セキュリティ
Cloud Insights

NetApp
May 09, 2024

目次

セキュリティ

Cloud Insights セキュリティ

ネットアップでは、製品とお客様にデータセキュリティを最大限に活用することが何よりも重要です。Cloud Insights は、リリースライフサイクル全体を通じてセキュリティのベストプラクティスに従い、顧客情報とデータを可能な限り最良の方法で保護します。

セキュリティの概要

物理的セキュリティ

Cloud Insights 本番インフラは、 Amazon Web Services （ AWS ）でホストされます。建物やドアで使用されるロックやキーなど、 Cloud Insights 本番サーバの物理的および環境的なセキュリティ関連制御は、 AWS によって管理されます。AWS によると、「ビデオ監視、侵入検知システム、その他の電子的手段を利用して、専門のセキュリティスタッフが、境界と建物の両方で物理アクセスを制御します。認定スタッフは、多要素認証メカニズムを利用してデータセンターのフロアにアクセスします。」

Cloud Insights は、のベストプラクティスに従います "共有責任モデル" AWS で説明されています。

製品のセキュリティ

Cloud Insights はアジャイルの原則に沿った開発ライフサイクルを採用しているため、リリースサイクル開発の方法論よりもセキュリティ指向のソフトウェアの不具合に迅速に対応できます。継続的な統合手法を使用することで、機能とセキュリティの両方の変化に迅速に対応できます。変更管理手順とポリシーは、変更がいつどのように発生するかを定義し、本番環境の安定性を維持するのに役立ちます。インパクトのある変更は、正式に伝達され、調整され、適切にレビューされ、本番環境にリリースされる前に承認されます。

ネットワークセキュリティ

Cloud Insights 環境内のリソースへのネットワークアクセスは、ホストベースのファイアウォールによって制御されます。各リソース（ロードバランサや仮想マシンインスタンスなど）にはホストベースのファイアウォールがあり、インバウンドトラフィックを、そのリソースが機能を実行するために必要なポートだけに制限します。

Cloud Insights は、侵入検知サービスなどのさまざまなメカニズムを使用して、本番環境のセキュリティ異常を監視します。

リスク評価

Cloud Insights チームは、正式なリスク評価プロセスに従い、リスクを識別して評価するための体系的かつ反復可能な方法を提供し、リスク治療計画を使用して適切に管理できるようにします。

データ保護

Cloud Insights の本番環境は、すべてのサービスおよびコンポーネントに複数のアベイラビリティゾーンを使用して、高度に冗長化されたインフラストラクチャでセットアップされます。可用性の高い冗長なコンピューティングインフラを利用するとともに、重要なデータを定期的にバックアップし、リストアを定期的にテストします。正式なバックアップ・ポリシーと手順により ' ビジネス・アクティビティの中断による影響を最小限に抑え ' 情報システムや災害の影響からビジネス・プロセスを保護し ' 適切なタイミングで適切な再開を実現

します

認証およびアクセス管理

Cloud Insights へのすべてのお客様アクセスは、 HTTPS を介したブラウザ UI インタラクションを通じて行われます。認証は、サードパーティのサービスである Auth0 を介して行われます。ネットアップでは、すべてのクラウドデータサービスの認証レイヤとして、この機能を一元化しています。

Cloud Insights は、 Cloud Insights 本番環境への論理アクセスに関する「最小特権」や「役割ベースのアクセス制御」など、業界のベストプラクティスに従っています。アクセスは厳密な必要性に基づいて制御され、多要素認証メカニズムを使用する一部の承認された担当者にのみ許可されます。

お客様のデータの収集と保護

すべてのお客様のデータは、パブリックネットワークを経由して転送中に暗号化され、保存中に暗号化されます。Cloud Insights は、システムのさまざまなポイントで暗号化を利用し、 Transport Layer Security （ TLS ）や業界標準の AES-256 アルゴリズムなどのテクノロジを使用してお客様のデータを保護します。

