ポスチャステート同期の設定およびトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco Identity Service Engine(ISE)3.1バージョンで導入されたポスチャステート同期(POST)の設定と使用について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ISEのポスチャフロー
- Cisco ISEでのポスチャコンポーネントの設定

任意のタイプの代わりにポスチャ設定が存在することが想定されています。

後述の概念をよく理解するために、次の項目を確認することをお勧めします。

- Cisco Identity Services Engine 管理者ガイド リリース 3.1
- 以前のISEバージョンとISE 2.2のISEポスチャフローとの比較
- ISEセッション管理とポスチャ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.1
- Cisco Secureクライアント5.0.00556

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

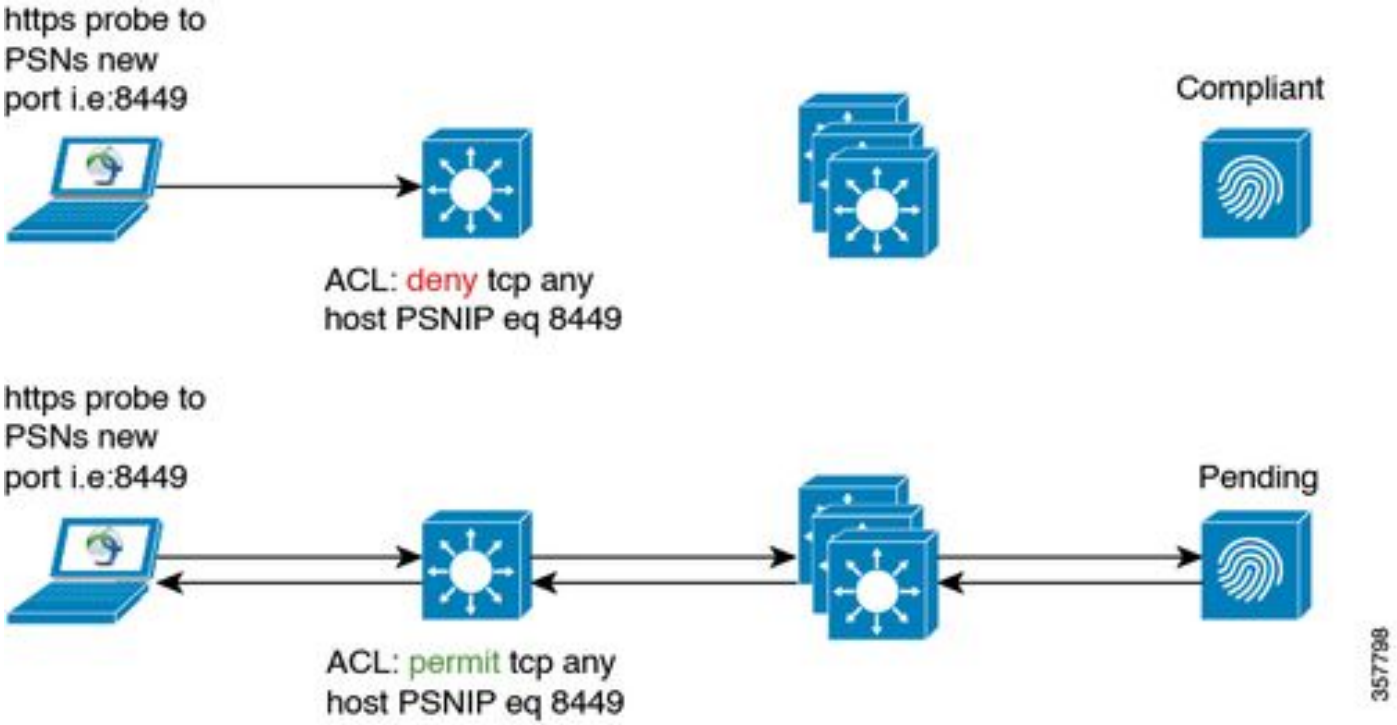
通常、ISEポスチャフローでは、ISEからクライアントでポスチャステータスを更新することはできません。Cisco Secure Client Posture Moduleは、エンドポイントのポスチャステータスを評価するために使用され、ネットワーク変更、定期的な再評価、またはその他のクライアント側トリガーまでエンドポイントのポスチャステータスを維持します。セッションの終了やその他の理由によってISEでエンドポイントのポスチャステータスが変更された場合、Secure Clientポスチャモジュールはその変更を認識しないため、エンドポイントはクライアント側トリガーのいずれかが発生するまで、制限付きネットワークアクセスでポスチャ不明の状態のままになります。

このドキュメントでは、この種の問題に対処し、ISEがエンドポイントの現在のポスチャステータスに関するセキュアクライアントポスチャモジュールへのフィードバックを提供できるようにするために開発された新機能であるポスチャステータス同期に焦点を当てています。

設定

ポスチャステータスプローブポートは、ポスチャ状態の同期が有効な場合（デフォルトではTCP 8449）に、各ISE PSNノードに導入されました。エンドポイントポスチャステータスがUnknownまたはPendingの場合は、エンドポイントから到達可能であり、エンドポイントステータスがCompliantの場合は到達不能であると想定されます。

