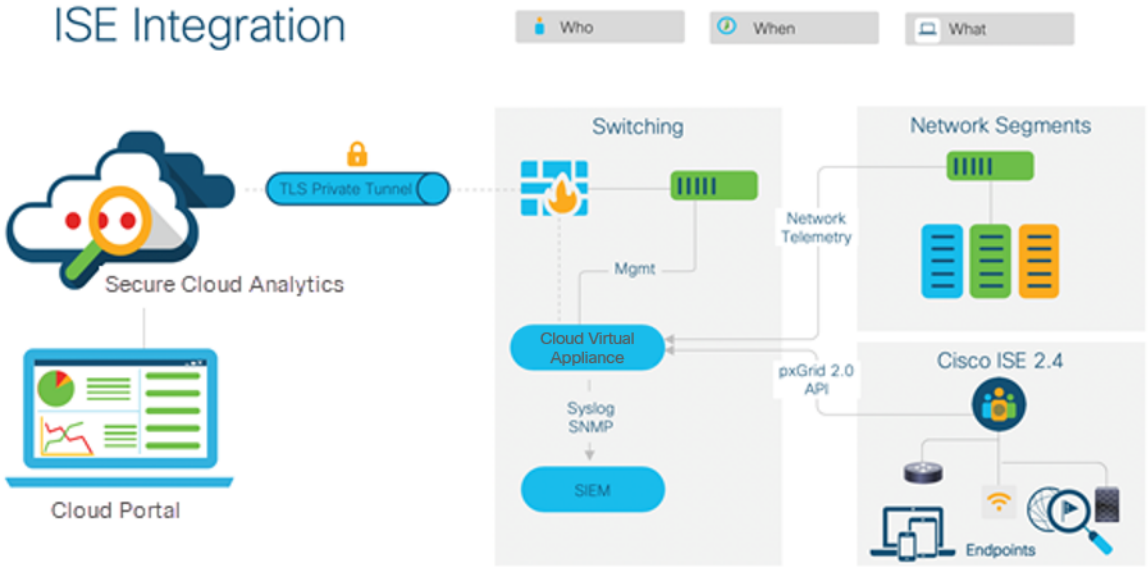
Cisco Secure Cloud Analytics

ISE 統合ガイド

目次

Secure Cloud Analytics ISE 統合の概要

Cisco Secure Cloud Analytics（以前の Stealthwatch Cloud）は、pxGrid を使用して Cisco Identity Services Engine（ISE）からユーザ属性データを取得できるようになりました。この統合により、Secure Cloud Analytics イベントビューアでのユーザアクティビティのレポートが可能になります。次の図に、Secure Cloud Analytics の ISE との統合のアーキテクチャ例の概要を示します。

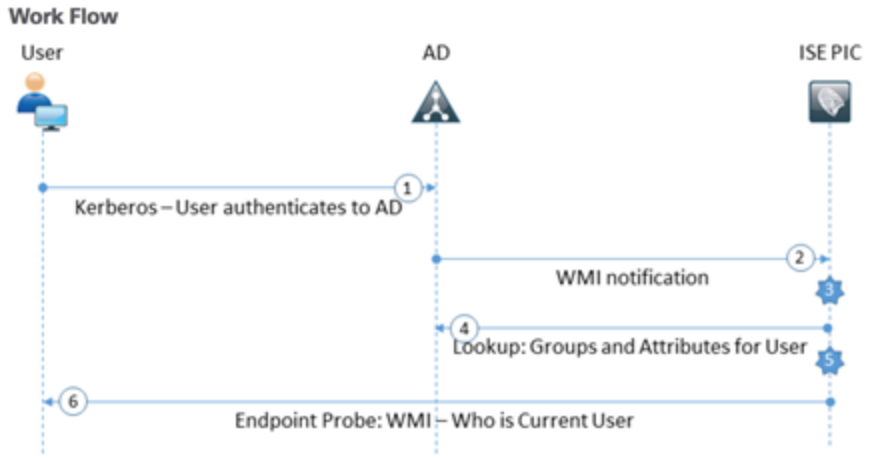


WMI を使用して AD サーバから ISE にユーザセッションをパッシブに取得する基本的なワークフローには、次の手順が含まれます。

1. ユーザがワークステーションにログインし、AD 経由で認証されます。
2. WMI は、この認証について ISE パッシブ ID に通知します。
3. ISE は、セッションディレクトリにバインディング `Username:IP_Address` を追加します。
4. ISE は AD ユーザグループと属性を取得します。
5. ISE はこの情報をセッションディレクトリに保存します。
6. ISE は、現在のユーザステータスを探索するように WMI に指示します。

