# Secure Firewall ASA イベントのモニタリング



# Secure Event Connector について

Secure Event Connector（SEC）は、Security Analytics and Logging SaaS ソリューションのコンポーネントです。ASA および FDM による管理デバイスからイベントを受信し、シスコクラウドに転送します。Security Cloud Control では、**[Event Logging]** ページにイベントが表示され、すべてのデバイスからのセキュリティイベントを一元的に分析できます。

SEC は、ネットワークに展開された Secure Device Connector、またはネットワークに展開された独自の Security Cloud Control コネクタ仮想マシン、あるいは AWS 仮想プライベートクラウド（VPC）にインストールします。

### Secure Event Connector ID

Cisco Technical Assistance Center（TAC）などの Security Cloud Control サポートと連携する場合、SEC の ID が必要になる場合があります。この ID は、Security Cloud Control の [セキュアコネクタ（Secure Connectors）] ページで確認できます。SEC ID を確認するには、次の手順を実行します。

1. 左側の Security Cloud Control メニューから **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** を選択します。
2. 確認する SEC をクリックします。
3. SEC ID は、[詳細（Details）] ペインの [テナントID（ Tenant ID）] の上に表示されている ID です。

**関連情報**：

- Cisco Security Analytics and Logging for ASA Devices
- SDC 仮想マシンへの Secure Event Connector のインストール （2 ページ）
- Security Cloud Control VM イメージを使用してテナントに複数の SEC をインストールする
- 作成した VM イメージを使用してテナントに複数の SEC をインストールする
- Terraform モジュールを使用した AWS VPC 上での Secure Event Connector のインストール（22 ページ）
- Secure Event Connector の削除
- Cisco Security Analytics and Logging（SaaS）をプロビジョニング解除する

# Secure Event Connector をインストールする

Secure Event Connector（SEC）は、SDC の有無にかかわらず、テナントにインストールできます。

SEC は Secure Device Connector（あれば）と同じ仮想マシンにインストールすることも、ネットワーク内で維持管理している独自の Security Cloud Control コネクタ仮想マシンにインストールすることもできます。

## SDC 仮想マシンへの Secure Event Connector のインストール

Secure Event Connector（SEC）は、Cisco ASA や FDM による管理デバイスからイベントを受信し、Cisco Cloud に転送します。Security Cloud Control は **[Event Logging]** ページにイベントを表示し、管理者はそこで、または Cisco Secure Cloud Analytics を使用してイベントを分析できます。

SEC は Secure Device Connector（あれば）と同じ仮想マシンにインストールすることも、ネットワーク内で維持管理している独自の Security Cloud Control コネクタ仮想マシンにインストールすることもできます。

この記事では、SDC と同じ仮想マシンに SEC をインストールする方法について説明します。他にも SEC をインストールする場合は、Security Cloud Control イメージを使用した SEC のインストール （5 ページ） または VM イメージを使用した SEC のインストール （13 ページ）を参照してください。

### 始める前に

- Cisco Security and Analytics Logging のライセンスを購入します。Cisco Security and Analytics Logging を最初に試す場合は、Security Cloud Control にログインし、メインナビゲーションバーで **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択し、**[Request Trial]** をクリックします。
- SDC がインストールされていることを確認します。詳細については、Secure Device Connector および Secure Event Connector を実行するための VM の展開を参照してください。
- SDC が Security Cloud Control と通信していることを確認します。
  1. 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。
  2. SEC をインストールする前に、SDC の最後のハートビートが 10 分以内であったこと、および SDC のステータスがアクティブであることを確認してください。
- システム要件：SDC を実行している仮想マシンに追加の CPU とメモリを割り当てます。
  - CPU：SEC 用に**追加**の 4 つの CPU を割り当て、CPU の合計が 6 つとなるようにします。
  - メモリ：SEC 用に**追加**の 8 GB のメモリを割り当てて、メモリの合計が 10 GB となるようにします。

    SEC に対応するように VM の CPU とメモリを更新したら、VM の電源を入れ、[セキュアコネクタ（Secure Connectors）] ページに SDC が「アクティブ」状態であることが示されていることを確認します。

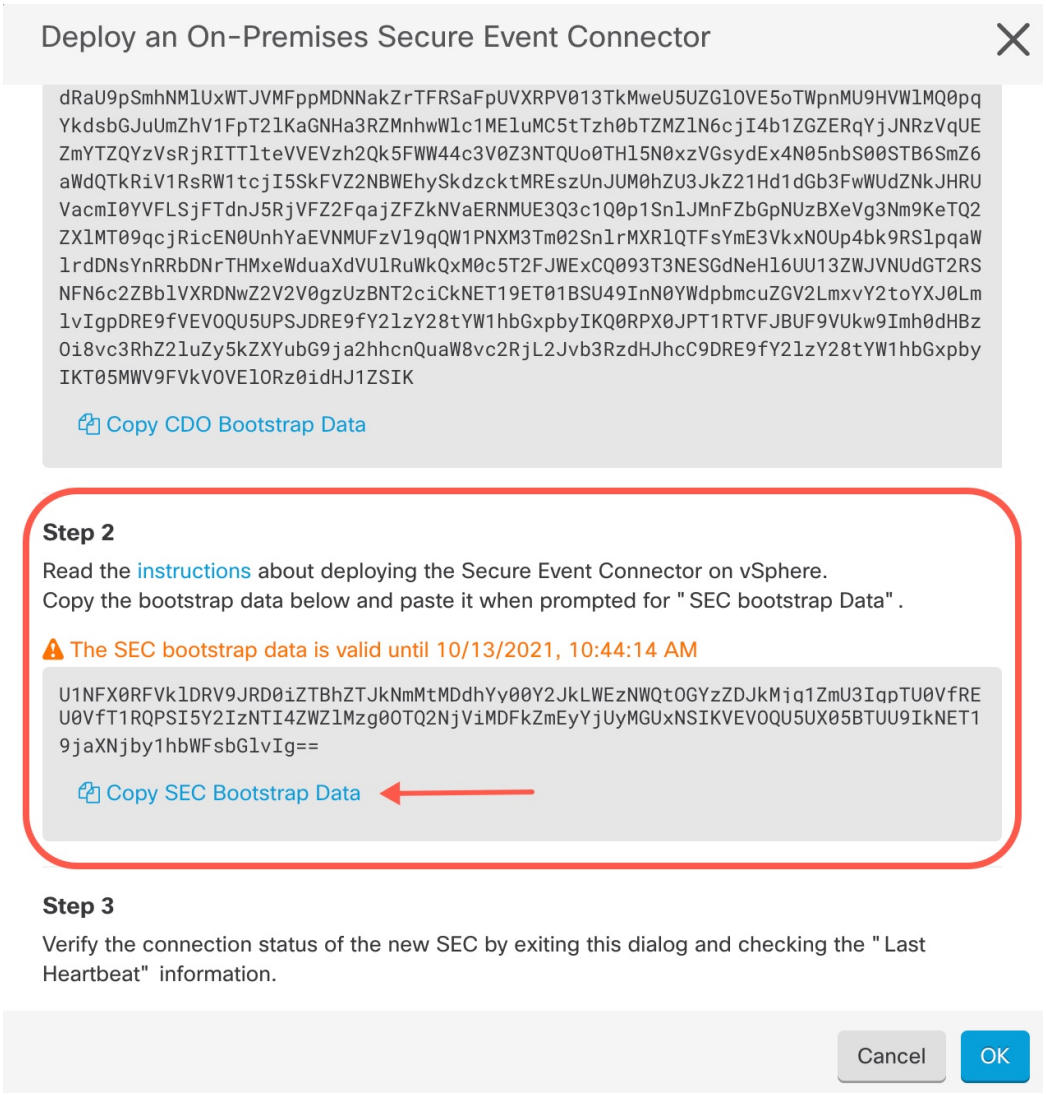
### 手順

**ステップ 1** Security Cloud Control にログインします。

**ステップ 2** 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

**ステップ 3**  アイコンをクリックし、[Secure Event Connector] をクリックします。

**ステップ 4** ウィザードのステップ 1 をスキップして、ステップ 2 に進みます。ウィザードのステップ 2で、 [SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。




**ステップ 5** ターミナルウィンドウを開き、SDC に「cdo」ユーザーとしてログインします。

**ステップ 6** ログインしたら、「sdc」ユーザーに切り替えます。パスワードの入力を求められたら、「cdo」ユーザーのパスワードを入力します。これらのコマンドの例を次に示します。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

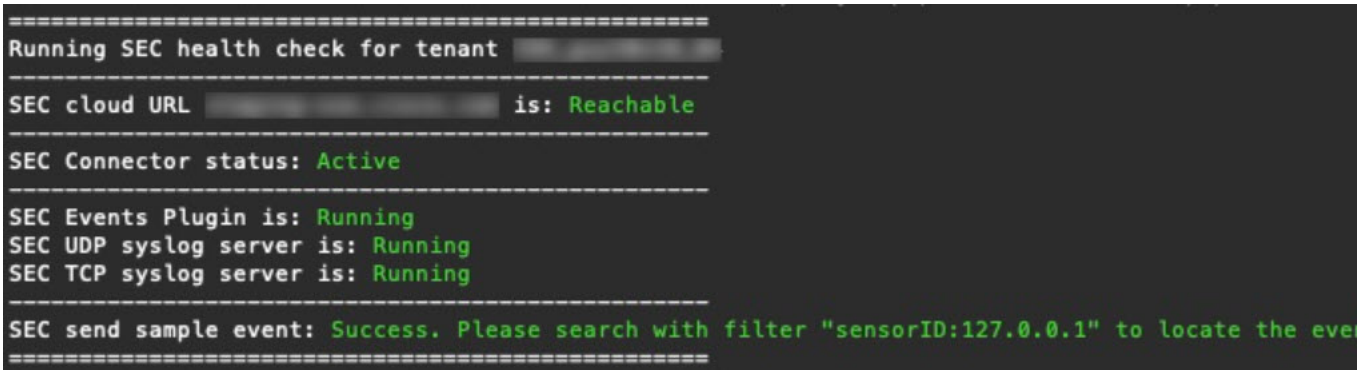
**ステップ 7** プロンプトで、**sec.sh setup** スクリプトを実行します。

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

**ステップ 8** プロンプトの最後に、手順4でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of Security Cloud Control:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。




登録に失敗したことや SEC のオンボーディングに失敗したことを示すメッセージを受け取った場合は、「Secure Event Connector オンボーディングのトラブルシューティング」を参照してください。

**ステップ 9** SDC と SEC が実行されている VM に追加の構成が必要かどうかを判断します。

- SDC を独自の仮想マシンにインストールした場合は、作成した VM にインストールされた SDC および Security Cloud Control コネクタの追加設定 （18 ページ） を続行します。
- Security Cloud Control イメージを使用して SDC をインストールした場合は、「次に行う作業」に進みます。

---

**次のタスク**

ASA デバイスに安全なロギング分析（SaaS）を導入する （45 ページ） に戻ってください。

**関連情報**：

- Secure Device Connector のトラブルシュート
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング
- Secure Event Connector の登録失敗のトラブルシューティング

# Security Cloud Control イメージを使用した SEC のインストール

Secure Event Connector（SEC）は、Cisco ASA と FTD からのイベントを Cisco Cloud に転送し、Security Cloud Control の**[Event Logging]** ページで表示できるようにします。

テナントに複数の Secure Event Connector（SEC）をインストールし、インストールした任意の SEC に ASA および FDM 管理対象デバイスからイベントを送信できます。複数の SEC を使用

すると、さまざまな場所に SEC をインストールし、Cisco Cloud にイベントを送信する作業を分散できます。

SEC のインストールは、2 つの部分からなるプロセスです。

1. Security Cloud Control VM イメージを使用して Secure Event Connector をサポートするための Security Cloud Control コネクタのインストール （6 ページ） インストールする SEC ごとに 1 つの Security Cloud Control コネクタが必要です。Security Cloud Control コネクタは、Secure Device Connector（SDC）とは異なります。
2. Security Cloud Control コネクタ仮想マシンへの Secure Event Connector のインストール （19 ページ）。

（注） 独自の VM を作成して Security Cloud Control コネクタを作成する場合は、「作成した VM イメージを使用してテナントに複数の SEC をインストールする」を参照してください。

**次に行う作業：**

Security Cloud Control VM イメージを使用して Secure Event Connector をサポートするための Security Cloud Control コネクタのインストール （6 ページ） に進みます。

# Security Cloud Control VM イメージを使用して Secure Event Connector をサポートするための Security Cloud Control コネクタのインストール

**始める前に**

- Cisco Security and Analytics Logging のライセンスを購入します。

  Security Analytics and Logging のトライアル版をリクエストする場合は、Security Cloud Control にログインし、メインナビゲーションバーで **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。

- Security Cloud Control は、厳密な証明書チェックを必要とし、Security Cloud Control コネクタとインターネットの間の Web/コンテンツプロキシ検査をサポートしていません。プロキシサーバーを使用している場合は、Security Cloud Control コネクタと Security Cloud Control の間のトラフィックの検査を無効にします。
- このプロセスでインストールされる Security Cloud Control コネクタには TCP ポート 443 でのインターネットへの完全なアウトバウンドアクセスが必要です。
- Security Cloud Control コネクタで適切なネットワーク接続を確立するには、「Secure Device Connector を使用した Security Cloud Control への接続」を参照してください。
- Security Cloud Control は、vSphere Web クライアントまたは ESXi Web クライアントを使用した Security Cloud Control コネクタ VM OVF イメージのインストールをサポートしています。

- Security Cloud Control は、VM vSphere デスクトップクライアントを使用した Security Cloud Control コネクタ VM OVF イメージのインストールをサポートしていません。
- ESXi 5.1 ハイパーバイザ。
- Security Cloud Control コネクタと SEC のみをホストすることを目的とした VM のシステム要件は以下のとおりです。
  - VMware ESXi ホストには 4 つの vCPU が必要です。
  - VMware ESXi ホストには 8 GB 以上のメモリが必要です。
  - VMware ESXi では、プロビジョニングの選択に応じて、仮想マシンをサポートするために 64GB のディスク容量が必要です。
- インストールを開始する前に、次の情報を収集します。
  - Security Cloud Control コネクタ VM に使用する静的 IP アドレス。
  - インストールプロセス中に作成する **root** ユーザーと Security Cloud Control ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - SDC アドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- Security Cloud Control Connector 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。

### 手順

**ステップ 1** Security Cloud Control コネクタを作成する Security Cloud Control テナントにログオンします。

**ステップ 2** 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

**ステップ 3**  アイコンをクリックし、[Secure Event Connector] をクリックします。

**ステップ 4** ステップ 1 で、[Security Cloud ControlコネクタVMイメージのダウンロード（Download the Security Cloud Control Connector VM image）] をクリックします。これは、SEC をインストールする特別なイメージです。最新のイメージを確実に使用するために、常に Security Cloud Control コネクタ VM をダウンロードしてください。


**ステップ 5** .zip ファイルからすべてのファイルを抽出します。これらは、次のようなものです。

- Security Cloud Control-SDC-VM-ddd50fa.ovf
- Security Cloud Control-SDC-VM-ddd50fa.mf
- Security Cloud Control-SDC-VM-ddd50fa-disk1.vmdk

**ステップ 6** vSphere Web クライアントを使用して、管理者として VMware サーバーにログオンします。

（注）
VM vSphere デスクトップクライアントは使用しないでください。

**ステップ 7** プロンプトに従って、OVF テンプレートからオンプレミスの Security Cloud Control コネクタ仮想マシンを展開します（テンプレートを展開するには、.ovf、.mf、および .vdk ファイルが必要です）。

**ステップ 8** セットアップが完了したら、VM の電源を入れます。

**ステップ 9** 新しい Security Cloud Control コネクタ VM のコンソールを開きます。

**ステップ 10** Security Cloud Control ユーザーとしてログインします。デフォルトのパスワードは `adm123` です。

**ステップ 11** プロンプトで、`sudo sdc-onboard setup` と入力します。

```
[cdo@localhost ~]$ sudo sdc-onboard setup
```

**ステップ 12** プロンプトで、Security Cloud Control ユーザーのデフォルトのパスワード（`adm123`）を入力します。

**ステップ 13** プロンプトに従って、**root** ユーザーの新しいパスワードを作成します。

**ステップ 14** プロンプトに従って、Security Cloud Control ユーザーの新しいパスワードを作成します。

**ステップ 15** プロンプトに従って、Security Cloud Control ドメイン情報を入力します。

**ステップ 16** Security Cloud Control コネクタ VM に使用する静的 IP アドレスを入力します。

**ステップ 17** Security Cloud Control コネクタ VM がインストールされているネットワークのゲートウェイ IP アドレスを入力します。

**ステップ 18** Security Cloud Control コネクタの NTP サーバーのアドレスまたは FQDN を入力します。

**ステップ 19** プロンプトで、Docker ブリッジの情報を入力するか、該当しない場合は空白のままにして、Enter キーを押します。

**ステップ 20** 入力内容を確定します。

**ステップ 21** 「Would you like to setup the SDC now?」というプロンプトで、**n** を入力します。

**ステップ 22** Security Cloud Control ユーザーとしてログインして、Security Cloud Control コネクタへの SSH 接続を作成します。

**ステップ 23** プロンプトで、**sudo sdc-onboard bootstrap** と入力します。

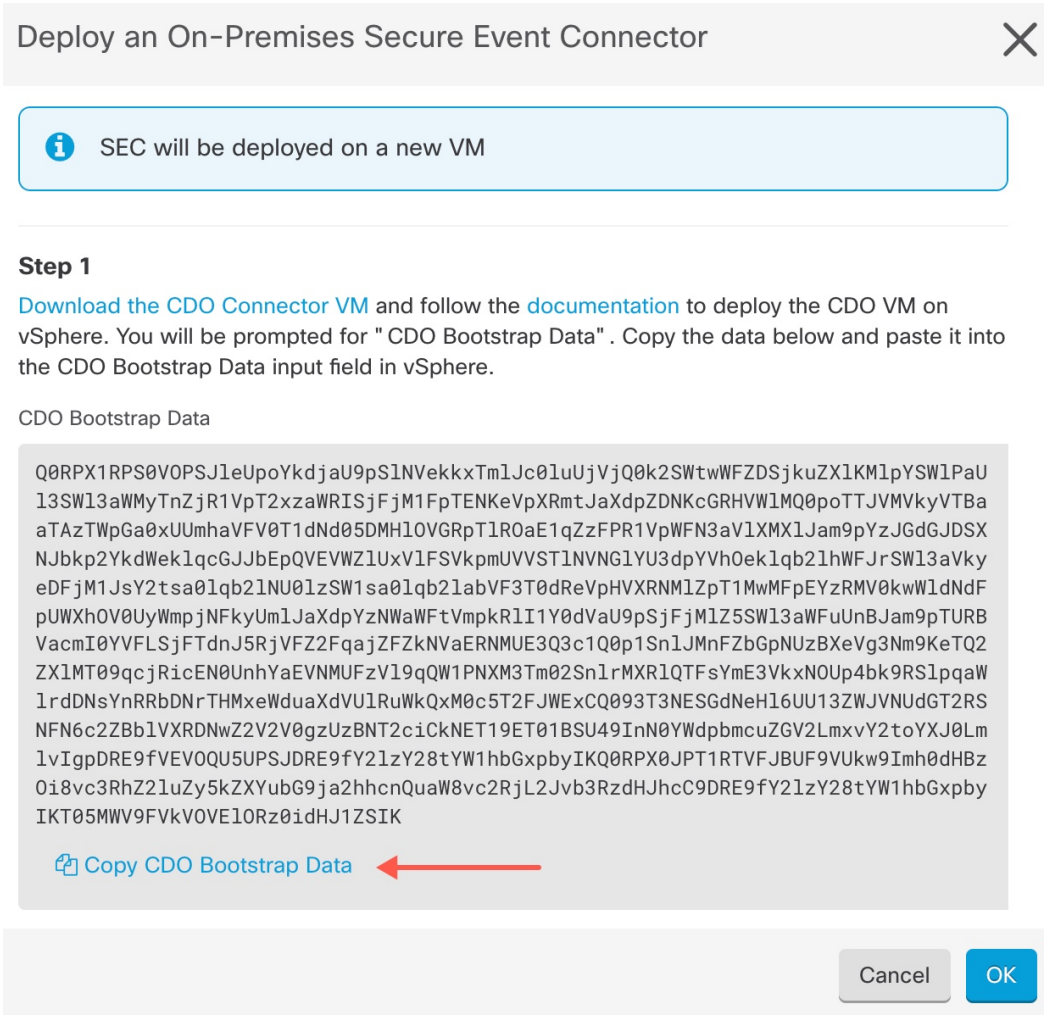
```
[cdo@localhost ~]$ sudo sdc-onboard bootstrap
```

