セキュリティ
Data Infrastructure Insights

NetApp
February 11, 2026

目次

セキュリティ

Data Infrastructure Insightsセキュリティ

NetAppでは、製品と顧客データのセキュリティが最も重要です。 Data Infrastructure Insights は、リリース ライフサイクル全体にわたってセキュリティのベスト プラクティスに従い、顧客情報とデータが可能な限り最善の方法で保護されるようにします。

セキュリティの概要

物理的なセキュリティ

Data Infrastructure Insights の運用インフラストラクチャは、Amazon Web Services (AWS) でホストされています。建物やドアに使用されるロックやキーを含む、 Data Infrastructure Insights実稼働サーバーの物理的および環境的なセキュリティ関連の制御は、AWS によって管理されます。 AWS によると、「物理的なアクセスは、ビデオ監視、侵入検知システム、その他の電子手段を利用する専門のセキュリティ スタッフによって、境界と建物の入口の両方で制御されます。」権限のあるスタッフは、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 によって説明されています。

製品セキュリティ

Data Infrastructure Insights は、アジャイル原則に沿った開発ライフサイクルに従うため、リリース サイクルが長い開発方法論と比較して、セキュリティ重視のソフトウェア欠陥に迅速に対処できます。継続的インテグレーション手法を使用することで、機能とセキュリティの両方の変更に迅速に対応できます。変更管理の手順とポリシーは、変更がいつどのように発生するかを定義し、運用環境の安定性を維持するのに役立ちます。影響のある変更は、実稼働環境にリリースされる前に正式に伝達、調整され、適切にレビューされ、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、そのリソースが機能を実行するために必要なポートのみに受信トラフィックを制限するホストベースのファイアウォールがあります。

Data Infrastructure 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、実稼働環境のセキュリティ異常を監視します。

リスクアセスメント

Data Infrastructure Insightsチームは、形式化されたリスク評価プロセスに従って、リスクを識別および評価するための体系的かつ反復可能な方法を提供し、リスク処理計画を通じてリスクを適切に管理できるようにします。

データ保護

Data Infrastructure Insights の運用環境は、すべてのサービスとコンポーネントに複数の可用性ゾーンを利用する、高度に冗長化されたインフラストラクチャ内にセットアップされています。可用性が高く冗長性のある

コンピューティング インフラストラクチャを活用するとともに、重要なデータは定期的にバックアップされ、復元は定期的にテストされます。正式なバックアップ ポリシーと手順により、ビジネス活動の中断の影響が最小限に抑えられ、情報システムの障害や災害の影響からビジネス プロセスが保護され、タイムリーかつ適切に再開されることが保証されます。

認証とアクセス管理

Data Infrastructure Insightsへのすべての顧客アクセスは、https 経由のブラウザ UI 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。 NetApp は、これをすべてのクラウド データ サービスの認証レイヤーとして一元化しています。

Data Infrastructure Insights は、 Data Infrastructure Insights の運用環境への論理アクセスに関する「最小権限」や「ロールベースのアクセス制御」などの業界のベスト プラクティスに従います。アクセスは厳密に必要に応じて制御され、多要素認証メカニズムを使用して、承認された特定の担当者にのみ許可されます。

顧客データの収集と保護

すべての顧客データは、パブリック ネットワーク経由での転送中および保存時に暗号化されます。 Data Infrastructure Insights は、システムのさまざまなポイントで暗号化を活用し、トランスポート層セキュリティ (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顧客データを保護します。

顧客のプロビジョニング解除

サブスクリプションの有効期限が近づいていることを顧客に通知するために、さまざまな間隔で電子メール通知が送信されます。サブスクリプションの有効期限が切れると、UI が制限され、データ収集の猶予期間が始まります。その後、顧客に電子メールで通知されます。試用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。猶予期間が過ぎると、2 日以内にアカウントが削除されることが電子メールで顧客に通知されます。有料のお客様は、サービスの利用停止を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、または顧客からのアカウント終了要求の確認時に、Data Infrastructure Insightsサイト オペレーション (SRE) チームによって削除されます。どちらの場合でも、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 呼び出しにより、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。顧客の削除は、同じ API を呼び出して、顧客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によって検証されます。

