AnyConnect バージョン 4.0 および NAC ポスチャ エージェントがポップアップ表示されない（ISE トラブルシューティング ガイド）

目次

概要

Identity Services Engine（ISE）のポスチャ機能は、ネットワーク アドミッション コントロール（NAC）エージェント（Microsoft Windows、Macintosh、または Web エージェントの場合）または AnyConnect バージョン 4.0 を使用する必要があります。 AnyConnect バージョン 4.0 ISE ポスチャ モジュールは NAC エージェントと同様に機能するため、このドキュメントでは NAC エージェントと呼ばれます。 クライアントでのポスチャ障害の最も一般的な症状は、NAC エージェントがポップアップ表示されないことです。適切に動作している場合は常に NAC エージェント ウィンドウがポップアップ表示され PC が分析されます。 このドキュメントは、ポスチャの失敗、つまり NAC エージェントがポップアップ表示されない状況を引き起こす可能性のあるさまざまな原因を絞り込むのに役立ちます。 NAC エージェント ログは Cisco Technical Assistance Center（TAC）のみが解読でき、また考えられる根本原因は多数存在しています。このため、このドキュメントはすべての情報を網羅しているわけではありません。 ただし、このドキュメントは状況を明確にし、単に「ポスチャ分析が原因でエージェントがポップアップ表示されなかった」と説明するというよりも問題を正確に特定することを目的としており、最も一般的な原因を解決する上で役立ちます。

前提条件

要件

このドキュメントで説明するシナリオ、症状、および手順は、初期セットアップの完了後に問題のトラブルシューティングを行うことを前提に作成されています。 初期設定については、Cisco.com にある『Cisco ISE でのポスチャ サービスのコンフィギュレーション ガイド』を参照してください。

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くものです。

- ISE バージョン 1.2.x
- NAC Agent for ISE バージョン 4.9.x
- AnyConnect バージョン 4.0

> **注:** このドキュメントの情報は、リリース ノートで主要な動作の変更が記述されていない限り、その他の ISE リリースにも適用されます。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

トラブルシューティング方法

エージェントがポップアップ表示される仕組み

エージェントは、ISE ノードを検出するとポップアップ表示されます。 エージェントは、ネットワークへの完全なアクセス権限がなく、ポスチャをリダイレクトする状況であることを検出すると、ISE ノードを常に検索します。

Cisco.com 資料がありますエージェント ディスカバリ プロセスの詳細を説明する: 『Identity Services Engine に対するネットワーク アドミッション コントロール（NAC）エージェントの検出プロセス』です。 内容の重複を避けるため、このドキュメントでは主要点だけを説明します。

クライアントは接続時に、RADIUS 認証（MAC フィルタリングまたは 802.1x）を行います。この認証の終わりで、ISE はリダイレクション アクセス コントロール リスト（ACL）とリダイレクション URL をネットワーク デバイス（スイッチ、適応型セキュリティ アプライアンス（ASA）、またはワイヤレス コントローラ）に返します。これは、クライアント トラフィックを制限し、IP アドレスとドメイン ネーム サーバ（DNS）の解決の取得だけを許可するためのものです。 ISE ポータル自体宛てのトラフィックを除く、クライアントからの HTTP（S）トラフィックはすべて、ISE 上の一意の URL（**CPP**（Client Posture and Provisioning）で終わる URL）にリダイレクトされます。 NAC エージェントは標準 HTTP GET パケットをデフォルト ゲートウェイに送信します。 エージェントは、CPP リダイレクション以外の回答を受信しない場合、または回答をまったく受信しない場合は、エージェント自体が完全に接続しているものと見なし、ポスチャに進みません。 特定の ISE ノードの終わりで、CPP URL へのリダイレクションである HTTP 応答を受信すると、ポスチャ プロセスを続行し、その ISE ノードと通信します。 その ISE ノードからポスチャ詳細を正常に受信した場合にのみポップアップ表示され、分析が開始されます。

NAC エージェントはまた、設定されているディスカバリ ホスト IP アドレスに到達します（複数のアドレスが設定されていることを NAC エージェントは想定しません）。 セッション ID を含むリダイレクション URL を取得するために、そこでもリダイレクトされることが予期されます。