**ステップ 24** プロンプトで、Security Cloud Control ユーザーのパスワードを入力します。

**ステップ 25** プロンプトで、Security Cloud Control に戻り、Security Cloud Control ブートストラップデータをコピーして、SSH セッションに貼り付けます。Security Cloud Control ブートストラップデータをコピーするには、次の手順を実行します。

1. Security Cloud Control にログインします。
2. 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。
3. オンボードを開始した Secure Event Connector を選択します。ステータスが「Onboarding」と表示されます。
4. [アクション（Actions）] ペインで、[オンプレミスの Secure Event Connector の展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

5. ダイアログボックスのステップ 1 で、Security Cloud Control ブートストラップデータをコピーしま




す。

**ステップ 26** 「Would you like to update these settings?」というプロンプトで、**n** を入力します。

**ステップ 27** Security Cloud Control の [オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] ダイアログに戻り、[OK] をクリックします。[セキュアコネクタ（Secure Connectors）] ページで、Secure Event Connector が黄色のオンボード状態であることを確認できます。

### 次のタスク

Security Cloud Control コネクタ VM への Secure Event Connector のインストール （11 ページ）に進みます。

# Security Cloud Control コネクタ VM への Secure Event Connector のインストール

### 始める前に

Security Cloud Control VM イメージを使用して Secure Event Connector をサポートするための Security Cloud Control コネクタのインストール （6 ページ） に記載があるように、Security Cloud Control コネクタ VM がインストールされている必要があります。

### 手順

**ステップ 1** Security Cloud Control にログインします。

**ステップ 2** 左側のペインで、**[管理（Administration）] > [セキュアコネクタ（Secure Connectors）]** を選択します。

**ステップ 3** 上記でオンボーディングした Security Cloud Control コネクタを選択します。セキュアコネクタテーブルでは、これはセキュアイベントコネクタと呼ばれ、「オンボーディング」ステータスのままである必要があります。

**ステップ 4** 右側の [アクション（Actions）] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

**ステップ 5** ウィザードの**ステップ 2**で、 [SECブートストラップデータのコピー（Copy SEC bootstrap data）] のリンクをクリックします。

**ステップ 6** Security Cloud Control コネクタへの SSH 接続を作成し、`cdo` ユーザーとしてログインします。

**ステップ 7** ログインしたら、**sdc**ユーザーに切り替えます。パスワードの入力を求められたら、「Security Cloud Control」ユーザーのパスワードを入力します。これらのコマンドの例を次に示します。

```
[cdo@sdc-vm ~]$ sudo su sdc
 [sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

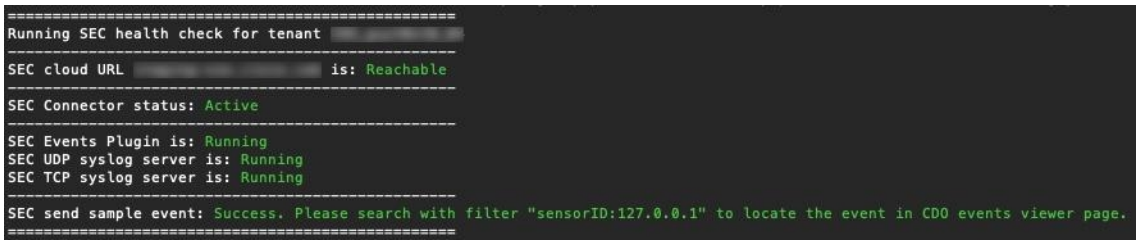
**ステップ 8** プロンプトで、sec.sh セットアップスクリプトを実行します。

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

**ステップ 9** プロンプトの最後に、手順4でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
 RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。




登録に失敗したことやSECのオンボーディングに失敗したことを示すメッセージを受け取った場合は、次を参照してください。SEC オンボーディング失敗のトラブルシューティング

成功メッセージを受け取った場合は、Security Cloud Control に戻り、[オンプレミスセキュアイベントコネクタの展開（Deploy an ON-Premise Secure Event Connector）] ダイアログボックスで [完了（Done）] をクリックします。

### 次のタスク

ASA デバイスに安全なロギング分析（SaaS）を導入する （45 ページ） に戻ってください。

**関連情報**：

- Secure Device Connector のトラブルシュート
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング

# Ubuntu 仮想マシンへの Secure Event Connector の展開

### 始める前に

Secure Device Connector および Secure Event Connector を実行するための VM の展開の説明に従って、Ubuntu VM に Secure Device Connector をインストールしておく必要があります。

### 手順

**ステップ 1** Security Cloud Control にログオンします。

**ステップ 2** 左側のペインで、**[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

**ステップ 3**  アイコンをクリックし、[Secure Event Connector] をクリックします。

**ステップ 4** ウィンドウの手順 2 の SEC ブートストラップデータをメモ帳にコピーします。

**ステップ 5** 次のコマンドを実行します。

```
[sdc@vm]:~$sudo su sdc
```

```
sdc@vm:/home/user$ cd /usr/local/cdo/toolkit
```

プロンプトが表示されたら、コピーした SEC ブートストラップデータを入力します。

```
sdc@vm:~/toolkit$ ./sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
Successfully on-boarded SEC
```

Security Cloud Control で Secure Event Connector が [アクティブ（Active）] になるまでに数分かかる場合があります。

# VM イメージを使用した SEC のインストール

Secure Event Connector（SEC）は、Cisco ASA と FTD からのイベントを Cisco Cloud に転送し、Security Cloud Control の **[Event Logging]** ページで表示できるようにします。

テナントに複数の Secure Event Connector（SEC）をインストールし、インストールした任意の SEC に ASA および FDM 管理対象デバイスからイベントを送信できます。複数の SEC を使用すると、さまざまなリージョンに SEC をインストールし、Cisco Cloud にイベントを送信する作業を分散できます。

独自の VM イメージを使用した複数の SEC のインストールは、3 つの部分からなるプロセスです。次の各手順を実行する必要があります。

1. VM イメージを使用して SEC をサポートするための Security Cloud Control コネクタのインストール （14 ページ）
2. 作成した VM にインストールされた SDC および Security Cloud Control コネクタの追加設定 （18 ページ）
3. Secure Event Connector のインストール

（注） Security Cloud Control コネクタに Security Cloud Control VM イメージを使用する方法は、Security Cloud Control コネクタをインストールする最も簡単で正確な推奨される方法です。その方法を使用する場合は、Security Cloud Control イメージを使用した SEC のインストール （5 ページ）を参照してください。

**次に行う作業：**

VM イメージを使用して SEC をサポートするための Security Cloud Control コネクタのインストール （14 ページ）に進みます。

# VM イメージを使用して SEC をサポートするための Security Cloud Control コネクタのインストール

Security Cloud Control コネクタ VM は、SEC をインストールする仮想マシンです。Security Cloud Control コネクタの唯一の目的は、Cisco Security Analytics and Logging（SaaS）のお客様向けに SEC をサポートすることです。

これは、Secure Event Connector（SEC）をインストールして設定するために完了する必要がある 3 つの手順の 1 番目です。この手順の後、次の手順を実行する必要があります。

- 作成した VM にインストールされた SDC および Security Cloud Control コネクタの追加設定 （18 ページ）
- Secure Event Connector のインストール

## 始める前に

- Security and Analytics Logging（SaaS）サブスクリプションプランを購入してください。サブスクリプションプランの詳細については、『Security Cloud Control Firewall Management Ordering Guide』を参照してください。

  Security Analytics and Logging のトライアル版をリクエストする場合は、Security Cloud Control にログインし、メインナビゲーションバーで **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択し、[トライアルのリクエスト（Request Trial）] をクリックします。

- Security Cloud Control は、厳密な証明書チェックを必要とし、Security Cloud Control コネクタとインターネット間の Web プロキシやコンテンツプロキシをサポートしていません。
- **Security Cloud Control コネクタは TCP ポート 443 でインターネットへの完全なアウトバウンド接続を確立する必要があります。**
- コネクタで適切なネットワーク接続を確立するには、「Secure Device Connector を使用した Security Cloud Control への接続」を参照してください。**Security Cloud Control**
- vCenter Web クライアントまたはr ESXi Web クライアントを使用してインストールされた VMware ESXi ホスト。

（注） vSphere デスクトップクライアントを使用したインストールはサポートしていません。

- ESXi 5.1 ハイパーバイザ。
- Ubuntu 22.04 および Ubuntu 24.04。
- Security Cloud Control コネクタと SEC のみをホストする VM のシステム要件は以下のとおりです。
  - CPU：SEC 用に 4 つの CPU を割り当てます。

- メモリ：SEC 用に 8 GB のメモリを割り当てます。
- ディスク領域：64 GB

- この手順を実行するユーザーは、Linux 環境の操作と **vi** ビジュアルエディタによるファイルの編集に慣れている必要があります。
- インストールを開始する前に、次の情報を収集します。
  - Security Cloud Control コネクタに使用する静的 IP アドレス。
  - インストールプロセス中に作成する **root** ユーザーと **Security Cloud Control** ユーザーのパスワード。
  - 組織で使用する DNS サーバーの IP アドレス。
  - Security Cloud Control コネクタアドレスが存在するネットワークのゲートウェイ IP アドレス。
  - タイムサーバーの FQDN または IP アドレス。
- Security Cloud Control Connector 仮想マシンは、セキュリティパッチを定期的にインストールするように設定されており、これを行うには、ポート 80 のアウトバウンドを開く必要があります。
- **始める前に**：手順内のコマンドは、コピーして端末ウィンドウに貼り付けるのではなく入力するようにしてください。一部のコマンドに含まれる「n ダッシュ」は、カットアンドペーストのプロセスで「m ダッシュ」として適用される場合があり、コマンドが失敗する原因となります。

### 手順

**ステップ 1** Security Cloud Control にログオンします。

**ステップ 2** 左側のペインで、**[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

**ステップ 3**  アイコンをクリックし、[Secure Event Connector] をクリックします。

**ステップ 4** 表示されたリンクを使用して、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] ウィンドウの手順 2 で SEC ブートストラップデータをコピーします。

**ステップ 5** インストールしたら、Security Cloud Control コネクタ の IP アドレス、サブネットマスク、ゲートウェイの指定など、ネットワークの基本設定を行います。

**ステップ 6** DNS（ドメインネームサーバー）を設定します。

**ステップ 7** NTP（ネットワーク タイム プロトコル）サーバーを設定します。

**ステップ 8** Security Cloud Control コネクタの CLI と簡単にやり取りできるように、SSH サーバーをインストールします。

**ステップ 9** **AWS CLI パッケージ**をインストールします（https://docs.aws.amazon.com/cli/latest/userguide/awscli-install-linux.html を参照）。

（注）
`--user` フラグは使用しないでください。

**ステップ 10** **Docker CE パッケージ**をインストールします（https://docs.docker.com/install/linux/docker-ce/centos/#install-docker-ce を参照）。

（注）
「リポジトリを使用したインストール」方法を使用します。

**ステップ 11** Docker サービスを開始し、起動時に開始できるようにします。

```
[root@sdc-vm ~]# systemctl start docker
 [root@sdc-vm ~]# systemctl enable docker
Created symlink from /etc/systemd/system/multiuser.target.wants/docker.service to
/usr/lib/systemd/system/docker.service.
```

**ステップ 12** **Security Cloud Control** と **sdc** の 2 つのユーザーを作成します。Security Cloud Control ユーザーは、管理機能を実行するためにログインするユーザーです（つまりルートユーザーを直接使用する必要はありません）。sdc ユーザーは、Security Cloud Control コネクタの docker コンテナを実行するユーザーです。

```
[root@sdc-vm ~]# useraddSecurity Cloud Control
 [root@sdc-vm ~]# useradd sdc -d /usr/local/Security Cloud Control
```

**ステップ 13** crontab を使用するように sdc ユーザーを設定します。

```
[root@sdc-vm ~]# touch /etc/cron.allow
[root@sdc-vm ~]# echo "sdc" >> /etc/cron.allow
```

**ステップ 14** Security Cloud Control ユーザーのパスワードを設定します。

```
[root@sdc-vm ~]# passwd Security Cloud Control
Changing password for user Security Cloud Control.
New password: <type password>
Retype new password: <type password>
passwd: all authentication tokens updated successfully.
```

**ステップ 15** Security Cloud Control ユーザーを「wheel」グループに追加し、管理者（sudo）権限を付与します。

```
[root@sdc-vm ~]# usermod -aG wheelSecurity Cloud Control
 [root@sdc-vm ~]#
```

**ステップ 16** Docker がインストールされると、ユーザーグループが作成されます。CentOS/Docker のバージョンに応じて、「docker」または「dockerroot」と呼ばれます。/etc/group ファイルでどのグループが作成されたかを確認したら、sdc ユーザーをそのグループに追加します。

```
 [root@sdc-vm ~]# grep docker /etc/group
docker:x:993:
[root@sdc-vm ~]#
[root@sdc-vm ~]# usermod -aG docker sdc
[root@sdc-vm ~]#
```

**ステップ 17** `/etc/docker/daemon.json` ファイルが存在しない場合は作成し、以下の内容を入力します。作成したら、docker デーモンを再起動します。

（注）
「group」キーに入力したグループ名が、/etc/group ファイルで見つけたグループと一致していることを確認してください。

```
[root@sdc-vm ~]# cat /etc/docker/daemon.json
{
 "live-restore": true,
 "group": "docker"
}
[root@sdc-vm ~]# systemctl restart docker
[root@sdc-vm ~]#
```

**ステップ 18** 現在 vSphere コンソールセッションを使用している場合は、SSH に切り替えて、**Security Cloud Control** ユーザーでログインします。ログインしたら、**sdc** ユーザーに切り替えます。パスワードの入力を求められたら、**Security Cloud Control** ユーザーのパスワードを入力します。

```
[Security Cloud Control@sdc-vm ~]$ sudo su sdc
[sudo] password for Security Cloud Control: <type password for Security Cloud Control user >
[sdc@sdc-vm ~]$
```

**ステップ 19** ディレクトリを **/usr/local/**Security Cloud Control に変更します。

**ステップ 20** **bootstrapdata** という新しいファイルを作成し、展開ウィザードの手順1 のブートストラップデータを、このファイルに貼り付けます。[保存（Save）] をクリックしてファイルを保存します。[vi] または [nano] を使用してファイルを作成できます。

**ステップ 21** ブートストラップデータは base64 でエンコードされていますので、復号して **extractedbootstrapdata** というファイルにエクスポートします。

```
[sdc@sdc-vm ~]$ base64 -d /usr/local/Security Cloud Control/bootstrapdata > /usr/local/Security
 Cloud Control/extractedbootstrapdata
[sdc@sdc-vm ~]$
```

cat コマンドを実行して復号したデータを表示します。コマンドおよび復号したデータは次のようになります。

```
[sdc@sdc-vm ~]$ cat /usr/local/Security Cloud Control/extractedbootstrapdata
Security Cloud Control_TOKEN="<token string>"
Security Cloud Control_DOMAIN="www.defenseorchestrator.com"
Security Cloud Control_TENANT="<tenant-name>"
<Security Cloud Control_URL>/sdc/bootstrap/Security Cloud
Control_acm="https://www.defenseorchestrator.com/sdc/bootstrap/tenant-name/<tenant-name-SDC>"
ONLY_EVENTING="true"
```

**ステップ 22** 以下のコマンドを実行して、復号したブートストラップデータの一部を環境変数にエクスポートします。

```
[sdc@sdc-vm ~]$ sed -e 's/^/export /g' extractedbootstrapdata > secenv && source secenv
[sdc@sdc-vm ~]$
```

**ステップ 23** Security Cloud Control からブートストラップバンドルをダウンロードします。

```
[sdc@sdc-vm ~]$ curl -H "Authorization: Bearer $Security Cloud Control_TOKEN" "$Security Cloud
Control_BOOTSTRAP_URL" -o $Security Cloud Control_TENANT.tar.gz
100 10314 100 10314 0 0 10656 0 --:--:-- --:--:-- --:--:-- 10654
[sdc@sdc-vm ~]$ ls -l /usr/local/Security Cloud Control/*SDC
-rw-rw-r--. 1 sdc sdc 10314 Jul 23 13:48 /usr/local/Security Cloud Control/Security Cloud
Control_<tenant_name>
```

**ステップ 24** Security Cloud Control コネクタ tarball を展開し、bootstrap_sec_only.sh ファイルを実行して Security Cloud Control コネクタパッケージをインストールします。