顧客のプロビジョニング解除

E メール通知はさまざまな間隔で送信され、お客様のサブスクリプションが期限切れになることを通知します。サブスクリプションの期限が切れると、 UI は制限され、データ収集の猶予期間が始まります。その後、お客様に E メールで通知します。トライアルサブスクリプションには 14 日間の猶予期間があり、有料サブスクリプションアカウントには 28 日間の猶予期間があります。猶予期間が終了すると、お客様にはアカウントが 2 日以内に削除されることを電子メールで通知します。有料のお客様は、サービスを利用しないよう直接リクエストすることもできます。

期限切れのテナントおよび関連するすべての顧客データは、猶予期間の終了時、または顧客のアカウント終了要求の確認時に、 Cloud Insights Operations （ SRE ）チームによって削除されます。どちらの場合も、 SRE チームは API 呼び出しを実行してアカウントを削除します。API 呼び出しで、テナントインスタンスとすべての顧客データが削除されます。カスタマーの削除は、同じ API を呼び出し、カスタマーテナントのステータスが「削除済み」であることを確認することで確認できます。

セキュリティインシデント管理

Cloud Insights は、ネットアップの Product Security Incident Response Team （ PSIRT ）プロセスと統合されており、既知の脆弱性の検索、評価、解決に利用できます。PSIRT は、カスタマーレポート、内部エンジニアリング、 CVE データベースなどの広く認識されているソースなど、複数のチャネルから脆弱性情報を取得します。

Cloud Insights エンジニアリングチームが問題を検出すると、チームは PSIRT プロセスを開始し、評価を行い、問題を修正する可能性があります。

また、 Cloud Insights のお客様や調査担当者が、 Cloud Insights 製品を使用してセキュリティ問題を特定し、問題をテクニカルサポートに報告したり、ネットアップのインシデント対応チームに直接報告したりすることも可能です。このような場合、 Cloud Insights チームは PSIRT プロセスを開始し、問題を評価し、修正する可能性があります。

脆弱性および侵入テスト

Cloud Insights は業界のベストプラクティスに従い、社内外のセキュリティプロフェッショナルと企業を使用して、定期的な脆弱性および侵入テストを実行します。

セキュリティ認識トレーニング

すべての Cloud Insights 担当者は、個々の役割向けに開発されたセキュリティトレーニングを受けて、各従業員がそれぞれの役割の特定のセキュリティ指向の課題に対応できるようにします。

コンプライアンス

Cloud Insights は、 SOC 2 監査の完了を含め、外部のライセンス済み CPA 企業のセキュリティ、プロセス、およびサービスについて、第三者による監査および検証を独立して実施します。

NetAppセキュリティアドバイザリ

ネットアップが提供しているセキュリティアドバイザリを表示できます。 "こちらをご覧ください"。

情報と地域

ネットアップでは、お客様の情報のセキュリティを非常に重視しています。ここでは、Cloud Insights がお客様の情報をどこにどのように保存するかを示します

Cloud Insights にはどのような情報が保存されますか

Cloud Insights は次の情報を保存します。

- パフォーマンスデータ

  パフォーマンスデータは、監視対象のデバイス / ソースのパフォーマンスに関する情報を提供する時系列のデータです。たとえば、ストレージシステムによって配信される IOS の数、ファイバチャネルポートのスループット、 Web サーバによって配信されるページ数、データベースの応答時間などです。

- インベントリデータ

  インベントリデータは、監視対象のデバイス / ソースを記述するメタデータと、その設定方法で構成されます。たとえば、インストールされているハードウェアとソフトウェアのバージョン、ストレージシステム内のディスクとLUN、CPUコア、RAMと仮想マシンのディスク、データベースの表領域、SANスイッチ上のポートの数とタイプ、ディレクトリとファイルの名前（ストレージワークロードのセキュリティが有効な場合）などです

- 設定データ

  これは、顧客のインベントリや操作を管理するために使用される、顧客から提供された構成データの要約です。たとえば、監視対象デバイスのホスト名や IP アドレス、ポーリング間隔、タイムアウト値などです

