



トラブルシューティング

この章は、次のセクションで構成されています。

- [ASA デバイス \(1 ページ\)](#)
- [証明書エラーのため ASA の導入準備ができない \(2 ページ\)](#)
- [リポート後の ASA と CDO の再接続に失敗 \(2 ページ\)](#)
- [CLI コマンドを使用した ASA のトラブルシューティング \(4 ページ\)](#)
- [ASA リモートアクセス VPN のトラブルシューティング \(6 ページ\)](#)
- [既存の RA VPN 設定に ASA を追加できない \(7 ページ\)](#)
- [ASA パケットトレーサ \(7 ページ\)](#)
- [ASA リアルタイムロギング \(10 ページ\)](#)
- [Cisco ASA Advisory cisco-sa-20180129-asa1 \(11 ページ\)](#)
- [ASA 実行設定サイズを確認する \(12 ページ\)](#)
- [Secure Device Connector に影響を与えるコンテナ特権昇格の脆弱性 : cisco-sa-20190215-runc \(13 ページ\)](#)
- [大きな ASA 実行設定ファイル \(15 ページ\)](#)
- [Secure Device Connector のトラブルシューティング \(15 ページ\)](#)
- [Secure Event Connector のトラブルシューティング \(19 ページ\)](#)
- [CDO のトラブルシューティング \(31 ページ\)](#)
- [デバイスの接続状態 \(41 ページ\)](#)
- [SecureX のトラブルシューティング \(54 ページ\)](#)

ASA デバイス

次の項目を使用して、ASA デバイスのトラブルシューティングを行います。

- [リポート後の ASA と CDO の再接続に失敗](#)
- [ASA パケットトレーサ](#)
- [ASA リアルタイムロギング](#)
- [ASA 実行設定サイズを確認する](#)

- 大きな ASA 実行設定ファイル
- Cisco ASA Advisory cisco-sa-20180129-asa1
- 新規フィンガープリントを検出状態の解決
- 新規証明書の問題のトラブルシューティング

証明書エラーのため ASA の導入準備ができない

環境：ASA はクライアント側の証明書認証で設定されています。

解決策：クライアント側の証明書認証を無効にします。

詳細：ASA はログイン情報ベースの認証とクライアント側の証明書認証をサポートします。CDO はクライアント側の証明書認証を使用する ASA に接続できません。ASA を CDO に導入準備する前に、次の手順を使用して、クライアント側の証明書認証が有効になっていないことを確認してください。

ステップ 1 ターミナルウィンドウを開き、SSH を使用して ASA に接続します。

ステップ 2 グローバル コンフィギュレーション モードを開始します。

ステップ 3 hostname (config)# プロンプトで、次のコマンドを入力します。

```
no ssl certificate-authentication interface interface-name port 443
```

インターフェイス名は、CDO が接続するインターフェイスの名前です。

リポート後の ASA と CDO の再接続に失敗

ASA のリポート後に CDO と ASA が接続しない場合、ASA が、CDO の Secure Device Connector (SDC) でサポートされていない OpenSSL 暗号スイートを再び使用するようになったことが原因である可能性があります。このトラブルシューティングトピックでは、そのようなケースをテストし、修復手順を示します。

症状

- ASA のリポート後、CDO と ASA が再接続されません。CDO に「再接続に失敗しました (Failed to reconnect)」というメッセージが表示されます。
- ASA を導入準備しようとする、CDO に次のメッセージが表示されます。
「<ASA_IP_Address> の証明書を取得できませんでした (Certificate could not be retrieved for <ASA_IP_Address>)」

ASA で使用する OpenSSL 暗号スイートの特定

この手順を使用して、ASA で使用されている OpenSSL 暗号スイートを識別します。コマンド出力で指定された暗号スイートが、CDO の Secure Device Connector でサポートされる暗号スイートにない場合、SDC はその暗号スイートをサポートしていないため、ASA の暗号スイートを更新する必要があります。

ステップ 1 SDC に到達可能なコンピュータでコンソールウィンドウを開きます。

ステップ 2 SSH を使用して SDC に接続します。CDO や SDC などの通常のユーザー、または作成した他のユーザーとしてログインできます。root としてログインする必要はありません。

ヒント SDC IP アドレスを特定するには、次の手順を実行します。

1. CDO を開きます。
2. ユーザーメニューから、[Secure Device Connector] を選択します。
3. 表に示されている SDC をクリックします。SDC の IP アドレスが、デバイスの詳細ペインに表示されます。

ステップ 3 コマンドプロンプトで次のように入力します。 `openssl s_client -showcerts -connect ASA_IP_Address:443`

ステップ 4 コマンド出力で次の行を探します。

```
New, TLSv1/SSLv3, Cipher is DES-CB3-SHA
or
SSL-Session:
    Protocol: TLSv1.2
    Cipher: DES-CB3-SHA
```

この例では、ASA で使用されている暗号スイートは DES-CB3-SHA です。

CDO の Secure Device Connector でサポートされる暗号スイート

CDO の Secure Device Connector は、最新かつ最も安全な暗号のみを受け入れる node.js を使用します。したがって、CDO の SDC は次の暗号のリストのみをサポートします。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256

- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA256

ASA で使用する暗号スイートがこのリストにない場合、SDC はその暗号スイートをサポートしていないため、[ASA の暗号スイートの更新](#)必要があります。

ASA の暗号スイートの更新

ASA で TLS 暗号スイートを更新するには、次の手順を実行します。

ステップ 1 SSH を使用して ASA に接続します。

ステップ 2 ASA に接続したら、グローバル コンフィギュレーション モードに **権限を昇格**させます。プロンプトは次のようになります。 `asaname(config)#`

ステップ 3 プロンプトで、次のようなコマンドを入力します。

```
ssl cipher tlsv1.2 custom "ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 DHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA256 DHE-RSA-AES256-SHA256"
```

(注) このコマンドで ASA がサポートするように設定する暗号スイートは、引用符の間および単語 `custom` の後に入力されます。このコマンドの場合、指定された暗号スイートは `ECDHE-RSA-AES128-GCM-SHA256` で始まり、`DHE-RSA-AES256-SHA256` で終わります。ASA でコマンドを入力するときに、ASA がサポートしないことがわかっている暗号スイートをすべて削除します。

ステップ 4 コマンドを送信したら、プロンプトで「write memory」と入力して、ローカル設定を保存します。例：

```
asaname (config) #write memory
```

CLI コマンドを使用した ASA のトラブルシューティング

このセクションでは、ASA のトラブルシューティングと基本的な接続のテストに使用できる重要なコマンドのいくつかについて説明します。他のトラブルシューティング シナリオと CLI コマンドを確認するには、『[CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide](#)』を参照してください。「System Administration」セクションで、「Testing and Troubleshooting」の章に移動します。

各 ASA デバイスで使用可能な CDO CLI インターフェイスを使用して、これらのコマンドを実行できます。CDO での CLI インターフェイスの使用方法については、「[CDO 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。

NAT ポリシーの設定

NAT 設定を決定するための重要なコマンドの例を次に示します。

- NAT ポリシーの統計情報を確認するには、**show nat** を使用します。
- 割り当てられたアドレスとホスト、および割り当て回数を含めて、NAT プールを確認するには、**show nat pool** を使用します。

NAT に関連したその他のコマンドについては、『[CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide](#)』を参照し、「Network Address Translation (NAT)」の章に移動してください。

基本接続のテスト：アドレス向けの ping の実行

ASA CLI インターフェイスで **ping <IP address>** コマンドを使用して ASA デバイスに ping できます。次を確認するには

ルーティング テーブルの表示

show route コマンドを使用してルーティングテーブル内のエントリを表示します。

ciscoasa# show route

ASA のルーティングテーブルの出力例：

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF

Gateway of last resort is 192.168.0.254 to network 0.0.0.0
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.0.254, management
C 10.0.0.0 255.0.0.0 is directly connected, Outside
L 10.10.10.1 255.255.255.255 is directly connected, Outside
C 192.168.0.0 255.255.255.0 is directly connected, management
L 192.168.0.118 255.255.255.255 is directly connected, management
```

スイッチポートのモニタリング

- **show interface**

インターフェイス統計情報を表示します。

- **show interface ip brief**

インターフェイスの IP アドレスとステータスを表示します。

- **show arp**

ダイナミック、スタティック、およびプロキシ ARP エントリを表示します。ダイナミック ARP エントリには、ARP エントリの秒単位のエイジングが含まれています。

ARP エントリの出力例：

```
management 10.10.32.129 0050.568a.977b 0
management 10.10.32.136 0050.568a.5387 21
LANFAIL 20.20.21.1 0050.568a.4d70 96
outsi 10.10.16.6 0050.568a.e6d3 3881
outsi 10.10.16.1 0050.568a.977b 5551
```

ASA リモートアクセス VPN のトラブルシュート

このセクションでは、ASA デバイスでリモートアクセス VPN を設定するときに発生する可能性がある、いくつかのトラブルシューティングの問題について説明します。

RA VPN モニタリングページに情報が無い

この問題は、外部インターフェイスが Webvpn に対して有効になっていない場合に発生する可能性があります。

解決策：

1. ナビゲーションウィンドウで、[デバイスとサービス] をクリックします。
2. [デバイス] タブをクリックしてから、[ASA] タブをクリックします。
3. 問題のある RA VPN ヘッドエンド ASA デバイスを選択します。
4. 右側の [管理] ペインで、[構成] をクリックします。
5. [編集] をクリックして、「webvpn」を検索します。
6. **Enter** キーを押して、`enable interface_name` を追加します。ここで `interface_name` は、リモートアクセス VPN 接続を確立するときにユーザーが接続する外部インターフェイスの名前です。これは通常外部（インターネットに接続された）インターフェイスですが、デバイスとこの接続プロファイルがサポートしているエンドユーザー間のインターフェイスのいずれかを選択します。

次に例を示します。