```
 [sdc@sdc-vm ~]$ tar xzvf /usr/local/Security Cloud Control/tenant-name-SDC
<snipped - extracted files>
[sdc@sdc-vm ~]$
[sdc@sdc-vm ~]$ /usr/local/Security Cloud Control/bootstrap/bootstrap_sec_only.sh
[2018-07-23 13:54:02] environment properly configured
download: s3://onprem-sdc/toolkit/prod/toolkit.tar to toolkit/toolkit.tar
toolkit.sh
common.sh
es_toolkit.sh
sec.sh
healthcheck.sh
troubleshoot.sh
no crontab for sdc
-bash-4.2$ crontab -l
*/5 * * * * /usr/local/Security Cloud Control/toolkit/es_toolkit.sh upgradeEventing 2>&1 >>
/usr/local/Security Cloud Control/toolkit/toolkit.log
0 2 * * * sleep 30 && /usr/local/Security Cloud Control/toolkit/es_toolkit.sh es_maintenance 2>&1
 >> /usr/local/Security Cloud Control/toolkit/toolkit.log
You have new mail in /var/spool/mail/sdc
```

### 次のタスク

作成した VM にインストールされた SDC および Security Cloud Control コネクタの追加設定 （18 ページ） に進みます。

# 作成した VM にインストールされた SDC および Security Cloud Control コネクタの追加設定

Security Cloud Control コネクタを独自の CentOS 7 仮想マシンにインストールした場合は、イベントが SEC に到達できるように、次の付加的な設定手順のいずれかを実行します。

- CentOS 7 VM の firewalld サービスの無効化：これは、シスコが提供する SDC VM の設定と一致します。
- firewalld サービスの実行を許可し、ファイアウォールルールを追加して、イベントトラフィックが SEC に到達できるようにします。 （19 ページ） ：こちらは、インバウンドイベント トラフィックを許可するためのより詳細なアプローチです。

### 始める前に：

これは、SEC をインストールして設定するために完了する必要がある 3 つの手順の 2 番目です。まだ行っていない場合は、これらの設定変更を行う前に、VM イメージを使用して SEC をサポートするための Security Cloud Control コネクタのインストール （14 ページ） を完了してください。

ここで説明されている追加の設定変更のいずれかを完了したら、Secure Event Connector のインストールを実行します。

### CentOS 7 VM での firewalld サービスの無効化

1. SDC VM の CLI に「Security Cloud Control」ユーザーとしてログインします。
2. firewalld サービスを停止してから、続く VM の再起動時に無効のままになっていることを確認します。プロンプトが表示されたら、**Security Cloud Control** ユーザーのパスワードを入力します。

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl stop firewalld
Security Cloud Control@SDC-VM ~]$ sudo systemctl disable firewalld
```

3. Docker サービスを再起動して、Docker 固有のエントリをローカルファイアウォールに再挿入します。

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart docker
```

4. Secure Event Connector のインストールに進みます。

### firewalldサービスの実行を許可し、ファイアウォールルールを追加して、イベントトラフィックが SEC に到達できるようにします。

1. SDC VM の CLI に「Security Cloud Control」ユーザーとしてログインします。
2. ローカル ファイアウォール ルールを追加して、設定した TCP、UDP、または NSEL ポートから SEC への着信トラフィックを許可します。SEC で使用されるポートについては、「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。プロンプトが表示されたら、**Security Cloud Control** ユーザーのパスワードを入力します。コマンドの例を次に示します。別のポート値の指定が必要になる場合があります。

```
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10125/tcp
Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10025/udp
[Security Cloud Control@SDC-VM ~]$ sudo firewall-cmd --zone=public --permanent
--add-port=10425/udp
```

3. firewalldサービスを再起動して、新しいローカル ファイアウォール ルールをアクティブかつ持続的なものにします。

```
[Security Cloud Control@SDC-VM ~]$ sudo systemctl restart firewalld
```

4. Secure Event Connector のインストールに進みます。

## Security Cloud Control コネクタ仮想マシンへの Secure Event Connector のインストール

### 始める前に

これは、Secure Event Connector（SEC）をインストールして設定するために完了する必要がある 3 つの手順の 3 番目です。まだ完了していない場合は、この手順を続行する前に、次のタスクを完了してください。

- VM イメージを使用して SEC をサポートするための Security Cloud Control コネクタのインストール （14 ページ）。

- 作成した VM にインストールされた SDC および Security Cloud Control コネクタの追加設定 （18 ページ）。

### 手順

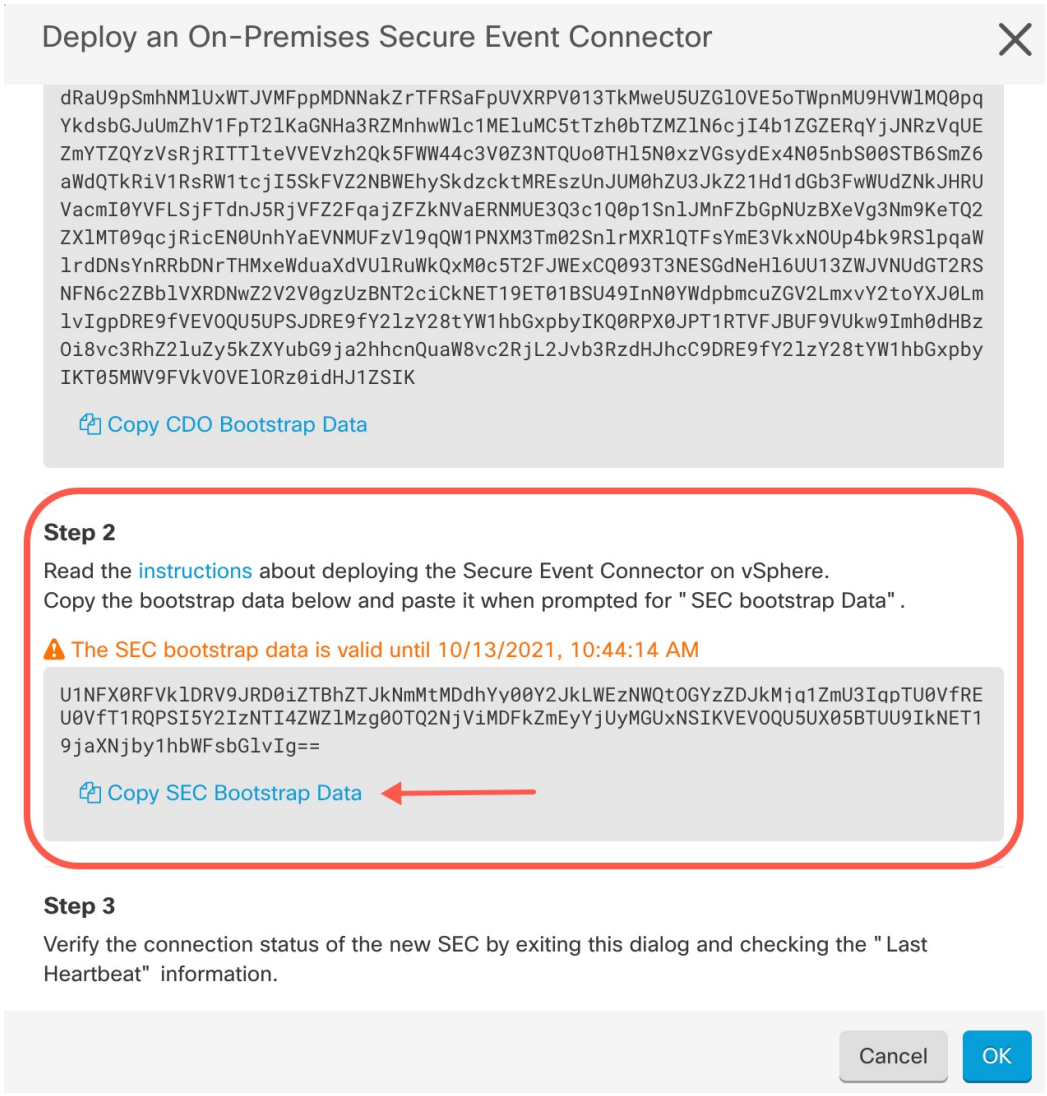
**ステップ 1** Security Cloud Control にログインします。

**ステップ 2** 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** をクリックします。

**ステップ 3** 上記の前提条件の手順を使用してインストールした Security Cloud Control コネクタを選択します。[セキュアコネクタ（Secure Connectors）] テーブルでは、「Secure Event Connector」と表示されます。

**ステップ 4** 右側の [アクション（Actions）] ペインで、[オンプレミスのSecure Event Connectorの展開（Deploy an On-Premises Secure Event Connector）] をクリックします。

**ステップ 5** ウィザードの**ステップ 2**で、 [SEC ブートストラップデータのコピー（Copy SEC bootstrap data）] のリンク




をクリックします。

**ステップ 6** SSH を使用してセキュアコネクタに接続し、Security Cloud Control ユーザーとしてログインします。

**ステップ 7** ログインしたら、**sdc** ユーザーに切り替えます。パスワードの入力を求められたら、「Security Cloud Control」ユーザーのパスワードを入力します。これらのコマンドの例を次に示します。

```
[cdo@sdc-vm ~]$ sudo su sdc
[sudo] password for cdo: <type password for cdo user>
[sdc@sdc-vm ~]$
```

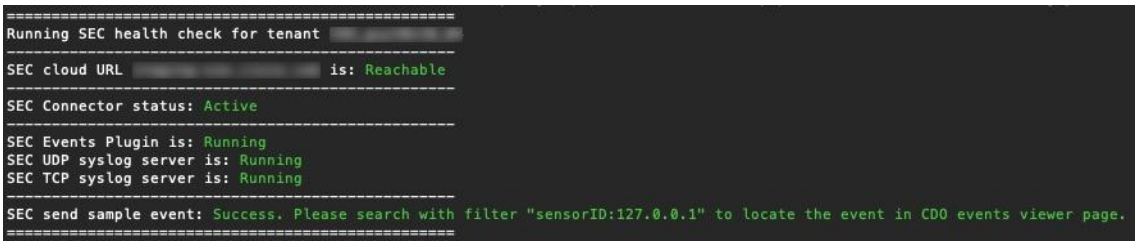
**ステップ 8** プロンプトで、sec.sh セットアップスクリプトを実行します。

```
[sdc@sdc-vm ~]$ /usr/local/cdo/toolkit/sec.sh setup
```

**ステップ 9** プロンプトの最後に、手順 4 でコピーしたブートストラップデータを貼り付けて、**Enter** キーを押します。

```
Please copy the bootstrap data from Setup Secure Event Connector page of CDO:
 KJHYFuYTFuIGhiJKlKnJHvHfgxTewrtwE
RtyFUiyIOHKNkJbKhvhgyRStwterTyufGUihoJpojP9UOoiUY8VHHGFXREWRtygfhVjhkOuihIuyftyXtfcghvjbkhB=
```

SEC がオンボーディングされると、sec.sh は、SEC のヘルスをチェックするスクリプトを実行します。すべてのヘルスチェックが「正常」の場合、ヘルスチェックはサンプルイベントをイベントログに送信します。このサンプルイベントは、「sec-health-check」という名前のポリシーとしてイベントログに表示されます。




登録に失敗したことや SEC のオンボーディングに失敗したことを示すメッセージを受け取った場合は、「Secure Event Connector オンボーディングのトラブルシューティング」を参照してください。

成功メッセージを受け取った場合は、[オンプレミスの Secure Event Connector の展開（Deploy an ON-Premise Secure Event Connector）] ダイアログボックスで [完了（Done）] をクリックします。VM イメージへの SEC のインストールは完了です。

### 次のタスク

この手順に戻って、SAL SaaS の実装を続行します：ASA デバイスに安全なロギング分析（SaaS）を導入する （45 ページ）

**関連情報**：

- Secure Device Connector のトラブルシュート
- Secure Event Connector のトラブルシューティング
- SEC オンボーディング失敗のトラブルシューティング
- SEC 登録失敗のトラブルシューティング

# Terraform モジュールを使用した AWS VPC 上での Secure Event Connector のインストール

### 始める前に

- このタスクを実行するには、Security Cloud Control テナントで SAL を有効にする必要があります。このセクションでは、SAL ライセンスがあることを前提としています。ない場合は、Cisco Security and Analytics Logging の Logging and Troubleshooting ライセンスを購入します。
- 新しい SEC がインストールされていることを確認します。新しい SEC を作成するには、SDC 仮想マシンへの Secure Event Connector のインストール （2 ページ）を参照してください。
- SEC をインストールするときは、Security Cloud Control ブートストラップデータと SEC ブートストラップデータを必ずメモしてください。

### 手順

**ステップ 1** Terraform レジストリの [Secure Event Connector Terraform Module] に移動し、手順に従って SEC Terraform モジュールを Terraform コードに追加します。https://registry.terraform.io/modules/CiscoDevNet/cdo-sec/aws/latest

**ステップ 2** Terraform コードを適用します。

**ステップ 3** `instance_id` および `sec_fqdn` の出力は、後の手順で必要になるため、必ず出力してください。

（注）
SEC のトラブルシューティングを行うには、AWS Systems Manager Session Manager（SSM）を使用して SEC インスタンスに接続する必要があります。SSM を使用したインスタンスへの接続の詳細については、「AWS Systems Manager Session Manager 」ドキュメントを参照してください。

SSH を使用して SDC インスタンスに接続するためのポートは、セキュリティ上の理由により公開されません。

**ステップ 4** ASA から SEC へのログの送信を有効にするには、作成した SEC の証明書チェーンを取得し、ステップ 3 の出力を使用して次のコマンドを実行してリーフ証明書を削除します。

```
rm -f /tmp/cert_chain.pem && openssl s_client -showcerts -verify 5 -connect <FQDN>:10125 < /dev/null
 | awk '/BEGIN CERTIFICATE/,/END CERTIFICATE/{ if(/BEGIN CERTIFICATE/){a++};
out="/tmp/cert_chain.pem"; if(a > 1) print >>out}'
```

**ステップ 5** `/tmp/cert_chain.pem` の内容をクリップボードにコピーします。

**ステップ 6** 次のコマンドを使用して、SEC の IP アドレスをメモします。

```
nslookup <FQDN>
```

**ステップ 7** Security Cloud Control にログインし、新しいトラストポイント オブジェクトの追加を開始します。詳細については、「Adding a Trusted CA Certificate Object」を参照してください。[追加（Add）] をクリックす

る前に、[その他のオプション（Other Options）] の [基本制約の拡張でCAフラグを有効にする（Enable CA flag in basic constraints extension）] チェックボックスをオフにしてください。

**ステップ 8** [追加（Add）] をクリックし、Security Cloud Control によって生成された CLI コマンドを [証明書のインストール（Install Certificate）] ページにコピーして、[キャンセル（Cancel）] をクリックします。

**ステップ 9** `enrollment terminal` の下に、テキストクリップボードの `no ca-check` を追加します。

**ステップ 10** ASA デバイスに SSH 接続するか、Security Cloud Control で ASA CLI オプションを使用して、次のコマンドを実行します。

```
DataCenterFW-1> en
Password: ****************
DataCenterFW-1# conf t
DataCenterFW-1(config)# <paste your modified ASA CLIs here and press Enter>
DataCenterFW-1(config)# wr mem
Building configuration...
Cryptochecksum: 6634f35f 4c5137f1 ab0c5cdc 9784bdb6
```

### 次のタスク

SEC が AWS SSM を使用してパケットを受信しているかどうかを確認できます。

次のようなログが表示されます。

```
time="2023-05-10T17:13:46.135018214Z" level=info
msg="[ip-10-100-5-19.ec2.internal][util.go:67 plugin.createTickers:func1] Events -
Processed - 6/s, Dropped - 0/s, Queue size - 0"
```

# Secure Event Connector の削除

**警告**：この手順により、Secure Event Connector が Secure Device Connector から削除されます。これを行うと、Secure Logging Analytics（SaaS）を使用できなくなります。この操作は元に戻せません。質問や懸念事項がある場合は、このアクションを実行する前に Security Cloud Control サポートまでお問い合わせください。

Secure Device Connector から Secure Event Connector を削除するには、次の 2 段階のプロセスを実行します。

1. Security Cloud Control から SEC を削除します。
2. SDC から SEC ファイルを削除します。

**次に行う作業**：Security Cloud Control からの SEC の削除を続行します

# Security Cloud Control からの SEC の削除

### 始める前に

Secure Event Connector の削除 （23 ページ）を参照してください。

### 手順

**ステップ 1** Security Cloud Control にログインします。

**ステップ 2** 左側のペインで **[管理（Administration）]** > **[セキュアコネクタ（Secure Connectors）]** を選択します。

**ステップ 3** デバイスタイプが [Secure Event Connector] の行を選択します。

**警告**
Secure Device Connector を選択しないように注意してください。

**ステップ 4** [アクション（Actions）] ペインで、[削除（Remove）] をクリックします。

**ステップ 5** [OK] をクリックして確認します。

### 次のタスク

Secure Device Connector VM からの Secure Event Connector の削除 （24 ページ） に進みます。

# Secure Device Connector VM からの Secure Event Connector の削除

この項目は、SDC から Secure Event Connector を削除する 2 つの部分から成る手順の 2 番目の部分です。開始する前に「Secure Event Connector の削除 （23 ページ）」を参照してください。

### 手順

**ステップ 1** 仮想マシンのハイパーバイザを開き、SDC のコンソールセッションを開始します。

**ステップ 2** `[cdo@sdc]$ sudo su sdc` コマンドを使用して SDC ユーザーに切り替えます。

**ステップ 3** SDC 仮想マシンから SEC を削除するには、次のいずれかのコマンドを使用します。

- テナントセレクタを使用する場合（または VM にテナントが 1 つしかない場合）は、次の手順を実行します。

  ```
  [sdc@tenant toolkit]$ sdc eventing delete
  ```

- コマンド引数でテナントを直接指定する場合は、次のようにします。