ネットワーク図



コンフィギュレーション

ポスチャ状態同期機能の設定は、次の2つの部分で構成されます。

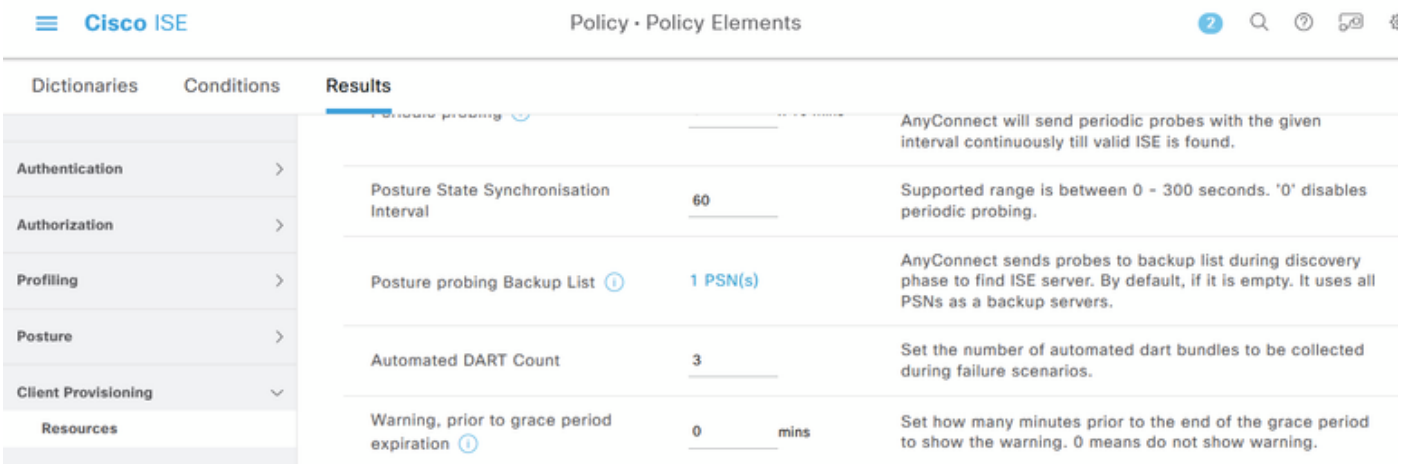
1. AnyConnectポスチャプロファイルの設定

   1.1 Cisco ISE GUIで、Policy > Policy Elements > Results > Client Provisioning > Resourcesの順に移動します。

   1.2すでに使用しているAnyConnectポスチャプロファイルを選択するか、新しいプロファイルを作成します。

   1.3 Agent Behavior領域で、Posture State Synchronization Intervalを1 ~ 300秒の範囲の任意の値に設定します。0：ポスチャ状態の同期を無効にします。

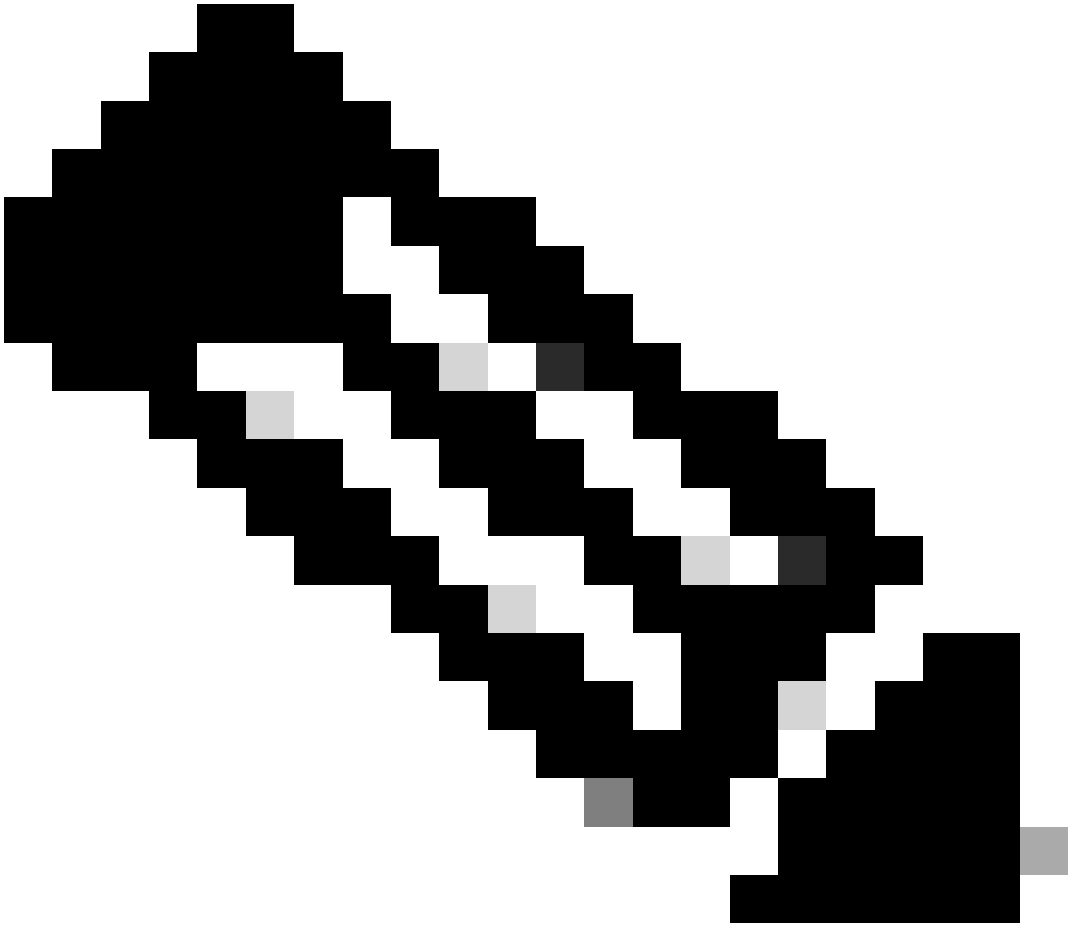
   1.4 ポスチャプロービングのバックアップリストを設定できる：セキュアクライアントはこのリストを使用して、選択したPSNのポスチャ状態をチェックします。PSNを選択しない場合、接続されたPSNと任意の2つのバックアップサーバが、ポスチャ状態の同期のバックアップとして使用されます。