セキュリティインシデント管理

Data Infrastructure Insights は、既知の脆弱性を発見、評価、解決するために、NetApp の製品セキュリティ インシデント レスポンス チーム (PSIRT) プロセスと統合されています。 PSIRT は、顧客レポート、社内エンジニアリング、CVE データベースなどの広く認知されているソースを含む複数のチャ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 チームによって問題が検出された場合、チームは PSIRT プロセスを開始し、問題を評価し、場合によっては修復します。

また、 Data Infrastructure Insights の顧客または研究者が、 Data Infrastructure Insights製品のセキュリティ問題を特定し、その問題をテクニカル 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可能性もあります。このような場合、Data Infrastructure Insightsチームは PSIRT プロセスを開始し、問題を評価し、場合によっては修復します。

脆弱性と侵入テスト

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のテストを実行します。

セキュリティ意識向上トレーニング

すべてのData Infrastructure Insights従業員は、それぞれの役割に合わせて開発されたセキュリティ トレーニングを受け、各従業員が自分の役割に特有のセキュリティ重視の課題に対処できるようにしています。

コンプライアンス

Data Infrastructure Insights は、 SOC 2 監査の完了を含め、セキュリティ、プロセス、サービスについて、外部の認定 CPA 事務所による独立したサードパーティ監査と検証を実行します。

NetAppセキュリティアドバイザリ

NetAppのセキュリティアドバイザリは以下からご覧いただけます。"ここをクリックしてください。" 。

情報と地域

NetApp は顧客情報のセキュリティを非常に重視しています。 Data Infrastructure Insights が情報を保存する方法と場所は次のとおりです。

Data Infrastructure Insights はどのような情報を保存しますか?

Data Infrastructure Insightsには次の情報が保存されます。

- 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データです。これには、たとえば、ストレージ システムによって配信される IO の数、ファイバーチャネル ポートのスループット、Web サーバー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が含まれます。

- 在庫データ

  インベントリ データは、監視対象のデバイス/ソースとその構成方法を記述するメタデータで構成されます。これには、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、仮想マシンの RAM とディスク、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/ファイル名 (ストレージ ワークロード セキュリティが有効な場合) などが含まれます。

- 構成データ

  これは、監視対象デバイスのホスト名または IP アドレス、ポーリング間隔、タイムアウト値など、顧客のインベントリと操作を管理するために使用される顧客提供の構成データを要約したものです。

- 秘密

  シークレットは、Data Infrastructure Insights取得ユニットが顧客のデバイスやサービスにアクセスするた

めに使用する資格情報で構成されます。これらの資格情報は強力な非対称暗号化を使用して暗号化され、秘密鍵は取得ユニットにのみ保存され、顧客環境から外に出ることはありません。この設計により、特権を持つData Infrastructure Insights SRE であっても、プレーンテキストで顧客の秘密にアクセスすることはできません。

- 機能データ

  これは、 NetApp がクラウド データ サービスを提供した結果として生成されるデータであり、 NetApp にクラウド データ サービスの開発、導入、運用、保守、セキュリティ保護に関する情報を提供します。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 Consoleが地域の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 (ユーザー認証に関連するデータを含む)。

- ストレージワークロードセキュリティユーザーディレクトリデータ

  Workload Security 機能が有効になっていて、顧客がユーザー ディレクトリ コレクターを有効にすることを選択した場合、システムはユーザーの表示名、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を保存します。

> ユーザー ディレクトリ データとは、Workload Security ユーザー ディレクトリ データ コレクターによって収集されたユーザー ディレクトリ情報を指し、 Data Infrastructure Insights/Workload Security のユーザー自体に関するデータではありません。

*明示的な個人データは*インフラストラクチャおよびサービス リソースから収集されません。収集される情報は、 NetApp自動サポートや ActiveIQ などの多くのベンダーの電話サービスと同様に、パフォーマンス メトリック、構成情報、インフラストラクチャ メタデータのみで構成されます。ただし、顧客の命名規則によっては、共有、ボリューム、VM、qtree、アプリケーションなどのデータに個人を特定できる情報が含まれる場合があります。

Workload Security が有効になっている場合、システムは個人を特定できる情報が含まれている可能性のある 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も確認します。お客様が Workload Security User Directory Collector (基本的には Active Directory を通じて Windows SID をユーザー名にマッピングします) を有効にすると、表示名、会社の電子メール アドレス、および選択された追加属性が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 ログが保持され、サービスへのログインに使用されたユーザーの IP アドレスと電子メール アドレスが含まれます。

私の情報はどこに保存されますか?