  ```
  [sdc@tenant toolkit]$ sdc eventing delete CDO_{tenant-name}
  ```

**ステップ 4** SEC ファイルの削除を確定します。

# Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索

Secure Logging Analytics（SaaS）を使用すると、ご使用の ASA または FDM による管理デバイスから、Secure Event Connector（SEC）上の特定の UDP、TCP、または NSEL ポートにイベントを送信できます。その後、SEC はそれらのイベントを Cisco Cloud に転送します。

まだ使用されていないポートの場合、SEC はそれらのポートを使用してイベントを受信できるようにします。Secure Logging Analytics（SaaS）のマニュアルでは、機能を設定するときにポートを使用することが推奨されています。

- TCP：10125
- UDP：10025
- NSEL：10425

すでに使用されているポートの場合は、Secure Logging Analytics（SaaS）を設定する前に、SEC デバイスの詳細を調べて、イベントの受信に実際に使用しているポートを特定します。

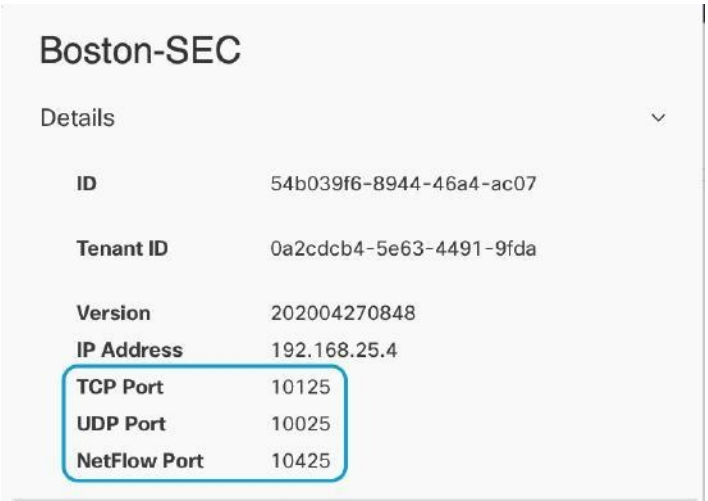
SEC が使用するポート番号を見つけるには、次の手順を実行します。

### 手順

**ステップ 1** 左側のペインで **[管理（Administration）]** > **[統合（Integrations）]** > **[Firewall Management Center]** をクリックし、[セキュアコネクタ（Secure Connectors）] タブをクリックします。

**ステップ 2** [セキュアコネクタ（Secure Connectors）] ページで、イベントを送信する SEC を選択します。

**ステップ 3** [詳細（Details）] ペインに、イベントの送信先となる TCP、UDP、および NetFlow（NSEL）ポートが表示されます。




# Security Cloud Control の Security Analytics and Logging（SaaS）について

**用語に関する注** ： このドキュメントでは、Cisco Security Analytics and Logging（Software as a Service（SaaS）製品）が、セキュリティイベントのモニタリングのために Security Cloud Control で使用されている場合、この統合は Cisco Security Analytics and Logging（SaaS）または SAL（SaaS）と呼ばれています。

Cisco Security Analytics and Logging（SAL）を使用すると、すべてのファイアウォールデバイスからサポートされているタイプのセキュリティイベントをキャプチャし、Security Cloud Control の 1 か所で表示できます。イベントは、セキュリティ分析およびロギングクラウドに保存され、 **[Event Logging]** ページから表示できます。**[Event Logging]** ページでは、セキュリティイベントデータを検索、フィルタ処理、および分析して、ネットワーク内でトリガーされているセキュリティルールを把握できます。

# Security Cloud Control のイベントタイプ

Secure Logging Analytics（SaaS）によって記録されたセキュリティイベントをフィルタ処理する場合、Security Cloud Control がサポートする ASA、FTD、および のイベントタイプのリストから選択できます。Security Cloud Control メニューから、**[分析（Analytics）]** > **[イベントロギング（Event Logging）]** に移動し、フィルタアイコンをクリックしてイベントを選択します。これらのイベントタイプは、syslog ID のグループを表します。次の表は、どのイベントタイプにどの syslog ID が含まれるかを示しています。特定の syslog ID の詳細については、「Cisco ASA Series Syslog Messages」または「Cisco Secure Firewall Threat Defense Syslog Messages」で検索できます。

一部の syslog イベントには、追加の属性「EventName」があります。属性:値のペアでフィルタ処理することにより、EventName 属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。「Syslog イベントのイベント名属性」を参照してください。

一部の syslog イベントには、追加の属性「EventGroup」および「EventGroupDefinition」があります。属性:値のペアでフィルタ処理することにより、これらの追加属性を使用してイベントテーブルをフィルタ処理し、イベントを見つけることができます。「一部の Syslog メッセージの EventGroup および EventGroupDefinition 属性」を参照してください。

NetFlow イベントは、syslog イベントとは異なります。**NetFlow** フィルタは、NSEL レコードになったすべての NetFlow イベント ID を検索します。これらの NetFlow イベント ID は、『Cisco ASA NetFlow 実装ガイド』で定義されています。

次の表に、Security Cloud Control がサポートするイベントタイプと、イベントタイプに対応する syslog または NetFlow イベント番号を示します。

| フィルタ名（**Filter Name**） | 説明 | 対応する **Syslog** イベントまたは **NetFlow** イベント |
|---|---|---|
| AAA | これらは、AAA が設定されている場合に、認証、許可、またはネットワーク内のリソースを使い果たすことを目的として失敗した試行または無効な試行が発生したときにシステムが生成するイベントです。 | 109001-109035<br>113001-113027 |
| BotNet | これらのイベントは、マルウェアに感染したホスト（ボットネットの可能性あり）を含む可能性のある悪意のあるネットワークにユーザーがアクセスしようとしたとき、またはダイナミックフィルタブロックリストにあるドメインまたは IP アドレスとの間でやり取りされるトラフィックをシステムが検出したときにログに記録されます。 | 338001-338310 |

| フィルタ名（**Filter Name**） | 説明 | 対応する **Syslog** イベントまたは **NetFlow** イベント |
|---|---|---|
| フェールオーバー | これらのイベントは、システムがステートフルおよびステートレス フェールオーバー構成でエラーを検出した場合、またはフェールオーバーが発生したときにセカンダリ ファイアウォール ユニットでエラーを検出した場合にログに記録されます。 | 101001-101005、102001、103001-103007、104001-104004、105001-105048<br>210001-210022<br>311001-311004<br>709001-709007 |
| Firewall Denied | これらのイベントは、さまざまな理由でファイアウォール システムがネットワーク パケットのトラフィックを拒否したときに生成されます。この理由は、セキュリティ ポリシーによるパケットのドロップから、ネットワークへの攻撃を意味する可能性がある、同じ送信元 IP と宛先 IP を持つパケットをシステムが受信したことによるドロップまでさまざまです。<br>Firewall Denied イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。 | 106001、106007、106012、106013、106015、106016、106017、106020、106021、106022、106023、106025、106027 |

| フィルタ名（**Filter Name**） | 説明 | 対応する **Syslog** イベントまたは **NetFlow** イベント |
|---|---|---|
| Firewall Traffic | これらは、ネットワークでのさまざまな接続試行、ユーザーアイデンティティ、タイムスタンプ、終了したセッションなどに応じてログに記録されるイベントです。<br>Firewall Traffic イベントは NetFlow に含まれている場合があり、syslog ID だけでなく NetFlow イベント ID と共に報告される場合もあります。 | 106001-106100、108001-108007、110002-110003<br>201002-201013、209003-209005、215001<br>302002-302304、302022-302027、303002-303005、313001-313008、317001-317006、324000-324301、337001-337009<br>400001-400050、401001-401005、406001-406003、407001-407003、408001-408003、415001-415020、416001、418001-418002、419001-419003、424001-424002、431001-431002、450001<br>500001-500005、508001-508002<br>607001-607003、608001-608005、609001-609002、616001<br>703001-703003、726001 |
| IPsec VPN | これらのイベントは、IPsec セキュリティ アソシエーションで不一致が発生した場合、またはシステムが受信した IPsec パケットでエラーを検出した場合に、IPsec VPN が設定されたファイアウォールに記録されます。 | 402001-402148、602102-602305、702304-702307 |

| フィルタ名（**Filter Name**） | 説明 | 対応する **Syslog** イベントまたは **NetFlow** イベント |
|---|---|---|
| NAT | これらのイベントは、NAT エントリが作成または削除されたとき、およびNATプール内のすべてのアドレスが使用されて使い果たされたときに、NAT が設定されたファイアウォールに記録されます。 | 201002-201013、202001-202011、305005-305012 |
| SSL VPN | これらのイベントは、WebVPN セッションが作成または終了したとき、ユーザーアクセスエラー、およびユーザーアクティビティが発生したときに、SSL VPN が設定されたファイアウォールに記録されます。 | 716001-716060、722001-722053、723001-723014、724001-724004、725001-725015 |
| NetFlow | これらのイベントは、ネットワークパケットがインターフェイスを出入りする際の IP ネットワークトラフィックを中心に、タイムスタンプ、ユーザーアイデンティティ、および転送されたデータ量がログに記録されます。 | 0、1、2、3、5 |

| フィルタ名（**Filter Name**） | 説明 | 対応する **Syslog** イベントまたは **NetFlow** イベント |
|---|---|---|
| Connection | ユーザーが生成するトラフィックがシステムを通過する場合、この接続に対してイベントを生成できます。これらのイベントを生成するには、アクセス ルールで接続ロギングを有効にします。また、セキュリティ インテリジェンス ポリシーおよび SSL 復号ルールでロギングを有効にすると、接続イベントを生成できます。<br><br>接続イベントには、検出されたセッションに関するデータも含まれています。個々の接続イベントで入手可能な情報はいくつかの要因に応じて異なりますが、一般的には次のものがあります。<br>• 基本的な接続プロパティ：タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど。<br>• システムによって検出または推測される追加の接続プロパティ：アプリケーション、要求される URL、または接続に関連付けられているユーザーなど。<br>• 接続がログに記録された理由に関するメタデータ：トラフィックを処理した設定、接続が許可またはブロックされていたかどうか、暗号化された接続および復号された接続に関する詳細など。 | 430002、430003 |

| フィルタ名（Filter Name） | 説明 | 対応する Syslog イベントまたは NetFlow イベント |
|---|---|---|
| Intrusion | システムは、ネットワークを通過するパケットを検査し、ホストとそのデータの可用性、整合性、および機密性に影響を与える可能性がある、悪意のあるアクティビティについて調べます。システムは潜在的な侵入を識別すると、侵入イベントを生成します。これには、エクスプロイトの日時とタイプ、攻撃とそのターゲットについての状況説明が記録されます。侵入イベントは、アクセス制御ルールのロギング設定に関係なく、ブロックまたはアラートするように設定された侵入ルールに対して生成されます。 | 430001 |
| ファイル（File） | ファイル イベントは、作成したファイル ポリシーに基づき、ネットワーク トラフィック内でシステムによって検出（オプションとしてブロック）されたファイルを表します。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールに対してファイル ロギングを有効にする必要があります。<br><br>システムはファイル イベントを生成する場合、基になったアクセス コントロール ルールのロギング設定にかかわらず、関連する接続の終了についても記録します。 | 430004 |

| フィルタ名（Filter Name） | 説明 | 対応する Syslog イベントまたは NetFlow イベント |
|---|---|---|
| マルウェア | システムは、全体的なアクセス コントロール設定の一環として、ネットワーク トラフィックのマルウェアを検出できます。AMP for Firepower は、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データを含むマルウェア イベントを生成できます。これらのイベントを生成するには、ファイル ポリシーを適用するアクセス ルールに対してファイル ロギングを有効にする必要があります。<br><br>ファイルの判定結果は、正常からマルウェア、マルウェアから正常などに変更できます。AMP for Firepower が AMP クラウドにファイルについて照会し、クエリから 1 週間以内に判定結果が変更されたことがクラウドに特定されると、システムはレトロスペクティブ マルウェア イベントを生成します。 | 430005 |

| フィルタ名（Filter Name） | 説明 | 対応する Syslog イベントまたは NetFlow イベント |
|---|---|---|
| セキュリティ インテリジェンス（Security Intelligence） | セキュリティ インテリジェンス イベントは、ポリシーによってブロックまたはモニターされた各接続のセキュリティ インテリジェンス ポリシーによって生成された接続イベントの一種です。すべてのセキュリティ インテリジェンス イベントには、自動入力された[セキュリティインテリジェンスカテゴリ（Security Intelligence Category）] フィールドがあります。<br><br>これらの各イベントには、対応する「通常」の接続イベントがあります。セキュリティ インテリジェンス ポリシーはアクセス コントロールなどのその他多数のセキュリティ ポリシーより前に評価されるため、セキュリティ インテリジェンスによって接続がブロックされると、その結果のイベントには、以降の評価から収集される情報（ユーザー アイデンティティなど）は含まれません。 | 430002、430003 |

| フィルタ名（**Filter Name**） | 説明 | 対応する **Syslog** イベントまたは **NetFlow** イベント |
|---|---|---|
| AI Defense | AI防御イベントは、AI環境内のアクティビティの詳細な記録を提供します。これにより、送信されたプロンプト、生成された応答、トリガーされたAI防御ポリシー違反などのインタラクションがキャプチャされます。これらのイベントには、タイムスタンプ、関係するアプリケーションとAIモデル、トリガーされた特定のルール、実行されたアクションなどの重要な情報が含まれます。これらのイベントログにより、AIの使用状況を実数でモニターして、脅威を検出し、セキュリティポリシーを効果的に適用することができます。 | |

# Cisco Security Analytics and Logging（SaaS）をプロビジョニング解除する

Cisco Security Analytics and Logging（SaaS）の有料サブスクリプションの有効期限が切れると、新しいイベントの収集はすぐに停止します。有効期限から 90 日が経過すると、既存のイベントデータを表示またはクエリできなくなります。サブスクリプションを更新するには180日間の猶予期間があります。

180 日間の猶予期間が経過すると、システムはすべてのイベントデータを消去します。**[Event Logging]** ページでセキュリティイベントを表示することも、ダイナミック エンティティ モデリング（DEM）の動作分析をセキュリティイベントおよびネットワークフローデータに適用することもできなくなります。

# セキュリティ分析とロギング ライセンス

### セキュリティ分析とロギング サブスクリプションの概要

SAL と Security Cloud Control サブスクリプションを組み合わせることができます。Security Cloud Control を使用してファイアウォールを管理する場合、次の方法でセキュリティ分析とロギング の権限を取得できます。

- 無制限のロギングを使用したデバイス管理：このオプションを使用すると、デバイスごとのライセンスが提供されます。ファイアウォール デバイスのデバイス管理機能と、直近 90 日間の無制限のログストレージが含まれています。
- オプションのクラウドロギングのみを使用したデバイス管理：このオプションでは、管理専用のデバイスごとのライセンスを購入する必要があります。その後、セキュリティ分析とロギング を個別のクラウド ロギング サブスクリプションとして追加できます。これにより、特定の運用および規則遵守のニーズに基づいて、ロギングデータのストレージとログの保持をカスタマイズできます。

### 90 日の無料試用版

Security Cloud Control にログインし、**[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** タブに移動することで、90 日間のトライアルをリクエストして、日次取り込み率を正確に見積もることができます。『Security Cloud Control Firewall Management Ordering Guide』の手順に従って、必要なサブスクリプションプランを購入してサービスを継続できます。

### セキュリティ分析とロギング 有料サブスクリプション階層

無制限のロギングオプションによるデバイス管理を使用しない場合は、ロギング容量を個別に購入できます。このスタンドアロンの セキュリティ分析とロギング サブスクリプションを利用すると、柔軟性が向上し、デフォルトの保持が長く、ストレージ権限も増加します。これらのサブスクリプション階層のデフォルトの最小保持期間は1年です。

次の場合は、これらの回数変更可能 セキュリティ分析とロギング サブスクリプション階層を選択します。

- ファイアウォールが別の注文の一部としてすでに購入されている。
- 特定のロギングの見積もりがあり、固定量の取り込み、ストレージ、およびロギングの保持に基づいて階層を購入する必要がある。
- 90 日を超えるログ保持期間が必要である。

セキュリティ分析とロギング サブスクリプションは Essentials、Advantage、Premier の 3 つの階層に分類されます。次の表に、各階層で利用可能なストレージ容量とログ保持期間を示します。

| 説明 | 保持期間 | ストレージ制限 | サブスクリプション期間 |
|---|---|---|---|
| Cisco SAL Essentials サブスクリプション | 1、2、または 3 年 | 2 TB | 0 ～ 5 年 |
| Cisco SAL Advantage サブスクリプション | 1、2、または 3 年 | 4 TB | 0 ～ 5 年 |
| Cisco SAL Premier サブスクリプション | 1、2、または 3 年 | 10 TB | 0 ～ 5 年 |

サブスクリプションプランの詳細については、『Security Cloud Control Firewall Management Ordering Guide』を参照してください。

（注） 有料サブスクリプションの場合、セキュリティ分析とロギングは自動的にイベントデータを管理して、ライセンス供与された保持期間に合わせます。セキュリティ分析とロギングは、指定された保持期間よりも古いイベントデータを毎日削除し、完全な保持期間内のすべてのイベントデータに常にアクセスできるようにします。

### 日次取り込み率の見積り

Cisco Cloud がオンボーディングされたファイアウォールデバイスから 1 日に受け取るイベント数を反映したサブスクリプションプランを購入する必要があります。これは「日次取り込み率」と呼ばれます。Logging Volume Estimator ツールを使用して、日次取り込み率を推定でき、率が変化すると、サブスクリプションプランを更新できます。

# セキュリティ分析とロギング ライセンスに登録する

### セキュリティ分析とロギング トライアルサブスクリプションを開始

オンボーディングされたセキュリティデバイスが Cisco Cloud に送信する 1 日あたりの件数と一致するデータストレージプランを購入します。このボリュームは、1 日の取り込み率と呼ばれます。購入する前に、セキュリティ分析とロギングの無料トライアルに参加して、日次取り込み率を正確に推定してください。

- このトライアルプランでは、90 日間すべての セキュリティ分析とロギング 機能にアクセスできます。
- 90 日間のトライアル期間中、オンボーディングされたファイアウォールはイベントを セキュリティ分析とロギングに送信します。イベントの取り込み率をモニターし、ストレージ要件を把握し、パフォーマンスを評価します。このデータは、最適な有料サブスクリプションを計画および選択するのに役立ちます。

- トライアルがアクティブな状態で有料の セキュリティ分析とロギング サブスクリプションをアクティブ化すると、Security Cloud Control ではその製品インスタンスのトライアルライセンスが有料ライセンスに置き換えられ、トライアルが終了します。
- 有料サブスクリプションをトライアルに適用しないことを選択した場合、イベントの取り込みは 90 日後に自動的に停止します。これを過ぎると、セキュリティ分析とロギング 機能にアクセスできません。ただし、既存のログデータは、トライアルの有効期限からさらに 90 日間、セキュリティ分析とロギング クラウドに残ります。

（注） この 90 日間の猶予期間内に有料 セキュリティ分析とロギング ライセンスに登録しない場合、すべてのトライアルデータが完全に削除されます。

### 有料 セキュリティ分析とロギング サブスクリプションを注文する

トライアル後に セキュリティ分析とロギング を引き続き使用する場合、または既存のロギング機能をアップグレードするには、次の手順を実行します。

1. トライアルで得たインサイト（日次取り込み率、必要な保持、ストレージ量）を活用して、最適な セキュリティ分析とロギング サブスクリプションプランを決定します。
2. Cisco 担当者または認定パートナーと協力して、適切な セキュリティ分析とロギング サブスクリプションを購入します。

### セキュリティ分析とロギング サブスクリプションを要求

新しい セキュリティ分析とロギング サブスクリプションを購入すると、Security Cloud Control 以内にアクティブ化するための要求コードを受信します。サブスクリプション要求コードを含むウェルカムメールが、購入プロセス中に指定したプロビジョニング担当者に自動的に送信されます。エンドカスタマーの担当者が含まれている場合は、それらの担当者もコピーを受信します。この電子メールは、サブスクリプションのリクエストされた開始日に届きます。

Security Cloud Control 管理者は、クレームコードを使用して組織のサブスクリプションをアクティブ化します。サブスクリプションのクレームおよびアクティブ化に関する詳細は、「サブスクリプションのクレーム」を参照してください。

### セキュリティ分析とロギング サブスクリプションの更新

アクティブな セキュリティ分析とロギング サブスクリプションを維持することで、継続的なロギングと履歴データへのアクセスが保証されます。

- セキュリティ分析とロギング サブスクリプションが更新されずに期限切れになる場合、ファイアウォールからのイベントの取り込みが直ちに停止します。
- サブスクリプションの有効期限が切れた後 90 日間は、既存のイベントデータを引き続き表示および検索できます。90 日が経過すると、イベントデータにアクセスできなくなります。