2. ダウンロード可能ACL(dACL)を設定して、クライアントポスチャステータスが準拠または非準拠の場合にCisco ISEのポスチャ状態同期ポートへのアクセスをブロックする。エンドポイントステータスが既知の場合にポスチャ状態同期ポートへのアクセスを制限するには、準拠エンドポイントに使用されるACLの先頭で、各PSNのポスチャ状態同期ポートを使用して、アクセスコントロール拒否エントリを追加する必要があります。次に例を示します。

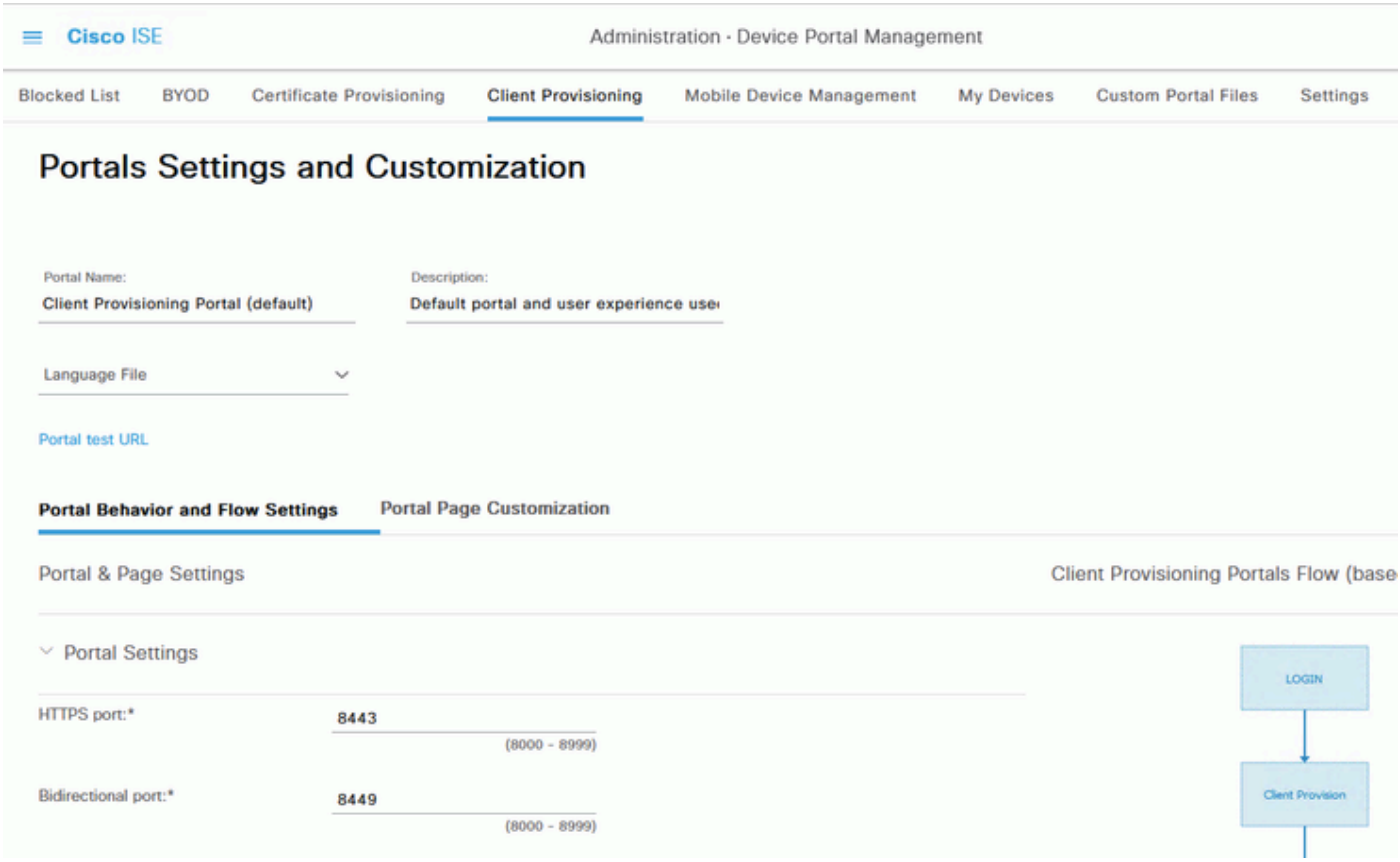
```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

permit ip any anyは必須ではなく、必要に応じて任意のルールセットで置き換えることができます。



注：dACLのdenyエントリが設定されていない場合、ポスチャ設定検出アラームがCisco ISEダッシュボードでトリガーされ、Cisco Secure Clientが再起動されるまで、エンドポイントでのポスチャ状態同期が無効になります。

ポスチャ状態同期ポート（双方向ポート）は、クライアントプロビジョニングポータルの設定ページで変更できます。Administration > Device Portal Management > Client Provisioning > Select desired portal > Portal Behavior and Flow Settingsの順に移動し、Portal Settingsを開きます。デフォルトのクライアントプロビジョニングポータルのポスチャ状態同期ポートは変更できません。



確認

DARTバンドルから

ポスチャステータスの同期は、DARTバンドルからCisco Secure Client Posture Moduleログ(AnyConnect_ISEPosture.txt)を調べることで、クライアント側から確認できます。

1. ポスチャ評価が完了し、ポスチャステータスが準拠しています。

