



セキュリティ

Data Infrastructure Insights

NetApp
December 19, 2024

目次

セキュリティ	1
データインフラ分析情報のセキュリティ	1
情報と地域	3
securityadminツール	5

セキュリティ

データインフラ分析情報のセキュリティ

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。Data Infrastructure Insightsは、リリースの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、可能な限り最善の方法でお客様の情報とデータを確実に保護します。

セキュリティの概要

物理的セキュリティ

Data Infrastructure Insightsの本番インフラは、Amazon Web Services (AWS) でホストされています。Data Infrastructure 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の制御（建物やドアで使用されるロックやキーなど）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。」

Data Infrastructure Insightsは、"**共有責任モデル**"AWSで説明されているのベストプラクティスに従っています。

製品のセキュリティ

Data Infrastructure Insightsは、アジャイルの原則に沿った開発ライフサイクルに従います。そのため、リリースサイクルの長い開発手法と比較して、セキュリティ志向のソフトウェアの不具合に迅速に対処することができます。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

Data Infrastructure 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。

Data Infrastructure Insightsは、侵入検出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

Data Infrastructure Insightsチームは、形式化されたリスクアセスメントプロセスに従い、リスクを特定して評価する体系的で反復可能な方法を提供し、リスクをリスク治療計画を通じて適切に管理できるようにします。

データ保護

Data Infrastructure Insights本番環境は、すべてのサービスとコンポーネントに対して複数のアベイラビリティゾーンを使用して、非常に冗長なインフラ内に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

Data Infrastructure Insightsへのすべてのアクセスは、HTTPSを介したブラウザUIの操作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。

Data Infrastructure Insightsは、Data Infrastructure Insights本番環境への論理アクセスに関する「最小権限」や「ロールベースアクセス制御」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ものみ許可されます。

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經由して転送中に暗号化され、保存中に暗号化されます。Data Infrastructure Insightsは、システム内のさまざまなポイントでの暗号化を利用して、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ー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と関連するすべての顧客データは、猶予期間の終了時、またはお客様からアカウントの終了を要求されたことを確認した時点で、Data Infrastructure 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

Data Infrastructure Insightsは、NetAppの製品セキュリティインシデント対応チーム (PSIRT) プロセスと統合されており、既知の脆弱性を検出、評価、解決します。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、複数のチャンネルから脆弱性情報を取得します。

Data Infrastructure Insightsエンジニアリングチームが問題を検出した場合、チームはPSIRTプロセスを開始し、問題を評価し、潜在的に修正します。

また、Data Infrastructure Insightsのお客様やリサーチャーは、Data Infrastructure Insights製品のセキュリティ上の問題を特定し、テクニカルサポートまたはNetAppのインシデント対応チームに直接報告することもできます。このような場合は、Data Infrastructure InsightsチームがPSIRTプロセスを開始し、問題を評価して、潜在的に修正します。

脆弱性および侵入テスト

Data Infrastructure 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専門家や企業を使用して定期的に脆弱性と侵入テストを実施します。

セキュリティ認識トレーニング

Data Infrastructure Insightsのすべての担当者は、それぞれの役割に応じて開発されたセキュリティトレーニングを受けています。これにより、各担当者は、それぞれの役割に固有のセキュリティ関連の課題に対処できるようになります。

コンプライアンス

Data Infrastructure Insightsは、セキュリティ、プロセス、サービスについて外部の公認会計士事務所から独立した第三者監査および検証を実施しています。これには、SOC 2監査の完了も含まれます。

NetAppセキュリティアドバイザリ

NetAppで利用可能なセキュリティアドバイザリを表示できます["ここをクリック"](#)。

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。Data Infrastructure Insightsで情報を保存する方法と場所をご紹介します。

Data Infrastructure Insightsにはどのような情報が保存されますか？

Data Infrastructure Insightsには次の情報が格納されます。

- 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、Data Infrastructure Insights Acquisition Unitがお客様のデバイスやサービスにアクセスするために使用す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。Privileged Data Infrastructure InsightsのSREであっても、この設計により、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

NetApp BlueXP が各地域のData Infrastructure Insightsサイトと通信できるようにする認証およびアクセス情報（ユーザの承認に関連するデータなど）。

- 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、ワークロードセキュリティユーザディレクトリ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であり、データインラインサイト/ワークロードセキュリティのユーザ自身に関するデータではありません。

- 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。お客様がWorkload Security User Directory Collector（Active Directoryを介してWindows SIDをユーザ名にマッピングする）を有効にした場合、表示名、企業のEメールアドレス、および選択したその他の属性がData Infrastructure Insightsによって収集され、保存されます。

さらに、Data Infrastructure Insightsへのアクセスログは維持され、サービスへのログインに使用されたユーザの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？

Data Infrastructure Insightsには、環境が作成されたリージョンに基づい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

- Data Infrastructure Insights内のユーザアクティビティに関する情報を監査
- 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

以下の情報は、Data Infrastructure Insights環境をホストしているリージョンに関係なく、米国内に存在します。

- 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。
- NetApp BlueXP が各地域のData Infrastructure Insightsサイトと通信できるようにするための情報（ユーザの承認に関連する情報を含む）。
- Data Infrastructure Insightsのユーザとテナントの関連に関する情報。

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

Data Infrastructure Insightsには、強化されたセキュリティで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。

データソース暗号化されたパスワードはData Infrastructure Insightsに保存されます。Data Infrastructure Insightsでは、ユーザがデータコレクタの設定ページでパスワードを入力すると、公開鍵を使用してパスワードが暗号化されます。Data Infrastructure 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、Data Infrastructure Insightsのセキュリティオプションを管理できます。このツールはAcquisition Unitシステムで実行されます。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。

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-cis2-285941inaw 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 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.)
```

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、Data Infrastructure Insightsはスクリプトを実行し、`_key id_`と`_key type_`の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 <code>-/var/log/cloudinsights/securityadmin/ NetApp securityadmin.log /var/log/cloudinsights/acq/ NetApp acq.log</code> にあります。

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  
  
ciYJAMPdEncBsLQwF2gobbiERL4Jrwb7tLW0fYhu0dERGZUZ3L+uWfcCXdNSXTWr6SFuumwsWVfIb3h78vnM0s6vM7G/2k1Bd8gqJiQ+tS/LZkmJ6XKgTdcf3LGN8UqzQy  
Rn0v5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpju0G5UmeZz1KGCT0aBTggri/JIYyyr4w2ZLnG0w21  
LGm59vor70GU0iKZYablD+7LpsdCCBi1eF86BCj2RkxX0of891sHN+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。

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"  }
```

`_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+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"
  }
}
```

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。