- 既存のデータは、サブスクリプションの期限日から180日間の猶予期間中、セキュリティ分析とロギング クラウドに残ります。
- この 180 日間の猶予期間内に セキュリティ分析とロギング サブスクリプションが更新されない場合、すべてのイベントデータが セキュリティ分析とロギング クラウドから完全に削除されます。

# セキュリティ分析とロギングライセンス情報の表示

セキュリティ分析とロギングライセンス情報を表示し、利用資格がある月間保存容量やイベントストレージ保持期間を確認します。個別の セキュリティ分析とロギング ライセンスとデータプランがない場合は、90日間のローリングデータストレージの詳細がライセンス情報に表示されます。

**手順**

**ステップ 1** **[管理（Administration）] > [ロギングの設定（Logging Settings）]**を選択します。

**ステップ 2** **[View Logging Storage Usage]** をクリックします。

**ヒント**
または、**[イベントとログ（Events & Logs）]>[イベント（Events）]>[イベントロギング（Events Logging）]** に移動してから **[Storage Utilization]** ボタンをクリックして、セキュリティ分析とロギング のライセンス情報を表示します。

**[Event Logging Insights and Storage Usage]** のダッシュボードには、セキュリティ分析とロギング ライセンス サブスクリプションの包括的な概要が表示されます。

- **保持ポリシー（Retention policy）**：サブスクリプションに応じて、イベントログの保持期間を表示します。保持期間よりも古いイベントデータは毎日削除され、常に保持期間内のすべてのイベントデータにアクセスできます。
- **ストレージ容量（Storage capacity）**：セキュリティ分析とロギング ライセンスの下で付与されたデータの合計、現在使用されているストレージの量、および残りの使用可能なストレージを表示します。

# Security Analytics and Logging ストレージの使用状況の表示およびイベント取り込み率の表示

現在のセキュリティ分析およびロギングストレージの使用率を表示し、イベントロギングの傾向を分析します。ストレージ使用率のトレンドをイベントタイプ、デバイスタイプ、および個々のデバイス別に分析して、ストレージ使用率パターンに関するより深い知見を得ることができます。データの可視化を使用して、迅速かつ簡単に分析を行えます。これは、現在のストレージキャパシティを評価し、ストレージ使用率がセキュリティ分析およびロギングライセン

スで指定される制限に近づいた場合に、ロギングレートを減らすための対策を実行するのに役立ちます。

### 手順

**ステップ 1** **[管理（Administration）] > [ロギングの設定（Logging Settings）]** を選択します。

**ステップ 2** **[View Logging Storage Usage]** をクリックします。

ヒント
または、左側のナビゲーションバーから **[イベントとログ（Events & Logs）] > [イベント（Events）] > [イベントロギング（Events Logging）]** に移動し、**[Storage Utilization]** ボタンをクリックして、Security Analytics and Logging のストレージ使用状況とイベント取り込みトレンドを表示します。

**ステップ 3** 次のダッシュボードを活用して、ストレージ使用率をカスタマイズおよび分析し、ファイアウォール展開におけるイベントロギングの傾向に関するインサイトを得ることができます。

- **使用状況のトレンド（Usage Trends）**：過去 12 か月のイベントロギングのストレージ使用量が表示されます。バーにカーソルを合わせると、該当する月のデータ量が表示されます。
- **1 秒あたりのイベント数（EPS）トレンド（Events per second (EPS) trends）**：オンボードされたデバイスのイベント取り込み率が表示されます。特定の期間またはデバイスにおけるイベント/秒あたりのトレンドビューをカスタマイズして、より詳細なデータを取得できます。過去 1 週間、2 週間、3 週間、または 1 か月のデータをフィルタ処理できます。

  （注）
  デバイスドロップダウンリストには、Cisco Security Cloud にイベントを送信している管理されたファイアウォールデバイスが表示されます。

- **イベントタイプ別の使用率の傾向（Utilization by event type trends）**：さまざまなイベントタイプについて、使用されているイベントデータストレージを日次バイト単位で表示します。このウィジェットを使用して、イベントタイプごとのストレージ使用状況をモニターし、特定のイベントタイプのストレージ使用量にサージ（存在する場合）や異常な変更を特定します。このインサイトにより、特定のイベントタイプのロギング設定を調整し、ストレージ使用状況を管理できます。
- **デバイスタイプ別の使用率の傾向（Utilization by device type trends）**：管理対象の各デバイスタイプについて、使用されているイベントデータストレージを日次バイト単位で表示します。このウィジェットを使用して、デバイスタイプごとのストレージ使用状況をモニターし、特定のタイプのデバイスのストレージ使用量にサージや異常な変化がある場合を特定します。
- **デバイス別の使用率の傾向（Utilization by device trends）**：セキュリティ クラウド コントロールにイベントを送信する各セキュリティデバイスについて、使用されているイベントデータストレージを日次バイト単位で表示します。このウィジェットでは、ストレージ使用率が平均バイト/秒値を超えているデバイスに焦点が当てられ、使いやすさが向上する上位 5 つのデバイスのみが表示されます。このウィジェットを使用して、各デバイスのストレージ使用状況をモニターし、サージや異常な変更を特

定します。このインサイトにより、特定のデバイスのロギング設定を調整し、ストレージ使用率を効果的に管理できます。

# イベントストレージ期間の延長およびイベントストレージ容量の増加

ローリング イベント ストレージを拡張するか、イベントクラウドストレージの量を増やすには、次の手順を実行します。

**手順**

**ステップ 1** Cisco Commerce のアカウントにログインします。

**ステップ 2** Security Cloud Control PID を選択します。

**ステップ 3** プロンプトに従って、ストレージの期間または容量をアップグレードします。

増加したコストは、既存のライセンスの残りの期間に基づいて比例配分されます。詳細な手順については、「Cisco Defense Orchestrator 製品の引用に関するガイドライン」を参照してください。

# セキュリティ分析とロギング アラートの表示

管理対象ファイアウォールデバイスの セキュリティ分析とロギング 設定およびイベント設定に関するアラートと通知を表示します。

**手順**

**ステップ 1** **[管理（Administration）]** > **[ロギングの設定（Logging Settings）]**を選択します。

**ステップ 2** **[View Logging Storage Usage]** ボタンをクリックします。

**ヒント**
または、左側のナビゲーションバーから **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** に移動し、**[Storage Utilization]** ボタンをクリックして、セキュリティ分析とロギング のライセンス情報を表示します。

[Alerts and Notifications] セクションには、イベントロギングに影響を与える設定に関するアラートが表示されます。これらのアラートにより、問題を解決するためのアクションを実行できます。一部の設定：

- クラウド設定へのイベントの送信は無効になっています。
- クラウド設定へのイベントの送信はデバイスレベルで無効になっています。
- Secure Event Connector が使用できなくなります。

- イベントの取り込み率を上げます。

# セキュリティ分析とロギングライセンスに関するよくある質問（FAQ）

**セキュリティ分析とロギング 割り当てに対してどのデータがカウントされますか。**

Cisco Cloud クラウドに直接、または Secure Event Connector に送信されたイベントはすべて、セキュリティ分析とロギング に蓄積され、データ割り当てに対してカウントされます。

イベントビューアをフィルタリングしても、セキュリティ分析とロギングに保存されているイベントの数は減少しません。これにより、イベントビューアに表示されるイベントの数が減少するだけです。

**ストレージの割り当てをすぐに使い果たしてしまいます。何をすればよいですか。**

この問題に対処するアプローチは次の 2 つです。

- より多くのストレージをリクエストする。
- イベントを記録するルールの数を減らすことを考える。SSL ポリシールール、セキュリティ インテリジェンス ルール、アクセス制御ルール、侵入ポリシー、ファイルおよびマルウェアポリシーからのイベントをログに記録できます。現在のロギング設定を確認して、設定したすべてのルールおよびポリシーからイベントをログに記録する必要があるかどうかを判断します。

**セキュリティ分析とロギング のライセンスの有効期限が切れた場合、データはどうなりますか。**

有料 セキュリティ分析とロギング ライセンスの有効期限が切れると、ファイアウォールからのイベントの取り込みが直ちに停止します。ただし、180 日間の猶予期間中は、既存のデータは セキュリティ分析とロギング クラウドでアクセスできます。この猶予期間中に有料ライセンスを更新した場合は、サービスが中断されません。この 180 日間以内に更新しない場合、すべてのデータが完全に削除されます。

**保持期間が 1 年、保持期間が 5 年の セキュリティ分析とロギング サブスクリプションを購入した場合、データは 5 年間すべて保存されますか。**

保持期間は、各ログを保存する期間を定義します。保持期間が 1 年の場合、最新の 1 年のログデータのみを任意の時点で利用できます。新しいデータが収集されると、1 年を超えたログデータが上書きまたは削除されます。5 年の期間は、その期間のデータが取り込まれ続けますが、保持制限はログデータ自体に適用されることを意味します。

# ASA の Security Analytics and Logging（SAL SaaS）について

Security Analytics and Logging（SaaS）を使用すると、すべての syslog イベントと NetFlow Secure Event Logging（NSEL）を ASA からキャプチャし、Security Cloud Control の 1 ヵ所で表示できます。

イベントは Cisco Cloud に保存され、Security Cloud Control の [イベントロギング（Event Logging）] ページから表示できます。イベントをフィルタリングして確認し、ネットワークでトリガーされているセキュリティルールを明確に理解できます。それらの機能は、**Logging and Troubleshooting** パッケージで提供されます。

### ライセンシング

このソリューションを設定するには、次のアカウントとライセンスが必要です。

- **Security Cloud Control**： Security Cloud Control テナントが必要です。
- **Secure Device Connector**：Secure Device Connector 用の個別のライセンスはありません。
- **Secure Event Connector**：Secure Event Connector 用の個別のライセンスはありません。
- **Secure Logging Analytics（SaaS）**：セキュリティ分析とロギング ライセンス （36 ページ） を参照してください。
- **適応型セキュリティ アプライアンス（ASA）**：基本ライセンス以上。

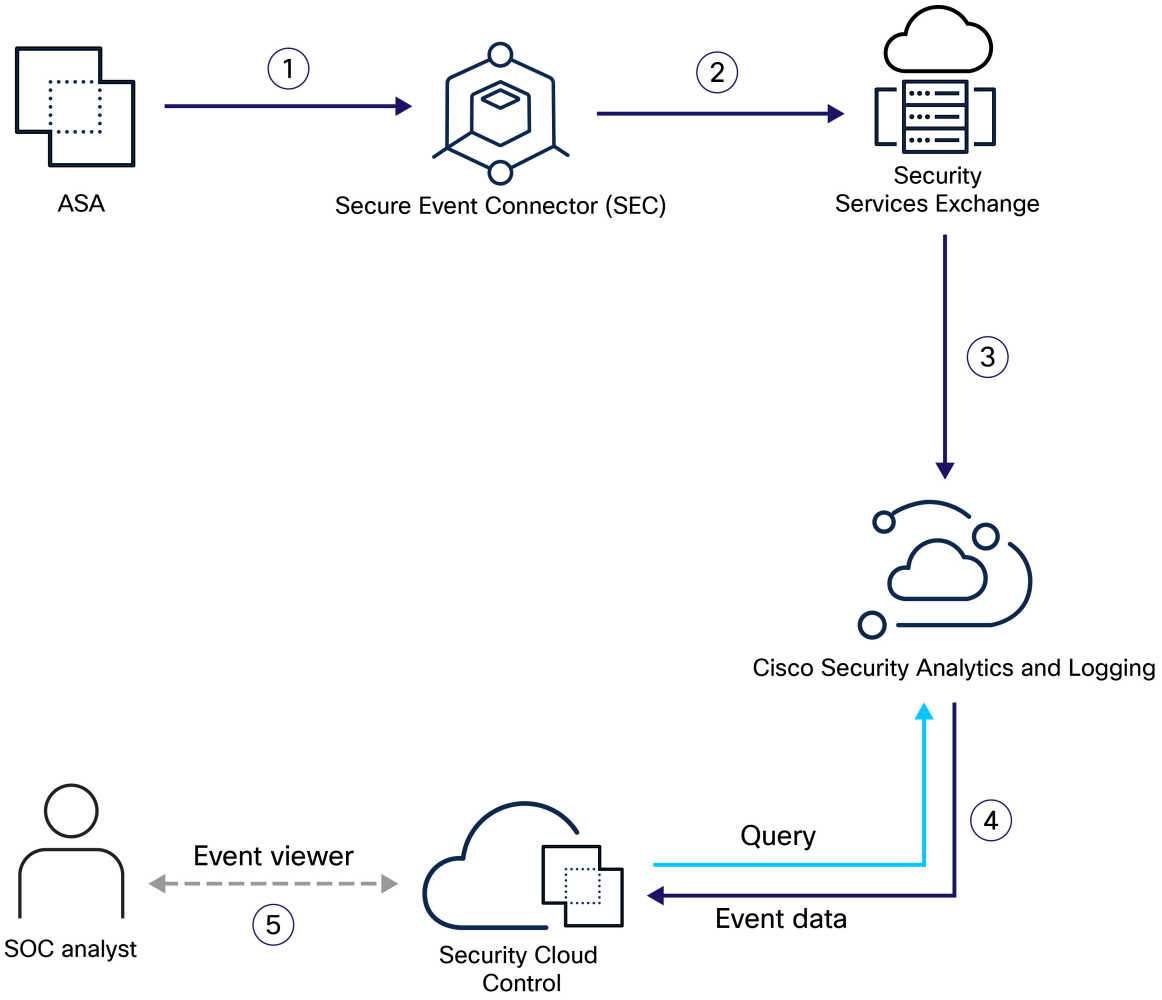
### 次のステップ

「ASA デバイス用の Secure Logging Analytics（SaaS）の実装」に移動します。

# ASA イベントを Security Cloud Control に表示する方法

この図は、ASA デバイスが syslog および NSEL イベントを Security Cloud Control と共有する方法を示しています。

図 *1 : Cisco Security Cloud Control* での *Cisco ASA* イベントの表示方法




| ステップ | 説明 |
|---|---|
| 1 | ASA を設定して、syslog および NSEL イベントを、syslog サーバーであるかのように任意の Secure Event Connectors に転送し、デバイスでのロギングを有効にします。<br><br>Syslog イベントと NSEL イベントは、ロギングが ASA で有効になっていて、ネットワークトラフィックがアクセス制御ルールの基準に一致するときに生成されます。ASA デバイスは、syslog と NSEL イベントを設定済みの Secure Event Connector に転送します。 |
| 2 | Secure Event Connector は syslog イベントを Security Services Exchange へ転送します。 |
| 3 | Security Services Exchange は、すべての ASA デバイスからイベントデータを集約し、JSON 形式に変換して、ストレージ用に セキュリティ分析とロギング に送信します。 |

| ステップ | 説明 |
|---|---|
| 4 | セキュリティ分析とロギングは、さまざまなサービスを使用してイベントデータを分類および強化し、Security Cloud Control で使用できるようにします。 |
| 5 | Cisco Security Cloud Control は、クラウドデータストアにイベントデータを保存します。Security Cloud Control は、SOC アナリストに関連情報を提供するために、保存されたデータをクエリします。 |

# ASA デバイスに安全なロギング分析（SaaS）を導入する

### はじめる前に

- 『ASA デバイスの安全なロギング分析（SaaS）』で以下について確認してください。
  - Cisco Cloud へのイベントの送信方法
  - ソリューションに含まれるアプリケーション
  - 必要なライセンス
  - 必要なデータプラン
- すでにマネージド サービス プロバイダーまたは Security Cloud Control セールス担当者に問い合わせて Security Cloud Control テナントを作成しました。
- Secure Device Connector についてを確認してください。SDC を使用して Security Cloud Control を ASA に接続することは「ベストプラクティス」と考えられますが、必須ではありません。
- ネットワークで SDC を展開する場合、次の方法を使用してインストールできます。
  - Secure Device Connector および Secure Event Connector を実行するための VM の展開 を使用します。
- テナントに 1 つ以上の SEC がインストールされており、任意の ASA から、テナントにオンボーディングされた任意の SEC にイベントを送信できます。

### Cisco Security Analytics and Logging（SaaS）の展開と Secure Event Connector を介した Cisco Cloud へのイベント送信のワークフロー

1. 上の「はじめる前に」を参照し、環境が適切に構成されていることを確認してください。
2. ユーザー名とパスワードを使用した ASA デバイスの Security Cloud Control への導入準備
3. ASA Syslog イベントを Cisco Cloud に送信します。
4. Security Cloud Control マクロを使用して ASA デバイスの NSEL を設定します。

5. Security Cloud Control にイベントが表示されていることを確認します。ナビゲーションバーから **[イベントとログ（Events & Logs）]** > **[イベント（Events）]** > **[イベントロギング（Events Logging）]** を選択します。ライブイベントを表示するには、[ライブ（Live）] タブをクリックします。

### Secure Event Connector に関する問題のトラブルシューティング

ステータス情報とロギング情報の収集については、次のトラブルシューティングトピックを使用してください。

- Secure Event Connector オンボーディングのトラブルシューティング
- イベントロギングのトラブルシューティング ログ ファイル
- Secure Event Connector の状態を把握するためのヘルスチェックの使用

### ワークフロー

「Security and Analytics Logging イベントを使用したトラブルシューティング」では、Cisco Security Analytics and Logging から生成されたイベントを使用して、ユーザーがネットワークリソースにアクセスできなかった原因を特定する方法について説明しています。

「Firepower Threat Defense イベントに基づくアラートの使用」も参照してください。

# Security Cloud Control マクロを使用した Cisco Cloud への Cisco ASA Syslog イベントの送信

「コマンド ライン インターフェイスを使用した Cisco Cloud への Cisco ASA Syslog イベントの送信」で説明されているすべてのコマンドを使用する Security Cloud Control マクロを作成し、同じバッチのすべての Cisco ASA でそのマクロを実行することにより、すべての Cisco ASA を設定してイベントを Cisco Cloud に送信します。

Security Cloud Control のマクロツールを使用すると、CLI コマンドのリストを作成し、コマンドシンタックスの要素をパラメータに変換してから、コマンドのリストを保存して、複数回使用できるようにできます。マクロは、一度に複数のデバイスで実行することもできます。

実証済みのマクロを使用すると、デバイス間の設定の一貫性が促進され、コマンド ライン インターフェイスの使用時に発生する可能性のあるシンタックスエラーが防止されます。

先に進む前に、「Security Cloud Control 設定ガイド」でマクロを確認し、マクロの使用方法を把握してください。この記事では、最終的なマクロの作成についてのみ説明します。

## ASA セキュリティ分析とロギング（SaaS）マクロを作成する

次の手順では、Cisco ASA CLI コマンドとマクロ形式の 2 種類の形式を使用できます。Cisco ASA CLI コマンドは、Cisco ASA の構文表記法に従うように記述されています。CLI の詳細に

ついては、「コマンドライン インターフェイスの使用」を参照してください。Security Cloud Control

開始する前に、マクロを作成しながらコマンドの説明を読むことができるように、別ウィンドウで「Cisco Cloud への ASA Syslog イベントの送信」を開き、この手順と並行して読めるようにしてください。

（注） Cisco ASA にロギング設定がすでに存在する場合、Security Cloud Control からマクロを実行しても、最初に既存のロギング設定がすべてクリアされるわけではありません。その代わり、Security Cloud Control マクロで定義された設定は、既存の設定にマージされます。

### 手順

**ステップ 1** プレーンテキストエディタを開き、以下の手順とオプションに基づいて、マクロに変換するコマンドのリストを作成します。Security Cloud Control は、マクロに記述された順序でコマンドを実行します。一部のコマンドには、{{parameters}} に変換する値が含まれます。これは、マクロの実行時に入力することになります。

**ステップ 2** SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように Cisco ASA を設定します。

**logging host** コマンドを使用して、メッセージ送信先の syslog サーバーとして SEC を指定します。テナントにオンボーディングした SEC のいずれかにイベントを送信できます。

**logging host** コマンドは、イベント送信先の TCP または UDP ポートを指定します。どのポートを使用するかを判断するには、「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

**logging host***interface_nameSEC_IP_address*{**tcp/port** | **udp/port**}

syslog イベントを SEC に送信するために使用するプロトコルに応じて、このコマンドを 2 つの異なるマクロのいずれかに変換します。

logging host {{interface_name}} {{SEC_ip_address}} tcp/{{port_number}}

logging host {{interface_name}} {{SEC_ip_address}} udp/{{port)_number}}

（任意）TCP を使用する場合、次のコマンドをマクロのコマンドリストに追加できます。パラメータは必要としません。

**logging permit-hostdown**

**ステップ 3** **syslog サーバに送信する syslog メッセージを指定します。**

**logging trap** コマンドを使用して、syslog サーバーに送信する syslog メッセージを指定します。

**logging trap**{*severity_level* | *message_list*}

SEC に送信されるイベントをシビラティ（重大度）レベルで定義する場合は、コマンドを次のマクロに変換します。

logging trap {{severity_level}}

メッセージリストの一部であるイベントのみを SEC に送信する場合は、コマンドを次のマクロに変換します。

logging trap {{message_list_name}}

前のステップで **logging trap message_list** コマンドを選択した場合は、メッセージリスト内で syslog を定義する必要があります。マクロを作成しながらコマンドの説明を読むことができるように、「カスタムイベントリストの作成」を開いておきます。次のコマンドで開始します。

**logging list***name* {**level***level* [**class***message_class*] | **message***start_id* [*-end_id*] }

次に、これを次のバリエーションに分割します。

logging list {{message_list_name}} level {{security_level}}

logging list {{message_list_name}} level {{security_level}} class {{message_class}}

logging list {{message_list_name}} message {{syslog_range_or_number}}

最後のバリエーションでは、メッセージパラメータ{{syslog_range_or_number}} は、単一の syslog ID（106023）または範囲（302013-302018）として入力できます。メッセージリストを作成するには、1 つまたは複数のコマンドバリエーションを任意の行数で使用します。単一のマクロでは、同じ名前のすべてのパラメータで、入力した同じ値が使用されることに注意してください。Security Cloud Control は、空のパラメータを含むマクロを実行しません。

**重要**
マクロでは、**logging list** コマンドは **logging trap** コマンドの前に置く必要があります。最初にリストを定義すると、**logging trap** コマンドでそれを使用できます。下のサンプルマクロを参照してください。

**ステップ 4** （任意）**syslog timestamp** を追加します。 Cisco ASA の syslog メッセージから生じたメッセージに日付と時刻を追加する場合は、このコマンドを追加します。タイムスタンプの値は **SyslogTimestamp** フィールドに表示されます。このコマンドをコマンドのリストに追加します。パラメータは必要としません。

**logging timestamp**

（注）
バージョン 9.10(1) 以降、Cisco ASA には、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションが用意されています。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。