```
2022/11/09 12:22:47 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0xC60 Fil
```

2. ポスチャステータス同期プローブが開始されます。

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

3. ポスチャ状態同期ポート(8449)でISE PSNへのHTTPS接続が開始されます。

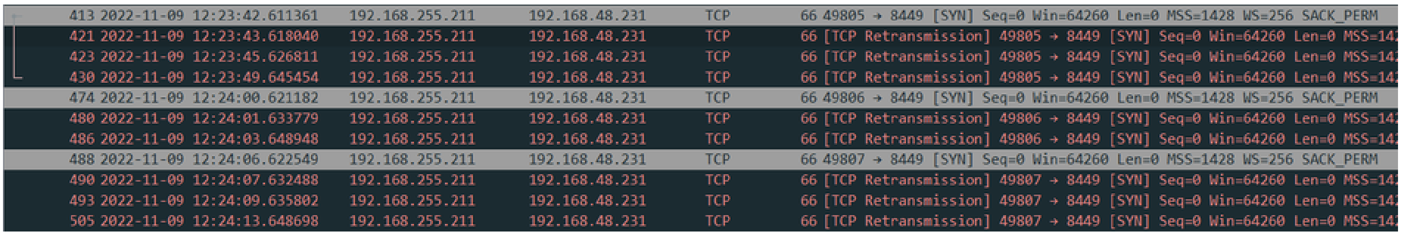
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. ポスチャステータス同期プローブのタイムアウト。

```
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_winhttp_post Thread Id: 0x296C File
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_post Thread Id: 0x296C File: hs_tra
2022/11/09 12:22:54 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

クライアントのパケットキャプチャから

クライアントで取得されたパケットキャプチャには、ISE PSNからSYN-ACK応答なしでポスチャ状態同期ポート(8449)上のISE PSNノードに向けて送信されたSYNパケットが示されます。



413	2022-11-09 12:23:42.611361	192.168.255.211	192.168.48.231	TCP	66 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
421	2022-11-09 12:23:43.618040	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
423	2022-11-09 12:23:45.626811	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
430	2022-11-09 12:23:49.645454	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
474	2022-11-09 12:24:00.621182	192.168.255.211	192.168.48.231	TCP	66 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
480	2022-11-09 12:24:01.633779	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
486	2022-11-09 12:24:03.648948	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
488	2022-11-09 12:24:06.622549	192.168.255.211	192.168.48.231	TCP	66 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
490	2022-11-09 12:24:07.632488	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
493	2022-11-09 12:24:09.635802	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
505	2022-11-09 12:24:13.648698	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14

ISE から

ポスチャ状態同期ポート(8449)での接続が失敗すると考えられるため、正しいポスチャステータス同期設定をISE側から確認できません。

ポスチャステータス変更時のポスチャの再起動

1)Cisco Secure Clientが「Compliant」状態のときに、ポスチャステータスが「Unknown」のセッション状態情報をISEから受信した。

```
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
```

2) Cisco Secure Clientがポスチャステータスの変更を確認し、ポスチャディスカバリを再起動します。

```
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
```