ディスカバリ IP アドレスが ISE ノードである場合、正しいセッション ID を取得するためにリダイレクトされるまで待機するので、エージェントはこれ以上処理を行いません。 したがって通常はディスカバリ ホストは不要ですが、（VPN シナリオのように）リダイレクションをトリガーするため、リダイレクト ACL の範囲内の IP アドレスとしてディスカバリ ホストが設定されていると便利です。

考えられる原因

リダイレクションが発生しなかった

これは最も一般的な原因です。 有効または無効にするため、エージェントがポップアップ表示されない PC でブラウザを開き、任意の URL を入力して、ポスチャ エージェントのダウンロード ページにリダイレクトされるかどうかを確認します。 **また、DNS の問題の発生を回避するため、ランダムな IP アドレス（http://1.2.3.4 など）を入力することもできます（IP アドレスがリダイレクトされるが、Web サイト名がリダイレクトしない場合は、DNS を調べます）。**

リダイレクトされたら、（ポスチャおよびスイス モジュールがデバッグ モードの状態で）エージェント ログと ISE サポート バンドルを収集し、Cisco TAC に連絡してください。 これは、エージェントが ISE ノードを検出したが、ポスチャ データの取得中に何らかの操作が失敗したことを示します。

リダイレクションが発生しない場合はそれが第一の原因ですが、根本原因を調べる必要があります。 最初にネットワーク アクセス デバイス（ワイヤレス LAN コントローラ（WLC）またはスイッチ）の設定を調べ、次にこのドキュメントの次の項目に進みます。

属性がネットワーク デバイスにインストールされていない

この問題は、**リダイレクションが発生しない**状況の 2 次的な原因です。 リダイレクションが発生しない場合はまず最初に、（特定クライアントでこの問題が発生した場合に）スイッチまたはワイヤレス アクセス層によってクライアントが正しいステータスになっていることを確認します。