WMI の詳細については、https://msdn.microsoft.com/en-us/library/aa384642(v=vs.85).aspx を参照してください。

次の図は、このワークフローについて説明しています。



以降のガイドでは、次に示す項目の設定方法を説明します。

- ISE パッシブ ID コネクタ（ISE PIC）と Active Directory（AD）。Windows Management Instrumentation（WMI）にマッピングし、ISE PIC が AD からユーザセッションを取得できるようにします。
- そのユーザ情報を取得するサブスクライバとしての Secure Cloud Analytics センサー（以前の Stealthwatch Cloud センサー）。

> Secure Cloud Analytics との統合には、ISE バージョン 2.4 以降が必要です。

手順の概要

正常に統合するには、次の手順を完了してください。

1. **Secure Cloud Analytics ISE 統合の前提条件**を確認します。
2. Active Directory を展開している場合は、「**ISE PIC の設定**」を参照してください。
   アクセス制御に ISE を使用する場合は、このセクションをスキップしてください。
3. **Secure Cloud Analytics センサーバージョンの確認**して、センサーが最新であることを確認します。
4. **ISE との統合**の手順に従って、統合を設定します。基本設定または手動設定を選択できます。

Secure Cloud Analytics ISE 統合の前提条件

Secure Cloud Analytics と ISE を統合するには、次のコンポーネントを展開します。

コンポーネント	必須	注記
Identity Services Engine（ISE）	○	バージョン 2.4 以降
Secure Cloud Analytics センサー	○	バージョン 5.1.0 以降
Microsoft Active Directory（AD）	推奨	外部 ID ソースとして AD を Windows Management Instrumentation（WMI）にマッピングします。詳細については、このリンクを参照してください。
ISE パッシブ ID コネクタ（ISE PIC）	○（AD が展開されている場合）	適用対象外

設定を完了するには、次の情報も必要です。

- AD を外部 ID ストアとして設定したときに設定した AD 参加パスワード
- ISE サーバの IP アドレスおよびホスト名

ISE PIC の設定

アクセス制御に Active Directory（AD）を使用している場合は、ポリシーサービスノード（PSN）で ISE PIC を設定します。次に、ドメインで AD ログイン情報と WMI を設定します。最後に、ISE UI からライブ認証をテストします。

ポリシーサービスノードで ISE PIC を設定します。

はじめる前に

- ISE UI に管理者としてログインします。

手順

1. [管理（Administration）] > [システム（System）] > [展開（Deployment）] の順に選択します。
2. PSN ノードを選択します。
3. [パッシブIDサービスの有効化（Enable Passive Identity Service）] を選択します。
4. [保存（Save）] をクリックします。

AD クレデンシャルとWMI を使用してドメインを設定します。

手順

1. ISE UI から、[ワークセンター（Work Centers）] > [PassiveID] > [プロバイダー（Providers）] の順に選択します。
2. メインの Active Directory ノードを選択します。
3. [PassiveID] タブをクリックします。
4. ドメインを選択し、[編集（Edit）] をクリックします。
5. AD を外部 ID ストアとして設定したときに設定した AD 参加**パスワード**を入力します。
6. [保存（Save）] をクリックします。
7. [テスト（Test）] をクリックしてクレデンシャルを確認します。次の選択肢があります。
   - 接続が正常に確立されたことを示すメッセージが表示されたら、次の手順に進みます。
   - エラーメッセージが表示された場合は、パスワードを確認して再試行してください。
8. [PassiveID] タブをクリックします。
9. ドメインを選択し、[WMIの設定（Config WMI）] をクリックします。
10. 設定が完了するまで数分待ちます。
11. 設定が終了したら、[OK] をクリックします。