- 秘密

  シークレットは、 Cloud Insights Acquisition Unit で顧客のデバイスやサービスにアクセスするために使用されるクレデンシャルで構成されます。これらのクレデンシャルは強力な非対称暗号化を使用して暗号化され、秘密鍵はAcquisition Unitにのみ格納され、お客様の環境から離れることはありません。この設計により、 Privileged Cloud Insights SRE でもプレーンテキストで顧客シークレットにアクセスできません。

- 機能データ

このデータは、ネットアップがクラウドデータサービスを提供することで生成されます。このサービスは、クラウドデータサービスの開発、導入、運用、メンテナンス、セキュリティの各分野をネットアップに通知します。機能データには、顧客情報や個人情報は含まれません。

- ユーザーアクセスデータ

  ユーザ許可に関連するデータなど、 NetApp Cloud Central が地域の Cloud Insights サイトと通信できるようにするための認証およびアクセスに関する情報。

- ストレージワークロードのセキュリティユーザディレクトリデータ

  ワークロードセキュリティ機能が有効になっていて、ユーザーディレクトリコレクタを有効にすることを選択した場合、ユーザー表示名、企業の電子メールアドレス、およびActive Directoryから収集されたその他の情報が保存されます。

> ユーザディレクトリデータとは、Cloud Insights /ワークロードセキュリティ自体のユーザに関するデータではなく、ワークロードセキュリティユーザディレクトリのデータコレクタによって収集されたユーザディレクトリ情報のことです。

- 明示的な個人データは一切ありません。 * インフラストラクチャとサービスのリソースから収集されます。収集される情報は、パフォーマンス指標、設定情報、インフラメタデータのみで構成され、ネットアップの自動サポートや ActiveIQ など、多くのベンダーの電話ホームと同様です。ただし、お客様の命名規則に応じて、共有、ボリューム、 VM 、 qtree のデータ アプリケーションなどには、個人を特定できる情報が含まれる場合があります。

ワークロードのセキュリティが有効になっている場合、システムはさらに、個人を特定可能な情報を含むSMBまたはその他の共有上のファイル名とディレクトリ名を調べます。ワークロードセキュリティユーザディレクトリコレクタ（基本的にはWindows SIDをActive Directory経由でユーザ名にマッピング）を有効にすると、表示名、企業の電子メールアドレス、および選択したその他の属性がCloud Insights によって収集され、保存されます。

また、 Cloud Insights へのアクセスログも維持され、サービスへのログインに使用するユーザの IP アドレスと E メールアドレスが記録されます。

情報はどこに保存されますか？

Cloud Insights では、環境が作成された地域に応じて情報が格納されます。

ホスト領域には、次の情報が格納されます。

- カウンタやパフォーマンス指標などの計測情報と資産 / オブジェクト情報
- Acquisition Unit の情報
- 機能データ
- Cloud Insights 内のユーザアクティビティに関する監査情報
- ワークロードセキュリティActive Directoryの情報
- ワークロードのセキュリティ監査情報

Cloud Insights 環境をホストしている地域に関係なく、次の情報は米国にあります。

- サイト / アカウント所有者などの環境サイト（「テナント」とも呼ばれる）情報。
- ネットアップクラウドセントラルが、地域の Cloud Insights サイト（ユーザ認証とのやり取りを含む）と通信できるようにするための情報。
- Cloud Insights ユーザとテナントとの関係に関連する情報。

ホストリージョン

ホスト領域は次のとおりです。

- US ： us-east-1
- EMEA ： EU-central -1
- APAC ： AP-南東 部 -2

詳細情報

ネットアップのプライバシーとセキュリティの詳細については、次のリンクを参照してください。

- "トラストセンター"
- "クロスボーダーデータ転送"
- "企業規則の拘束"
- "サードパーティのデータ要求への対応"
- "ネットアッププライバシーの原則"

securityadminツール

Cloud Insights には、セキュリティを強化して環境を運用できるセキュリティ機能が含まれています。この機能には、暗号化、パスワードハッシュの改善、内部ユーザパスワードの変更、およびパスワードの暗号化と復号化を行うキーペアの変更が含まれます。