```
webvpn
enable outside
```

7. [保存 (Save)] をクリックします。
8. 構成を [プレビューしてデバイスに展開](#) します。

既存の RA VPN 設定に ASA を追加できない

始める前に

手順の概要

- 1.

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	例 :	

例

次のタスク

ASA パケットトレーサ

パケットトレーサを使用すると、合成パケットをネットワークに送信し、既存のルーティング設定、NAT ルール、およびポリシー設定がそのパケットにどのように影響するかを評価できます。次の種類の問題をトラブルシューティングするには、このツールを使用します。

- アクセスできるはずのリソースにアクセスできないとユーザーが報告している。
- 到達できないはずのリソースに到達できるとユーザーが報告している。
- ポリシーをテストして、期待どおりに機能するかどうかを判断します。

パケットトレーサは、稼働中のオンライン ASA デバイス（物理または仮想）で使用できます。パケットトレーサは [ASA モデルデバイス](#) では動作しません。パケットトレーサでは ASA に保存された設定に基づいてパケットが評価されます。CDO の段階的な変更はパケットトレーサでは評価されません。

同期状態の ASA でパケットトレーサを実行することがベストプラクティスです。デバイスが同期されていない場合でもパケットトレーサは動作しますが、予期しない結果が生じる可能性があります。たとえば、CDO のステージングされた設定でルールを削除し、パケットトレース中にこの同じルールが ASA でトリガーされた場合、CDO はパケットとそのルールとの相互作用の結果を表示できません。

ASA パケットトレーサによるトラブルシューティング

パケットトレーサは、ASA のルーティング設定、NAT ルール、およびセキュリティポリシーを介してパケットを送信するため、各ステップでのパケットのステータスが表示されます。パケットがポリシーによって許可されている場合、緑色のチェックマークが表示されます。✔ パケットが拒否されてドロップされた場合、CDO には赤い X マークが表示されます。✖

パケットトレーサでは、パケットトレース結果のリアルタイムログも表示されます。以下の例では、ルールによって tcp パケットが拒否された場所を確認できます。

LOGGING					
✔	6	10/10/2017, 8:36:09 PM	605005	Login permitted from 10.82.109.213/55400 to outside:10.82.109.113/https for user *	*
✔	4	10/10/2017, 8:36:09 PM	106023	Deny tcp src inside:10.82.109.113/80 dst outside:10.82.109.176/80 by access-group "inside_access_in" [0xbe9efe96, 0x0]	
✔	5	10/10/2017, 8:36:09 PM	111008	User ' ' executed the 'packet-tracer input inside tcp 10.82.109.113 80 10.82.109.176 80 detailed xml' command.	
✔	5	10/10/2017, 8:36:09 PM	111010	User ' ', running 'CLJ' from IP 0.0.0.0, executed 'packet-tracer input inside tcp 10.82.109.113 80 10.82.109.176 80 detailed xml'	

ASA デバイスのセキュリティポリシーのトラブルシューティング

- ステップ 1 [デバイスとサービス] ページから ASA を選択し、[アクション] ペインで [トラブルシューティング (Troubleshoot)] をクリックします。
- ステップ 2 [値 (Values)] ペインで、ASA を介して仮想的に送信するインターフェイスとパケットタイプを選択します。
- ステップ 3 (オプション) セキュリティグループタグの値がレイヤ 2 CMD ヘッダーに埋め込まれたパケットを追跡する (Trustsec) 場合は、[SGT 番号 (SGT number)] をオンにして、セキュリティグループタグの番号 (0 ~ 65535) を入力します。
- ステップ 4 送信元と接続先を指定します。Cisco TrustSec を使用する場合は、IPv4 または IPv6 アドレス、完全修飾ドメイン名 (FQDN)、またはセキュリティグループの名前あるいはタグを指定できます。送信元アドレスに対して、Domain/username 形式でユーザー名を指定することもできます。
- ステップ 5 他のプロトコルの特性を指定します。
 - [ICMP] : ICMP タイプ、ICMP コード (0 ~ 255)、およびオプションで ICMP 識別子を入力します。
 - [TCP/UDP/SCTP] : リストから選択するか、ポートコンボボックスに値を入力して、送信元ポートと宛先ポートを入力します。
 - [IP] : プロトコル番号 (0 ~ 255) を入力します。
- ステップ 6 [パケットトレーサを実行 (Run Packet Tracer)] をクリックします。

ステップ7 [パケットトレーサ結果の分析 (Analyze Packet Tracer Results)] [パケットトレーサ結果の分析 \(10 ページ\)](#)に進みます。

アクセスルールのトラブルシューティング

ステップ1 [ポリシー (Policies)] > [ネットワークポリシー (Network Policies)] > . を選択します。

ステップ2 ASA に関連付けられているポリシーを選択します。

ステップ3 トラブルシューティングするネットワークポリシーのルールを選択し、詳細ペインで [トラブルシューティング (Troubleshoot)] [Troubleshoot](#) をクリックします。トラブルシューティング ページの値パネルでは、多くのフィールドに、選択したルールの属性が事前に入力されています。

ステップ4 残りの必要なフィールドに情報を入力します。すべての必須フィールドに入力すると、[パケットトレーサを実行 (Run Packet Tracer)] ボタンが有効になります。

ステップ5 [パケットトレーサを実行 (Run Packet Tracer)] をクリックします。

ステップ6 [パケットトレーサ結果の分析 (Analyze Packet Tracer Results)] [パケットトレーサ結果の分析 \(10 ページ\)](#)に進みます。

NAT ルールのトラブルシューティング

ステップ1 [デバイスとサービス] ページから ASA を選択し、[アクション] ペインで [NATルールの表示 (View NAT Rules)] [View NAT Rules](#) をクリックします。

ステップ2 トラブルシューティングを行うルールを NAT ルールテーブルから選択し、[詳細] ペインで [トラブルシューティング (Troubleshoot)] [Troubleshoot](#) をクリックします。[トラブルシューティング (Troubleshoot)] ページの値パネルでは、多くのフィールドに、選択したルールの属性が事前に入力されています。

ステップ3 残りの必要なフィールドに情報を入力します。すべての必須フィールドに入力すると、[パケットトレーサを実行 (Run Packet Tracer)] が有効になります。

ステップ4 [パケットトレーサを実行 (Run Packet Tracer)] をクリックします。

ステップ5 [パケットトレーサ結果の分析 (Analyze Packet Tracer Results)] [パケットトレーサ結果の分析 \(10 ページ\)](#)に進みます。

Twice NAT ルールのトラブルシューティング

ステップ1 [デバイスとサービス] ページから ASA を選択し、[アクション] ペインで [NATルールの表示 (View NAT Rules)] [View NAT Rules](#) をクリックします。

- ステップ 2** トラブルシュートを行うルールを NAT ルールテーブルから選択し、[詳細] ペインで [トラブルシュート (Troubleshoot)] の Troubleshoot をクリックします。双方向の Twice NAT ルールの場合、これによりドロップダウンが開き、ソースパケット変換または宛先パケット変換のトラブルシューティングを選択できます。
- ステップ 3** 残りの必要なフィールドに情報を入力します。すべての必須フィールドに入力すると、[パケットトレーサを実行 (Run Packet Tracer)] が有効になります。
- ステップ 4** [パケットトレーサを実行 (Run Packet Tracer)] をクリックします。

パケットトレーサ結果の分析

パケットがドロップされたか、許可されたかに関係なく、パケットトレーサテーブルの行を展開し、そのアクションに関連するルールまたはロギング情報を読むことで理由を把握できます。以下の例では、パケットトレーサが、任意の送信元から着信して任意の接続先に向かう IP パケットを拒否するルールを含むアクセスリストポリシーを特定しています。このアクションが必要でない場合は、[ネットワークポリシーで表示] リンクをクリックして、そのルールをすぐに編集できます。ルールを編集したら、その構成変更を ASA に展開してから、パケットトレーサを再実行して期待どおりのアクセス結果が得られることを確認してください。

パケットトレーサの結果とともに、CDO は ASA からの [ASA リアルタイムロギング](#) を表示します。

PACKET TRACE

ROUTE-LOOKUP

ACCESS-LIST

ACTION	PROTOCOL	SOURCE	PORT	DESTINATION	PORT	HITS (DAY)
	icmp	oded-obj1	-	oded-obj2	-	-
	ip	any	any	any	any	-
	icmp	oded-range1	-	oded-obj2	-	-

View in Network Policies

Expand the row showing where the packet was dropped.

View the rule that denied the action.

Click View in Network Policies to view and edit the rule in the Network Policies table.

ASA リアルタイムロギング

リアルタイムロギングを使用すると、ログデータの最後の 20 秒またはログデータの最後の 10 KB のうち、先に制限に達した方が表示されます。CDO がリアルタイムデータを取得すると、ASDM の既存のロギング設定を確認し、デバッグレベルのデータを要求するように変更してから、ロギング設定を元の設定に戻します。ロギング CDO の表示には、ASDM で設定したロギングフィルタが反映されます。

変更ログを確認すると、ロギングを実行するために CDO が送信するコマンドを確認できます。以下は、変更ログエントリの例です。最初のエントリ (下部) は、CDO が logging enable コマンドでロギングを「有効」にし、ASDM ロギングレベルをデバッグに変更したことを示しま

す。2 番目のエントリ（上部）は、ロギングの設定が以前の状態に戻ったことを示します。no logging enable コマンドでロギングが「無効」になり、ASDM ロギングレベルが情報提供に戻りました。

LAST UPDATED	DEVICE NAME	LAST DESCRIPTION	CHANGE STATUS
11/21/2017, 2:39:38 PM	ASA1	Troubleshooting	ACTIVE
DATE	DESCRIPTION	USER	
Nov 21, 2017 10:50:45 AM	Troubleshooting	user1@example.com	
no logging enable logging asdm informational			
Nov 21, 2017 10:50:45 AM	Troubleshooting	user1@example.com	
logging enable logging asdm debugging			

ASA リアルタイムログの表示

- ステップ 1 [デバイスとサービス (Devices & Services)] 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、リアルタイムデータを表示するデバイスを選択します。
- ステップ 3 [トラブルシューティング (Troubleshoot)] > Troubleshoot をクリックします。
- ステップ 4 (任意) [リアルタイムログの表示 (View Real-time Log)] をクリックする前に、左側のペインでフィルタを定義して、ログ検索の結果を絞り込むことができます。
- ステップ 5 [リアルタイムログの表示 (View Real-time Log)] をクリックします。CDO は、フィルタ条件に基づいてリアルタイムのログデータを取得して、表示します。
- ステップ 6 追加の 20 秒のログデータまたは最後の 10 KB のログデータを表示するには、[リアルタイムログの表示 (View Real-Time Log)] をもう一度クリックします。

Cisco ASA Advisory cisco-sa-20180129-asa1

Cisco Product Security Incident Response Team (PSIRT; プロダクトセキュリティ インシデントレスポンス チーム) は、ASA および Firepower の重大なセキュリティの脆弱性について説明するセキュリティアドバイザリ [cisco-sa-20180129-asa1](#) を公開しました。影響を受ける ASA および Firepower のハードウェア、ソフトウェア、および設定の完全な説明については、[PSIRT チームのアドバイザリ全体をお読みください](#)。

ASA がアドバイザリの影響を受けていると判断した場合は、CDO を使用して、パッチが適用されたバージョンに ASA をアップグレードできます。次のプロセスを使用します。

- ステップ 1 影響を受ける各 ASA で [DNS サーバー](#) を設定します。
- ステップ 2 [アドバイザリ](#) に戻って、必要なソフトウェアパッチを決定します。
- ステップ 3 CDO を使用して ASA を ASA アドバイザリにリストされている修正済みリリースにアップグレードする方法が説明されているトピックについては、[単一 ASA 上の ASA と ASDM イメージのアップグレード](#) を参照

してください。アップグレードの前提条件から始めて、個々の ASA のアップグレード、アクティブ/スタンバイ設定での ASA のアップグレード、または ASA の一括アップグレードについて参照してください。

参考までに、シスコが報告したセキュリティアドバイザリの概要を以下に示します。

2018年2月5日更新：さらなる調査の結果、シスコは、この脆弱性の影響を受ける追加の攻撃ベクトルと機能を特定しました。さらに、元の修正が不完全なことが判明したため、修正された新しいコードバージョンが利用可能になりました。詳細については、「[Fixed Software](#)」セクションを参照してください。Cisco 適応型セキュリティプライアンス (ASA) ソフトウェアの XML パーサーの脆弱性により、認証されていないリモートの攻撃者が、影響を受けるシステムをリロードしたり、コードをリモートで実行したりする可能性があります。また、メモリ不足が原因で、ASA が着信仮想プライベートネットワーク (VPN) の認証要求の処理を停止する可能性もあります。この脆弱性は、悪意のある XML ペイロードを処理する際のメモリの割り当てと解放に関する問題に起因しています。攻撃者は、影響を受けるシステムの脆弱なインターフェイスに巧妙に細工された XML パケットを送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトにより、攻撃者は任意のコードを実行してシステムの完全な制御を取得し、影響を受けるデバイスのリロードを引き起こしたり、着信 VPN 認証要求の処理を停止したりする可能性があります。脆弱であるためには、ASA は、インターフェイス上でセキュアソケットレイヤ (SSL) サービスまたは IKEv2 リモートアクセス VPN サービスを有効にする必要があります。脆弱性がエクスプロイトされるリスクは、攻撃者がインターフェイスにアクセスできるかどうかによっても決まります。脆弱な ASA 機能の包括的なリストについては、「[Vulnerable Products](#)」セクションの表を参照してください。この脆弱性に対処するソフトウェアアップデートは、すでに Cisco からリリースされています。この脆弱性の影響を受けるすべての機能に対処する回避策はありません。このアドバイザリは、次のリンク先で確認できます。 <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1>

ASA 実行設定サイズを確認する

実行構成ファイルのサイズを確認するには、次の手順を実行します。

ステップ 1 次のいずれかの方法で、ASA のコマンドラインインターフェイスにアクセスします。

- ターミナルウィンドウを開き、SSH を使用して ASA にログインします。権限を「特権 EXEC」モードに昇格させます。これにより、表示されるプロンプトが `hostname#` になります。
- ASA の導入準備が完了している場合は、[デバイスとサービス (Devices & Service)] ページを開き、接続するデバイスを選択して、[デバイスアクション] ペインで [>_ コマンドラインインターフェイス (>_ Command Line Interface)] ボタンをクリックします。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。

ステップ 2 プロンプトで、`copy running-config flash` と入力します。

ステップ 3 コピー元ファイル名の入力を求められたら、何も入力せずに Enter キーを押します。

ステップ 4 コピー先ファイル名の入力を求められたら、出力ファイルの名前を入力します。指定した実行構成ファイルが ASA によってコピーされると、特権 EXEC プロンプトに戻ります。

ステップ 5 プロンプトで、`show flash` と入力します。

ステップ 6 長さ (length) の列を調べます。ファイルが 4718592 バイトを超えている場合は、4.5 MB を超えています。コマンドと出力の例を次に示します。

```
asa1# copy running-config flash
Source filename [running-config]?
Destination filename [running-config]? running-config-output
Cryptochecksum: 725f4c1c 4adfb8a9 8b3e7a6d 49e3420d
23648 bytes copied in 1.380 secs (23648 bytes/sec)
asa1# show flash
--#-- --length-- -----date/time----- path
 107 110325428 Feb 28 2019 15:41:42 asdm-8826067.bin
 122 5018592 Apr 30 2019 21:00:59 running-config-output
 111 102647808 Mar 12 2019 14:26:10 asa9-12-1-smp-k8.bin
```

Secure Device Connector に影響を与えるコンテナ特権昇格の脆弱性 : cisco-sa-20190215-runc

Cisco Product Security Incident Response Team (PSIRT) は、Docker の重大度の高い脆弱性について説明するセキュリティアドバイザリ `cisco-sa-20190215-runc` を公開しました。脆弱性の完全な説明については、[PSIRT チームのアドバイザリ全体をお読みください](#)。

この脆弱性は、すべての CDO ユーザーに影響します。

- CDO のクラウド展開された Secure Device Connector (SDC) を使用しているお客様は、修復手順が CDO 運用チームによってすでに実行されているため、何もする必要はありません。
- オンプレミスで展開された SDC を使用しているお客様は、最新の Docker バージョンを使用するように SDC ホストをアップグレードする必要があります。アップグレードするには、次の手順を使用します。

CDO 標準の SDC ホストの更新

[CDO イメージを使用して SDC を展開](#)した場合は、次の手順を使用します。

ステップ 1 SSH またはハイパーバイザコンソールを使用して SDC ホストに接続します。

ステップ 2 次のコマンドを実行して、Docker サービスのバージョンを確認します。

```
docker version
```

ステップ 3 最新の仮想マシン (VM) のいずれかを実行している場合、次のような出力が表示されます。

```
> docker version
Client:
  Version: 18.06.1-ce
  API version: 1.38
  Go version: go1.10.3
```

```
Git commit: e68fc7a
Built: Tue Aug 21 17:23:03 2018
OS/Arch: linux/amd64
Experimental: false
```

ここで古いバージョンが表示される可能性があります。

ステップ 4 次のコマンドを実行して Docker を更新し、サービスを再起動します。

```
> sudo yum update docker-ce
> sudo service docker restart
```

(注) Docker サービスの再起動中、CDO とデバイス間の接続が短時間停止します。

ステップ 5 `docker version` コマンドを再度実行します。次の出力が表示されます。