3)ポスチャ評価が実行されるまで、Cisco Secure Clientはポスチャステータス同期を停止します。

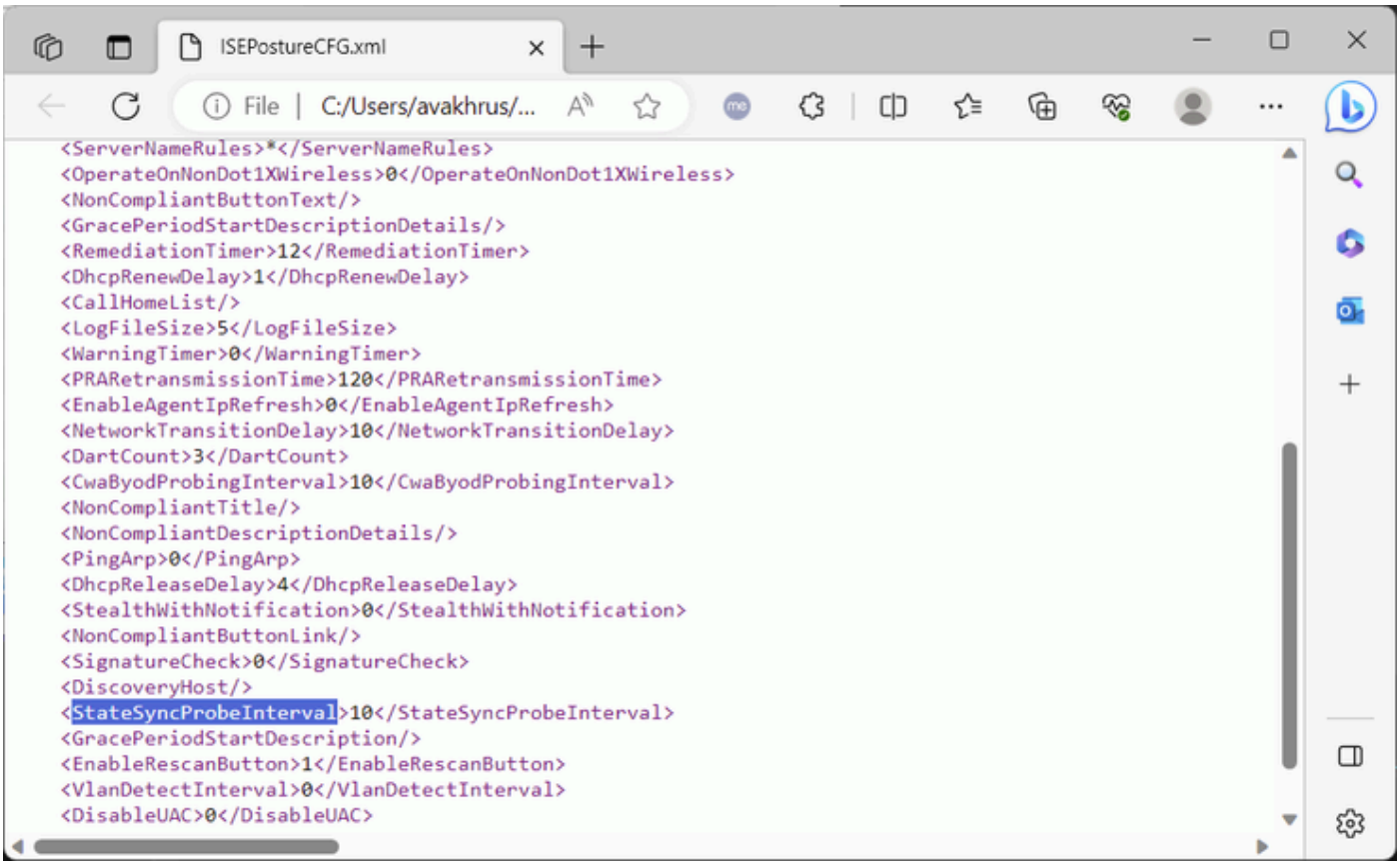
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: hs_transport_free Thread Id: 0xC60 File: hs_tran
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

トラブルシュート

ポスチャステータスの同期が開始しない

AnyConnect_ISEPosture.txtログファイルにポスチャステータス同期の開始を示す表示がなく、クライアントがポスチャ状態同期ポート(8449)でISE PSNノードとの接続を確立しない場合は、DARTバンドルからポスチャ設定ファイルISEPostureCFG.xmlを確認するか、Windows PCのクライアントマシン「%ProgramData%\Cisco\Secure Client\ISE ポスチャ\」を確認します。