ライブ認証を検証します。

手順

- ISE UI から、[ワークセンター（Work Centers）]>[PassiveID]>[概要（Overview）]>[ライブセッション（Live Sessions）] の順に選択します。設定が正しい場合は、ライブ認証がここに表示されます。ライブ認証が表示されない場合は、設定を確認します。

Secure Cloud Analytics センサーバージョンの確認

ISE UI 統合では、Secure Cloud Analytics センサー バージョン 5.1.0 以降を展開する必要があります。これにより、センサーは pxGrid 2.0 を介して ISE と通信し、ユーザセッション情報を受信できます。

センサーバージョンの確認：

はじめる前に

- センサーに SSH ログインします。

手順

- コマンドラインで次のコマンドを入力して、Enter キーを押します。

```
cat /opt/obsrvbl-ona/version
```

コンソールに 5.1.0 以降ではないバージョンが表示される場合は、Secure Cloud Analytics UI からダウンロードした ISO イメージを使用してセンサーを再展開します。詳細については、https://ebooks.cisco.com/story/swc-sensor-install.html を参照してください。

センサーを再展開せずに、センサーの設定をバックアップし、センサーパッケージを手動でアップグレードして、設定を復元する方法もあります。

> ⚠ この手順で操作を誤ると、センサーが使用できない状態になる可能性があります。

センサーのパッケージを現在のバージョンにアップグレードする：

はじめる前に

- センサーに SSH ログインします。

手順

1. コマンドラインから次のコマンドを入力し、Enter キーを押してセンサーサービスを停止します。プロンプトが表示されたら、ルートパスワードを入力します。

   ```
   sudo systemctl stop obsrvbl-ona.service
   ```

2. 次のコマンドを入力し、Enter キーを押して `config.auto` 構成ファイルをバックアップします。

   ```
   sudo cp /opt/obsrvbl-ona/config.auto
   ```

3. 次のコマンドを入力し、Enter キーを押して config.local 構成ファイルをバックアップします。

   ```
   sudo cp /opt/obsrvbl-ona/config.local
   ```

4. 次のコマンドを入力し、Enter キーを押してセンサーサービスパッケージを削除します。

   ```
   sudo apt remove --purge ona-service
   ```

5. 次のコマンドを入力して Enter キーを押し、最新のセンサーサービスパッケージをダウンロードします。

   ```
   sudo wget https://s3.amazonaws.com/onstatic/

   ona-service/master/ona-service_UbuntuXenial_amd64.deb
   ```

6. 次のコマンドを入力し、Enter キーを押してセンサーサービスパッケージをインストールします。

   ```
   sudo apt install ./ona-service_UbuntuXenial_amd64.deb
   ```

7. 次のコマンドを入力し、Enter キーを押して config.auto 構成ファイルのファイル所有権設定を変更します。

   ```
   sudo chown obsrvbl_ona: config.auto
   ```

8. 次のコマンドを入力し、Enter キーを押して config.local 構成ファイルのファイル所有権設定を変更します。

   ```
   sudo chown obsrvbl_ona: config.local
   ```

9. 次のコマンドを入力し、Enter キーを押して config.auto 構成ファイルを復元します。

   ```
   sudo cp config.auto /opt/obsrvbl-ona/config.auto
   ```

10. 次のコマンドを入力し、Enter キーを押して config.local 構成ファイルを復元します。

    ```
    sudo cp config.local /opt/obsrvbl-ona/config.local
    ```

11. 次のコマンドを入力し、Enter キーを押してセンサーサービスを再開します。

    ```
    sudo systemctl restart obsrvbl-ona.service
    ```

ISE との統合

ISE と統合するように Secure Cloud Analytics センサーを設定するには、次のいずれかの手順に従います。

- **ISE と統合するための基本設定**
- **ISE との統合のための手動設定**

ISE と統合するための基本設定

統合を設定する前に、前述の手順を完了してください。詳細については、「**手順の概要**」を参照してください。

基本セットアップの設定

はじめる前に

- Secure Cloud Analytics ポータルにログインします。

手順

1. [設定(Settings)]>[統合(Integrations)]>[ISE] に移動します。
2. 画面の右側に表示される指示に従います。
3. セットアップ手順を完了すると、ステータスアイコンが緑色に変わります。これには最大 30 分かかる場合があります(ISE セッションのボリュームによって異なります)。
4. ステータスアイコンが緑色に変わったら、[調査(Investigate)]>[イベントビューア(Event Viewer)]>[ISE] の順に移動します。ISE イベントが表示されていることを確認します。