```
 <166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

。

**ステップ 5** （任意）**非 EMBLEM 形式の syslog メッセージにデバイス ID を含めます。**マクロを作成しながらコマンドの説明を読むことができるように、「非 EMBLEM 形式の syslog メッセージへのデバイス ID の挿入」を開いておきます。次は、マクロのベースとなる CLI コマンドです。

**logging device-id** {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string***text*}

次に、これを次のバリエーションに分割します。

**logging device-id cluster-id**

**logging device-id context-name**

**logging device-id  hostname**

**logging device-id ipaddress** {{interface_name}} **system**

**logging device-id string** {{text_16_char_or_less}}

**ステップ 6**　**ロギングを有効にします。**次のコマンドをそのままマクロに追加します。パラメータはありません。

**logging enable**

**ステップ 7**　マクロの最終行に **write memory を追加しないでください。**代わりに、**show running-config logging** コマンドを追加して、入力したロギングコマンドの結果を確認してから、ロギングコマンドを Cisco ASA のスタートアップ コンフィギュレーションにコミットします。

**show running-config logging**

**ステップ 8**　設定の変更が行われたことを確認したら、**write memory** コマンド用に別のマクロを作成するか、Security Cloud Control一括コマンド ライン インターフェイス 機能を使用して、設定したすべてのデバイスにマクロを使用してコマンドを発行できます。

**write memory**

**ステップ 9**　**（任意）アクセスコントロールルール「許可」イベントのロギングを有効化します。**ASA Syslog イベントを Cisco Cloud に送信する手順で説明されているこのステップは、このマクロには含まれていません。代わりに Security Cloud Control GUI で実行されます。

**ステップ 10**　マクロを保存します。

---

**例**

1 つのマクロに結合されるコマンドのリストのサンプルを次に示します。

```
logging host {{interface_name}} {{SEC_ip_address}} {{tcp_or_udp}}/{{port_number}}
logging permit-hostdown
logging list {{message_list_name}} level {{security_level}}
logging list {{message_list_name}} message {{syslog_range_or_number_1}}
logging list {{message_list_name}} message {{syslog_range_or_number_2}}
logging trap {{message_list_name}}
logging device-id cluster-id
logging enable
show running-config logging
```

（注）　特定のさまざまな syslog ID または範囲を追加するための logging list コマンドがいくつかあります。{{syslog_range_or_number_X}} パラメータには、数値またはその他の差別化要因が必要です。そうしないと、マクロが入力されたときにすべての値が同じになります。また、すべてのパラメータに値が指定されていない場合、Security Cloud Control はマクロを実行しないため、マクロには実行するコマンドのみ含めてください。すべての syslog ID を同じリストに含める必要があるため、event_list_name は各行で同じままです。

### 次のタスク

#### マクロの実行

Cisco ASA Security Analytics and Logging マクロを作成して保存したら、マクロを実行して Cisco ASA syslog イベントを Cisco Cloud に送信します。

# コマンドラインインターフェイスを使用した Cisco Cloud への ASA Syslog イベントの送信

この手順では、ASA の syslog イベントを Secure Event Connector（SEC）に転送してから、ロギングを有効にする方法について説明します。以下の手順では、ワークフローの完了に必要な事柄のみを説明します。ASA でロギングを設定できるすべての方法の広範な説明については、『ASDM1: Cisco ASA Series General Operations ASDM Configuration Guide』または『CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide』のいずれかのモニタリングに関する章を参照してください。

### ASA コマンドのサポート制限

Security Cloud Control では、次の syslog コマンドまたはメッセージの形式はまだサポートされていません。

- syslog の EMBLEM 形式
- Secure Syslog

## Cisco ASA の Security Cloud Control コマンド ライン インターフェイス

この手順に含まれるタスクはすべて、Security Cloud Control の Cisco ASA 用のコマンド ライン インターフェイスで作業します。コマンド ライン インターフェイスのページを開くには、次の手順を実行します。

### 手順

**ステップ 1** 左側のナビゲーションバーで、**[セキュリティデバイス（Security Devices）]** をクリックします。

**ステップ 2** [デバイス] タブをクリックします。

**ステップ 3** 適切なデバイスタイプのタブをクリックし、ロギングを有効にする Cisco ASA を選択します。

**ステップ 4** 右側の[デバイスアクション（Device Actions）]ペインで、[>_コマンドラインインターフェイス（>_Command Line Interface）] をクリックします。

**ステップ 5** [コマンドラインインターフェイス（Command Line Interface）] タブをクリックします。プロンプトで以下に説明するコマンドを入力する準備ができました。

すべてのコマンドを入力したら、[送信（Send）] をクリックします。Security Cloud Control の CLI インターフェイスは Cisco ASA に直接接続されるため、コマンドはデバイスの実行コンフィギュレーションに即座に書き込まれます。Cisco ASA のスタートアップ コンフィギュレーションに変更を書き込むには、さらに `write memory` コマンドを発行する必要があります。

# ASA Syslog イベントの Secure Event Connector への転送

オンボードした Secure Event Connector（SEC）の 1 つに Cisco ASA syslog イベントを転送し、ロギングを有効にするには、次の手順で以下のタスクを完了する必要があります。

**手順**

**ステップ 1** SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように Cisco ASA を設定します。

**ステップ 2** すべてのログのシビラティ（重大度）レベル、または SEC に送信する syslog イベントのリストを決定します。

**ステップ 3** ロギングをイネーブルにします。

**ステップ 4** Cisco ASA のスタートアップ コンフィギュレーションに変更を保存します。

# CLI を使用した Cisco Cloud への Cisco ASA Syslog イベントの送信

**手順**

**ステップ 1** SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように Cisco ASA を設定します。

Cisco ASA から Cisco Cloud に syslog イベントを送信する場合、ユーザーは SEC が外部の syslog サーバーであるかのように SEC に転送し、SEC はメッセージを Cisco Cloud に転送します。

syslog メッセージを SEC に送信するには、次の手順を実行します。

1. TCP または UDP を使用して、SEC が syslog サーバーであるかのように、SEC にメッセージを送信するように Cisco ASA を設定します。SEC は、IPv4 アドレスまたは IPv6 アドレスを使用できます。TCP ポートと UDP ポートのいずれかにイベントを送信します。どのポートを使用するかを判断するには、「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。

   **logging host** コマンドシンタックスの例を次に示します。

   **logging host** *interface_name SEC_IP_address* [ [ **tcp/port** ] | [ **udp/port** ] ]

   例：

```
 > logging host mgmt 192.168.1.5 tcp/10125
> logging host mgmt 192.168.1.5 udp/10025
> logging host mgmt 2002::1:1 tcp/10125
> logging host mgmt 2002::1:1 udp/10025
```

- **interface_name** 引数は、syslog サーバーへのメッセージの送信元である Cisco ASA インターフェイスを指定します。SDC との通信にすでに使用されているのと同じ Cisco ASA インターフェイスを介して、syslog メッセージを SDC に送信するのが「ベストプラクティス」です。
- **SEC_IP_address** 引数には、SEC がインストールされている VM の IP アドレスが含まれている必要があります。
- キーワードと引数のペア **tcp/port** または **udp/port** は、TCP プロトコルと関連するポート、または UDP プロトコルと関連するポートのいずれかを使用して、syslog メッセージが送信されるように指定します。UDP または TCP のいずれかを使用して syslog サーバーにデータを送信するように ASA を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

  TCP を指定すると、ASA は syslog サーバーの障害を検出し、セキュリティ保護として ASA 経由の新しい接続をブロックします。TCP syslog サーバーへの接続状態に関係なく新しい接続を許可するには、ステップ b を参照してください。UDP を指定すると、syslog サーバーが動作状態に関係なく、Cisco ASA は新しい接続を許可し続けます。有効なポート値

  （注）
  Cisco ASA メッセージを 2 台の別の syslog サーバーに送信する場合は、もう一方の syslog サーバーの適切なインターフェイス、IP アドレス、プロトコル、およびポートを使用して、2 番目の logging host コマンドを実行できます。

2. （任意）TCP 経由で SEC にイベントを送信していて、SEC がダウンしているか、Cisco ASA のログ キューがいっぱいの場合、新しい接続はブロックされます。新しい接続は、syslog サーバーがバックアップされ、ログ キューがいっぱいでなくなった後に再度許可されます。TCP syslog サーバーへの接続の状態に関係なく新しい接続を許可するには、次のコマンドを使用して、TCP 接続された syslog サーバーがダウンしたときに新しい接続をブロックする機能を無効にします。

   **logging permit-hostdown**

   例：

   ```
    > logging permit-hostdown
   ```

**ステップ 2** 次のコマンドを使用して、**syslog サーバーに送信する syslog メッセージを指定します。**

**logging trap** { severity_level | message_list }

例：

```
> logging trap 3
> logging trap asa_syslogs_to_cloud
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。

message_list 引数は、カスタムイベントリストを作成した場合、そのリストの名前に置き換えられます。カスタムイベントリストの指定に必要な操作は、そのリストにある syslog メッセージを Secure Event Connector に送信することだけです。上記の例では、asa_syslogs_to_cloud がイベントリストの名前です。

message_list を使用すると、Cisco Cloud に送信する syslog メッセージを明確に指定できるため、費用を節約できます。

message_list を作成するには、「カスタムイベントリストの作成」を参照してください。詳細については、セキュリティ分析とロギング ライセンス （36 ページ） を参照してください。

### ステップ 3 （オプション）syslog タイムスタンプの追加

logging timestamp コマンドを使用して、Cisco ASA での syslog メッセージの発信日時をメッセージに追加します。タイムスタンプの値は **SyslogTimestamp** フィールドに表示されます。

**例**：

```
> logging timestamp
```

（注）
バージョン 9.10(1) 以降、Cisco ASA には、イベントの syslog で RFC 5424 に従ってタイムスタンプを有効にするオプションが用意されています。このオプションを有効にすると、Syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for protocol from
 src interface :src IP/src port to dest IP/dest port.
```

### ステップ 4 （オプション）非 EMBLEM 形式の Syslog メッセージにデバイス ID を含める

デバイス ID は、syslog メッセージに挿入できる識別子で、特定の Cisco ASA から送信されたすべての syslog メッセージを簡単に区別できます。詳細については、「非 EMBLEM 形式の Syslog メッセージにデバイス ID を含める」を参照してください。

### ステップ 5 （オプション）アクセス制御ルール「許可」イベントのロギングの有効化

アクセス制御ルールによってリソースへのアクセスが拒否されると、イベントが自動的にログに記録されます。アクセス制御ルールによってリソースへのアクセスが許可されたときに生成されたイベントもログに記録する場合は、アクセス制御ルールのロギングをオンにして、シビラティ（重大度）タイプを設定する必要があります。個々のネットワークアクセス制御ルールのロギングをオンにする方法については、「ログルールアクティビティ」を参照してください。

（注）
アクセス制御ルール「許可」イベントでのロギングを有効にすると、購入したデータプランはイベントの毎日の取り込み率に基づいているため、データの消費量が増大します。

### ステップ 6 ロギングの有効化

コマンドプロンプトで、「logging enable」と入力します。Cisco ASA では、個々のルールではなく、デバイス全体に対してロギングが有効になります。

例：

```
 > logging enable
```

（注）
現時点では、Security Cloud Control はセキュアロギングの有効化をサポートしていません。

**ステップ 7** スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、「write memory」と入力します。Cisco ASA では、個々のルールではなく、デバイス全体に対してロギングが有効になります。

例：

```
> write memory
```

**関連情報**：

- SDC 仮想マシンへの Secure Event Connector のインストール （2 ページ）
- テナントに 2 番目以降の SEC をインストールする

# カスタム イベント リストの作成

Cisco ASA syslog イベントを Cisco Cloud に送信するときに、次のいずれかの方法を使用してカスタムイベントリストを作成します。

- コマンド ライン インターフェイスを使用した Cisco Cloud への ASA Syslog イベントの送信
- Security Cloud Control マクロを使用した Cisco Cloud への Cisco ASA Syslog イベントの送信