機密データを保護するために、インストールまたはアップグレードの完了後にデフォルトキーと_Acquisition_userパスワードを変更することを推奨します。

データソースで暗号化されたパスワードはCloud Insights に保存されます。では、ユーザがデータコレクタ設定ページでパスワードを入力したときに、公開鍵を使用してパスワードが暗号化されます。Cloud Insights には、データコレクタのパスワードの復号化に必要な秘密鍵はありません。データコレクタのパスワードの復号化に必要なデータコレクタの秘密鍵があるのは、Acquisition Unit（AUS）だけです。

アップグレードとインストールに関する考慮事項

Insightシステムにデフォルト以外のセキュリティ設定が含まれている場合（パスワードのキーが変更されている場合など）は、セキュリティ設定をバックアップする必要があります。新しいソフトウェアをインストールするか、ソフトウェアをアップグレードする場合によっては、システムをデフォルトのセキュリティ設定に戻します。システムがデフォルトの設定に戻ったら、システムを正常に動作させるために、デフォルト以外の設定をリストアする必要があります。

Acquisition Unit上でセキュリティを管理する

SecurityAdminツールを使用すると、Cloud Insights のセキュリティオプションを管理でき、Acquisition Unitシステム上で実行できます。セキュリティの管理には、キーとパスワードの管理、作成したセキュリティ設定の保存とリストア、またはデフォルト設定への設定のリストアが含まれます。

作業を開始する前に

- Acquisition Unitソフトウェア（SecurityAdminツールを含む）をインストールするには、AUシステムに対する管理者権限が必要です。
- その後SecurityAdminツールにアクセスする必要がある管理者以外のユーザがいる場合は、そのユーザを_cisys_groupに追加する必要があります。_cisys_groupは、AUのインストール中に作成されます。

AUのインストール後、SecurityAdminツールはAcquisition Unitシステムの次のいずれかの場所にあります。

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

SecurityAdmin Toolを使用する

SecurityAdminツールを対話型モード（-i）で起動します。

> SecurityAdminツールは対話モードで使用することをお勧めします。これは、コマンドラインでシークレットが渡されないようにするためです。シークレットはログに記録されます。

次のオプションが表示されます。

```
[root@ci-qa-xitij-cis2-28594linau 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. * バックアップ *

   すべてのパスワードとキーが格納されているバックアップのzipファイルを作成し、そのファイルをユーザが指定した場所、または次のデフォルトの場所に置きます。

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

   ヴォールトバックアップには機密情報が含まれているため、安全に保管することを推奨します。

2. * 復元 *

   作成したバックアップのzipファイルをリストアします。リストアすると、すべてのパスワードとキーがバックアップ作成時の既存の値に戻ります。

   復元を使用すると、次の手順を使用して、複数のサーバーのパスワードとキーを同期できます。1) AUの暗号化キーを変更します。2）ヴォールトのバックアップを作成します。3）バックアップを各AUSにリストアします。

3. 外部キー取得スクリプトの登録/更新

   外部スクリプトを使用して、デバイスパスワードの暗号化または復号化に使用するAU暗号化キーを登録または変更します。

   暗号化キーを変更した場合、アップグレードまたはインストール後にリストアできるように、新しいセキュリティ設定をバックアップしておく必要があります。

注:このオプションはLinuxでのみ使用できます。

SecurityAdminツールで独自のキー取得スクリプトを使用する場合は、次の点に注意してください。

- 現在サポートされているアルゴリズムは、2048ビット以上のRSAです。
- スクリプトは、秘密鍵と公開鍵をプレーンテキストで返す必要があります。スクリプトは、暗号化された秘密鍵と公開鍵を返さないでください。
- スクリプトは、生のエンコードされた内容を返す必要があります（PEM形式のみ）。
- 外部スクリプトには_execute_permissionsが必要です。

4. 暗号化キーのローテーション

   暗号化キーをローテーションします（現在のキーの登録を解除し、新しいキーを登録します）。外部キー管理システムのキーを使用するには、公開鍵IDと秘密鍵IDを指定する必要があります。

5. デフォルトキーにリセット

   acquisitionユーザのパスワードとacquisitionユーザの暗号化キーをデフォルト値にリセットします。デフォルト値はインストール時に指定したパスワードと暗号化キーです。

6. 信頼ストアのパスワードの変更

   信頼ストアのパスワードを変更します。

7. キーストアパスワードの変更

   キーストアのパスワードを変更します。

8. コレクタパスワードの暗号化

   暗号化データコレクタのパスワード。

9. * 終了 *

   SecurityAdminツールを終了します。

設定するオプションを選択し、画面の指示に従います。

ツールを実行するユーザを指定します

管理されたセキュリティ意識の高い環境にいる場合は、_cisys_groupを持っていなくても、特定のユーザーにSecurityAdminツールを実行してもらいたい場合があります。

これを行うには、AUソフトウェアを手動でインストールし、アクセスするユーザ/グループを指定します。

- APIを使用して、CIインストーラをAUシステムにダウンロードして解凍します。
  - 1回限りの認証トークンが必要になります。API Swaggerのドキュメント（_Admin > API Access_および_API Documentation_linkを選択）を参照し、_get /au/oneTimeToken_APIのセクションを参照してください。
  - トークンを取得したら、_get /au/installers/｛platform｝/｛version｝_apiを使用してインストーラファ

イルをダウンロードします。プラットフォーム（LinuxまたはWindows）とインストーラのバージョンを指定する必要があります。

- ダウンロードしたインストーラファイルをAUシステムにコピーして解凍します。
- ファイルが格納されているフォルダに移動し、ユーザとグループを指定してrootとしてインストーラを実行します。

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

指定したユーザまたはグループが存在しない場合は、作成されます。ユーザーはSecurityAdminツールにアクセスできます。

プロキシを更新または削除しています

SecurityAdminツールでAcquisition Unitのプロキシ情報を設定または削除するには、次のように_- pr_パラメータを指定してツールを実行します。