トラブルシューティング

統合が機能しなくなる一般的な問題がいくつかあります。

はじめる前に

- センサーに SSH 接続し、管理者としてログインします。

手順

Secure Cloud Analytics ポータルが ISE と統合されていない場合は、センサーファイルを確認します。ファイルは、`/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log` にあります。次に、ファイルにエラーメッセージがあるかどうか確認します。次の各セクションで詳細を説明しています。

- `Name or service not known`:**DNS の問題**を参照してください
- `SSLCertVerificationError`:「**証明書の問題**」を参照してください
- `No sessions since...`:「**セッションが存在しない**」を参照してください

DNS の問題

`/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log` でセンサーファイルを確認します。`Name or service not known` を含む行が存在する場合、センサーは設定された ISE サーバのホスト名（例：ise.example.org）を解決できません。

次の操作を試してください。

- Web インターフェイスでサーバ名を関連する IP アドレスに置き換えます。または
- SSH 経由でセンサーにアクセスし、`/etc/hosts` ファイルにエントリを追加します。

証明書の問題

`/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log` でセンサーファイルを確認します。`SSLCertVerificationError` を含む行が存在する場合、ISE サーバは、設定したホスト名以外のホスト名の証明書を センサー に提示している可能性があります。

次のことを試してください。

- ISE サーバインターフェイスにログインし、証明書を確認します。正しいホスト名で証明書を再設定します。
- ホスト名ではなくIP アドレスを使用して ISE サーバを再設定します。

セッションが存在しない

`/opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log` でセンサーファイルを確認します。`No sessions since...` を含む行が存在する場合、設定は正しいですが、pxGrid から使用できるセッションがありません。

次を確認します。

- ISE サーバは、Active Directory、RADIUS、TACACS などと統合するように設定されている。
- ISE サーバにログインしているアクティブなセッションが存在する。
- ISE サーバとセンサーの時刻が正しい。

ISE との統合のための手動設定

Make sure you complete the preceding procedures before you configure the integration. 詳細については、「**手順の概要**」を参照してください。

要件

ISE サーバに対してセッションデータを照会するようにオンプレミスセンサーを設定するには、次のものが必要です。

- クライアント証明書
- RSA 形式のクライアントキーと、クライアントキーを復号化するためのパスフレーズ
- サーバ証明書とチェーン

証明書バンドルの生成

はじめる前に

- Secure Cloud Analytics ポータルにログインします。

手順

1. [設定(Settings)]>[統合(Integrations)]>[ISE] に移動します。
2. ページの指示に従って、証明書バンドルを生成します。

   次に、ファイルリストの例を示します。

   ```
   CertificateServicesEndpointSubCA-ise_.cer
   CertificateServicesNodeCA-ise_.cer
   CertificateServicesRootCA-ise_.cer
   SSL.comRootCertificationAuthorityRSA_.cer
   SSL.comRSASSLsubCA_.cer
   swc-sensor_.cer
   swc-sensor_.key
   ```

   次の手順では、この例のリストを使用します。

3. 関連するファイルをターゲットセンサーに転送します(たとえば WinSCP を使用)。

クライアントキーの入手

1. 次のコマンドを実行して、クライアントキーを復号化します。パスフレーズの入力も求められます。

   ```
   openssl rsa -in swc-sensor_.key -out decrypted-swc-
   sensor_.key
   ```

2. 復号後、ファイルの最初の行は次のようになります。

   -----BEGIN RSA PRIVATE KEY-----

証明書チェーンの作成

1. クライアント証明書ファイルを特定します。使用している例では `swc-sensor_.cer` です。
2. クライアント証明書ファイルを除くすべての証明書ファイルをリンクします。

```
cat CertificateServicesEndpointSubCA-ise_.cer \
CertificateServicesNodeCA-ise_.cer \
CertificateServicesRootCA-ise_.cer \
SSL.comRootCertificationAuthorityRSA_.cer > server_
chain.cer
```