クライアントが接続されるスイッチで奪取 される **<interface number> detail コマンド**（いくつかのプラットフォームの端に**詳細を**追加しなければならないかもしれません）の出力例はここにあります。 ステータスが「Authz success」であること、URL リダイレクト ACL が該当するリダイレクト ACL を正しく指し示していること、URL リダイレクトが、予期される ISE ノード（URL の末尾が **CPP**）を指し示していることを確認する必要があります。 ACS ACL フィールドは必須ではありません。このフィールドは、ISE で認可プロファイルにダウンロード可能なアクセス リストを設定している場合にだけ表示されます。 ただし、このフィールドを調べ、リダイレクト ACL との競合がないことを確認することが重要です（競合が疑われる場合は、ポスチャ設定に関するドキュメントを参照してください）。

```
01-SW3750-access#show access-sess gi1/0/12 det
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
```

```
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

AireOS が稼働する WLC のトラブルシューティングを行うには **show wireless client detail <MAC アドレス>** を入力してください。Cisco IOS-XE が稼働する WLC のトラブルシューティングを行うには **show wireless client mac-address <MAC アドレス> detail** を入力してください。 同様のデータが表示されます。リダイレクト URL と ACL を確認し、クライアントが「POSTURE_REQD」または同様の状態（ソフトウェアのバージョンに応じて異なる）にあるかどうかを確認してください。

属性がない場合は、（[Operations] > [Authentications]に移動して）トラブルシューティング対象クライアントの ISE で認証の詳細を開き、[Result] セクションで、リダイレクション属性が送信されていることを確認する必要があります。 それらが送信 されなかった場合、属性がこの特定のクライアントのためになぜ戻らなかったか理解するために承認ポリシーを検討する必要があります。 条件のおそらく 1 つは一致する、従ってそれらを一つずつ解決することが得策です。

、リダイレクト ACL に関して、ことを割り当て文の Cisco IOS ® リダイレクト（そう ISE および DNS IP アドレスは否定される必要があります）間、Deny ステートメント（そう ISE および DNS のために許可されます）の WLC リダイレクトの AireOS 覚えています。

属性が存在するがネットワーク デバイスがリダイレクトしない

この状況の主な原因は設定の問題にあります。 Cisco.com にある設定ガイドと設定例を参照して、ネットワーク デバイスの設定を確認してください。 該当する場合は通常、ネットワーク デバイスのすべてのポートまたはアクセス ポイント（AP）にわたって問題が発生しています。 該当しない場合は、この問題は一部のスイッチポートまたは一部の AP でのみ発生する可能性があります。 この場合は、問題が発生しているポートまたは AP の設定と、ポスチャが適切に機能しているポートまたは AP を比較してください。

FlexConnect AP では問題が起こりやすくなっています。これは、FlexConnect AP ごとに固有の設定を行えるため、一部の AP でのみ ACL または VLAN を誤って設定することがよくあるためです。

もう 1 つの一般的な問題として、クライアント VLAN に SVI がないことがあります。 これはスイッチだけに該当するため、詳しくは『Catalyst 3750 シリーズ スイッチでの ISE トラフィック リダイレクション』で説明しています。 属性の点からはすべてが適切であるように見える可能性があります。

Downloadable Access-list（DACL）によるブロック

リダイレクト属性と同時に、DACL をスイッチに戻すと（ワイヤレス コントローラの場合は

Airespace-ACL ）、リダイレクトがブロックされることがあります。 DACL が最初に適用され、完全にドロップされるトラフィックと、処理に進むトラフィックが判別されます。 次にリダイレクト ACL が適用され、リダイレクト対象が決定します。

つまり、ほとんどの場合 DACL ではすべての HTTP トラフィックと HTTPS トラフィックを許可する必要があります。 これをブロックすると、トラフィックはリダイレクト前にドロップされ、リダイレクトされません。 ほとんどの場合、このトラフィックは後でリダイレクト ACL でリダイレクトされるため、これはセキュリティ上の問題ではありません。したがって、実際にはネットワーク上では許可されません。 ただし、この 2 種類のトラフィックが直後にリダイレクト ACL に到達できるようにするため、DACL でこれらのトラフィックを許可する必要があります。

正しくない NAC エージェント バージョン

特定の NAC エージェント バージョンが特定の ISE バージョンと突き合わせて検証されることは、容易に見過ごされることがあります。 多くの管理者は、ISE クラスタをアップグレードした場合に、関連する NAC エージェント バージョンをクライアント プロビジョニング結果データベースにアップロードし忘れます。

使用している NAC エージェント バージョンが ISE コードに対して古い場合、動作するかどうかが不確かであることに留意してください。 したがって、動作するクライアントと動作しないクライアントが存在することは特に驚くべきことではありません。 確認する方法として、Cisco.com でご使用の ISE バージョンに対応したダウンロード セクションに移動し、そのセクションにある NAC エージェント バージョンを調べる方法があります。 通常、ISE バージョンごとにいくつかのバージョンがサポートされています。 次の Web ページにはすべてのマトリックスがあります。 Cisco ISE 互換性情報