```
[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 Cloud 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.)
```

たとえば、プロキシを削除するには、次のコマンドを実行します。

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
コマンドの実行後にAcquisition Unitを再起動する必要があります。
```

プロキシを更新するには、コマンドを使用します

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

外部キーの取得

UNIXシェルスクリプトを指定すると、Acquisition Unitによって実行され、キー管理システムから*秘密鍵*と*公開鍵*を取得できます。

キーを取得するために、Cloud Insightsはスクリプトを実行し、_key id_and_key type_という2つのパラメータを渡します。キーID _は、キー管理システム内のキーを識別するために使用できます。_Key type _には、「public」または「private」を指定します。キータイプが「public」の場合、スクリプトは公開鍵を返す必要があります。キータイプが「private」の場合は、秘密鍵を返す必要があります。

Acquisition Unitにキーを戻すには、標準出力にキーを出力する必要があります。スクリプトは、標準出力にキーをprint_only_theで出力する必要があります。他のテキストは標準出力に出力しないでください。要求されたキーが標準出力に出力されると、スクリプトは終了コード0で終了する必要があります。その他の戻りコードはエラーと見なされます。

スクリプトはSecurityAdminツールを使用してAcquisition Unitに登録する必要があります。このツールでは、Acquisition Unitとともにスクリプトが実行されます。スクリプトには、rootおよび"cisys"ユーザに対する_read_and_execute_permissionが必要です。登録後にシェルスクリプトを変更した場合は、変更したシェルスクリプトをAcquisition Unitに再登録する必要があります。

入力パラメータ:キーID	顧客のキー管理システムでキーを識別するために使用するキー識別子。
入力パラメータ:キータイプ	パブリックまたはプライベート。
出力	要求されたキーを標準出力に出力する必要があります。現在、2048ビットRSAキーがサポートされています。キーは次の形式でエンコードおよび印刷する必要があります- 秘密鍵形式- PEM、DERエンコードPKCS8 PrivateKeyInfo RFC 5958 公開鍵形式- PEM、DERエンコードX.509 SubjectPublicKeyInfo RFC 5280
終了コード	成功のためのゼロの終了コード。他のすべての終了値は失敗と見なされます。
スクリプト権限	スクリプトには、rootおよび「cisys」ユーザに対する読み取りおよび実行権限が必要です。
ログ	スクリプトの実行が記録されます。ログは次の場所にあります。 /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