   結果のファイルには、複数の -----BEGIN CERTIFICATE----- 行と -----END CERTIFICATE----- 行が含まれているはずです。

設定の更新

ファイルの移動

次のコマンドを実行して、クライアント証明書、復号化されたクライアントキー、およびサーバチェーンを永続的な場所に移動します。

1. `sudo mkdir /etc/ise_poller`
2. `sudo mv swc-sensor_.cer /etc/ise_poller/ise_client_cert.pem`
3. `sudo mv decrypted-swc-sensor_.key /etc/ise_poller/ise_client_key.pem`
4. `sudo mv server_chain.cer /etc/ise_poller/ise_server_cert.pem`
5. `sudo chown obsrvbl_ona: /etc/ise_poller/*`
6. `sudo chmod 0600 /etc/ise_poller/*`

センサーの設定

前の手順で移動したファイルをポイントするようにセンサーを設定します。

1. `/opt/obsrvbl-ona/config.local` ファイルを開き、次の例に示すように行を追加します。`OBSRVBL_ISE_SERVER_NAME` が、ISE サーバのプライマリノードに一致

するように設定してください。

```
OBSRVBL_ISE_POLLER="true"
OBSRVBL_ISE_SERVER_NAME="your-ise-server.local"
OBSRVBL_ISE_CLIENT_CERT="/etc/ise_poller/ise_client_
cert.pem"
OBSRVBL_ISE_CLIENT_KEY="/etc/ise_poller/ise_client_
key.pem"
OBSRVBL_ISE_CA_CERT="/etc/ise_poller/ise_server_cert.pem"
```

センサーサービスの再起動

1. 次のコマンドを実行します。

   ```
   sudo systemctl restart obsrvbl-ona.service
   ```

統合の確認

はじめる前に

- Secure Cloud Analytics ポータルにログインします。

手順

1. [設定(Settings)]>[統合(Integrations)]>[ISE] に移動します。
2. 設定が完了すると、ステータスアイコンが緑色に変わります。これには最大 30 分かかる場合があります(ISE セッションのボリュームによって異なります)。
3. ステータスアイコンが緑色に変わったら、[調査(Investigate)]>[イベントビューア(Event Viewer)]>[ISE] の順に移動します。ISE イベントが表示されていることを確認します。

トラブルシューティング

1. 次の センサー ファイルを確認し、エラーメッセージを確認します。

   ```
   /opt/obsrvbl-ona/logs/ona_service/ona-ise-poller.log
   ```

   ファイルが `SSLCertVerificationError` で終了し、証明書チェーンに `self signed certificate in certificate chain` という文字列が含まれている場合、サーバ証明書チェーンは不完全です。手順を確認し、関連するすべての証明書が証明書チェーンに含まれていることを確認します。

その他のリソースおよびサポート

さらにサポートが必要な場合は、support@obsrvbl.com まで電子メールでお問い合わせください。

Secure Cloud Analytics の詳細については、次を参照してください。

- 概要については、https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html を参照してください。
- 60 日間の無料トライアルに登録するには、https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html にアクセスしてください。
- ドキュメントリソースについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html を参照してください。
- Secure Cloud Analytics 無料トライアルのガイドなど、インストールおよび設定ガイドについては、https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html を参照してください。

変更履歴

リビジョン	改訂日	説明
1.0	2019 年 11 月 21 日	最初のバージョン
1.1	2020 年 11 月 4 日	Stealthwatch Cloud ISE 統合の最新情報に基づいて更新。
1.2	2021 年 7 月 8 日	• センサー のバージョンを更新。 • 「センサーのパッケージを現在のバージョンにアップグレードする」の手順を更新。 • 統合の手順を更新。基本設定と手動設定を追加。 • ブランド用語を更新。
1.3	2021 年 8 月 6 日	ロゴを更新。

著作権情報