```
> docker version
Client:
 Version: 18.09.2
 API version: 1.39
 Go version: go1.10.6
 Git commit: 6247962
 Built: Sun Feb XX 04:13:27 2019
 OS/Arch: linux/amd64
 Experimental: false
```

ステップ 6 これで追加されました。パッチが適用された最新バージョンの Docker にアップグレードされました。

カスタム SDC ホストを更新する

独自の SDC ホストを作成している場合は、Docker のインストール方法に基づいた更新手順に従う必要があります。CentOS、yum、Docker-ce（コミュニティ版）を使用した場合は、前述の手順で動作します。

Docker-ee（エンタープライズ版）をインストールした場合、または別の方法を使用して Docker をインストールした場合は、Docker の修正バージョンが異なる場合があります。正しいインストールバージョンは、Docker のページ（[Docker Security Update and Container Security Best Practices](#)）で確認できます。

バグトラッキング

シスコでは、この脆弱性を引き続き評価し、追加情報が利用可能になりしだい、アドバイザリを更新します。アドバイザリに最終とマーキングされた後は、詳細については次の関連 Cisco Bug を参照してください。

[CSCvo33929-CVE-2019-5736 : runC コンテナのブレイクアウト](#)

大きな ASA 実行設定ファイル

CDO での現象

ASA が導入準備に失敗する、ASA の実行設定ファイルで定義されているすべての設定が CDO で表示されない、または CDO が変更ログへの書き込みに失敗するといった現象が見られる場合があります。

考えられる原因

ASA の実行設定ファイルが CDO に対して「大きすぎる」可能性があります。

ASA を CDO に導入準備すると、CDO は、そのデータベースに ASA の実行設定ファイルのコピーを保存します。一般に、その実行設定ファイルが大きすぎる（4.5 MB 以上）場合、含まれる行が多すぎる（約 22,000 行）場合、または単一のアクセスグループのアクセスリストエントリが多すぎる場合、CDO は、そのデバイスを予測どおりに管理できません。

実行設定ファイルのサイズを確認するには、「[ASA 実行設定サイズを確認する](#)」を参照してください。

回避策または解決策

シスコのアカウントチームに連絡して、セキュリティポリシーを中断することなく設定ファイルのサイズを安全に削減するための支援を得ます。

Secure Device Connector のトラブルシューティング

オンプレミスの Secure Device Connector (SDC) のトラブルシューティングを行うには、以下のトピックを参照してください。

これらのシナリオのいずれにも当てはまらない場合は、[Cisco Technical Assistance Center](#) でケースをオープンしてください。

SDC に到達不能

CDO からの 2 回のハートビート要求に連続して応答しなかった場合、SDC の状態は [到達不能 (Unreachable)] になります。SDC に到達不能な場合、テナントは、導入準備したどのデバイスとも通信できません。

CDO は、次の方法で SDC に到達不能であることを示します。

- 「一部の Secure Device Connector (SDC) に到達できません。該当する SDC に関連付けられたデバイスとは通信できません (Some Secure Device Connectors (SDC) are unreachable. You will not be able to communicate with devices associated with these SDCs)」というメッセージが CDO のホームページに表示されます。

- [セキュアコネクタ (Secure Connectors)] ページの SDC のステータスが [到達不能 (Unreachable)] になります。

この問題を解決するには、まず SDC とテナントの再接続を試行してください。

1. SDC 仮想マシンが実行中で、地域の CDO IP アドレスに到達できることを確認します。
「[Cisco Defense Orchestrator の管理対象デバイスへの接続](#)」を参照してください。
2. ハートビートを手動で要求して、CDO と SDC の再接続を試行します。SDC がハートビート要求に応答すると、[アクティブ (Active)] ステータスに戻ります。ハートビートを手動で要求するには、次の手順に従います。
 1. ユーザーメニューから、[セキュアコネクタ (Secure Connectors)] を選択します。
 2. 到達不能な SDC をクリックします。
 3. [操作 (Actions)] ウィンドウで、[ハートビートの要求 (Request heartbeat)] をクリックします。
 4. [再接続 (Reconnect)] をクリックします。
3. SDC を手動でテナントに再接続しようとしても、SDC が [アクティブ (Active)] ステータスに戻らない場合は、「[展開後 CDO で SDC ステータスがアクティブにならない \(16 ページ\)](#)」の指示に従ってください。

展開後 CDO で SDC ステータスがアクティブにならない

展開して約 10 分たっても SDC がアクティブになったことを CDO が示さない場合は、SDC の展開時に作成した cdo ユーザーおよびパスワードにより、SSH を使用して SDC VM に接続します。

ステップ 1 /opt/cdo/configure.log を確認します。ここには、入力した SDC の構成設定と、それらが正常に適用されたかどうかを示されます。セットアッププロセスでエラーが発生している場合または値が正しく入力されていない場合は、`sdc-onboard setup` を再度実行します。

- a) `[cdo@localhost cdo]$` プロンプトで、`sudo sdc-onboard setup` と入力します。
- b) cdo ユーザーのパスワードを入力します。
- c) プロンプトに従います。セットアップスクリプトの指示に従って、セットアップウィザードで行ったすべての設定手順を確認し、入力した値を変更することができます。

ステップ 2 ログを確認し、`sudo sdc-onboard setup` を実行しても、SDC がアクティブになったことを CDO が示さない場合は、[CDO サポートに連絡してください](#)。

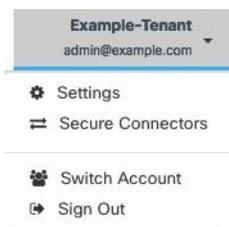
SDC の変更した IP アドレスが CDO に反映されない

SDC の IP アドレスを変更した場合、GMT の午前 3 時以降まで変更は CDO に反映されません。

デバイスと SDC の接続に関するトラブルシューティング

このツールを使用して、Secure Device Connector (SDC) を介した CDO からデバイスへの接続をテストします。デバイスが導入準備に失敗した場合、または導入準備の前に CDO がデバイスに到達できるかどうかを判断する場合は、この接続をテストすることができます。

ステップ 1 [アカウント (Account)]メニューをクリックし、[セキュアコネクタ (Secure Connectors)]を選択します。



ステップ 2 SDC を選択します。

ステップ 3 右側の [トラブルシューティング (Troubleshooting)] ペインで、[デバイスの接続 (Device Connectivity)] をクリックします。

ステップ 4 トラブルシューティングまたは接続しようとしているデバイスの有効な IP アドレスまたは FQDN とポート番号を入力し、[実行 (Go)] をクリックします。CDO は次の検証を実行します。

- a) [DNS 解決 (DNS Resolution)] : IP アドレスの代わりに FQDN を指定すると、SDC がドメイン名を解決でき、IP アドレスを取得できることを確認します。
- b) [接続テスト (Connection Test)] : デバイスが到達可能であることを確認します。
- c) [TLS サポート (TLS support)] : デバイスと SDC の両方がサポートする TLS バージョンと暗号を検出します。

- [サポートされていない暗号 (Unsupported Cipher)] : デバイスと SDC の両方でサポートされている TLS バージョンがない場合、CDO は、SDC ではなくデバイスでサポートされている TLS バージョンと暗号についてもテストします。

d) SSL 証明書 : トラブルシューティングでは、証明書情報が提供されます。

ステップ 5 デバイスの導入準備またはデバイスへの接続の問題が解消しない場合は、[Defense Orchestrator サポート](#) までお問い合わせください。

Secure Device Connector に影響を与えるコンテナ特権昇格の脆弱性 : cisco-sa-20190215-runc

Cisco Product Security Incident Response Team (PSIRT) は、Docker の重大度の高い脆弱性について説明するセキュリティアドバイザリ **cisco-sa-20190215-runc** を公開しました。脆弱性の完全な説明については、[PSIRT チームのアドバイザリ全体をお読みください](#)。

この脆弱性は、すべての CDO ユーザーに影響します。

- CDO のクラウド展開された Secure Device Connector (SDC) を使用しているお客様は、CDO 運用チームによってすでに修復手順が実行されているため、何もする必要はありません。
- オンプレミスで展開された SDC を使用しているお客様は、最新の Docker バージョンを使用するように SDC ホストをアップグレードする必要があります。アップグレードするには、次の手順を使用します。
 - [CDO 標準の SDC ホストの更新 \(13 ページ\)](#)
 - [カスタム SDC ホストを更新する \(14 ページ\)](#)
 - [バグトラッキング \(14 ページ\)](#)

CDO 標準の SDC ホストの更新

[CDO イメージを使用して SDC を展開した場合は](#)、次の手順を使用します。

ステップ 1 SSH またはハイパーバイザコンソールを使用して SDC ホストに接続します。

ステップ 2 次のコマンドを実行して、Docker サービスのバージョンを確認します。

```
docker version
```

ステップ 3 最新の仮想マシン (VM) のいずれかを実行している場合、次のような出力が表示されます。

```
> docker version
Client:
 Version: 18.06.1-ce
 API version: 1.38
 Go version: go1.10.3
 Git commit: e68fc7a
 Built: Tue Aug 21 17:23:03 2018
 OS/Arch: linux/amd64
 Experimental: false
```

ここで古いバージョンが表示される可能性があります。

ステップ 4 次のコマンドを実行して Docker を更新し、サービスを再起動します。

```
> sudo yum update docker-ce
> sudo service docker restart
```

(注) Docker サービスの再起動中、CDO とデバイス間の接続が短時間停止します。

ステップ 5 `docker version` コマンドを再度実行します。次の出力が表示されます。

```
> docker version
Client:
  Version: 18.09.2
  API version: 1.39
  Go version: go1.10.6
  Git commit: 6247962
  Built: Sun Feb XX 04:13:27 2019
  OS/Arch: linux/amd64
  Experimental: false
```

ステップ 6 これで追加されました。パッチが適用された最新バージョンの Docker にアップグレードされました。

カスタム SDC ホストを更新する

独自の SDC ホストを作成している場合は、Docker のインストール方法に基づいた更新手順に従う必要があります。CentOS、yum、Docker-ce（コミュニティ版）を使用した場合は、前述の手順で動作します。

Docker-ee（エンタープライズ版）をインストールした場合、または別の方法を使用して Docker をインストールした場合は、Docker の修正バージョンが異なる場合があります。正しいインストールバージョンは、Docker のページ（[Docker Security Update and Container Security Best Practices](#)）で確認できます。

バグトラッキング

シスコでは、この脆弱性を引き続き評価し、追加情報が利用可能になりしだい、アドバイザリを更新します。アドバイザリに最終とマーキングされた後は、詳細については次の関連 Cisco Bug を参照してください。

[CSCvo33929-CVE-2019-5736](#) : runC コンテナのブレイクアウト

Secure Event Connector のトラブルシューティング

いずれのシナリオにも当てはまらない場合は、[Cisco Technical Assistance Center](#) でケースを開いてください。

SEC オンボーディング失敗のトラブルシューティング

以下のトラブルシューティングのトピックでは、Secure Event Connector（SEC）の導入準備の失敗に関連するさまざまな症状について説明します。

SEC の導入準備に失敗しました

症状：SEC の導入準備に失敗しました。

修復：SEC を取り外して、再度導入準備します。

このエラーが表示された場合：

1. 仮想マシンコンテナから [Secure Event Connector](#) とそのファイルを削除します。
2. [Secure Device Connector](#) の更新。通常、SDC は自動的に更新されるためこの手順を行う必要はありませんが、トラブルシューティングではこの手順が役立ちます。
3. [SDC 仮想マシンへの Secure Event Connector のインストール](#)。



ヒント SECを導入準備するときは、常にコピーリンクを使用してブートストラップデータをコピーします。



(注) この手順で問題が解決しない場合は、[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](#)し、マネージド サービス プロバイダーまたは [Cisco Technical Assistance Center](#) に連絡してください。

SEC ブートストラップデータが指定されていません

メッセージ：ERROR cannot bootstrap Secure Event Connector, bootstrap data not provided, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
Please input the bootstrap data from Setup Secure Event Connector page of CDO:
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector, bootstrap data not
provided, exiting.
```

診断：プロンプトが表示されたときに、ブートストラップデータがセットアップスクリプトに入力されませんでした。

修復：導入準備時にブートストラップデータの入力を求められたら、CDO UI で生成された SEC ブートストラップデータを指定します。

ブートストラップ構成ファイルが存在しません

メッセージ：ERROR Cannot bootstrap Secure Event Connector for tenant: <tenant_name>, bootstrap config file ("/usr/local/cdo/es_bootstrapdata") does not exist, exiting.

診断：SEC ブートストラップ データ ファイル ("/usr/local/cdo/es_bootstrapdata") が存在しません。

修復：CDO UI で生成された SEC ブートストラップデータをファイル `/usr/local/cdo/es_bootstrapdata` に配置し、導入準備を再試行します。

1. 導入準備手順を繰り返します。
2. ブートストラップデータをコピーします。
3. 「sdc」ユーザーとして SEC VM にログインします。

4. CDO UI で生成された SEC ブートストラップデータをファイル `/usr/local/cdo/es_bootstrapdata` に配置し、導入準備を再試行します。

ブートストラップデータのデコードに失敗しました

メッセージ : ERROR cannot bootstrap Secure Event Connector for tenant: <tenant_name>, faile to decode SEC bootstrap data, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
base64: invalid input
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
failed to decode SEC bootstrap data, exiting.
```

診断 : ブートストラップデータのデコードに失敗しました

修復 : SEC ブートストラップデータを再生成し、導入準備を再試行します。

ブートストラップデータに SEC を導入準備するために必要な情報がありません

メッセージ :

- ERROR cannot bootstrap Secure Event Connector container for tenant: <tenant_name>, SSE_FQDN not set, exiting.
- ERROR cannot bootstrap Secure Event Connector container for tenant: <tenant_name>, SSE_OTP not set, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
SSE_FQDN not set, exiting.

[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR cannot bootstrap Secure Event Connector for tenant: tenant_XYZ,
SSE_OTP not set, exiting.
```

診断 : ブートストラップデータに SEC を導入準備するために必要な情報がありません。

修復 : ブートストラップデータを再生成し、導入準備を再試行します。

ツールキット cron が現在実行中

メッセージ : ERROR SEC toolkit already running, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR SEC toolkit already running.
```

診断 : ツールキット cron が現在実行中です。

修復 : 導入準備コマンドを再試行します。

十分な CPU とメモリがない

メッセージ : ERROR unable to setup Secure Event Connector, minimum 4 cpus and 8 GB ram required, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, minimum 4 cpus and
8 GB ram required, exiting.
```

診断：十分な CPU とメモリがありません。

修復：VM の SEC 専用に最低 4 つの CPU と 8 GB の RAM がプロビジョニングされていることを確認し、導入準備を再試行します。

SEC がすでに実行中

メッセージ：ERROR Secure Event Connector already running, execute 'cleanup' before onboarding a new Secure Event Connector, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
[2020-06-10 04:37:26] ERROR Secure Event Connector already running, execute 'cleanup'
before onboarding a new Secure Event Connector, exiting.
```

診断：SEC がすでに実行中です。

修復：新しい SEC を導入準備する前に、[SEC クリーンアップコマンド](#)を実行します。

SEC ドメインに到達不能

メッセージ：

- Failed connect to api-sse.cisco.com:443; Connection refused
- ERROR unable to setup Secure Event Connector, domain api-sse.cisco.com unreachable, exiting.

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh setup
curl: (7) Failed connect to api-sse.cisco.com:443; Connection refused
[2020-06-10 04:37:26] ERROR unable to setup Secure Event Connector, domain
api-sse.cisco.com unreachable, exiting.
```

診断：SEC ドメインに到達できません。

修復：オンプレミス SDC にインターネット接続があることを確認し、導入準備を再試行します。

導入準備 SEC コマンドはエラーなしで成功しましたが、SEC Docker コンテナが起動していません

症状：導入準備 SEC コマンドはエラーなしで成功しましたが、SEC Docker コンテナが起動していません

診断：導入準備 SEC コマンドはエラーなしで成功しましたが、SEC docker コンテナが起動していません

修復：

1. 「sdc」ユーザーとして SEC にログインします。
2. SEC Docker コンテナの起動ログ (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/startup.log) でエラーがないか確認してください。
3. エラーがある場合は、[SEC クリーンアップコマンド](#)を実行して、導入準備を再試行してください。

CDO サポートに連絡する

いずれのシナリオにも当てはまらない場合は、[Cisco Technical Assistance Center](#) でケースを開いてください。

Secure Event Connector の登録失敗のトラブルシューティング

症状：クラウドイベントサービスへの Cisco Secure Event Connector の登録が失敗します。

診断：SEC がイベントクラウドサービスに登録できない最も一般的な理由は、次のとおりです。

- SEC が SEC からイベントクラウドサービスに到達できない

修復：インターネットがポート 443 でアクセス可能であり、DNS が正しく設定されていることを確認します。

- SEC ブートストラップデータの無効または期限切れのワンタイムパスワードによる登録の失敗

修復：

ステップ 1 「sdc」ユーザーとして SDC にログオンします。

ステップ 2 コネクタログ (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) を表示して、登録状態を確認します。