次の 3 つの基準に基づいて、message_list とも呼ばれるイベントリストを作成できます。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（syslog サーバーや Secure Event Connector など）に送信するカスタムイベントリストを作成するには、次の手順を実行します。

**手順**

**ステップ 1** 左側のナビゲーションバーで、**[セキュリティデバイス（Security Devices）]** をクリックします。
**ステップ 2** [デバイス] タブをクリックします。
**ステップ 3** 適切なタブをクリックして、syslog メッセージをカスタムイベントリストに含める Cisco ASA を選択します。

**ステップ 4** [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

**ステップ 5** 次のコマンドシンタックスを使用して、**logging list** コマンドを Cisco ASA に発行します。

**logging list** *name* { **level** *level* [ **class** *message_class* ] | **message** *start_id* [ *-end_id* ] }

*name* 引数には、リストの名前を指定します。キーワードと引数のペア **level** *level* により、シビラティ（重大度）が指定されます。キーワードと引数のペア **class** *message_class* により、特定のメッセージクラスが指定されます。キーワードと引数のペア **message** *start_id* [*-end_id*] により、個々の syslog メッセージ番号または番号の範囲が指定されます。

（注）
重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベントリスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベントリスト名は使用しないでください。

- **シビラティ（重大度）に基づいてイベントリストに syslog メッセージを追加します。**たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。

  例：

  ```
  > logging list asa_syslogs_to_cloud level 3
  ```

- **他の基準に基づいて syslog メッセージをイベントリストに追加します。**

  前回の手順で使用したものと同じコマンドを入力し、既存のメッセージ リストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

  - ID が 302013 ～ 302018 の範囲の syslog メッセージ。
  - シビラティ（重大度）が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
  - シビラティ（重大度）が warning 以上（emergency、alert、critical、error、または warning）のすべての HA クラス syslog メッセージ。

    例：

    ```
    > logging list asa_syslogs_to_cloud message 302013-302018
    > logging list asa_syslogs_to_cloud level critical
    > logging list asa_syslogs_to_cloud level warning class ha
    ```

    （注）
    syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

**ステップ 6** スタートアップ コンフィギュレーションへの変更の保存

コマンドプロンプトで、「**write memory**」と入力します。

例：

```
> write memory
```

# 非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

非 EMBLEM 形式の syslog メッセージにデバイス ID を含めるように Cisco ASA を設定できます。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。この手順は、次の手順によって参照されます。

- コマンド ライン インターフェイスを使用した Cisco Cloud への ASA Syslog イベントの送信
- Security Cloud Control マクロを使用した Cisco Cloud への Cisco ASA Syslog イベントの送信

このデバイス ID は、[イベントロギング（Event Logging）] ページに表示される syslog イベントの SensorID フィールドに反映されます。

## 手順

**ステップ 1** デバイス ID を割り当てる syslog メッセージが属す Cisco ASA を選択します。

**ステップ 2** [デバイスアクション（Device Actions）] ペインで、[>_コマンドラインインターフェイス（>_ Command Line Interface）] をクリックします。

**ステップ 3** 次のコマンドシンタックスを使用して、デバイスに **logging device-id** コマンドを発行します。

**logging device-id** { **cluster-id** | **context-name** | **hostname** | **ipaddress***interface_name* [ **system** ] | **string***text* }

例：

```
> logging device-id hostname
> logging device-id context-name
> logging device-id string Cambridge
```

**context-name** キーワードは、現在のコンテキストの名前を装置 ID として使用することを示します（マルチ コンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**システム**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注）
Cisco ASA クラスタでは、選択したインターフェイスのプライマリユニットの IP アドレスが常に使用されます。

**Cluster-id** キーワードは、デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

**hostname** キーワードは、ASA のホスト名をデバイス ID として使用するように指定します。

**ipaddress** *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッ

セージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。

**string** *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

**ステップ 4　スタートアップ コンフィギュレーションへの変更の保存**

コマンドプロンプトで、「**write memory**」と入力します。

例：

```
> write memory
```

# ASA デバイス向け NetFlow Secure Event Logging（NSEL）

Cisco ASA からの基本的な Syslog メッセージには、Cisco ASA によって報告されたイベントが脅威を示しているかどうかを Cisco Security Analytics および Logging が判断するために必要なデータが不足しています。Netflow Secure Event Logging（NSEL）は、そのデータを Cisco Security Analytics および Logging に提供します。

「フローは、ネットワークデバイスを通過する、いくつかの共通プロパティを持つ一方向のパケットシーケンスとして定義されます。これらの収集されたフローは、外部デバイスである NetFlow コレクターにエクスポートされます。ネットワークフローは非常に細分化されています。たとえば、フローレコードには IP アドレス、パケット数とバイト数、タイムスタンプ、タイプオブサービス（ToS）、アプリケーションポート、入出力インターフェースなどの詳細が含まれます。」[1]

Cisco ASA では、NetFlow バージョン 9 サービスがサポートされています。ASA の NSEL を実装することで、フロー内の重要なイベントを示すレコードだけをエクスポートする、ステートフルな IP フローのトラッキング方式が可能となります。ステートフル フロー トラッキングでは、追跡されるフローは一連のステートの変更を通過します。

このドキュメントでは、Security Cloud Control マクロを使用して ASA に NetFlow を設定するための簡単なアプローチについて説明します。『Cisco ASA NetFlow Implementation Guide』には、ASA に NetFlow を設定することに関する非常に詳細な説明が記載されており、このコンテンツに付随する貴重なリソースとなっています。

### 次の作業

「Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定」を参照してください。

### 関連記事

- Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定
- ASA から NetFlow Secure Event Logging（NSEL）を削除する
- ASA グローバルポリシーの名前を決定する

1. （『Cisco Systems NetFlow Services Export Version 9』インターネット技術特別委員会、ネットワーク ワーキング グループ、コメント要求: 3954、2004 年 10 月、B. Claise 編集。https://www.ietf.org/rfc/rfc3954.txt）

# Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定

ASA は、NetFlow Secure Event Logging（NSEL）を使用して詳細な接続イベントデータをレポートします。この接続イベントデータ（双方向フロー統計を含む）に Cisco Secure Cloud Analytics を適用できます。この手順では、ASA デバイスで NSEL を設定し、NSEL イベントをフローコレクタに送信する方法について説明します。このケースでは、フローコレクタは Secure Event Connector（SEC）です。

この手順では、**Configure NSEL** マクロを参照します。

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate {{timeout_rate_in_mins}}
flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
flow-export active refresh-interval {{refresh_interval_in_mins}}
class-map {{flow_export_class_name}}
     match {{add_this_traffic_to_class_map}}
policy-map {{global_policy_map_name}}
     class {{flow_export_class_name}}
          flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}
service-policy {{global_policy_map_name}} global
logging flow-export-syslogs disable
show run flow-export
show run policy-map {{global_policy_map_name}}
show run class-map {{flow_export_class_name}}
```

クラスマップの一般名、グローバルポリシーに追加されたクラスマップなど、すべてのデフォルト値が入力された Configure NSEL マクロの例を次に示します。これらの手順を完了すると、マクロは次のようになります。

```
 flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}
flow-export template timeout-rate 60
flow-export delay flow-create 55
flow-export active refresh-interval 1
class-map flow_export_class_map
```

```
     match any
policy-map global_policy
     class flow_export_class_map
          flow-export event-type all destination {{SEC_IPv4_address}}
logging flow-export-syslogs disable
show run flow-export
show run policy-map global_policy
show run class-map flow_export_class_map
```

### はじめる前に

次の情報を用意します。

- これまでに Security Cloud Control のマクロを使用したことがない場合は、Security Cloud Control のコンフィギュレーション ガイドでマクロについて参照してください。
- ASA からデータを受け取る SEC の IPv4 アドレス
- SEC にデータを送信する ASA のインターフェイス
- NetFlow イベントの転送に使用する UDP ポート番号「Secure Logging Analytics（SaaS）に使用されるデバイスの TCP、UDP、および NSEL ポートの検索 （25 ページ）」を参照してください。
- ASA グローバルポリシーの名前の決定 （67 ページ）

### ワークフロー（Workflow）

Security Cloud Control マクロを使用して ASA デバイスの NSEL を設定するには、次のワークフローに従います。各手順に従う必要があります。

1. [NSELの設定（Configuring NSEL）] マクロを開く （60 ページ）。
2. NSEL メッセージの宛先と SEC に送信される間隔の定義 （60 ページ）。
3. SEC に送信される NSEL イベントを定義するクラスマップの作成 （61 ページ）。
4. NSEL イベントのポリシーマップの定義 （62 ページ）。
5. 冗長な Syslog メッセージの無効化 （63 ページ）。
6. マクロのレビューと送信 （65 ページ）。

### 次の作業

[NSELの設定（Configuring NSEL）] マクロを開く （60 ページ）に移動して、前述のワークフローを開始します。

# [NSELの設定（Configuring NSEL）] マクロを開く

### 始める前に

これは長いワークフローの最初の部分です。開始する前に Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定 （58 ページ） を参照してください。

### 手順

**ステップ 1** **[セキュリティデバイス（Security Devices）]** ページで [デバイス（Devices）] タブをクリックします。

**ステップ 2** 適切なデバイスタイプのタブをクリックし、NetFlow セキュアイベントロギング（NSEL）を設定する ASA を選択します。

**ステップ 3** [デバイスアクション（Device Actions）] ペインで、[コマンドラインインターフェイス（Command Line Interface）] をクリックします。

**ステップ 4** マクロスター  Macros をクリックして、使用可能なマクロのリストを表示します。

**ステップ 5** マクロのリストから、[NSELの設定（Configuring NSEL）] を選択します。

**ステップ 6** [マクロ（Macro）] ボックスで、[パラメータの表示（View Parameters）] をクリックします。

### 次のタスク

NSEL メッセージの宛先と SEC に送信される間隔の定義 （60 ページ） に進みます。

# NSEL メッセージの宛先と SEC に送信される間隔の定義

NSEL メッセージは、テナントにオンボーディングした SEC のいずれかに送信できます。以下の手順では、このセクションのマクロを参照しています。

flow-export destination {{interface}} {{SEC_IPv4_address}} {{SEC_NetFlow_port}}

flow-export template timeout-rate {{timeout_rate_in_mins}}

flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

flow-export active refresh-interval {{refresh_interval_in_mins}}

### 始める前に

この手順は、より大きなワークフローの一部です。始める前にSecurity Cloud Control マクロを使用した ASA デバイスの NSEL の設定 （58 ページ）を参照してください。

### 手順

**ステップ 1** **flow-export destination** コマンドは、NetFlow パケットの送信先のコレクタを定義します。この場合、SEC に送信します。次のパラメータのフィールドに入力します。

- **{{interface}}**：NetFlow イベントの送信元である ASA のインターフェイス名を入力します。
- **{{SEC_IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{SEC_NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

**ステップ 2** **flow-export template timeout-rate** コマンドは、テンプレートレコードがすべての設定された出力先に送信される間隔を指定します。

- **{{timeout_rate_in_mins}}**：テンプレートが再送信されるまでの分数を入力します。60 分の値を使用することをお勧めします。SEC はテンプレートを処理しません。数字を大きくすると、SEC へのトラフィックが減少します。

**ステップ 3** **flow-export delay flow-create** コマンドは、flow-create イベントの送信を指定した秒数遅らせます。この値は、推奨されるアクティブタイムアウト値と一致し、ASA からエクスポートされるフローイベントの数を減らします。この場合、NSEL イベントが最初に Security Cloud Control に表示されるのは、接続の終了時または接続の作成から 55 秒以内のいずれか早い方となると考えてください。このコマンドが設定されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。

- **{{delay_flow_create_rate_in_secs}}**：flow-create イベントの送信間の遅延秒数を入力します。55 秒の値を使用することをお勧めします。

**ステップ 4** **flow-export active refresh-interval** コマンドは、長時間フローのステータスの更新が ASA から送信される頻度を定義します。有効な値は 1 ～ 60 分です。[フロー更新間隔（Flow Update Interval）] フィールドで、**flow-export active refresh-interval** を **flow-export delay flow-create interval** よりも少なくとも 5 秒長く設定すると、flow-update イベントが flow-creation イベントの前に表示されなくなります。

- **{{refresh_interval_in_mins}}**：**値を 1 分にすることをお勧めします。**有効な値は 1 ～ 60 分です。

### 次のタスク

SEC に送信される NSEL イベントを定義するクラスマップの作成 （61 ページ） に進みます。

## SEC に送信される NSEL イベントを定義するクラスマップの作成

マクロ内の次のコマンドは、クラス内のすべての NSEL イベントをグループ化し、そのクラスを Secure Event Connector（SEC）にエクスポートします。以下の手順では、このセクションのマクロを参照しています。

```
class-map {{flow_export_class_name}}
match {{add_this_traffic_to_class_map}}
```

### 始める前に

この手順は、より大きなワークフローの一部です。始める前にSecurity Cloud Control マクロを使用した ASA デバイスの NSEL の設定 （58 ページ）を参照してください。

### 手順

**ステップ 1** **class-map** コマンドは、SEC にエクスポートされる NSEL トラフィックを識別するクラスマップに名前を付けます。

- **{{flow-export-class-name}}**：クラスマップの名前を入力します。名前の長さは最大 40 文字です。名前「class-default」と、「_internal」または「_default」で始まる名前はすべて予約されています。すべてのタイプのクラスマップで同じ名前空間が使用されるため、別のタイプのクラスマップですでに使用されている名前は再度使用できません。

**ステップ 2** クラスマップに関連付けられる（一致する）トラフィックを識別します。**{{add_this_traffic_to_class_map}}** の値として、次のいずれかのオプションを選択します。

- **{{add_this_traffic_to_class_map}}** フィールドに **any** と入力します。NSEL トラフィックのすべてのトラフィックタイプが監視されます。**値「any」を使用することをお勧めします。**
- **{{add_this_traffic_to_class_map}}** フィールドに **access-list *name-of-access-list*** と入力します。作成したアクセスリストに関連付けられたすべてのトラフィックが関連付けられます。詳細については、Cisco ASA NetFlow 実装ガイド [英語] の「Configure Flow-Export Actions Through Modular Policy Framework」を参照してください。

### 次のタスク

NSEL イベントのポリシーマップの定義 （62 ページ） に進みます。

## NSEL イベントのポリシーマップの定義

このタスクでは、前のタスクで作成したクラスに NetFlow エクスポートアクションを割り当て、そのクラスを新しいポリシーマップに割り当てます。以下の手順では、このセクションのマクロを参照しています。

policy-map {{global_policy_map_name}}

class {{flow_export_class_name}}

flow-export event-type {{event_type}} destination {{SEC_IPv4_address}}

### 始める前に

この手順は、より大きなワークフローの一部です。始める前にSecurity Cloud Control マクロを使用した ASA デバイスの NSEL の設定 （58 ページ）を参照してください。

手順

**ステップ 1** **policy-map** コマンドは、ポリシーマップを作成します。次のタスクでは、このポリシーマップをグローバルポリシーに関連付けます。

- **{{global_policy_map_name}}**：ポリシーマップの名前を入力します。ファイアウォールの既存のグローバルポリシーがある場合は、その名前を使用することをお勧めします。グローバルポリシーのデフォルト名は **global_policy** です。「ASA グローバルポリシーの名前の決定」を参照してください。新しいポリシーマップを作成し、『Cisco ASA NetFlow 実装ガイド』の「モジュラ ポリシー フレームワークを使用した flow-export アクションの設定」に従ってグローバルに適用すると、残りの検査ポリシーは非アクティブ化されます。

**ステップ 2** **class** コマンドでは、SEC に送信される NSEL イベントを定義するクラスマップの作成 （61 ページ）で作成したクラスマップの名前が継承されます。

**ステップ 3** **flow-export event-type** {{event-type}} **destination** {{IPv4_address}} コマンドは、フローコレクター（この場合は SEC）に送信する必要があるイベントタイプを定義します。

- **{{event-type}}**：event_type キーワードは、フィルタリングされるサポートされているイベントの名前です。値「all」を使用することをお勧めします。
- **{{SEC_IPv4_address}}**：これは SEC の IPv4 アドレスです。その値は、NSEL メッセージの宛先と SEC に送信される間隔の定義 （60 ページ）で入力した値から継承されます。

次のタスク

冗長な Syslog メッセージの無効化 （63 ページ） に進みます。

## 冗長な Syslog メッセージの無効化

以下の手順では、このセクションのマクロを参照しています。コマンドを変更する必要はありません。

logging flow-export-syslogs disable

NetFlow でフロー情報をエクスポートできるようにすると、次の表に記載されている syslog メッセージが冗長になります。パフォーマンスの向上のためには、同じ情報が NetFlow を通してエクスポートされるため、冗長な syslog メッセージを無効化することをお勧めします。

（注） NSEL メッセージと syslog メッセージの両方がイネーブルにされている場合、2 つのロギングタイプ間が時系列順になる保証はありません。

| syslog メッセージ | 説明 | NSEL イベント ID | NSEL 拡張イベント ID |
|---|---|---|---|
| 106100 | アクセスコントロールルール（ACL）が発生するたびに生成されます。 | 1：フローが作成されました（ACLがフローを許可した場合）。<br>3：フローが拒否されました（ACLがフローを拒否した場合）。 | 0：ACL がフローを許可した場合。<br>1001：入力 ACL によってフローが拒否されました。<br>1002：出力 ACL によってフローが拒否されました。 |
| 106015 | 最初のパケットがSYNパケットではなかったため、TCPフローが拒否されました。 | 3：フローが拒否されました。 | 1004：最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。 |
| 106023 | **access-group** コマンドによってインターフェイスに接続されたACLによってフローが拒否された場合。 | 3：フローが拒否されました。 | 1001：入力 ACL によってフローが拒否されました。<br>1002：出力 ACL によってフローが拒否されました。 |
| 302013、302015、302017、302020 | TCP、UDP、GRE、および ICMP 接続の作成。 | 1：フローが作成されました。 | 0：無視します。 |
| 302014、302016、302018、302021 | TCP、UDP、GRE、およびICMP接続のティアダウン。 | 2：フローが削除されました。 | 0：無視します。<br>> 2000：フローが切断されました。 |
| 313001 | デバイスへの ICMP パケットが拒否されました。 | 3：フローが拒否されました。 | 1003：To-the-box フローが設定のために拒否されました。 |
| 313008 | デバイスへの ICMP v6 パケットが拒否されました。 | 3：フローが拒否されました。 | 1003：To-the-box フローが設定のために拒否されました。 |
| 710003 | デバイスインターフェイスへの接続の試行が拒否されました。 | 3：フローが拒否されました。 | 1003：To-the-box フローが設定のために拒否されました。 |

冗長なsyslogメッセージを無効にしない場合は、このマクロを編集して、次の行のみを削除できます。

**logging flow-export-syslogs disable**

後に NetFlow 関連の Syslog メッセージの無効化と再有効化の手順を実行することで、個別の syslog メッセージを有効化または無効化できます。

## マクロのレビューと送信

### 始める前に

この手順は、より大きなワークフローの一部です。始める前に、「Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定 （58 ページ）」を参照してください。

### 手順

**ステップ 1** マクロのフィールドに入力したら、[確認（Review）] をクリックして、コマンドを ASA への送信前に確認します。

**ステップ 2** コマンドへの応答に問題がなければ、[送信（Send）] をクリックします。

**ステップ 3** コマンドを送信した後で、「一部のコマンドが実行コンフィギュレーションに変更を加えた可能性があります」というメッセージが 2 つのリンクとともに表示されることがあります。


- [ディスクへの書き込み（Write to Disk）] をクリックすると、このコマンドによって加えられた変更と、実行コンフィギュレーションのその他の変更がデバイスのスタートアップ構成に保存されます。
- [取り消す（Dismiss）] をクリックすると、メッセージが取り消されます。

Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定 （58 ページ） で説明されているワークフローが完了しました。

# ASA から NetFlow Secure Event Logging（NSEL）を削除する

この手順では、Secure Event Connector（SEC）を NSEL フローコレクタとして指定する ASA で NetFlow Secure Event Logging（NSEL）の構成を削除する方法について説明します。この手順では、「Security Cloud Control マクロを使用した ASA デバイスの NSEL の設定」で説明されているマクロを元に戻します。

この手順では、以下のようにマクロ **DELETE NSEL** を参照しています。