ポスチャステータス同期を行うパラメータは「StateSyncProbeInterval」です。このパラメータには0より大きい値を設定することが想定されています。



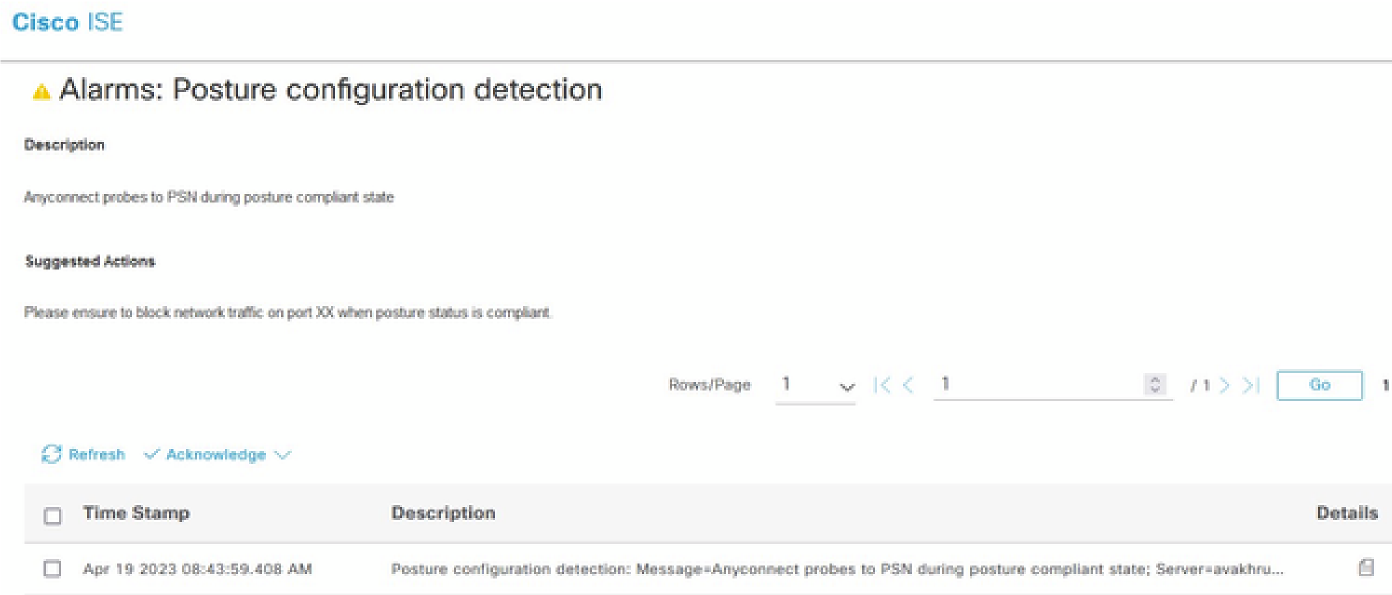
「StateSyncProbeInterval」または値「0」がない場合、ポスチャステータス同期が無効になっています。

ISEのポスチャプロファイルで「ポスチャ状態同期間隔」が設定されていても、それがクライアントのコンフィギュレーションファイルに反映されていない場合は、ポスチャプロビジョニングを調査する必要があります。

ISEダッシュボードのアラームでポスチャステータス同期が失敗する

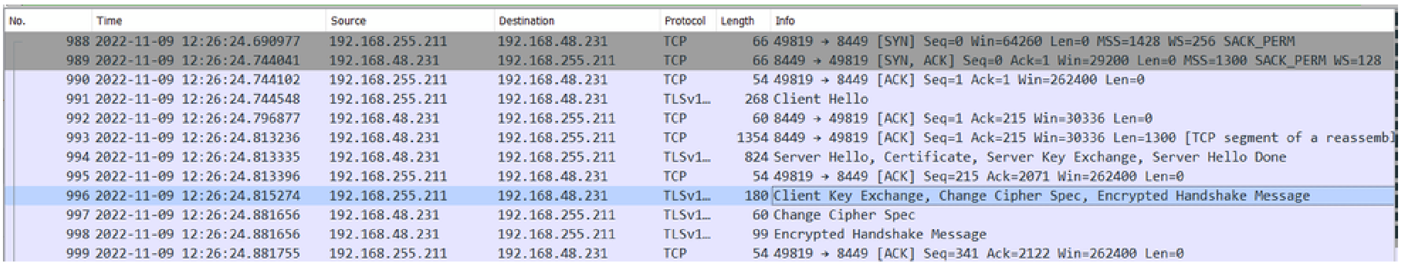
ISEのアラームでポスチャステート同期が失敗する場合、Cisco Secure Clientがポスチャ状態同期ポート(8449)でISEに到達でき、「Compliant」ステータスのセッションのステータスを要求したことを意味します。

- ISE GUIのアラーム：



- パケットキャプチャからの検証

ポスチャ状態同期ポート(8449)でTCP接続が確立されます。



No.	Time	Source	Destination	Protocol	Length	Info
988	2022-11-09 12:26:24.690977	192.168.255.211	192.168.48.231	TCP	66	49819 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
989	2022-11-09 12:26:24.744041	192.168.48.231	192.168.255.211	TCP	66	8449 → 49819 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM WS=128
990	2022-11-09 12:26:24.744102	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=1 Ack=1 Win=262400 Len=0
991	2022-11-09 12:26:24.744548	192.168.255.211	192.168.48.231	TLSv1…	268	Client Hello
992	2022-11-09 12:26:24.796877	192.168.48.231	192.168.255.211	TCP	60	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=0
993	2022-11-09 12:26:24.813236	192.168.48.231	192.168.255.211	TCP	1354	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=1300 [TCP segment of a reassembl
994	2022-11-09 12:26:24.813335	192.168.48.231	192.168.255.211	TLSv1…	824	Server Hello, Certificate, Server Key Exchange, Server Hello Done
995	2022-11-09 12:26:24.813396	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=215 Ack=2071 Win=262400 Len=0
996	2022-11-09 12:26:24.815274	192.168.255.211	192.168.48.231	TLSv1…	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
997	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	60	Change Cipher Spec
998	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	99	Encrypted Handshake Message
999	2022-11-09 12:26:24.881755	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=341 Ack=2122 Win=262400 Len=0