無効なトークンが原因で登録に失敗した場合は、ログファイルに次のようなエラーメッセージが表示されます。

```
context>(*contextImpl).handleFailed] registration - CE2001: Registration failed - Failed to register the device because of invalid token. Retry with a new valid token. - Failed"
```

ステップ 3 SDC VM で [SEC クリーンアップコマンド](#) 手順を実行して、[セキュアコネクタ (Secure Connectors)] ページから SEC を削除します。

ステップ 4 新しい SEC ブートストラップデータを生成し、SEC 導入準備手順を再試行します。

Security and Analytics Logging イベントを使用したネットワーク問題のトラブルシューティング

これは、イベントビューアを使用してネットワークの問題をトラブルシューティングするための基本的なフレームワークです。

このシナリオでは、ネットワーク運用チームが、ユーザーがネットワーク上のリソースにアクセスできないという報告を受け取ったと想定しています。問題とその場所を報告しているユーザーに基づいて、ネットワーク運用チームは、どのファイアウォールがユーザーによるリソースへのアクセスを制御しているかを把握しています。



(注) また、このシナリオでは、ネットワークトラフィックを管理するファイアウォールが FTD デバイスであると想定しています。Security Analytics and Logging は、他のデバイスタイプからロギング情報を収集しません。

- ステップ 1** ナビゲーションウィンドウで、[モニタリング]>[イベントロギング]をクリックします。
- ステップ 2** [履歴] タブをクリックします。
- ステップ 3** [時間範囲] によるイベントのフィルタ処理を開始します。デフォルトでは、[履歴] タブには過去 1 時間のイベントが表示されます。それが正しい時間範囲である場合は、現在の日付と時刻を [終了] 時刻として入力します。それが正しい時間範囲でない場合は、報告された問題の時間を含む開始時間と終了時間を入力します。
- ステップ 4** [センサーID] フィールドに、ユーザーのアクセスを制御していると考えられるファイアウォールの IP アドレスを入力します。ファイアウォールが複数の可能性がある場合は、検索バーで属性:値のペアを使用してイベントをフィルタ処理します。2 つのエントリを作成し、それらを OR ステートメントで結合します。
例: SensorID:192.168.10.2 OR SensorID:192.168.20.2。
- ステップ 5** イベントフィルタバーの [送信元 IP] フィールドにユーザーの IP アドレスを入力します。
- ステップ 6** ユーザーがリソースにアクセスできない場合は、そのリソースの IP アドレスを [接続先 IP] フィールドに入力します。
- ステップ 7** 結果に表示されるイベントを展開し、その詳細を確認します。以下に表示される詳細の一部を示します。
- **AC_RuleAction** : ルールがトリガーされたときに実行されたアクション (許可、信頼、ブロック)。
 - **FirewallPolicy** : イベントをトリガーしたルールが存在するポリシー。
 - **FirewallRule** : イベントをトリガーしたルールの名前。値が Default Action の場合、イベントをトリガーしたのはポリシーのデフォルトアクションであり、ポリシー内のルールの 1 つではありません。
 - **UserName** : イニシエータの IP アドレスに関連づけられたユーザー。イニシエータ IP アドレスは送信元 IP アドレスと同じです。
- ステップ 8** ルールのアクションがアクセスを妨げている場合は、[FirewallRule] フィールドと [FirewallPolicy] フィールドを確認して、アクセスをブロックしているポリシー内のルールを特定します。

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パッケージ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 パッケージが SEC に送信されていることを確認する
- NetFlow パッケージが Cisco Cloud 受信されていることを確認する

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 (SEC) の `troubleshoot.sh` は、すべてのイベントストリーマログを収集して、単一の `.tar.gz` ファイルに圧縮します。

次の手順を使用して、`compressed.tar.gz` ファイルを作成し、ファイルを解凍します。

1. [トラブルシューティング スクリプトの実行 \(25 ページ\)](#)。
2. [sec_troubleshoot.tar.gz ファイルの圧縮解除 \(26 ページ\)](#)。

トラブルシューティング スクリプトの実行

Secure Event Connector (SEC) の `troubleshoot.sh` は、すべてのイベントストリーマログを収集して、単一の `.tar.gz` ファイルに圧縮します。次の手順に従って、`troubleshoot.sh` スクリプトを実行します。

ステップ 1 VM ハイパーバイザを開き、Secure Device Connector (SDC) のコンソールセッションを開始します。

ステップ 2 ログインしてから、[ルート (root)] ユーザーに切り替えます。

```
[cdo@localhost ~]$sudo su root
```

- (注) SDC ユーザーに切り替える一方で `root` として操作することもできます。その場合、IP テーブルの情報も受信することになります。IP テーブルの情報には、デバイス上でファイアウォールが実行中であることと、すべてのファイアウォールルールが表示されます。ファイアウォールが Secure Event Connector TCP ポートまたは UDP ポートをブロックしている場合、[イベントロギング] テーブルにイベントが表示されません。IP テーブルは、そのような状況が発生しているかどうかを判断する際に役立ちます。

ステップ 3 プロンプトで、トラブルシューティング スクリプトを実行し、テナント名を指定します。コマンド構文は次のとおりです。

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_[tenant_name]
```

次に例を示します。

```
[root@localhost ~]$ /usr/local/cdo/toolkit/troubleshoot.sh --app sec --tenant CDO_example_tenant
```

コマンド出力で、sec_troubleshoot ファイルが SDC の `/tmp/troubleshoot` ディレクトリに保存されていることがわかります。ファイル名は、**sec_troubleshoot-timestamp.tar.gz** の表記法に従います。

ステップ 4 ファイルを取得するには、CDO ユーザーとしてログインし、SCP または SFTP を使用してダウンロードします。

次に例を示します。

```
[root@localhost troubleshoot]# scp sec_troubleshoot-timestamp.tar.gz
root@server-ip:/scp/sec_troubleshoot-timestamp.tar.gz
```

次のタスク

[sec_troubleshoot.tar.gz ファイルの圧縮解除 \(26 ページ\)](#) に進みます。

sec_troubleshoot.tar.gz ファイルの圧縮解除

Secure Event Connector (SEC) の [トラブルシューティング スクリプトの実行](#) は、すべてのイベントストリーマログを収集して、単一の sec_troubleshoot.tar.gz ファイルに圧縮します。sec_troubleshoot.tar.gz ファイルの圧縮を解除するには、次の手順を実行します。

1. VM ハイパーバイザを開き、Secure Device Connector (SDC) のコンソールセッションを開始します。
2. ログインしてから、[ルート (root)] ユーザーに切り替えます。

```
[cdo@localhost ~]$sudo su root
```

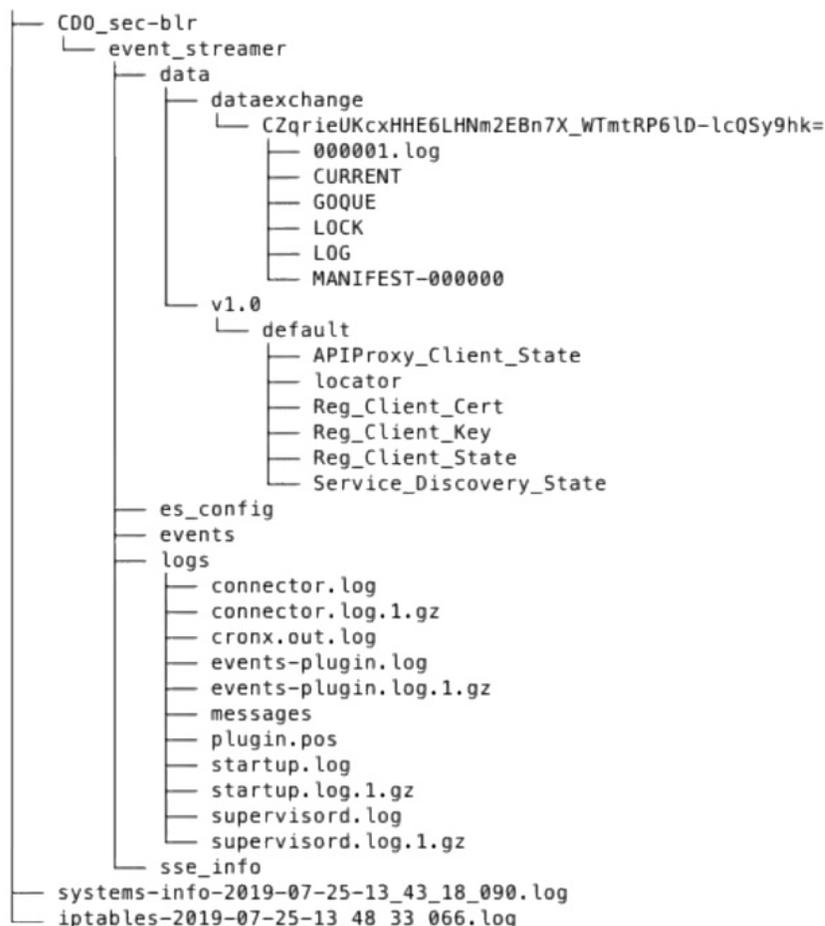


(注) **sdc** ユーザーに切り替える一方で **root** として操作することもできます。その場合、IP テーブルの情報も受信することになります。IP テーブルの情報には、デバイス上でファイアウォール実行中であることと、すべてのファイアウォールルールが表示されます。ファイアウォール Secure Event Connector TCP ポートまたは UDP ポートをブロックしている場合、[イベントロギング] テーブルにイベントが表示されません。IP テーブルは、そのような状況が発生しているかどうかを判断する際に役立ちます。

3. プロンプトで、次のコマンドを入力します。

```
[root@localhost ~]$ tar xvf sec_troubleshoot-timestamp.tar.gz
```

ログファイルは、テナントにちなんで名付けられたディレクトリに保存されます。これらのタイプのログは、sec_troubleshoot-timestamp.tar.gz ファイルに保存されます。root ユーザーとしてすべてのログファイルを収集した場合は、iptables ファイルが含まれています。



SEC ブートストラップデータの生成に失敗しました。

症状：CDO で SEC ブートストラップデータを生成しているときに、「ブートストラップの生成」ステップでエラーが発生し、次のメッセージが表示されます。「ブートストラップデータの取得中にエラーが発生しました。再試行してください」。

修復：ブートストラップデータの生成を再試行します。それでも失敗する場合は、[CDO サポートまでお問い合わせください](#)。

導入準備後、[CDOセキュアコネクタ (CDO Secure Connectors)] ページで SEC ステータスが [非アクティブ (Inactive)] になる

症状：次のいずれかの理由により、[CDOセキュアコネクタ (CDO Secure Connectors)] ページで Secure Event Connector のステータスが [非アクティブ (Inactive)] と表示されます。

- ハートビートに失敗した
- コネクタの登録に失敗した

SECは「オンライン」ですが、CDO イベントログページにはイベントがありません

修復：

- ハートビートに失敗した：SEC ハートビートを要求し、[セキュアコネクタ (Secure Connector)] ページを更新して、ステータスが[アクティブ (Active)] になるか確認します。変わらない場合は、Secure Device Connector の登録が失敗していないか確認します。
- コネクタの登録に失敗した：「[Secure Event Connector の登録失敗のトラブルシューティング](#)」を参照してください。

SEC は「オンライン」ですが、CDO イベントログページにはイベントがありません

症状：Secure Event Connector の CDO セキュアコネクタページには「アクティブ」と表示されているのに、CDO イベントビューアにイベントが表示されません。

解決策または回避策：

ステップ 1 オンプレミス SDC の VM に「sdc」ユーザーとしてログインします。プロンプトで、**sudo su - sdc** と入力します。

ステップ 2 次のチェックを実行します。

- SEC コネクタのログ (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/connector.log) を確認し、SEC 登録が成功していることを確認します。成功していない場合は、「[Secure Event Connector の登録失敗のトラブルシューティング](#)」を参照してください。
- SEC イベントのログ (/usr/local/cdo/data/<tenantDir>/event_streamer/logs/events-plugin.log) を確認し、イベントが処理されていることを確認します。処理されていない場合は、[CDO サポートにお問い合わせ](#)してください。
- SEC Docker コンテナにログインし、コマンド「supervisorctl -c /opt/cssp/data/conf/supervisord.conf」を実行します。出力が以下ようになり、すべてのプロセスが RUNNING 状態であることを確認します。そうでない場合は、[CDO サポートにお問い合わせ](#)ください。

estreamer-connector RUNNING pid 36, uptime 5:25:17

estreamer-cron RUNNING pid 39, uptime 5:25:17

estreamer-plugin RUNNING pid 37, uptime 5:25:17

estreamer-rsyslog RUNNING pid 38, uptime 5:25:17

- オンプレミス SDC のファイアウォールルールが、[セキュアコネクタ (Secure Connectors)] ページの SEC に表示される UDP および TCP ポートをブロックしていないことを確認します。どのポートを開くかを判断するには、「[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。

ID	Type	Deployment	Status	Last Heartbeat
CDO_solution_es1-SDC	Secure Device Connector	# On-Prem	Active	5/31/2019, 3:00:21 PM
6c24d6bb-e307-4a05-9dd7-4f6f6c084d6b	Secure Event Connector	# On-Prem	Active	5/31/2019, 3:00:23 PM

6c24d6bb-e307-4a05-9dd7-4f6f6c084d6b

Details

Version 83a49e199bdd85b7cdfb8dd05972e50c5929abf4

IP Address 192.168.0.191

TCP Port 10125

UDP Port 10025

- 独自の CentOS 7 VM を使用して SDC を手動でセットアップし、ファイアウォールが着信要求をブロックするように設定している場合は、次のコマンドを実行して UDP および TCP ポートのブロックを解除できます。

firewall-cmd --zone=public --add-port=<udp_port>/udp --permanent

firewall-cmd --zone=public --add-port=<tcp_port>/tcp --permanent

firewall-cmd --reload

- 選択した Linux ネットワークツールを使用して、これらのポートでパケットが受信されているかどうかを確認します。受信していない場合は、FTD ログ設定を再確認してください。

上記のいずれの修復も機能しない場合は、[CDO サポートにサポートチケットを提出](#)します。

SEC クリーンアップコマンド

Secure Event Connector (SEC) クリーンアップコマンドは、SEC コンテナとその関連ファイルを Secure Device Connector (SDC) VM から削除します。このコマンドは、[Secure Event Connector の登録失敗のトラブルシューティング \(23 ページ\)](#) または導入準備が失敗した場合に実行できます。

このコマンドを実行するには、次の手順を実行します。

始める前に

このタスクを実行するには、自分のテナントの名前を知っている必要があります。テナント名を見つけるには、CDO でユーザーメニューを開き、[設定] をクリックします。ページを下にスクロールして、[テナント名 (Tenant Name)] を見つけます。

ステップ 1 「sdc」ユーザーとして SDC にログインします。プロンプトで、`sudo su - sdc` と入力します。

ステップ 2 `/usr/local/cdo/toolkit` ディレクトリに接続します。

ステップ 3 `sec.sh removetenant_name` を実行し、SEC を削除することを確認します。

例：