```
policy-map {{flow_export_policy_name}}
no class {{flow_export_class_name}}
no class-map {{flow_export_class_name}}
no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}
no flow-export template timeout-rate {{timeout_rate_in_mins}}
no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}
no flow-export active refresh-interval {{refresh_interval_in_mins}}
logging flow-export-syslogs enable
show run flow-export
```

```
show run policy-map {{flow_export_policy_name}}
show run class-map {{flow_export_class_name}}
```

## DELETE-NSEL マクロを開く

手順

**ステップ 1** **[セキュリティデバイス（Security Devices）]** ページで [デバイス（Devices）] タブをクリックします。

**ステップ 2** 適切なデバイスタイプのタブをクリックし、NetFlow Secure Event Logging（NSEL）の設定を削除する Cisco ASA を選択します。

**ステップ 3** [デバイスアクション（Device Actions）] ペインで、[コマンドラインインターフェイス（Command Line Interface）] をクリックします。

**ステップ 4** マクロスター  をクリックして、使用可能なマクロのリストを表示します。

**ステップ 5** マクロのリストで、[DELETE-NSEL] を選択します。

**ステップ 6** [マクロ（Macro）] ボックスで、[パラメータの表示（View Parameters）] をクリックします。

## マクロに値を入力して No コマンドを完成させる

Cisco ASA CLI では、コマンドの「no」形式を使用してそのコマンドを削除します。マクロのフィールドに入力して、コマンドの「no」形式を完成させます。

手順

**ステップ 1** policy-map {{flow_export_policy_name}}

- **{{flow_export_policy_name}}**：policy-map 名の値を入力します。

**ステップ 2** no class {{flow_export_class_name}}

- **{{flow_export_class_name}}**：class-map 名の値を入力します。

**ステップ 3** no class-map {{flow_export_class_name}}

- **{{flow_export_class_name}}**：class-map 名の値は、上記の手順から継承されます。

**ステップ 4** no flow-export destination {{interface}} {{IPv4_address}} {{NetFlow_port}}

- **{{interface}}**：NetFlow イベントの送信元である Cisco ASA のインターフェイス名を入力します。
- **{{IPv4_address}}**：SEC の IPv4 アドレスを入力します。SEC はフローコレクタとして機能します。
- **{{NetFlow_port}}**：NetFlow パケットが送信された SEC の UDP ポート番号を入力します。

**ステップ 5** no flow-export template timeout-rate {{timeout_rate_in_mins}}

- **{{timeout_rate_in_mins}}**：flow-export template のタイムアウトレートを入力します。

**ステップ 6** no flow-export delay flow-create {{delay_flow_create_rate_in_secs}}

- **{{delay_flow_create_rate_in_secs}}**：flow-export delay flow-create のレートを入力します。

**ステップ 7** no flow-export active refresh-interval {{refresh_interval_in_mins}}

- **{{refresh_interval_in_mins}}**：flow-export active refresh-interval の間隔を入力します。

# ASA グローバルポリシーの名前の決定

ASA のグローバルポリシーの名前を決定するには、次の手順に従います。

**手順**

**ステップ 1** [インベントリ（Inventory）][セキュリティデバイス（Security Devices）] ページで、グローバルポリシーの名前を検索するデバイスを選択します。

**ステップ 2** [デバイスアクション（Device Actions）] ペインで、[>_Command Reference] を選択します。

**ステップ 3** コマンド ライン インターフェイス ウィンドウのプロンプトで、次のように入力します。

**show running-config service-policy**

以下の例の出力では、global_policy はグローバルポリシーの名前です。

例：

> **show running-config service-policy**

**service-policy global_policy global**

# NSEL データフローのトラブルシューティング

Netflow Secure Event Logging（NSEL）を設定したら、次の手順を使用して、NSEL イベントが ASA から Cisco Cloud に送信されていること、および Cisco Cloud がそれらのイベントを受信していることを確認します。

NSEL イベントを Secure Event Connector（SEC）に送信してから Cisco Cloud に送信するように ASA を設定すると、データはすぐには流れないことに注意してください。ASA で NSEL 関連のトラフィックが生成されていると仮定すると、最初の NSEL パケットが到着するまでに数分かかることがあります。

（注） このワークフローは、「flow-export counters」コマンドと「capture」コマンドを単純に使用してNSELデータフローをトラブルシューティングする方法を示しています。これらのコマンドの使用法の詳細については、CLI ブック 1：Cisco ASA シリーズ CLI コンフィギュレーションガイド（一般的な操作）[英語] および Cisco ASA NetFlow 実装ガイド [英語] の「Monitoring NSEL」を参照してください。

次のタスクを実行します。

- NetFlow パケットが SEC に送信されていることを確認する
- NetFlow パケットが Cisco Cloud 受信されていることを確認する

## NSEL イベントが SEC に送信されたことを確認する

次の 2 つのコマンドのいずれかを使用して、NSEL パケットが SEC に送信されていることを確認します。

- flow-export counters
- capture

**「flow-export counters」コマンドは、送信中の flow-export パケットと NSEL エラーをチェックするために使用します。**

- NSEL イベントを SEC に送信するように Cisco ASA が設定されていることを確認してください。「Security Cloud Control マクロを使用した Cisco ASA デバイスの NSEL の設定」を参照してください。
- SEC IP アドレスは、NSEL イベントのフローコレクタアドレスです。テナントに複数の SEC をオンボードしている場合は、正しい IP アドレスを使用していることを確認してください。
- NetFlow イベントの転送に使用する UDP ポート番号を検索します。「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。
- Cisco ASA から NSEL イベントを送信するための推奨インターフェイスは管理インターフェイスですが、お使いのインターフェイスは異なる場合があります。

Security Cloud Control のコマンド ライン インターフェイスを使用して、NSEL 用に設定した Cisco ASA にこれらのコマンドを送信します。

### 手順

**ステップ 1** ナビゲーションウィンドウで、**[セキュリティデバイス（Security Devices）]** をクリックします。
**ステップ 2** [デバイス] タブをクリックします。

**ステップ 3** 適切な [デバイス（Device）] のタブをクリックし、NSEL イベントを SEC に送信するように設定した Cisco ASA を選択します。

**ステップ 4** 右側の [デバイスアクション（Device Actions）] ペインで、[コマンドラインインターフェイス（Command Line Interface）] をクリックします。

**ステップ 5** `clear flow-export counters` コマンドを実行して、フローエクスポートカウンタをリセットします。これにより、エクスポートフローカウンタがクリアされてゼロになるため、新しいイベントの発生を簡単に知ることができます。

例：

```
> clear flow-export counters

Done!
```

**ステップ 6** show flow-export counters コマンドを実行して、NSEL パケットの宛先、送信されたパケットの数、およびエラーを確認します。

例：

```
>show flow-export counters

destination: management 209.165.200.225 10425

Statistics:

packets sent 25000

エラー：

block allocation errors 0

invalid interface 0

template send failure 0

no route to collector 0

source port allocation 0
```

上記の出力では、宛先行は、NSEL イベントの送信元の Cisco ASA のインターフェイス、SEC の IP アドレス、SEC のポート 10425 を示しています。また、25000 のパケットが送信されたことも示しています。

エラーがなく、パケットが送信されている場合は、以下の「NetFlow パケットが Cisco Cloud によって受信されていることを確認する」にスキップしてください。

---

エラーの説明：

- [ブロック割り当てエラー（block allocation errors）]：ブロック割り当てエラーを受け取った場合、Cisco ASA はフローエクスポーターにメモリが割り当てません。
  - 回復処置：Cisco Technical Assistance Center（TAC）に連絡してください。
- [無効なインターフェイス（invalid interface）]：NSEL イベントを SEC に送信しようとしていますが、フローエクスポート用に定義したインターフェイスがそれを行うように設定されていないことを示します。

- 回復処置：NSEL の設定時に選択したインターフェイスを確認します。管理インターフェースを使用することをお勧めします。お使いのインターフェースが異なる場合があります。

- [テンプレート送信失敗（template send failure）]：NSEL を定義するためのテンプレートが正しく解析されませんでした。
  - 回復処置：Security Cloud Control のサポートに連絡してください。

- [コレクタへのルートがない（no route to collector）]：Cisco ASA から SEC へのネットワークルートがないことを示します。
  - 回復処置：
    - NSEL を設定したときに SEC に使用した IP アドレスが正しいことを確認してください。
    - SEC のステータスがアクティブで、最近のハートビートが送信されていることを確認します。SDC に到達不能を参照してください。
    - Secure Device Connector のステータスがアクティブで、最近のハートビートが送信されていることを確認します。

- [送信元ポートの割り当て（source port allocation）]：Cisco ASA にポート不良がある可能性を示しています。

## 「capture」コマンドを使用して、ASAからSECに送信されたNSELパケットをキャプチャする

- NSEL イベントを SEC に送信するように Cisco ASA が設定されていることを確認してください。「Security Cloud Control マクロを使用した Cisco ASA デバイスの NSEL の設定」を参照してください。
- SEC IP アドレスは、NSEL イベントのフローコレクタアドレスです。テナントに複数の SEC をオンボードしている場合は、正しい IP アドレスを使用していることを確認してください。
- NetFlow イベントの転送に使用する UDP ポート番号を検索します。「Cisco Security Analytics and Logging に使用されるデバイスの TCP、UDP、および NSEL ポートの検索」を参照してください。
- Cisco ASA から NSEL イベントを送信するための推奨インターフェイスは管理インターフェイスですが、お使いのインターフェイスは異なる場合があります。

Security Cloud Control のコマンド ライン インターフェイスを使用して、NSEL 用に設定した Cisco ASA にこれらのコマンドを送信します。

手順

**ステップ 1** ナビゲーションウィンドウで、**[セキュリティデバイス（Security Devices）]** をクリックします。

**ステップ 2** [デバイス] タブをクリックします。

**ステップ 3** 適切な [デバイスタイプ（Device Type）] タブをクリックし、NSEL イベントを SEC に送信するように設定した Cisco ASA を選択します。

**ステップ 4** 右側の [デバイスアクション（Device Actions）] ペインで、[コマンドラインインターフェイス（Command Line Interface）] をクリックします。

**ステップ 5** コマンドウィンドウで、以下の [キャプチャ（capture）] コマンドを実行します。

>**capture***capture_name***interface***interface_name* **match udp any host** *IP_of_SEC***eq***NetFlow_port*

引数の説明

- *capture_name* は、パケットキャプチャの名前です。
- *interface_name* は、Cisco ASA から NSEL パケットが送信されるインターフェイスの名前です。
- *IP_of_SEC* は、SEC VM の IP アドレスです。
- *NetFlow_port* は、NSEL イベントが送信されるポートです。

これにより、パケットキャプチャが開始されます。

**ステップ 6** キャプチャされたパケットを表示するには、**show capture** コマンドを実行します。

**> show capture***capture_name*

ここで、*capture_name* は、前の手順で定義したパケットキャプチャの名前です。

キャプチャの時刻、パケットの送信元の IP アドレス、IP アドレス、およびパケットの送信先ポートを示す出力の例を次に示します。この例では、192.168.25.4 は SEC の IP アドレスであり、ポート 10425 は NSEL イベントを受信する SEC 上のポートです。

```
6 パケットがキャプチャされました
1: 14:23:51.706308 192.168.0.169.16431 > 192.168.25.4.10425: udp 476
2: 14:23:53.923017 192.168.0.169.16431 > 192.168.25.4.10425: udp 248
3: 14:24:07.411904 192.168.0.169.16431 > 192.168.25.4.10425: udp 1436
4: 14:24:07.411920 192.168.0.169.16431 > 192.168.25.4.10425: udp 1276
5: 14:24:21.021208 192.168.0.169.16431 > 192.168.25.4.10425: udp 112
6: 14:24:27.444755 192.168.0.169.16431 > 192.168.25.4.10425: udp 196
```

**ステップ 7** パケットキャプチャを手動で停止するには、**capture stop** コマンドを実行します。

**> capture** *capture_name***stop**

ここで、*capture_name* は、前の手順で定義したパケットキャプチャの名前です。

# NetFlow パケットが Cisco Cloud 受信されていることを確認する

### はじめる前に

Cisco ASA から NSEL イベントが送信されていることを確認します。

## ライブ NSEL イベントの確認

ライブイベントと履歴イベントの両方を確認します。

この手順では、過去 1 時間以内に Cisco Cloud が受信した NSEL イベントをフィルタ処理します。

### 手順

**ステップ 1** 左側のペインで、**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[イベントロギング（Events Logging）]** を選択します。

**ステップ 2** [ライブ（Live）] タブをクリックします。

**ステップ 3** イベントフィルタを開いた状態でピン留めします。

**ステップ 4** [Cisco ASAイベント（ASA Events）] セクションで、[NetFlow] がオンになっていることを確認します。

**ステップ 5** [センサーID（Sensor ID）] フィールドで、NSEL イベントを送信するために設定した Cisco ASA の IP アドレスを入力します。

**ステップ 6** フィルタの一番下の [NetFlowイベントを含める（Include NetFlow Events）] がオンになっていることを確認します。

## NSEL のイベント履歴の確認

この手順では、指定した時間枠内に Cisco Cloud が受信した NSEL イベントをフィルタリングします。

### 手順

**ステップ 1** 左側のペインで、**[イベントとログ（Events & Logs）]**>**[イベント（Events）]**>**[イベントロギング（Events Logging）]** を選択します。

**ステップ 2** [履歴（Historic）] タブをクリックします。

**ステップ 3** イベントフィルタを開いた状態でピン留めします。

**ステップ 4** [Cisco ASAイベント（ASA Events）] セクションで、[NetFlow] がオンになっていることを確認します。

**ステップ 5** Security Cloud Control が NSEL イベントを受信したことがあるか確認するために、時間を十分にさかのぼって [開始時刻（Start Time）] を設定します。

**ステップ 6** [センサーID（Sensor ID）] フィールドで、NSEL イベントを送信するために設定した Cisco ASA の IP アドレスを入力します。

**ステップ 7** フィルタの一番下の [NetFlowイベントを含める（Include NetFlow Events）] がオンになっていることを確認します。

# 解析された ASA Syslog イベント

解析済みの syslog イベントは、他の syslog イベントよりも多くのイベント属性を含んでおり、特定の解析済みフィールドの検索を可能にします。SEC は、指定したすべての ASA イベントを Cisco Cloud に転送しますが、解析されるのは以下の表の syslog メッセージのみです。すべての解析済みの Syslog イベントは、識別しやすいように EventType が斜体で表示されます。

syslog の詳細な説明については、『Cisco ASA Series Syslog Messages』を参照してください。

| Syslog ID | syslog カテゴリ | syslog メッセージの目的 |
|---|---|---|
| 106015 | Firewall | 州外 TCP の拒否を表します。 |
| 106023 | Firewall | 実際の IP パケットが ACL によって拒否されました。このメッセージは、ACL に対して **log** オプションをイネーブルにしていない場合でも表示されます。 |
| 106100 | アクセスリスト/ユーザーセッション | パケットは ACL によって許可または拒否されました。 |
| 113019 | ユーザー認証（User Authentication） | クリティカルな AnyConnect |
| 302013、302015、302017、302020 | ユーザ セッション | TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。 |
| 302014, 302016, 302018, 302021 | ユーザ セッション | TCP、UDP、GRE、および ICMP 接続作成の接続開始 syslog と接続終了 syslog。 |
| 302020 ～ 302021 | ユーザ セッション | ICMP セッションの確立と解除。 |
| 305006 | ユーザーセッション/NAT および PAT | NAT 接続の失敗 |

| Syslog ID | syslog カテゴリ | syslog メッセージの目的 |
|---|---|---|
| 305011 ～ 305014 | ユーザーセッション/NAT および PAT | NAT 確立/解除関連 |
| 313001、313008 | IP スタック | ボックスへの接続が拒否されたことを表します。 |
| 414004 | システム（System） | クリティカルな AnyConnect |
| 609001 ～ 609002 | Firewall | ネットワーク状態コンテナは、ゾーンに接続されたホスト **ip-address** 用に予約済み/削除済みでした。 |
| 710002、710004、710005 | ユーザ セッション | ボックスへの接続の失敗 |
| 710003 | ユーザ セッション | ボックスへの接続が拒否されたことを表します。 |
| 746012、746013 | ユーザ セッション | クリティカルな AnyConnect |

**関連情報**：

- コマンド ライン インターフェイスを使用した Cisco Cloud への ASA Syslog イベントの送信
- [イベントロギング（Event Logging）] ページでのイベントのフィルタリング

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。