Data Infrastructure Insights は、環境が作成されたリージョンに応じて情報を保存します。

ホスト領域には次の情報が保存されます。

- カウンターやパフォーマンス メトリックを含むテレメトリと資産/オブジェクト情報
- 取得ユニット情報
- 機能データ

- Data Infrastructure Insights内のユーザー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 情報
- ワークロードセキュリティ監査情報

次の情報は、 Data Infrastructure Insights環境をホストしている地域に関係なく、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」と呼ばれることもあります) の情報。
- NetApp Consoleが地域のData Infrastructure Insightsサイトと通信できるようにする情報 (ユーザー認証に関連するものを含む)。
- Data Infrastructure Insightsユーザーとテナント間の関係に関する情報。

ホスト地域

ホスト地域は次のとおりです:

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

詳細情報

NetApp のプライバシーとセキュリティの詳細については、次のリンクをご覧ください。

- "信頼センター"
- "国境を越えたデータ転送"
- "拘束的企業準則"
- "サードパーティのデータ要求への対応"
- "NetAppプライバシー原則"

セキュリティ管理ツール

Data Infrastructure Insightsには、環境を強化されたセキュリティで運用できるようにするセキュリティ機能が含まれています。機能には、暗号化、パスワード ハッシュの改善、内部ユーザー パスワードの変更機能、およびパスワードを暗号化および復号化するキー ペアの変更機能が含まれます。

機密データを保護するために、 NetApp、インストールまたはアップグレード後にデフォルトのキーと *Acquisition* ユーザー パスワードを変更することをお勧めします。

データ ソースの暗号化されたパスワードはData Infrastructure Insightsに保存され、ユーザーがデータ コレクター構成ページでパスワードを入力すると、公開キー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 コレクターのパスワードを復号化するために必要な秘密キーがありません。データ コレクターのパスワードを復号化するために必要なデータ コレクターの秘密キーを持っているのは、Acquisition Unit (AU) 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構成が含まれている場合 (つまり、パスワードのキーを変更した場合)、セキュリティ構成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したり、場合によってはソフトウェアをアップグレードしたりすると、システムはデフォルトのセキュリティ構成に戻ります。システムをデフォルト構成に戻す場合、システムが正しく動作するために、デフォルト以外の構成を復元する必要があります。

買収部門のセキュリティ管理

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、取得ユニット システムで実行されます。セキュリティ管理には、キーとパスワードの管理、作成したセキュリティ構成の保存と復元、構成をデフォルト設定に復元することが含まれます。

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。
- 後で 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ーがいる場合は、そのユーザーを *cisys* グループに追加する必要があります。 *cisys* グループは AU インストール中に作成されます。

AU のインストール後、SecurityAdmin ツールは取得ユニット システムの次のいずれかの場所にあります。

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

SecurityAdminツールの使用

SecurityAdmin ツールを対話モード (-i) で起動します。

ログに記録される可能性のある秘密をコマンド ラインで渡すことを避けるため、SecurityAdmin ツールを対話型モードで使用することをお勧めします。

次のオプションが表示されます。

[SecurityAdmin ツールのオプション (Linux)]

1. バックアップ

   すべてのパスワードとキーを含む Vault のバックアップ zip ファイルを作成し、そのファイルをユーザーが指定した場所、または次のデフォルトの場所に配置します。

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

ボ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お勧めします。

2. 復元する

   作成されたボールトの zip バックアップを復元します。復元されると、すべてのパスワードとキーはバックアップ作成時の値に戻ります。

   復元を使用すると、複数のサーバー上のパスワードとキーを同期できます。たとえば、次の手順に従います。1) AU の暗号化キーを変更します。 2) ボールトのバックアップを作成します。 3) 各 AU に Vault バックアップを復元します。

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、デバイスのパスワードを暗号化または復号化するために使用される AU 暗号化キーを登録または変更します。

   暗号化キーを変更する場合は、アップグレードまたはインストール後に復元できるように、新しいセキュリティ構成をバックアップする必要があります。

   このオプションは Linux でのみ使用可能であることに注意してください。

   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、最小 2048 ビットの 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してはなりません。
   - スクリプトは、生のエンコードされたコンテンツ (PEM 形式のみ) を返す必要があります。
   - 外部スクリプトには *execute* 権限が必要です。