```
[sdc@localhost~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ
Are you sure you want to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y
```

次のタスク

このコマンドで SEC の削除に失敗した場合は、[SEC クリーンアップコマンドの失敗 \(30 ページ\)](#)に進みます。

SEC クリーンアップコマンドの失敗

[SEC クリーンアップコマンド \(29 ページ\)](#) が失敗した場合は、この手順を使用します。

メッセージ : SEC が見つかりません。終了します。

症状 : Cleanup SEC コマンドが既存の SEC のクリーンアップに失敗します。

```
[sdc@localhost ~]$ /usr/local/cdo/toolkit/sec.sh remove tenant_XYZ Are you sure you want
to remove Secure Event Connector for tenant tenant_XYZ? (y/n): y [2020-06-10 04:50:42]
SEC not found, exiting.
```

修復 : クリーンアップコマンドが失敗した場合、Secure Event Connector を手動でクリーンアップします。

すでに実行中の SEC docker コンテナを削除します。

ステップ 1 「sdc」ユーザーとして SDC にログインします。プロンプトで、`sudo su - sdc` と入力します。

ステップ 2 `docker ps` コマンドを実行して、SEC コンテナの名前を探します。SEC 名は、"es_name" の形式になります。

ステップ 3 `docker stop` コマンドを実行して、SEC コンテナを停止します。

ステップ 4 `rm` コマンドを実行して、SEC コンテナを削除します。

例 :

```
$ docker stop <SEC_docker_container_name>
$ docker rm <SEC_docker_container_name>
```

Secure Event Connector の状態を把握するためのヘルスチェックの使用

Secure Event Connector (SEC) のヘルスチェックスクリプトは、SEC の状態に関する情報を提供します。

ヘルスチェックを実行するには、次の手順に従います。

ステップ 1 VM ハイパーバイザを開き、Secure Device Connector (SDC) のコンソールセッションを開始します。

ステップ 2 「CDO」ユーザーとして SDC にログインします。

ステップ 3 「SDC」ユーザーに切り替えます。

```
[cdo@tenant]$sudo su sdc
```

ステップ 4 プロンプトで `healthcheck.sh` スクリプトを実行し、テナント名を指定します。

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_[tenant_name]
```

次に例を示します。

```
[sdc@host ~]$ /usr/local/cdo/toolkit/healthcheck.sh --app sec --tenant CDO_example_tenant
```

スクリプトの出力には、次のような情報が表示されます。

```
=====
Running SEC health check for tenant
-----
SEC cloud URL [redacted] is: Reachable
-----
SEC Connector status: Active
-----
SEC Events Plugin is: Running
SEC UDP syslog server is: Running
SEC TCP syslog server is: Running
-----
SEC send sample event: Success. Please search with filter "sensorID:127.0.0.1" to locate the event in CDO events viewer page.
=====
```

ヘルスチェック出力の値：

- [SECクラウドURL (SEC Cloud URL)]：CDO クラウド URL と、SEC が CDO に到達できるかどうかを表示します。
- [SECコネクタ (SEC Connector)]：SEC コネクタが正しく導入準備され、開始されている場合は、「実行中 (Running)」と表示されます。
- [SEC UDP syslogサーバー (SEC UDP syslog server)]：UDP syslog サーバーが UDP イベントを送信する準備ができている場合は、「実行中 (Running)」と表示されます。
- [SEC TCP syslogサーバー (SEC TCP syslog server)]：TCP syslog サーバーが TCP イベントを送信する準備ができている場合は、「実行中 (Running)」と表示されます。
- [SECコネクタのステータス (SEC Connector status)]：SEC が実行中で、CDO への導入準備が完了している場合は、[アクティブ (Active)]と表示されます。
- [SEC送信サンプルイベント (SEC Send sample event)]：ヘルスチェックの終了時点ですべてのステータスチェックが「緑色」になっている場合、ツールはサンプルイベントを送信します。(いずれかのプロセスが[停止中 (Down)]になっている場合、ツールはテストイベントの送信をスキップします)。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。

CDO のトラブルシューティング

ログインの失敗のトラブルシューティング

正しくない CDO リージョンに誤ってログインしているため、ログインに失敗する

適切な CDO リージョンにログインしていることを確認してください。

<https://sign-on.security.cisco.com> にログインすると、アクセスするリージョンを選択できます。[CDO] タイルをクリックして defenseorchestrator.com にアクセスするか、[CDO (EU)] をクリックして defenseorchestrator.eu にアクセスします。

移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、CDO へのログインに失敗する

解決法 CDO にログインしようとして、正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Secure Sign-On アカウントを作成せずにログインを試みた可能性があります。新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定の手順に従って、新しい Cisco Secure Sign-On アカウントにサインアップする必要があります。

Cisco Secure Sign-On ダッシュボードへのログインは成功するが、CDO を起動できない

解決法 CDO アカウントとは異なるユーザー名で Cisco Secure Sign-On アカウントを作成している可能性があります。CDO と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center (TAC) に連絡してください。 <http://cdo.support@cisco.com>

保存したブックマークを使用したログインに失敗する

解決法 ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが <https://cdo.onelogin.com> を指している可能性があります。

解決法 <https://sign-on.security.cisco.com> にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、[アカウントを作成](#) します。
- **解決法** 新しいアカウントを作成している場合は、ダッシュボードで Cisco Defense Orchestrator (米国)、Cisco Defense Orchestrator (欧州)、または Cisco Defense Orchestrator (アジア太平洋/日本/中国) に対応する CDO タイルをクリックします。
- **解決法** <https://sign-on.security.cisco.com> を指すようにブックマークを更新します。

アクセスと証明書のトラブルシューティング

CDO でのユーザーアクセスのトラブルシューティング

ユーザーがアクセスする必要があるリソースへのアクセスを拒否された場合を考えてみましょう。問題を診断して修復するために実行できるアプローチを次に示します。

ステップ 1 ユーザーは、リソースへのアクセスがブロックされていることをセキュリティチームに通知します。そのリソースの通常のアクセス方法を確認します。IP アドレスは何か。特定のポートに到達するか。リソースに情報を送信するために使用されるプロトコルは何か。

ステップ 2 [デバイスとサービス] ページで、[デバイス] タブをクリックします。

ステップ 3 [FTD] タブをクリックして ASA を選択し、パケットトレーサを実行します。詳細については、「[ASA パケットトレーサ](#)」を参照してください。

ステップ 4 リソースへのアクセスを拒否した可能性のあるルールについて、パケットトレーステーブルを調べます。

- ステップ5** アクセスを拒否しているルールを特定したら、CDO で変更リクエストラベルを作成して有効にします。「[変更リクエスト管理](#)」を参照してください。これは、リソースへのアクセスを許可するために行った変更ログポリシーの変更を特定するのに役立ちます。
- ステップ6** CDO のルールを編集して、動作を修正します。ASA は CDO と同期していません。
- ステップ7** [デバイスとサービス] ページから ASA に変更を展開します。CDO は、CDO でステージングされた設定ではなく、ASA に保存された設定を通じてパケットをトレースします。CDO でステージングされた他の設定変更も ASA に展開することに注意してください。
- ステップ8** パケットトレーサを再実行して、ポリシーの変更によって望ましい結果が得られるかどうかを判断します。ユーザーがリソースにアクセスできることを確認します。
- ステップ9** ユーザーがアクセスできるようになったと見なして、CDO の変更リクエストラベルをクリアすると、無関係なアクティビティがこの修正に関連付けられないようになります。
- (注) 行った変更で問題が解決しないか、新たな問題が発生し、以前の設定に戻りたい場合は、ASA の設定を復元できます。「[ASA の設定の復元](#)」を参照してください。

新規フィンガープリントを検出状態の解決

- ステップ1** ナビゲーションバーで、[デバイスとサービス] 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ます。
- ステップ4** [新しいフィンガープリントを検出] 状態のデバイスを選択します。
- ステップ5** [新しいフィンガープリントを検出] ペインで [フィンガープリントの確認] をクリックします。
- ステップ6** フィンガープリントを確認して承認するように求められたら、以下の手順を実行します。
1. [フィンガープリントのダウンロード] をクリックして確認します。
 2. フィンガープリントに問題がなければ [承認] をクリックします。問題がある場合は、[キャンセル] をクリックします。
- ステップ7** 新しいフィンガープリントの問題を解決した後、デバイスの接続状態が [オンライン] と表示され、構成ステータスが [非同期] または [競合検出] と表示される場合があります。[構成の競合の解決] を確認し、CDO とデバイス間の構成の差異を確認して解決します。[設定の競合の解決](#)

SecurityandAnalyticsLogging イベントを使用したネットワーク問題のトラブルシューティング

これは、イベントビューアを使用してネットワークの問題をトラブルシューティングするための基本的なフレームワークです。

このシナリオでは、ネットワーク運用チームが、ユーザーがネットワーク上のリソースにアクセスできないという報告を受け取ったと想定しています。問題とその場所を報告しているユー

ザーに基づいて、ネットワーク運用チームは、どのファイアウォールがユーザーによるリソースへのアクセスを制御しているかを把握しています。



(注) また、このシナリオでは、ネットワークトラフィックを管理するファイアウォールが FTD デバイスであると想定しています。Security Analytics and Logging は、他のデバイスタイプからロギング情報を収集しません。

ステップ 1 ナビゲーションウィンドウで、[モニタリング]>[イベントロギング]をクリックします。

ステップ 2 [履歴] タブをクリックします。

ステップ 3 [時間範囲] によるイベントのフィルタ処理を開始します。デフォルトでは、[履歴] タブには過去 1 時間のイベントが表示されます。それが正しい時間範囲である場合は、現在の日付と時刻を [終了] 時刻として入力します。それが正しい時間範囲でない場合は、報告された問題の時間を含む開始時間と終了時間を入力します。

ステップ 4 [センサーID] フィールドに、ユーザーのアクセスを制御していると考えられるファイアウォールの IP アドレスを入力します。ファイアウォールが複数の可能性がある場合は、検索バーで属性:値のペアを使用してイベントをフィルタ処理します。2 つのエントリを作成し、それらを OR ステートメントで結合します。
例: SensorID:192.168.10.2 OR SensorID:192.168.20.2。

ステップ 5 イベントフィルタバーの [送信元IP] フィールドにユーザーの IP アドレスを入力します。

ステップ 6 ユーザーがリソースにアクセスできない場合は、そのリソースの IP アドレスを [接続先IP] フィールドに入力します。

ステップ 7 結果に表示されるイベントを展開し、その詳細を確認します。以下に表示される詳細の一部を示します。

- **AC_RuleAction** : ルールがトリガーされたときに実行されたアクション (許可、信頼、ブロック)。
- **FirewallPolicy** : イベントをトリガーしたルールが存在するポリシー。
- **FirewallRule** : イベントをトリガーしたルールの名前。値が Default Action の場合、イベントをトリガーしたのはポリシーのデフォルトアクションであり、ポリシー内のルールの 1 つではありません。
- **UserName** : イニシエータの IP アドレスに関連づけられたユーザー。イニシエータ IP アドレスは送信元 IP アドレスと同じです。

ステップ 8 ルールのアクションがアクセスを妨げている場合は、[FirewallRule] フィールドと [FirewallPolicy] フィールドを確認して、アクセスをブロックしているポリシー内のルールを特定します。

SSL 暗号解読の問題のトラブルシューティング

復号再署名がブラウザでは機能するがアプリでは機能しない Web サイトの処理 (SSL または認証局 ピニング)

スマートフォンおよびその他のデバイス用の一部のアプリケーションでは「SSL (または認証局) ピニング」と呼ばれる手法が使用されます。SSL ピニング手法では、元のサーバー証明書

のハッシュがアプリケーション自体の内部に埋め込まれます。その結果、アプリケーションが再署名された証明書を Firepower Threat Defense デバイスから受け取ると、ハッシュ検証に失敗し、接続が中断されます。

Webサイトのアプリケーションを使用してそのサイトに接続することができないにもかかわらず、Webブラウザを使用する場合は、接続に失敗したアプリケーションを使用したデバイス上のブラウザでも接続できるというのが主な症状です。たとえば、Facebook の iOS または Android アプリケーションを使用すると接続に失敗しますが、Safari または Chrome で <https://www.facebook.com> を指定すると接続に成功します。

SSL ピニングは特に中間者攻撃を回避するために使用されるため、回避策はありません。次のいずれかの選択肢を使用する必要があります。

詳細の表示

サイトがブラウザでは機能するのに同じデバイス上のアプリケーションでは機能しない場合は、ほぼ確実に SSL ピニングによるものと考えられます。ただし、詳しく調べる必要がある場合は、ブラウザのテストに加えて、接続イベントを使用して SSL ピニングを識別できます。

アプリケーションは、次の 2 つの方法でハッシュ検証の失敗に対処する場合があります。

- グループ 1 のアプリケーション (Facebook など) は、サーバから SH、CERT、SHD メッセージを受け取るとすぐに SSL ALERT メッセージを送信します。アラートは、通常、SSL ピニングを示す「Unknown CA (48)」アラートです。アラートメッセージの後に TCP リセットが送信されます。イベントの詳細情報で次のような症状が見られます。
 - SSL フロー フラグには ALERT_SEEN が含まれます。
 - SSL フロー フラグには APP_DATA_C2S または APP_DATA_S2C は含まれません。
 - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE です。
- グループ 2 のアプリケーション (Dropbox など) はアラートを送信しません。代わりに、ハンドシェイクが完了するまで待ってから TCP リセットを送信します。イベントで次のような症状が見られます。
 - SSL フロー フラグには ALERT_SEEN、APP_DATA_C2S または APP_DATA_S2C は含まれません。
 - SSL フロー メッセージは、通常、CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED です。

移行後のログイン失敗のトラブルシューティング

ユーザー名またはパスワードが正しくないため、CDO へのログインに失敗する

解決法 CDO にログインしようとして、正しいユーザー名とパスワードを使用しているにもかかわらずログインに失敗する場合、または「パスワードを忘れた場合」を試しても有効なパスワードを回復できない場合は、新しい Cisco Secure Sign-On アカウントを作成せずにログイン

を試みた可能性があります。新規 Cisco Secure Sign-On アカウントの作成と Duo 多要素認証の設定の順に従って、新しい Cisco Secure Sign-On アカウントにサインアップする必要があります。

Cisco Secure Sign-On ダッシュボードへのログインは成功するが、CDO を起動できない

解決法 CDO アカウントとは異なるユーザー名で Cisco Secure Sign-On アカウントを作成している可能性があります。CDO と Cisco Secure Sign-On の間でユーザー情報を標準化するには、Cisco Technical Assistance Center (TAC) に連絡してください。 <http://cdo.support@cisco.com>