- Cisco Secure Clientポスチャモジュールログからの検証

DARTバンドルからAnyConnect_ISEPosture.txtを確認します。

1)ポスチャ状態同期ポート(8449)でISE PSNへのHTTPS接続が開始されます。

```
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
```

2)セッションステート情報が、ポスチャステータスが「Compliant」のISEから受信されました。

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

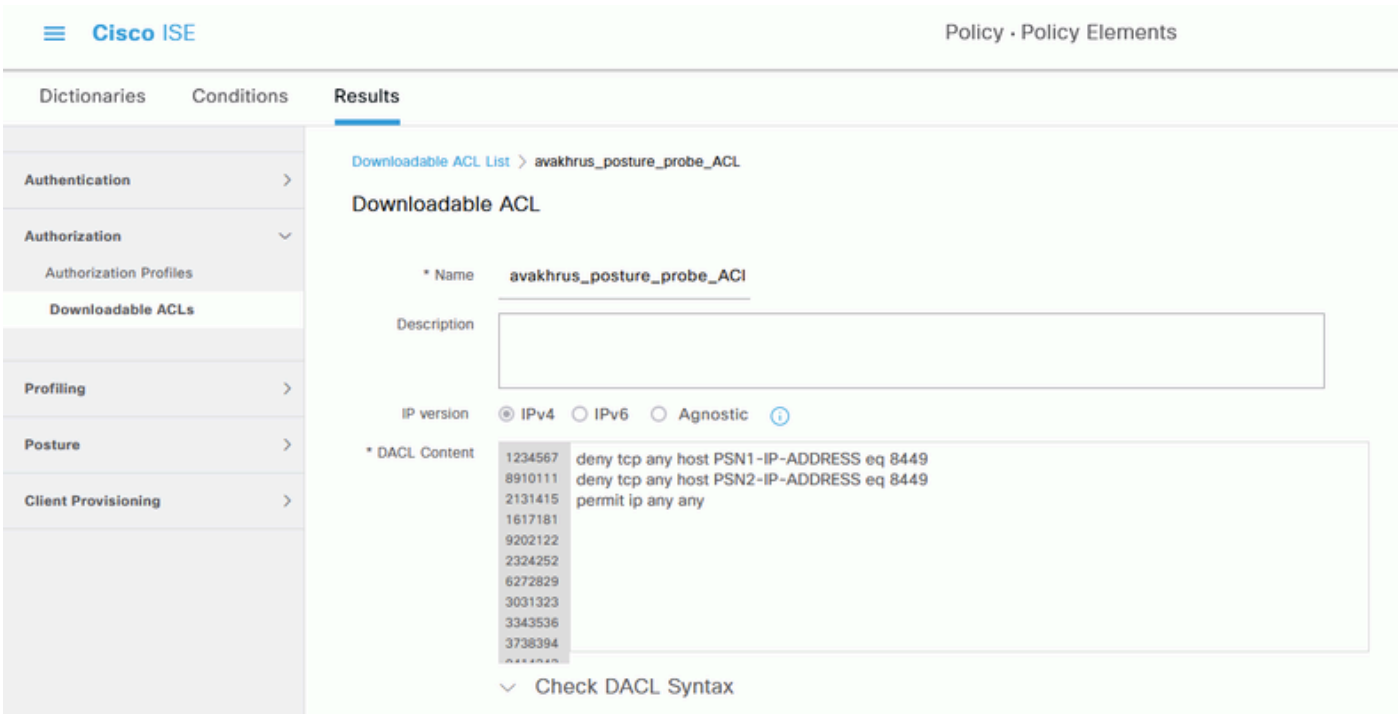
3)誤った設定が検出されたため、ポスチャ状態の同期が停止します。

```
2022/11/09 12:26:34 [Error] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x2750 File
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
```

ポスチャ評価またはネットワーク変更を再開しても、Cisco Secure Client GUIからポスチャ状態同期を再開することはできません。その代わり、ポスチャ状態の同期が再度機能するように、Cisco Secure Clientを再起動する必要があります。

ポスチャ「準拠」認可プロファイルに設定されたdACLの確認

1. ポスチャ「Compliant」認証プロファイルに対して適切なdACLが設定されていることを検証します。



2.「準拠」エンドポイントの認証の結果、詳細認証レポートdACLが正しく送信されたことを検証します。

CPMSessionID	c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0
CiscoAVPair	aaa:service=ip_admission,aaa:event=acl-download

