適応型ネットワーク制御のセットアップ

Cisco ISE での適応型ネットワーク制御の有効化

ANC は、デフォルトで無効になっています。pxGrid が有効にされた場合にのみ有効になり、管理者ポータルでサービスを手動で無効にするまで有効のままになります。

関連トピック

ネットワーク アクセスの設定 （1 ページ）

ネットワーク アクセスの設定

ANC によって、ネットワーク アクセス ステータスをリセットして、ポートを隔離、隔離解除、またはシャットダウンすることができます。これにより、ネットワーク アクセス ステータスに応じたネットワークへの許可が定義されます。

エンドポイントの隔離や隔離解除、またはエンドポイントが接続されているネットワーク アクセス サーバ（NAS）ポートのシャットダウンを行うには、エンドポイントの IP アドレスまたは MAC アドレスを使用します。同時に実行しない限り、同じエンドポイントに複数回、隔離操作および隔離解除操作を実行できます。ネットワーク上に悪意のあるエンドポイントを見つけた場合は、ANC を使用してそのエンドポイントのアクセスをシャットダウンし、NAS ポートを閉じることができます。

ANC ポリシーをエンドポイントに割り当てるには、次の手順を実行します。

始める前に

- ANC を有効にする必要があります。
- ANC の許可プロファイルおよび例外タイプの許可ポリシーを作成する必要があります。

ステップ 1 **[操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [ポリシーリスト（Policy List）]** の順に選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 ANC ポリシーの名前を入力し、ANC アクションを指定します。次のオプションを使用できます。

- 検疫（Quarantine）
- シャットダウン（Shut_Down）
- ポートバウンス（Port_Bounce）

1 つまたは複数のアクションを選択できますが、[シャットダウン（Shut_Down）] および [ポート バウンス（Port_Bounce）] を他の ANC アクションと組み合わせることはできません。

ステップ 4 [ポリシー（Policy）] > [ポリシー セット（Policy Sets）] を選択して、ポリシー セットを展開します。

ステップ 5 ANCPolicy 属性を使用して ANC ポリシーを対応する許可ポリシーに関連付けます。

ステップ 6 [操作（Operations）] > [適応型ネットワーク制御（Adaptive Network Control）] > [エンドポイント割り当て（Endpoint Assignment）] の順に選択します。

ステップ 7 [追加（Add）] をクリックします。

ステップ 8 エンドポイントの IP アドレスまたは MAC アドレスを入力し、[ポリシー割り当て（Policy Assignment）] ドロップダウン リストからポリシーを選択します。

ステップ 9 **[送信（Submit）]** をクリックします。

関連トピック

隔離済みエンドポイントがポリシー変更の後に認証を更新しない （2 ページ）

隔離済みエンドポイントがポリシー変更の後に認証を更新しない

問題

ポリシー変更または ID の追加後に認証が失敗し、再認証が行われません。認証が失敗するか、問題のエンドポイントがネットワークに接続できなくなります。この問題は、ユーザ ロールに割り当てられるポスチャ ポリシーごとのポスチャ評価に失敗するクライアント マシンで頻繁に発生します。

考えられる原因

クライアント マシンで認証タイマーが正しく設定されていないか、またはスイッチ上で認証間隔が正しく設定されていません。

ソリューション

この問題には、解決策がいくつか考えられます。

1. Cisco ISE で、指定された NAD またはスイッチの Session Status Summary レポートを検査し、インターフェイスに適切な認証間隔が設定されていることを確認します。
2. NAD/スイッチ上で "show running configuration" と入力し、適切な「authentication timer restart」設定でインターフェイスが設定されていることを確認します（たとえば、「authentication timer restart 15」および「authentication timer reauthenticate 15」）。
3. NAD/スイッチ上で "interface shutdown" および "no shutdown" と入力してポートをバウンスし、Cisco ISE で変更があったと考えられる場合には再認証を適用します。

（注） CoA は MAC アドレスまたはセッション ID を必要とするので、Network Device SNMP レポートに表示されるポートをバウンスしないように推奨しています。

適応型ネットワーク制御

適応型ネットワーク制御（ANC）は、管理ノードで実行されるサービスで、エンドポイントのネットワーク アクセスのモニタリングと制御に使用できます。 ANCは、ISE管理者が管理GUIで呼び出すことも、サードパーティ システムから pxGrid を介して呼び出すこともできます。ANC は有線展開とワイヤレス展開をサポートし、Plus ライセンスが必要です。