保存したブックマークを使用したログインに失敗する

解決法 ブラウザに保存された古いブックマークを使用してログインしようとしているかもしれません。ブックマークが <https://cdo.onelogin.com> を指している可能性があります。

解決法 <https://sign-on.security.cisco.com> にログインします。

- **解決法** Cisco Secure Sign-On アカウントをまだ作成していない場合は、[アカウントを作成](#) します。
- **解決法** 新しいアカウントを作成している場合は、ダッシュボードで Cisco Defense Orchestrator (米国)、Cisco Defense Orchestrator (欧州)、または Cisco Defense Orchestrator (アジア太平洋/日本/中国) に対応する CDO タイルをクリックします。
- **解決法** <https://sign-on.security.cisco.com> を指すようにブックマークを更新します。

オブジェクトのトラブルシューティング

重複オブジェクトの問題の解決

重複オブジェクトとは、同じデバイス上にある、名前は異なるが値は同じである2つ以上のオブジェクトです。通常、重複したオブジェクトは誤って作成され、同じ目的を果たし、さまざまなポリシーによって使用されます。重複オブジェクトの問題を解決した後、CDO は、影響を受けるすべてのオブジェクト参照を残されたオブジェクト名で更新します。

重複オブジェクトの問題を解決するには以下の手順を実行します。

ステップ 1 [オブジェクト] ページを開き、オブジェクトを [フィルタ処理](#) して、重複オブジェクトの問題を見つけます。

ステップ 2 結果の中から 1 つを選択します。オブジェクトの詳細パネルに、該当する重複の数を示す [重複] フィールドが表示されます。

 DUPLICATE **2** [Resolve](#) | [Ignore](#)

ステップ 3 [解決 (Resolve)] をクリックします。CDO は、重複オブジェクトを比較できるように表示します。

ステップ 4 比較するオブジェクトを 2 つ選択します。

ステップ 5 以下のオプションがあります。

- オブジェクトの 1 つを別のオブジェクトで置き換える場合は、保持するオブジェクトで [選択] をクリックし、[解決] をクリックして影響を受けるデバイスとネットワークポリシーを確認し、変更の問題が

なければ[確認]をクリックします。CDOは、選択したオブジェクトに置き換えて保持し、重複を削除します。

- リストにあるオブジェクトを無視する場合は、[無視]をクリックします。オブジェクトを無視すると、CDOが表示する重複オブジェクトのリストから削除されます。
- オブジェクトを保持するものの、重複オブジェクトの検索でCDOがそれを検出しないようにするには、[すべて無視]をクリックします。

ステップ 6 重複オブジェクトの問題が解決したら、行った変更を今すぐ[レビューして展開する](#)か、待機してから複数の変更を一度に展開します。

未使用オブジェクトの問題の解決

未使用オブジェクト  は、デバイス構成に存在するものの、別のオブジェクト、アクセスリスト、NAT ルールによって参照されていないオブジェクトです。

関連情報：

- [デバイスとサービスのリストのエクスポート](#)
- [CDO へのデバイス一括再接続](#)

未使用オブジェクトの問題の解決

ステップ 1 メニューバーで[オブジェクト]をクリックし、オブジェクトを[フィルタ処理](#)して、未使用のオブジェクトの問題を見つけます。

ステップ 2 1つ以上の未使用のオブジェクトを選択します。

ステップ 3 以下のオプションがあります。

- 操作ウィンドウで[削除]  をクリックして、未使用のオブジェクトをCDOから削除します。
- [問題] ペインで、[無視] をクリックします。オブジェクトを無視すると、CDOは未使用のオブジェクトの結果にそのオブジェクトを表示しなくなります。

ステップ 4 未使用のオブジェクトを削除した場合は、行った変更を今すぐ[すべてのデバイスの構成変更のプレビューと展開](#)か、待機してから複数の変更を一度に展開します。

(注) 未使用のオブジェクトの問題を一括で解決するには、「[オブジェクトの問題を一度に解決する](#)」を参照してください。

未使用オブジェクトの一括削除

ステップ1 [オブジェクト] ページを開き、オブジェクトを [フィルタ処理](#) して、未使用オブジェクトの問題を見つけます。

ステップ2 削除する未使用のオブジェクトを選択します。

- ページ上のすべてのオブジェクトを選択するには、オブジェクトテーブルのヘッダー行にあるチェックボックスをクリックします。
- オブジェクトテーブルで未使用のオブジェクトを個別に選択します。

ステップ3 右側の [アクション] ペインで [削除]  をクリックして、CDO で選択した未使用のオブジェクトをすべて削除します。99 個のオブジェクトを同時に削除できます。

ステップ4 [OK] をクリックして、未使用のオブジェクトを削除することを確認します。

ステップ5 これらの変更の展開には、つぎの2つの方法があります。

- 行った変更を今すぐ [レビューして展開する](#) か、待機してから複数の変更を一度に展開します。
- [デバイスとサービス] ページを開き、変更の影響を受けたデバイスを特定します。変更の影響を受けるすべてのデバイスを選択し、[管理] ペインで [すべて展開 (Deploy All)]  をクリックします。警告を読み、適切なアクションを実行します。

不整合オブジェクトの問題を解決する

不整合オブジェクト  INCONSISTENT  [Resolve](#) | [Ignore](#) とは、2 つ以上のデバイス上にある、名前は同じだが値は異なるオブジェクトです。ユーザーが異なる構成の中で、同じ名前と内容のオブジェクトを作成することがあります。これらのオブジェクトの値が時間の経過につれて相互に異なる値になり、不整合が生じます。

注： 不整合オブジェクトの問題を一括で解決するには、「[オブジェクトの問題を一度に解決する](#)」を参照してください。

不整合オブジェクトに対して次のことを実行できます。

- [無視]：CDO は、オブジェクト間の不整合を無視し、それらの値を保持します。このオブジェクトは、不整合カテゴリに表示されなくなります。
- [マージ (Merge)]：CDO は、選択されているすべてのオブジェクトとその値を 1 つのオブジェクトグループに結合します。
- [名前の変更 (Rename)]：CDO で、不整合オブジェクトの一つの名前を変更し、新しい名前を付けることができます。
- [共有ネットワークオブジェクトのオーバーライドへの変換 (Convert Shared Network Objects to Overrides)]：CDO で、不整合のある共有オブジェクトを (オーバーライドの有無にかかわらず)、オーバーライドのある単一の共有オブジェクトに結合できます。不整合オブ

ジェットの最も一般的なデフォルト値が、新しく形成されるオブジェクトのデフォルトとして設定されます。



(注) 共通のデフォルト値が複数ある場合は、そのうちの 하나가デフォルトとして選択されます。残りのデフォルト値とオーバーライド値は、そのオブジェクトのオーバーライドとして設定されます。

- [共有ネットワークグループの追加の値への変換 (Convert Shared Network Group to Additional Values)]: CDO で、不整合のある共有ネットワークグループを、追加の値のある単一の共有ネットワークグループに結合できます。この機能の基準は、「変換される不整合ネットワークグループに、同じ値を持つ少なくとも1つの共通オブジェクトが必要である」というものです。この基準に一致するすべてのデフォルト値がデフォルト値になり、残りのオブジェクトは、新しく形成されるネットワークグループの追加の値として割り当てられます。

たとえば、不整合のある2つの共有ネットワークグループがあるとします。1つ目のネットワークグループ「shared_network_group」は、「object_1」(192.0.2.x)と「object_2」(192.0.2.y)で形成されています。また、追加の値「object_3」(192.0.2.a)も含まれています。2つ目のネットワークグループ「shared_network_group」は、「object_1」(192.0.2.x)と追加の値「object_4」(192.0.2.b)で形成されます。共有ネットワークグループを追加の値に変換すると、新しく形成されるグループ「shared_network_group」には、デフォルト値として「object_1」(192.0.2.x)と「object_2」(192.0.2.y)が含まれ、追加の値として「object_3」(192.0.2.a)と「object_4」(192.0.2.b)が含まれます。



(注) 新しいネットワークオブジェクトを作成すると、CDOは、その値を同じ名前の既存の共有ネットワークオブジェクトへのオーバーライドとして自動的に割り当てます。これは、新しいデバイスがCDOに導入準備される場合にも当てはまります。

自動割り当ては、次の条件が満たされている場合にのみ発生します。

1. 新しいネットワークオブジェクトがデバイスに割り当てられる必要があります。
2. テナントには、同じ名前とタイプの共有オブジェクトが1つだけ存在する必要があります。
3. 共有オブジェクトには、すでにオーバーライドが含まれている必要があります。

不整合オブジェクトの問題を解決するには、次の手順を実行します。

ステップ1 [オブジェクト] ページを開き、オブジェクトを [フィルタ処理](#) して、不整合オブジェクトの問題を見つけます。

ステップ2 不整合オブジェクトを選択します。オブジェクトの詳細パネルに、該当するオブジェクトの数を示す[不整合 (INCONSISTENT)] フィールドが表示されます。



ステップ3 [解決 (Resolve)] をクリックします。CDO は、不整合オブジェクトを比較できるように表示します。

ステップ4 以下のオプションがあります。

• [すべて無視 (Ignore All)] :

1. 提示されるオブジェクトを比較し、いずれかのオブジェクトで[無視] をクリックします。または、すべてのオブジェクトを無視するために、[すべて無視 (Ignore All)] をクリックします。
2. [OK] をクリックして確認します。

• [オブジェクトをマージして解決 (Resolve by merging objects)] :

1. [Xつのオブジェクトをマージして解決 (Resolve by Merging X Objects)] をクリックします。
2. [確認 (Confirm)] をクリックします。

• [名前の変更 (Rename)] :

1. [名前の変更 (Rename)] をクリックします。
2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認 (Confirm)] をクリックします。

• [オーバーライドへの変換 (Convert to Overrides)] (不整合のある共有オブジェクトの場合) : 共有オブジェクトをオーバーライドと比較する場合、比較パネルには、[不整合のある値 (Inconsistent Values)] フィールドのデフォルト値のみが表示されます。

1. [オーバーライドへの変換 (Convert to Overrides)] をクリックします。すべての不整合オブジェクトは、オーバーライドを持つ単一の共有オブジェクトに変換されます。
2. [確認 (Confirm)] をクリックします。[共有オブジェクトの編集 (Edit Shared Object)] をクリックすると、新しく形成されたオブジェクトの詳細が表示されます。上向き矢印と下向き矢印を使用して、デフォルトとオーバーライドの間で値を移動することができます。

• [追加の値への変換 (Convert to Additional Values)] (不整合のあるネットワークグループの場合) :

1. [追加の値への変換 (Convert to Additional Values)] をクリックします。すべての不整合オブジェクトは、追加の値を持つ単一の共有オブジェクトに変換されます。
2. 該当するネットワークポリシーおよびデバイスへの変更を保存し、[確認 (Confirm)] をクリックします。

ステップ5 不整合を解決したら、行った変更を今すぐ[レビューして展開する](#)か、待機してから複数の変更を一度に展開します。

オブジェクトの問題を一度に解決する

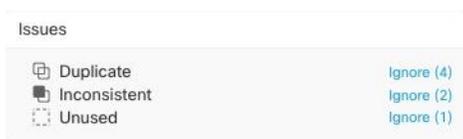
未使用オブジェクトの問題の解決、重複オブジェクトの問題の解決、不整合オブジェクトの問題を解決する (38 ページ) の問題のあるオブジェクトを解決する方法の 1 つは、それらを見捨てることです。オブジェクトに複数の問題がある場合でも、複数のオブジェクトを選択して見捨てるできます。たとえば、オブジェクトに一貫性がなく、さらに未使用の場合、一度に見捨てる問題タイプは 1 つだけです。



重要 後でオブジェクトが別の問題タイプに関連付けられた場合も、実行した見捨てるアクションは、その時に選択した問題にのみ影響します。たとえば、重複していたためにオブジェクトを見捨てるし、後でそのオブジェクトが不整合としてマークされた場合、そのオブジェクトを重複オブジェクトとして見捨てるしても、不整合のオブジェクトとして見捨てるわけではありません。

問題を一括で見捨てるには、以下の手順に従ってください。

- ステップ 1** [オブジェクト] ページを開きます。検索を絞り込むために、オブジェクトの問題を [フィルタ処理](#) できます。
- ステップ 2** オブジェクトテーブルで、見捨てるすべての該当するオブジェクトを選択します。問題ペインでは、問題タイプごとにオブジェクトがグループ化されます。



- ステップ 3** [見捨てる] をクリックして、問題をタイプ別に見捨てるします。問題タイプごとに個別に見捨てる必要があります。
- ステップ 4** [OK] をクリックして、それらのオブジェクトを見捨てることを確認します。

デバイスの接続状態

CDO テナントに導入準備されたデバイスの接続状態を表示できます。このトピックは、さまざまな接続状態を理解するのに役立ちます。[デバイスとサービス] ページの [接続 (Connectivity)] カラムに、デバイスの接続状態が表示されます。

デバイスの接続状態が「オンライン」の場合、デバイスの電源がオンになっていて、CDO に接続されていることを意味します。以下の表に記載されているその他の状態は、通常、さまざまな理由でデバイスに問題が発生した場合になります。この表は、このような問題から回復する方法を示しています。接続障害の原因となっている問題が複数ある可能性があります。再接続を試みると、CDO は、再接続を実行する前に、まずこれらの問題をすべて解決するように求めます。

デバイスの接続状態	考えられる原因	解像度
オンライン (Online)	デバイスの電源が入っていて、CDO に接続されています。	NA
オフライン	デバイスの電源が切れているか、ネットワーク接続が失われています。	デバイスがオフラインかどうかを確認します。
Insufficient licenses	デバイスに十分なライセンスがありません。	ライセンス不足のトラブルシューティング (42 ページ)
クレデンシャルが無効である	CDO がデバイスに接続するために使用するユーザー名とパスワードの組み合わせが正しくありません。	無効なログイン情報のトラブルシューティング (43 ページ)
New Certificate Detected	このデバイスの証明書が変更されました。デバイスが自己署名証明書を使用している場合、これはデバイスの電源を再投入したために発生した可能性があります。	新規証明書の問題のトラブルシューティング (43 ページ)
オンボーディングエラー	CDO が導入準備時にデバイスとの接続を失った可能性があります。	オンボーディングエラーのトラブルシューティング (53 ページ)

ライセンス不足のトラブルシューティング

デバイスの接続ステータスに[ライセンスが不足しています (Insufficient License)]と表示される場合は、以下の手順を実行します。

- デバイスがライセンスを取得するまでしばらく待ちます。通常、Cisco Smart Software Manager が新しいライセンスをデバイスに適用するには時間がかかります。
- デバイスのステータスが変わらない場合は、CDO からサインアウトしてから再度サインインすることで CDO ポータルを更新して、ライセンスサーバーとデバイスとの間のネットワーク通信の不具合を解決します。
- ポータルを更新してもデバイスのステータスが変更されない場合は、次の手順を実行します。

