0of891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

Per inviare la password crittografata a un data collector, è possibile utilizzare l'API di raccolta dati. Lo swagger per questa API si trova in **Admin > API Access** e fare clic sul collegamento "API Documentation". Selezionare il tipo di API "raccolta dati". Sotto l'intestazione `data_collection.data_collector`, scegliere l'API `/collector/datasources` POST per questo esempio.

data_collection.data_collector

POST /collector/datasources Create a data collector

Create a data collector

Parameters Try it out

Name	Description
preEncrypted boolean (query)	Optional, defaults to false. If preEncrypted query parameter set to true, directs server to treat all passed secret values as already encrypted Default value : false

Request body *required* application/json

Example Value | Schema

```
{  
  "acquisitionUnit": {  
    "additionalProp1": "string",  
    "additionalProp2": "string"
```

Se si imposta l'opzione *preEncrypted* su *True*, qualsiasi password passata attraverso il comando API verrà considerata come **già crittografata**; l'API non crittograferà nuovamente le password. Quando si crea l'API, è sufficiente incollare la password precedentemente crittografata nella posizione appropriata.

<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+1wE05gWwmmj1u0CB688nfOnB1xnIBVsAWyLmORxFAw
            vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
            4RoNF+84R/uFFGwKebIrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
            +nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQImM9QAYPoyw/JT0nXHDuf683uE
            K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.