ANC を使用すると、システムの許可ポリシー全体を変更することなく許可状態を変更できます。 ANC を使用すると、 ANCPolicy を確認してネットワーク アクセスを制限または拒否するように許可ポリシーが定義されている場合、確立された許可ポリシーの結果としてエンドポイントを隔離するときの許可状態を設定することができます。エンドポイントを隔離解除して、フル ネットワーク アクセスを可能にできます。ネットワークからエンドポイントを接続解除する Network Attached System（NAS）上のポートをシャットダウンすることもできます。

一度に隔離できるユーザの数に制限はなく、また隔離期間の長さにも制限はありません。

ANCによってネットワーク アクセスをモニタおよび制御するには、次の操作を実行できます。

- 隔離：例外ポリシー（許可ポリシー）を使用して、ネットワークへのエンドポイントアクセスを制限または拒否することができます。 ANCPolicyに応じて異なる許可プロファイル（権限）を割り当てるために、例外ポリシーを作成する必要があります。隔離状態に設定すると、基本的に、デフォルトの VLAN から指定した隔離 VLAN にエンドポイントが移動します。エンドポイントと同じ NAS でサポートされる隔離 VLAN を事前に定義する必要があります。
- 隔離解除：エンドポイントのネットワークへのフルアクセスを許可し、エンドポイントを元の VLAN に戻す隔離ステータスを反転することができます。
- シャットダウン：NAS上のポートを非アクティブ化し、ネットワークからエンドポイントを接続解除することができます。エンドポイントが接続されている NAS 上のポートが

シャットダウンされた後、エンドポイントがネットワークに接続できるようにするには、NAS 上のポートを手動で再度リセットする必要があります。このことは無線展開では実行できません。

アクティブ エンドポイントに対する隔離および隔離解除操作は、セッション ディレクトリ レポートからトリガーできます。

（注） 隔離されていたセッションが隔離解除された場合、新たに隔離解除されたセッションの開始方法は、スイッチ設定で指定されている認証方法によって決まります。

MAC および NAD IP で識別されるエンドポイント

Cisco ISE 2.6 パッチ 7 以降、Adaptive Network Control はエンドポイントをより適切に識別できます。

MAC アドレスは、エンドポイントの一意の識別子とは限りません。USB NIC ドングルは、複数のユーザが同じ MAC アドレスを持てることを意味します。さらに、一部のエンドポイントは同じ MAC アドレスを持ちます。MAC スプーフィングには、重複する MAC アドレスも表示されます。

ANC サービスのエンドポイントをより適切に識別するために、Cisco ISE は、エンドポイントが接続されているスイッチの IP アドレスを使用します。スイッチの IP アドレスは NAS-IPAddress 属性です。

エンドポイントセッションは、ANC ポリシーで MAC アドレスと NAS-IPAddress を使用できます。

MDM ベンダーは、pxGrid v2 API で NAS-IPAddress を使用できます。

新しい API で NAS-IPAddress を使用するには、PxGrid v2 が必要です。既存の API は引き続き動作します。ただし、新旧両方の API を一緒に使用できません。

関連トピック

ANC によるネットワーク アクセスの許可プロファイルの作成 （4 ページ）
ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する （5 ページ）
外部認証された管理者が ANC 操作を実行できない （5 ページ）

ANC によるネットワーク アクセスの許可プロファイルの作成

ANC に使用する許可プロファイルを作成する必要があります。許可プロファイルは、標準許可プロファイルのリストに表示されます。エンドポイントはネットワークで認証および許可されますが、ネットワークへのアクセスが制限されています。

ステップ 1 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [許可プロファイル（Authorization Profiles）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 許可プロファイルの一意の名前と説明を入力し、[アクセス タイプ（Access Type）] は [ACCESS_ACCEPT] のままにします。

ステップ 4 [DACL 名（DACL Name）] チェックボックスをオンにし、ドロップダウン リストから [DENY_ALL_TRAFFIC] を選択します。

ステップ 5 [送信（Submit）] をクリックします。

例外許可ポリシーは、特別な条件や権限、または緊急の要件を満たすために制限付きアクセスを許可することを目的としています。ANC 許可用に、すべての標準許可ポリシーの前に処理される隔離例外ポリシーを作成する必要があります。次の条件で例外ルールを作成する必要があります：Session:ANCPolicy EQUALS Quarantine

ANC 操作は IP アドレスまたは MAC アドレスが見つからない場合に失敗する

エンドポイントで実行する ANC 操作は、そのエンドポイントのアクティブなセッションに IP アドレスに関する情報が含まれていない場合に失敗します。このことは、そのエンドポイントの MAC アドレスおよびセッション ID にも適用されます。