ステップ 1 [Cisco Smart Software Manager](#) から新しいトークンを生成し、コピーします。詳細については、[スマートライセンスの生成](#)に関するビデオをご覧ください。

- ステップ2** CDO のナビゲーションバーで、[デバイスとサービス] ページをクリックします。
- ステップ3** [デバイス] タブをクリックします。
- ステップ4** 適切なデバイスタイプのタブをクリックし、ステータスが [ライセンスが不足しています (Insufficient License)] のデバイスを選択します。
- ステップ5** [デバイスの詳細] ペインで、[ライセンスが不足しています (Insufficient License)] に表示される [ライセンスの管理 (Manage Licenses)] をクリックします。[ライセンスの管理 (Manage Licenses)] ウィンドウが表示されます。
- ステップ6** [アクティブ化 (Activate)] フィールドで、新しいトークンを貼り付けて [デバイスの登録 (Register Device)] をクリックします。
- トークンがデバイスに正常に適用されると、接続状態が [オンライン] に変わります。

無効なログイン情報のトラブルシューティング

無効なログイン情報によるデバイスの切断を解決するには、次の手順を実行します。

- ステップ1** [デバイスとサービス] ページを開きます。
- 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、ステータスが [無効なログイン情報] のデバイスを選択します。
- ステップ4** [デバイスの詳細] ペインで、[無効なログイン情報] に表示される [再接続] をクリックします。CDO がデバイスとの再接続を試行します。
- ステップ5** デバイスの新しいユーザー名とパスワードの入力を求められたら、
- ステップ6** [続行 (Continue)] をクリックします。
- ステップ7** デバイスがオンラインになり、使用できる状態になったら、[閉じる] をクリックします。
- ステップ8** CDO がデバイスへの接続に間違ったログイン情報を使用しようとしたため、デバイスへの接続に CDO が使用するユーザー名とパスワードの組み合わせが、デバイス上で直接変更された可能性があります。デバイスは「オンライン」ですが、構成ステータスは [競合が検出されました] であることがわかります。[構成の競合の解決] を使用して、CDO とデバイス間の構成の差異を確認して解決します。 [設定の競合の解決](#)

新規証明書の問題のトラブルシューティング

CDO での証明書の使用

CDO は、デバイスに接続するときに証明書の有効性をチェックします。具体的には、CDO は次のことを要求します。

1. デバイスで TLS バージョン 1.0 以降を使用している。

2. デバイスにより提示される証明書が有効期限内であり、発効日が過去の日付である（すなわち、すでに有効になっており、後日に有効化されるようにスケジュールされていない）。
3. 証明書は、SHA-256 証明書であること。SHA-1 証明書は受け入れられません。
4. 次のいずれかが該当すること。
 - デバイスは自己署名証明書を使用し、その証明書は認可されたユーザーにより信頼された最新の証明書と同じである。
 - デバイスは、信頼できる認証局（CA）が署名した証明書を使用し、提示されたリーフ証明書から関連 CA にリンクしている証明書チェーンを形成している。

これらは、ブラウザとは異なる CDO の証明書の使用方法です。

- 自己署名証明書の場合、CDO は、デバイスの導入準備または再接続時に、ドメイン名チェックを無効にして、代わりに、その証明書が承認ユーザーによって信頼された証明書と完全に一致することをチェックします。
- CDO は、まだ内部 CA をサポートしていません。現時点では、内部 CA によって署名された証明書をチェックする方法はありません。

ASA デバイスの証明書チェックを、デバイスごとに無効にすることができます。ASA の証明書を CDO が信頼できない場合、そのデバイスの証明書チェックを無効にするオプションがあります。デバイスの証明書チェックの無効化を試みても依然としてデバイスを導入準備できない場合は、デバイスに関して指定した IP アドレスおよびポートが正しくないか到達可能ではない可能性があります。証明書チェックをグローバルに無効にする方法、またはサポートされている証明書を持つデバイスの証明書チェックを無効にする方法はありません。非 ASA デバイスの証明書チェックを無効にする方法はありません。

デバイスの証明書チェックを無効にしても、CDO は、引き続き TLS を使用してデバイスに接続しますが、接続の確立に使用される証明書を検証しません。つまり、パッシブ中間者攻撃者は接続を盗聴できませんが、アクティブ中間攻撃者は、無効な証明書を CDO に提供することによって、接続を傍受する可能性があります。

証明書の問題の特定

いくつかの理由で CDO がデバイスを導入準備できない場合があります。UI に「CDO cannot connect to the device using the certificate presented」というメッセージが表示される場合は、証明書に問題があります。このメッセージが UI に表示されない場合は、問題が接続の問題（デバイスに到達できない）またはその他のネットワークエラーに関連している可能性が高くなります。

CDO が特定の証明書を拒否する理由を判断するには、SDC ホスト、または関連デバイスに到達できる別のホストで、`openssl` コマンドラインツールを使用します。次のコマンドを使用して、デバイスによって提示された証明書を示すファイルを作成します。

```
openssl s_client -showcerts -connect <host>:<port> && <filename>.txt
```

このコマンドでは、対話型セッションが開始されるため、数秒後に Ctrl+C キーを押して終了する必要があります。

次のような出力を含むファイルが作成されます。

```

depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify return:1
depth=1 C = US, O = Google Inc, CN = Google Internet Authority G2
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google Inc, CN = *.google.com
verify return:1 CONNECTED(00000003)
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
  i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
  i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjqSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTALVT
...lots of base64...
tzw9TylihJpZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
  i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTALVT
...lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits

---
SSL handshake has read 4575 bytes and written 434 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 48F046F3360225D51BE3362B50CE4FE8DB6D6B80B871C2A6DD5461850C4CF5AB
    Session-ID-ctx:
    Master-Key:
9A9CCBAA4F5A25B95C37EF7C6870F8C5DD3755A9A7B4CCE4535190B793DEFF53F94203AB0A62F9F70B9099FBFEBAB1B6

    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 100800 (seconds)
    TLS session ticket:
0000 - 7a eb 54 dd ac 48 7e 76-30 73 b2 97 95 40 5b de z.T..H~v0s...@[.
0010 - f3 53 bf c8 41 36 66 3e-5b 35 a3 03 85 6f 7d 0c .S..A6f>[5...o).

```

```

0020 - 4b a6 90 6f 95 e2 ec 03-31 5b 08 ca 65 6f 8f a6 K..o....1[...eo..
0030 - 71 3d c1 53 b1 29 41 fc-d3 cb 03 bc a4 a9 33 28 q=.S.)A.....3(
0040 - f8 c8 6e 0a dc b3 e1 63-0e 8f f2 63 e6 64 0a 36 ..n....c...c.d.6
0050 - 22 cb 00 3a 59 1d 8d b2-5c 21 be 02 52 28 45 9d "...:Y...\!..R(E.
0060 - 72 e3 84 23 b6 f0 e2 7c-8a a3 e8 00 2b fd 42 1d r..#...|....+.B.
0070 - 23 35 6d f7 7d 85 39 1c-ad cd 49 f1 fd dd 15 de #5m.)9...I.....
0080 - f6 9c ff 5e 45 9c 7c eb-6b 85 78 b5 49 ea c4 45 ...^E.|.k.x.I..E
0090 - 6e 02 24 1b 45 fc 41 a2-87 dd 17 4a 04 36 e6 63 n.$.E.A....J.6.c
00a0 - 72 a4 ad
00a4 - <SPACES/NULS> Start Time: 1476476711 Timeout : 300 (sec)
Verify return code: 0 (ok)
---
```

この出力では、最初に、**確認リターン (verify return) コード**が示されている最後の行に注目してください。証明書に関する問題が存在する場合、このリターンコードはゼロ以外になり、エラーの説明が表示されます。

この証明書エラーコードのリストを展開して、一般的なエラーとその修正方法を確認してください。

0 X509_V_OK : 操作が成功しました。

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT : 信頼できない証明書の発行者証明書が見つかりませんでした。

3 X509_V_ERR_UNABLE_TO_GET_CRL : 証明書の CRL が見つかりませんでした。

4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE : 証明書の署名を暗号解読できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。これは、RSA キーについてのみ意味を持ちます。

5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE : CRL の署名を暗号解読できませんでした。これは、実際の署名値が、期待値と一致しないのではなく、判別できなかったことを意味します。未使用。

6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY : 証明書 SubjectPublicKeyInfo の公開キーを読み取れませんでした。

7 X509_V_ERR_CERT_SIGNATURE_FAILURE : 証明書の署名が無効です。

8 X509_V_ERR_CRL_SIGNATURE_FAILURE : 証明書の署名が無効です。

9 X509_V_ERR_CERT_NOT_YET_VALID : 証明書がまだ有効ではありません (notBefore の日付が現在時刻より後です)。詳細については、この後の「[確認リターンコード : 9 \(証明書がまだ有効ではありません\)](#)」を参照してください。

10 X509_V_ERR_CERT_HAS_EXPIRED : 証明書の有効期限が切れています (notAfter の日付が現在時刻より前です)。詳細については、この後の「[確認リターンコード : 10 \(証明書の有効期限が切れています\)](#)」を参照してください。

11 X509_V_ERR_CRL_NOT_YET_VALID : CRL がまだ有効ではありません。

12 X509_V_ERR_CRL_HAS_EXPIRED : CRL の有効期限が切れています。

13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD : 証明書の notBefore フィールドに無効な時刻が含まれています。

14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD : 証明書の notAfter フィールドに無効な時刻が含まれています。

15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD : CRL の lastUpdate フィールドに無効な時刻が含まれています。

16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD : CRL の nextUpdate フィールドに無効な時刻が含まれています。

17 X509_V_ERR_OUT_OF_MEM : メモリを割り当てようとしてエラーが発生しました。これは決して発生しないはずの問題です。

18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT : 渡された証明書は自己署名済みであり、信頼できる証明書のリストに同じ証明書が見つかりません。

19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN : 信頼できない証明書を使用して証明書チェーンを構築できましたが、ルートがローカルで見つかりませんでした。

20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY : ローカルでルックアップされた証明書の発行者証明書が見つかりませんでした。これは、通常、信頼できる証明書のリストが完全ではないことを意味します。

21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE : チェーンに証明書が 1 つしか含まれておらず、それが自己署名済みでないため、署名を検証できませんでした。詳細については、この後の「確認リターンコード : 21 (最初の証明書を検証できません)」を参照してください。詳細については、この後の「[確認リターンコード : 21 \(最初の証明書を検証できません\)](#)」を参照してください。

22 X509_V_ERR_CERT_CHAIN_TOO_LONG : 証明書チェーンの長さが、指定された最大深度を超えています。未使用。

23 X509_V_ERR_CERT_REVOKED : 証明書が失効しています。

24 X509_V_ERR_INVALID_CA : CA 証明書が無効です。CA ではないか、その拡張領域が、提供された目的と一致していません。

25 X509_V_ERR_PATH_LENGTH_EXCEEDED : basicConstraints の pathlength パラメータを超えています。

26 X509_V_ERR_INVALID_PURPOSE : 提供された証明書を、指定された目的に使用できません。

27 X509_V_ERR_CERT_UNTRUSTED : ルート CA が、指定された目的に関して信頼できるものとしてマークされていません。

28 X509_V_ERR_CERT_REJECTED : ルート CA が、指定された目的を拒否するようにマークされています。

29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH : 件名が現在の証明書の発行者名と一致しないため、現在の候補発行者証明書が拒否されました。-issuer_checks オプションが設定されている場合にのみ表示されます。

30 X509_V_ERR_AKID_SKID_MISMATCH : 件名キー識別子が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer_checks オプションが設定されている場合にのみ表示されます。

31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH : 発行者名とシリアル番号が存在し、現在の証明書の認証局キー識別子と一致しないため、現在の候補発行者証明書が拒否されました。-issuer_checks オプションが設定されている場合にのみ表示されます。

32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN : keyUsage 拡張領域が証明書の署名を許可していないため、現在の候補発行者証明書が拒否されました。

50 X509_V_ERR_APPLICATION_VERIFICATION : アプリケーション固有のエラーです。未使用。

「New Certificate Detected」メッセージ

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、CDO で、[設定 (Configuration)] ステータスと [接続 (Connectivity)] ステータスの両方として、「新しい証明書が検出されました (New Certificate Detected)」というメッセージが生成されることがあります。このデバイスを引き続き CDO から管理するには、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。



(注) 複数の管理対象デバイスを CDO に同時に一括再接続すると、CDO は、デバイス上の新しい証明書を自動的に確認して受け入れ、それらとの再接続を続行します。

新しい証明書を解決するには、次の手順を使用します。

1. [デバイスとサービス (Device & Services)] ページに移動します。
2. フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました (New Certificate Detected)] であるデバイスを表示し、必要なデバイスを選択します。
3. [アクション] ペインで、[証明書の確認 (Review Certificate)] をクリックします。CDO では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
4. [デバイス同期 (Device Sync)] ウィンドウで [承認 (Accept)] をクリックするか、[デバイスへの再接続 (Reconnecting to Device)] ウィンドウで [続行] をクリックします。

CDO は、デバイスを新しい自己署名証明書と自動的に同期します。同期されたデバイスを表示するには、[デバイスとサービス] ページを手動で更新する必要がある場合があります。

証明書エラーコード

確認リターンコード:0 (OK) (ただし、CDO は証明書エラーを返します)

CDO は、証明書を取得すると、「https://<device_ip>:<port>」への GET コールを実行することにより、デバイスの URL への接続を試みます。これが機能しない場合、CDO は証明書エラーを表示します。証明書が有効である（openssl が 0 つまり OK を返します）ことがわかった場合、接続しようとしているポートで別のサービスがリスンしている可能性があります。この場合、次のコマンドを使用できます。

```
curl -k -u <username>:<password>
https://<device_id>:<device_port>/admin/exec/show%20version
```

これにより、次のように、ASA と確実に通信しているかどうかを確認することができ、HTTPS サーバーが ASA の正しいポートで動作しているかどうかをチェックすることもできます。

```
# show asp table socket
Protocol          Socket           State            Local Address    Foreign Address
-----
SSL               00019b98        LISTEN          192.168.1.5:443  0.0.0.0:*
SSL               00029e18        LISTEN          192.168.2.5:443  0.0.0.0:*
TCP               00032208        LISTEN          192.168.1.5:22   0.0.0.0:*
```

確認リターンコード：9（証明書がまだ有効ではありません）

このエラーは、提供された証明書の発行日が将来の日付であるため、クライアントがそれを有効なものとして扱わないことを意味します。これは、証明書の不完全な作成が原因である可能性があります。また、自己署名証明書の場合は、証明書生成時のデバイスの時刻が間違っていたことが原因である可能性があります。