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 (現在のキーを登録解除し、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、公開キー ID と秘密キー 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

   取得ユーザーのパスワードと取得ユーザー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提供される値です。

6. **Truststore**のパスワードを変更する

   トラストストアのパスワードを変更します。

7. キーストアのパスワードを変更する

   キーストアのパスワードを変更します。

8. コレクターパスワードの暗号化

   データ コレクターのパスワードを暗号化します。

9. 出口

SecurityAdmin ツールを終了します。

設定するオプションを選択し、プロンプトに従います。

ツールを実行するユーザーを指定する

制御されたセキュリティ重視の環境の場合は、*cisys* グループがなくても、特定のユーザーに SecurityAdmin ツールを実行させたい場合があります。

これを実現するには、AU ソフトウェアを手動でインストールし、アクセスを許可するユーザー/グループを指定します。

- API を使用して、CI インストーラーを AU システムにダウンロードし、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 ドキュメント (*Admin > API Access* で *API Documentation* リンクを選択) を参照し、*GET /au/oneTimeToken* API セクションを見つけます。
  - 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ー 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) とインストーラー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ー ファイルを AU システムにコピーし、解凍します。
- ファイルが含まれているフォルダに移動し、ユーザーとグループを指定して、インストーラをルートとして実行します。

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

指定されたユーザー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。

プロキシの更新または削除

SecurityAdmin ツールを *-pr* パラメータ付きで実行することで、取得ユニットのプロキシ情報を設定または削除できます。

```
[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
```

コマンドを実行した後、取得ユニットを再起動する必要があります。

プロキシを更新するには、コマンドは

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

外部キーの取得

UNIX シェル スクリプトを提供すると、取得ユニットによってそのスクリプトが実行され、キー管理システム

から 秘密キー と 公開キー 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。 キー タイプは「公開」または「秘密」のいずれかです。キー タイプが「public」の場合、スクリプトは公開キーを返す必要があります。キー タイプが「private」の場合、秘密キーを返す必要があります。

キーを取得ユニットに送り返すには、スクリプトでキーを標準出力に出力する必要があります。スクリプトはキーのみを標準出力に出力する必要があります。他のテキストを標準出力に出力してはなりません。要求されたキーが標準出力に印刷されると、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 ツールを使用して取得ユニットに登録する必要があります。これにより、取得ユニットとともにスクリプトが実行されます。スクリプトには、ルートおよび「cisys」ユーザーに対する *read* および *execute* 権限が必要です。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 スクリプトを取得ユニット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されるキー識別子。
入力パラメータ: キータイプ	公立か私立か。
出力	要求されたキーは標準出力に印刷する必要があります。現在、2048 ビットの RSA キーがサポートされています。キーは以下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	成功した場合の終了コードはゼロです。その他の終了値はすべて失敗とみなされます。
スクリプト権限	スクリプトには、ルートおよび「cisys」ユーザーの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ログに記録されます。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 を使用すると、パスワードを暗号化して、API 経由でデータ コレクターに渡すことができます。

SecurityAdmin ツールを対話モードで起動し、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を入力するよう求められます。入力した文字は画面に表示されないことに注意してください。プロンプトが表示されたらパスワードを再入力します。

あるいは、スクリプト内でコマンドを使用する場合は、コマンド ラインで *securityadmin.sh* を "-enc" パラメ

ータとともに使用し、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。

[対話モードのパスワード暗号化、幅=640]

暗号化されたパスワードをデータ コレクターに送信するには、Data Collection API を使用できます。この API の Swagger は、管理 **> API** アクセス で「API ドキュメント」リンクをクリックすると見つかります。 「データ収集」API タイプを選択します。この例では、*data_collection.data_collector* の見出しの下で、*/collector/datasources* POST API を選択します。

[データ収集用のAPI]

preEncrypted オプションを *True* に設定すると、API コマンドを通じて渡すパスワードは すでに暗号化されている ものとして扱われ、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、以前に暗号化したパスワードを適切な場所に貼り付けるだけです。

[APIの例、幅=600]

著作権に関する情報

商標に関する情報