クライアントによって HTTP Web プロキシが使用される

HTTP Web プロキシの概念は、クライアント自体が Web サイトの DNS IP アドレスを解決することや、Web サイトに直接アクセスすることがないというものです。 代わりに、クライアントは要求を処理するプロキシ サーバに要求を送信するだけです。 通常の設定で発生する典型的な問題として、クライアントが Web サイト（例：www.cisco.com ）を解決するため、プロキシに対して Web サイトの HTTP GET を直接送信するが、これが代行受信され、正当に ISE ポータルへリダイレクトされることがあります。 ただし、クライアントは次の HTTP GET を ISE ポータルの IP アドレスに送信する代わりに、引き続きその要求をプロキシに送信します。

プロキシ宛ての HTTP トラフィックをリダイレクトしない場合は、（すべてのトラフィックはプロキシ経由で移動するため）ユーザが認証やポスチャリングなしで、インターネット全体に直接アクセスできます。 これに対する解決策は、クライアントのブラウザ設定を実際に変更し、プロキシ設定で ISE IP アドレスの例外を追加する方法です。 これにより、クライアントは ISE に到達する必要がある場合に、要求をプロキシではなく ISE に直接送信します。 この結果、クライアントが継続的にリダイレクトされ、ログイン ページが表示されないという無限ループを防止できます。

NAC エージェントは、システムに入力されているプロキシ設定の影響を受けず、引き続き通常どおりに動作します。 つまり Web プロキシを使用する場合、ユーザがブラウズするときにポスチャ ページへリダイレクトされた後で、NAC エージェントのディスカバリとユーザによるエージェントのセルフインストールを同時に実行することはできません。これは、NAC エージェントのディスカバリではポート 80 が使用されますが、ユーザのリダイレクトではプロキシ ポートが使用され、通常スイッチは複数ポートでリダイレクトできないためです。

ディスカバリ ホストが NAC エージェントで設定されていない

特に ISE バージョン 1.2 より後では、ディスカバリ ホストの動作に関する専門知識がない限り、NAC エージェントでディスカバリ ホストを設定しないでおくことが推奨されます。 NAC エージェントは、HTTP ディスカバリによって、クライアント デバイスを認証した ISE ノードを検出すると想定されています。 ディスカバリ ホストを使用する場合、NAC エージェントが、デバイスを認証したノードではない別の ISE ノードと通信しようとしますが、これが機能しません。 ISE バージョン 1.2 は NAC エージェントにリダイレクト URL からセッションID を得てほしい従ってこの方式は落胆しますのでディスカバリ ホスト プロセスによってノードを検出するエージェントを拒否します。

場合によっては、ディスカバリ ホストを設定できます。 その場合は、リダイレクト ACL によってリダイレクトされる IP アドレスを使用してホストを設定してください（IP アドレスが存在しない場合も含む）。また理想としては、ホストはクライアントと同じサブネットに含まれていないようにしてください。同じサブネットに含まれている場合、クライアントはホストに対して永久に ARP を実行し、HTTP ディスカバリ パケットを送信することがありません。

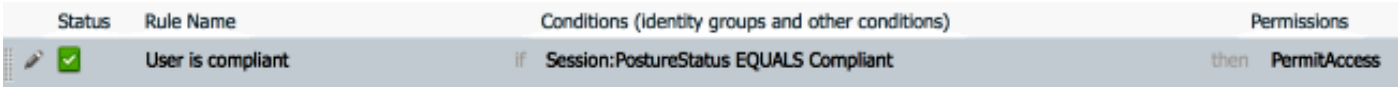
NAC エージェントがポップアップ表示されないことがある

この問題が断続的に発生し、ケーブル接続または WiFi 接続の切断と再接続などのアクションでポップアップが表示されるようになる場合は、問題の原因の特定は困難です。 これは、ISE で RADIUS アカウンティングによってセッション ID が削除されるという RADIUS セッション ID の問題の可能性があります（アカウントを無効にして、何らかの変更が発生するかどうかを確認します）。

ISE バージョン 1.2 を使用する場合は、クライアントから多数の HTTP パケットが送信され、ブラウザや NAC エージェントからの HTTP パケットが届かない可能性があります。 ISE バージョン 1.2 は、HTTP パケットの user-agent フィールドをスキャンし、パケットの送信元が NAC エージェントまたはブラウザであるかどうかを確認します。ただし、その他の多くのアプリケーションは、user-agent フィールドを含む HTTP トラフィックを送信しますが、オペレーティング システムやその他の有用な情報を指定しません。 次に、クライアントとの接続を切断するため、ISE バージョン 1.2 は認可変更を送信します。 ISE バージョン 1.3 はこれとは異なる方法で動作するため、この問題の影響を受けません。 解決策として、バージョン 1.3 にアップグレードする方法と、検出されたアプリケーションが ISE にリダイレクトされないように、リダイレクト ACL でこれらのアプリケーションをすべて許可する方法があります。

逆の問題： エージェントが繰り返しポップアップ表示される

エージェントがポップアップ表示され、ポスチャ分析を行い、クライアントを検証し、しばらくしてネットワーク接続が許可されてサイレントになる代わりに、エージェントが再びポップアップ表示されるという逆の問題が発生する場合があります。 これは、ポスチャが正常に完了した後でも、ISE の CPP ポータルに HTTP トラフィックが引き続きリダイレクトされるために発生します。 ISE 認可ポリシーを調べ、準拠クライアントを検出した時点で CPP リダイレクションを再び送信するのではなく、許可アクセスを送信するルール（または ACL と VLAN に関する類似のルール）を設定していることを確認することが推奨されます。



関連情報

- Cisco ISE コンフィギュレーション ガイドのポスチャ サービス
- ISE の NAC エージェント ディスカバリ プロセス

- Catalyst 3750 シリーズ スイッチでの ISE トラフィック リダイレクション
- テクニカル サポートとドキュメント – Cisco Systems