エラーには、証明書の notBefore の日付が含まれた行があります。

```
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
verify error:num=9:certificate is not yet valid
notBefore=Oct 21 19:43:15 2016 GMT
verify return:1
depth=0 CN = ASA Temporary Self Signed Certificate
notBefore=Oct 21 19:43:15 2016 GMT
```

このエラーから、証明書がいつ有効になるかを判別できます。

修復

証明書の notBefore の日付は過去の日付である必要があります。notBefore の日付をより早い日付にして証明書を再発行できます。この問題は、クライアントまたは発行デバイスのいずれかで時刻が正しく設定されていない場合にも発生する可能性があります。

確認リターンコード：10（証明書の有効期限が切れています）

このエラーは、提供された証明書の少なくとも1つの期限が切れていることを意味します。エラーには、証明書の notBefore の日付が含まれた行があります。

```
error 10 at 0 depth lookup:certificate has expired
```

この有効期限は、証明書の本文に含まれています。

修復

証明書が本当に期限切れの場合、唯一の修復方法は、別の証明書を取得することです。証明書の有効期限が将来の日付であるのに、openssl が期限切れであると主張する場合は、コンピュー

タの日付と時刻をチェックしてください。たとえば、証明書が 2020 年に期限切れになるように設定されているのに、コンピュータの日付が 2021 年になっている場合、そのコンピュータは証明書を期限切れとして扱います。

確認リターンコード：21（最初の証明書を検証できません）

このエラーは、証明書チェーンに問題があることと、デバイスによって提示された証明書を信頼できることを openssl が検証できないことを示しています。ここで、上記の例の証明書チェーンを調べて、証明書チェーンがどのように機能するのかを見てみましょう。

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2

-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TylihMjZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

-----BEGIN CERTIFICATE-----
MIID8DCCAtigAwIBAgIDAjgSMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
...lots of base64...
tzw9TylihMjZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBCwUAMEIxCzAJBgNVBAYTAlVT
...lots of base64...
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
```

証明書チェーンとは、サーバーによって提示される証明書のリストです。このリストは、サーバー自体の証明書から始まり、そのサーバーの証明書を認証局の最上位の証明書に結び付ける、段階的により上位の中間証明書が含まれます。各証明書には、その件名（「s:」で始まる行）とその発行者（「i:」で始まる行）のリストが示されています。

件名は、証明書によって識別されるエンティティです。これには、組織名が含まれており、場合によっては証明書の発行先エンティティの共通名も含まれます。

発行者は、証明書を発行したエンティティです。これには、組織フィールドも含まれており、場合によっては共通名も含まれます。

サーバーは、信頼できる認証局によって直接発行された証明書を持っている場合、証明書チェーンに他の証明書を含める必要がありません。次のような 1 つの証明書が表示されます。

```
--- Certificate chain 0 s:/C=US/ST=California/L=Anytown/O=ExampleCo/CN=*.example.com
i:/C=US/O=Trusted Authority/CN=Trusted Authority
-----BEGIN CERTIFICATE-----
MIIH0DCCBrigAwIBAgIIUOMfH+8ftN8wDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
...lots of base64...
tzw9TylihMjZcl4qihFVTgFM7rMU2VHulpJgA59gdbaO/Bf
-----END CERTIFICATE-----
```

この証明書を提供すると、`openssl` は、`*.example.com` の ExampleCo 証明書が、`openssl` の組み込み信頼ストアに存在する信頼できる認証局の証明書によって正しく署名されていることを検証します。その検証の後に、`openssl` は、デバイスに正常に接続します。

ただし、ほとんどのサーバーには、信頼できる CA によって直接署名された証明書がありません。代わりに、最初の例のように、サーバーの証明書は1つ以上の中間証明書によって署名されており、最上位の中間証明書が、信頼できる CA によって署名された証明書を持ちます。`OpenSSL` は、デフォルトでは、これらの中間 CA を信頼せず、信頼できる CA で終わる完全な証明書チェーンが提供されている場合にのみ、それらを検証できます。

中間認証局によって署名された証明書を持つサーバーが、信頼できる CA に結び付けられたすべての証明書（すべての中間証明書を含む）を提供することが非常に重要です。このチェーン全体が提供されない場合、`openssl` からの出力は次のようになります。

```
depth=0 OU = Example Unit, CN = example.com
verify error:num=20:unable to get local issuer certificate
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=27:certificate not trusted
verify return:1

depth=0 OU = Example Unit, CN = example.com
verify error:num=21:unable to verify the first certificate
verify return:1

CONNECTED(00000003)

---
Certificate chain
0 s:/OU=Example Unit/CN=example.com
i:/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
-----BEGIN CERTIFICATE-----
...lots of b64...
-----END CERTIFICATE-----
---
Server certificate
subject=/OU=Example Unit/CN=example.com
issuer=/C=US/ST=Massachusetts/L=Cambridge/O=Intermediate
Authority/OU=http://certificates.intermediateauth...N=Intermediate Certification
Authority/sn=675637734
---
No client certificate CA names sent
---
SSL handshake has read 1509 bytes and written 573 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: 24B45B2D5492A6C5D2D5AC470E42896F9D2DDDD54EF6E3363B7FDA28AB32414B
Session-ID-ctx:
Master-Key:
21BAF9D2E1525A5B935BF107DA3CAF691C1E499286CBEA987F64AE5F603AAF8E65999BD21B06B116FE9968FB7C62EF7C
```

新しい証明書が検出されました

```
Key-Arg : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1476711760
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

この出力は、サーバーが1つの証明書のみを提供しており、提供された証明書が信頼されたルート認証局ではなく中間認証局によって署名されていることを示しています。この出力には、特性検証エラーも示されています。

修復

この問題は、デバイスによって提示された証明書の設定が間違っているために発生します。この問題を修正してCDOまたはその他のプログラムがデバイスに安全に接続できるようにする唯一の方法は、正しい証明書チェーンをデバイスにロードして、接続しているクライアントに完全な証明書チェーンを提示することです。

中間CAをトラストポイントに含めるには、次のいずれか（CSRがASAで生成されたかどうかに応じて）のリンク先に記載されている手順に従ってください。

- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc13>
- <https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/200339-Configure-ASA-SSL-Digital-Certificate-I.html#anc15>

新しい証明書が検出されました

自己署名証明書を持つデバイスをアップグレードして、アップグレードプロセス後に新しい証明書が生成された場合、CDOは、[設定 (Configuration)] ステータスおよび [接続 (Connectivity)] の両方のステータスとして、「新しい証明書が検出されました (New Certificate Detected)」メッセージを生成する場合があります。このデバイスをCDOから管理する前に、この問題を手動で確認して解決する必要があります。証明書が同期されて、デバイスの状態が正常になったら、このデバイスを管理できます。



(注) 複数の管理対象デバイスを同時に **CDOに一括再接続** すると、CDOはデバイス上の新しい証明書を自動的に確認して受け入れ、それらとの再接続を続行します。

新しい証明書を解決するには、次の手順を使用します。

- ステップ1 ナビゲーションバーで、[デバイスとサービス (Devices & Services)] 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ます。
- ステップ4 フィルタを使用して、接続ステータスまたは設定ステータスが [新しい証明書が検出されました (New Certificate Detected)] であるデバイスを表示し、必要なデバイスを選択します。

- ステップ5** [アクション] ペインで、[証明書の確認 (Review Certificate)] をクリックします。CDO では、確認のために証明書をダウンロードし、新しい証明書を受け入れることができます。
- ステップ6** [デバイス同期 (Device Sync)] ウィンドウで [承認 (Accept)] をクリックするか、[デバイスへの再接続 (Reconnecting to Device)] ウィンドウで [続行] をクリックします。

CDO は、デバイスを新しい自己署名証明書と自動的に同期します。同期されたデバイスを表示するには、[デバイスとサービス] ページを手動で更新する必要がある場合があります。

オンボーディングエラーのトラブルシューティング

デバイスの導入準備エラーは、さまざまな理由で発生する可能性があります。次の操作を実行できます。

- ステップ1** [インベントリ] ページで [デバイス] 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、エラーが発生しているデバイスを選択します。場合によっては、右側にエラーの説明が表示されます。説明に記載されている必要なアクションを実行します。
- または
- ステップ3** CDO からデバイスインスタンスを削除し、デバイスの導入準備を再試行します。

[競合検出 (Conflict Detected)] ステータスの解決

CDO を使用すると、ライブデバイスごとに競合検出を有効化または無効化できます。[競合検出](#) が有効になっていて、CDO を使用せずにデバイスの設定に変更が加えられた場合、デバイスの設定ステータスには [競合検出 (Conflict Detected)] と表示されます。

[競合検出 (Conflict Detected)] ステータスを解決するには、次の手順に従います。

- ステップ1** ナビゲーションバーで、[デバイスとサービス (Devices & Services)] をクリックします。
- ステップ2** [デバイス] タブをクリックして、デバイスを見つけます。
- ステップ3** 適切なデバイスタイプのタブをクリックします。
- ステップ4** 競合を報告しているデバイスを選択し、右側の詳細ペインで [競合の確認 (Review Conflict)] をクリックします。
- ステップ5** [デバイスの同期 (Device Sync)] ページで、強調表示されている相違点を確認して、2つの設定を比較します。
- 「最後に認識されたデバイス設定 (Last Known Device Configuration)」というラベルの付いたパネルは、CDO に保存されているデバイス設定です。

- 「デバイスで検出 (Found on Device)」というラベルの付いたパネルは、ASA の実行構成に保存されている設定です。

ステップ 6 次のいずれかを選択して、競合を解決します。

- [デバイスの変更を承認 (Accept Device changes)]: 設定と、CDO に保存されている保留中の変更がデバイスの実行構成で上書きされます。

(注) CDO はコマンドライン インターフェイス以外での Cisco IOS デバイスへの変更の展開をサポートしていないため、競合を解決する際の Cisco IOS デバイスの唯一の選択肢は [レビューなしで承認 (Accept Without Review)]です。

- [デバイスの変更を拒否 (Reject Device Changes)]: デバイスに保存されている設定を CDO に保存されている設定で上書きします。

(注) 拒否または承認されたすべての設定変更は、変更ログに記録されます。

「未同期」ステータスの解決

次の手順を使用して、「未同期」の設定ステータスのデバイスを解決します。

ステップ 1 ナビゲーションバーで、[デバイスとサービス (Devices & Services)]をクリックします。

ステップ 2 [デバイス (Devices)] タブをクリックしてデバイスを見つけるか、[テンプレート (Templates)] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 適切なデバイスタイプのタブをクリックします。

ステップ 4 未同期と報告されたデバイスを選択します。

ステップ 5 右側の [未同期 (Not synced)] パネルで、次のいずれかを選択します。

- [プレビューして展開... (Preview and Deploy..)]: 設定の変更を CDO からデバイスにプッシュする場合は、今行った変更を **プレビューして展開する**か、待ってから一度に複数の変更を展開します。
- [変更の破棄 (Discard Changes)]: 設定の変更を CDO からデバイスにプッシュしたくない場合、または CDO で開始した設定の変更を「元に戻す」場合。このオプションは、CDO に保存されている設定を、デバイスに保存されている実行中の設定で上書きします。

SecureX のトラブルシューティング

SecureX と組み合わせて CDO を使用しようとする、エラーや警告が表示されたり、問題が発生したりする場合があります。SecureX UI に表示される問題については、SecureX のマニュアルを参照する必要があります。詳細については、SecureX の [Support](#) を参照してください。

CDO内の SecureX リボン機能、または SecureX リボンへのテナントアクセシビリティに関するケースを開くには、[CDO Cisco TAC](#) を参照してください。テナント ID の入力を求められる場合があります。

SecureX UI のトラブルシューティング

SecureX ダッシュボードに重複した CDO モジュールが表示される

SecureX では、単一製品の複数のモジュールを手動で設定できます。たとえば、複数の CDO テナントがある場合、テナントごとに 1 つの CDO モジュールを作成できます。重複モジュールは、同じ CDO テナントからの 2 つの異なる API トークンがあることを意味します。この冗長性により、混乱が生じ、ダッシュボードが乱雑になる可能性があります。

SecureX で CDO モジュールを手動で設定し、CDO の [一般設定 (General Settings)] ページで [SecureX に接続 (Connect SecureX)] を選択した場合、1 つのテナントが SecureX に複数のモジュールを持つ可能性があります。

回避策として、SecureX から元の CDO モジュールを削除し、複製したモジュールで CDO のパフォーマンスの監視を続けることをお勧めします。このモジュールは、より安全で、SecureX リボンと互換性のある、より堅牢な API トークンを使用して生成されます。

CDO UI のトラブルシューティング

SecureX 内の CDO モジュールに関するケースを開く場合、詳細については、SecureX の [Terms](#), [Privacy](#), [Support](#) の「サポート」セクションを参照してください。

OAuth エラー

メッセージ「ユーザーは必要なすべてのスコープまたは十分な権限を持っていないようです (The user does not seem to have all the required scopes or sufficient privilege)」が表示されて、OAuth エラーが発生する場合があります。この問題が発生した場合は、次の可能性を検討してください。

- アカウントがアクティブ化されていない可能性。<https://visibility.test.iroh.site/> を参照し、登録したメールアドレスを使用して、アカウントがアクティブ化されているか確認します。アカウントがアクティブ化されていない場合、CDO アカウントは SecureX とマージされない可能性があります。この問題を解決するには、Cisco TAC に連絡する必要があります。詳細については、[Contact Cisco TAC](#) を参照してください。

組織の間違ったログイン情報で SecureX にログインしている

[一般設定 (General Settings)] ページの [テナント設定] セクションで [SecureX に接続 (Connect SecureX)] オプションを使用して CDO イベントを SecureX に送信することを選択したが、間違ったログイン情報を使用して SecureX にログインした場合、間違ったテナントからのイベントが SecureX ダッシュボードに表示されることがあります。

回避策として、CDO の [一般設定 (General Settings)] ページで [SecureX の切断 (Disconnect SecureX)] をクリックします。SecureX 組織、つまり SecureX ダッシュボードとの情報の送受信に使用される読み取り専用 API ユーザーが終了します。

次に、[テナントをSecureXに接続 (Connect Tenant to SecureX)]を再度有効にし、SecureX へのログインを求められたら、正しい組織のログイン情報を使用する必要があります。

間違ったアカウントでリボンにログインしている

現時点では、間違ったアカウント情報でリボンにログインすると、リボンからログアウトできません。リボンのログインを手動でリセットするには、[Support Case Manager](#) でケースを開く必要があります。

SecureX リボンを起動できない

適切なスコープにアクセスできない可能性があります。この問題を解決するには、Cisco TAC に連絡する必要があります。詳細については、[Contact Cisco TAC](#) を参照してください。

SecureX リボンの動作の詳細については、[SecureX ribbon documentation](#) を参照してください。