APIで使用するパスワードの暗号化

オプション8では、パスワードを暗号化し、APIを介してデータコレクタに渡すことができます。

SecurityAdminツールを対話型モードで起動し、オプション8:_Encrypt Password_を選択します。

```
securityadmin.sh -i
```
暗号化するパスワードの入力を求められます。入力した文字は画面に表示されません。
プロンプトが表示されたら、パスワードを再入力します。

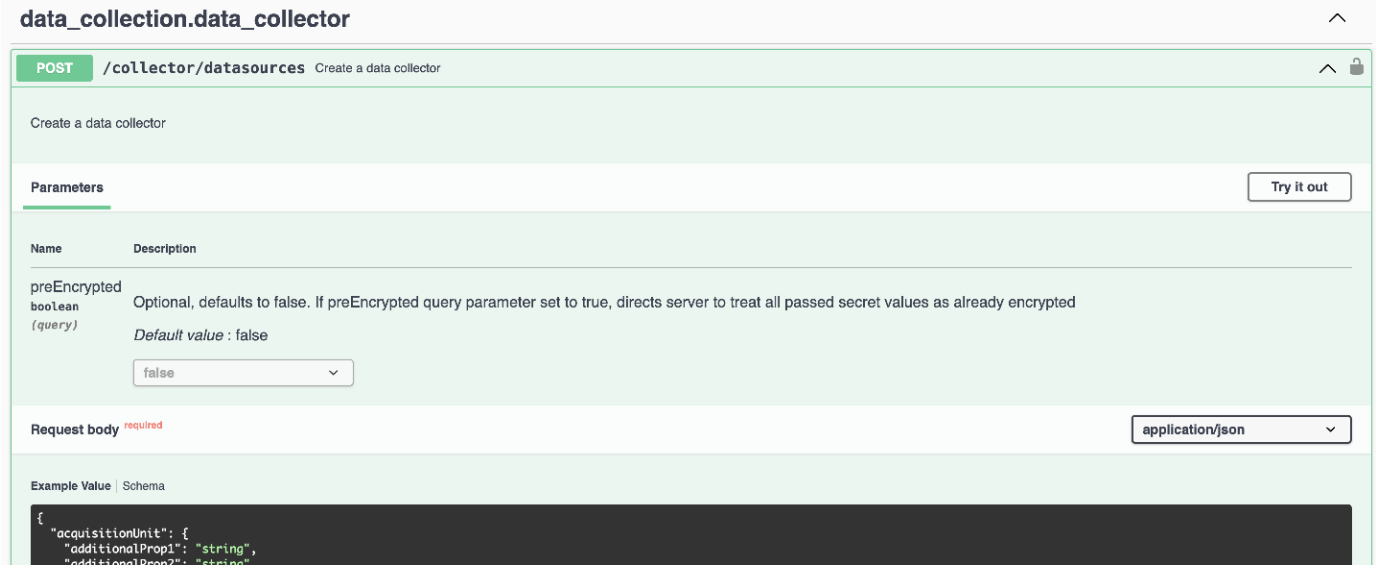
または、スクリプトでコマンドを使用する場合は、コマンドラインで「-enc」パラメータを指定して_securityadmin.sh_を使用し、暗号化されていないパスワードを渡します。

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

暗号化されたパスワードが画面に表示されます。先頭または末尾の記号を含む文字列全体をコピーします。

```
[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

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

暗号化されたパスワードをデータコレクタに送信するには、データ収集APIを使用します。このAPIのSwaggerは* Admin > API Access *にあり、[API Documentation]リンクをクリックします。「データ収集」APIタイプを選択します。 *data_collection.data_collector_heading*で、この例の_/collector/datasources_POST APIを選択します。



_preEncrypted_optionを_True_に設定した場合、APIコマンドを通過するパスワードは*すでに暗号化されている*として扱われます。APIはパスワードを再暗号化しません。APIを構築するときは、以前に暗号化されたパスワードを適切な場所に貼り付けるだけです。

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
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```