Result

Class	CACS:c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0:ISE-PSN-FQDN/482174459/480
cisco-av-pair	ip:inacl#1=deny tcp any host PSN1-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#2=deny tcp any host PSN2-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#3=permit ip any any

3. dACLがネットワークアクセスデバイスに正しく適用されていることを確認します。

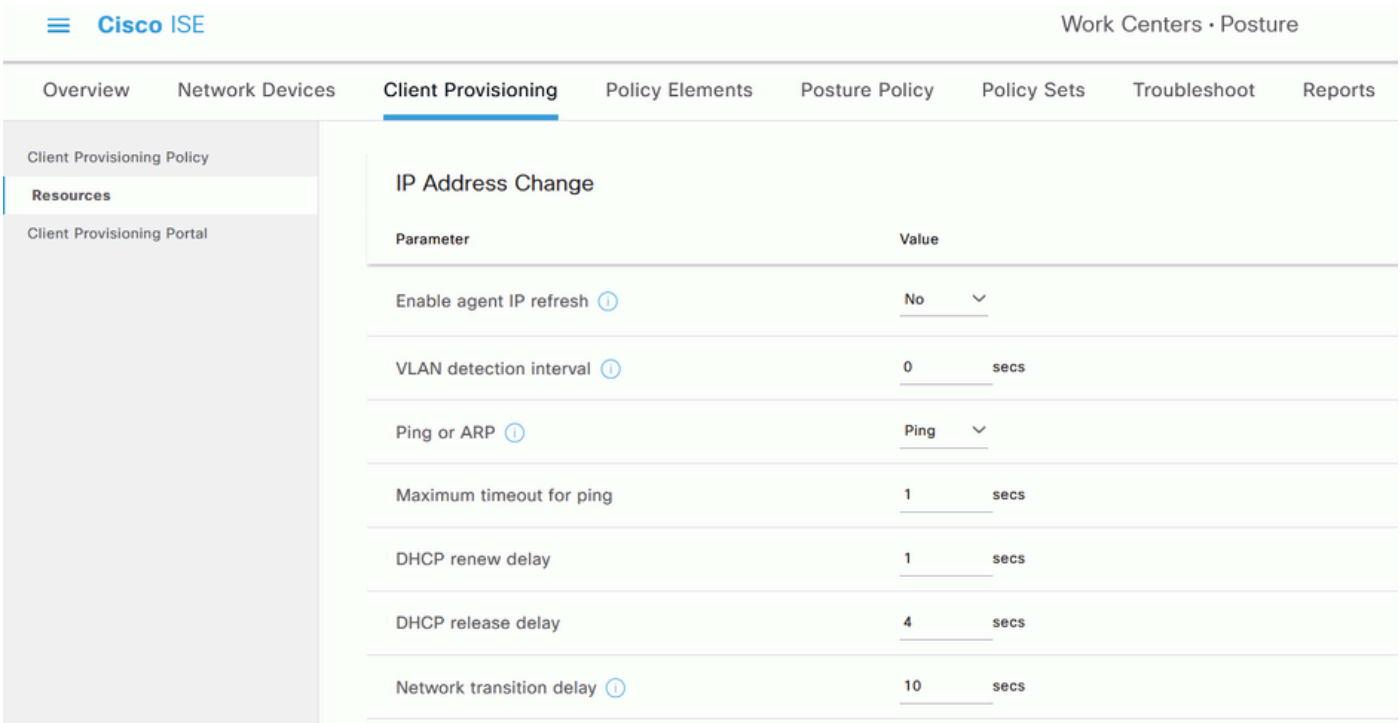
```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  172800s (local), Remaining: 92111s
       Session Uptime:  1515s
    Common Session ID:  C0A8FF0C00000012679EAF14
      Acct Session ID:  0x00000012
               Handle:  0x5D000005
       Current Policy:  POLICY_Fa0/12

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
             ACS ACL:  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac

Method status list:
       Method           State

       mab              Stopped
       dot1x            Authc Success

avakhrus_3560C#sh access-lists | s  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac
Extended IP access list xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac (per-user)
```

```
1 deny tcp any host PSN1-IP-ADDRESS eq 8449
2 deny tcp any host PSN2-IP-ADDRESS eq 8449
3 permit ip any any
```

既知の問題

ISEのアラームでポスチャ状態の同期が失敗する

適切なdACLがクライアントエンドポイントへのネットワークアクセスデバイス(NAD)に適用されている場合でも、ISEのアラームでポスチャ状態の同期が失敗する可能性があります。これは、ポスチャ状態同期プローブがdACLの適用時よりも速く実行される場合、またはポスチャ状態同期プローブがすでに進行中の場合に発生します。この問題は、Cisco Bug ID CSCwd58316 .回避策として、Anyconnectポスチャプロファイル（ISEポスチャエージェントプロファイル設定）で「ネットワーク移行遅延」を10秒に設定する必要があります。



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。