（注） ANC を介してエンドポイントの許可状態を変更する場合は、エンドポイントの IP アドレスまたは MAC アドレスを指定する必要があります。IP アドレスまたは MAC アドレスがエンドポイントのアクティブなセッションで見つからない場合、「この MAC アドレス、IP アドレスまたはセッション ID のアクティブなセッションが見つかりません。（No active session found for this MAC address, IP Address or Session ID.）」というエラー メッセージが表示されます。

外部認証された管理者が ANC 操作を実行できない

外部認証された管理者がライブ セッションから CoA 隔離を発行しようとすると、Cisco ISE は次のエラー メッセージを返します。

「xx: xx: xx: xx: xx: xx に対する隔離の CoA アクションを開始できません。（CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated.）原因：内部でユーザが見つかりません。（Cause:User not found internally.）サポートされていない外部認証されたユーザを使用している可能性があります（Possible use of unsupported externally authenticated user）」

外部認証された管理者が、エンドポイントの IP アドレスまたは MAC アドレスを使用して、Cisco ISE 管理者ポータル内の [操作（Operations）]>[適応型ネットワーク制御（Adaptive Network Control）] から ANC 操作を実行すると、Cisco ISE は次のエラー メッセージを返します。

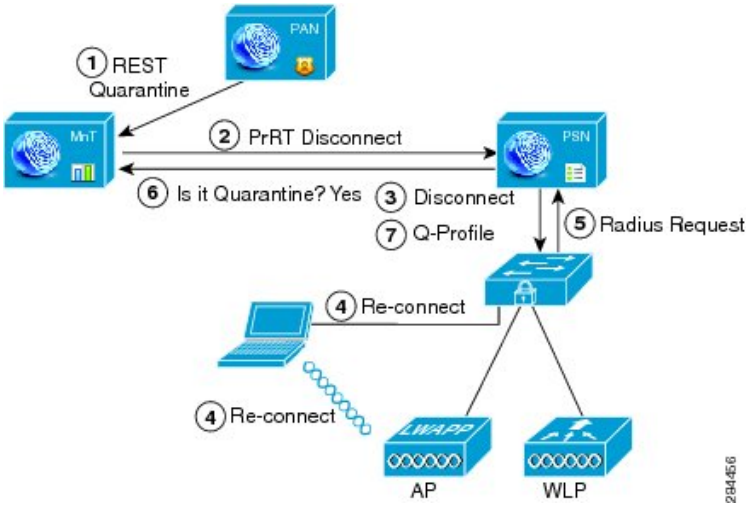
「サーバ障害：内部でユーザが見つかりません。（Server failure: User not found internally.）サポートされていない外部認証されたユーザを使用している可能性があります（Possible use of unsupported externally authenticated user）」

ANC 隔離と隔離解除フロー

選択したエンドポイントのネットワークへのアクセスを制限するために、 ANC を使用してこれらを隔離できます。エンドポイントを隔離し、ステータスに応じて異なる許可プロファイルを割り当てる例外許可ポリシーを確立できます。許可プロファイルは許可ポリシーで定義される権限のコンテナとして機能し、許可ポリシーによって特定のネットワーク サービスへのアクセスが許可されます。許可が完了すると、ネットワーク アクセス要求に権限が付与されます。エンドポイントの妥当性が認められた場合には、エンドポイントの隔離を解除してネットワークへのフル アクセスを許可できます。

この図は、隔離フローを示しています。許可ルールが設定され、 ANC セッションが確立されていることを前提としています。

図 *1 : ANC* 隔離フロー



1. クライアント デバイスがワイヤレス デバイス（WLC）を通じてネットワークにログインし、隔離の REST API コールが管理ノード（PAP）からモニタリング ノード（MnT）に発行されます。
2. 続いて、モニタリング ノードは、ポリシー サービス ISE ノード（PDP）を通じて PrRT をコールし、CoA を呼び出します。
3. クライアント デバイスが切断されます。
4. 続いて、クライアント デバイスが再認証および再接続されます。
5. クライアント デバイスに対する RADIUS 要求が、モニタリング ノードに返送されます。
6. チェックが行われている間、クライアント デバイスは隔離されます。
7. Q プロファイル許可ポリシーが適用され、クライアント デバイスの妥当性が確認されます。

8. クライアント デバイスの隔離が解除され、ネットワークにフル アクセスできるようになります。

ANC NAS ポートのシャットダウン フロー

エンドポイントのIPアドレスまたはMACアドレスを使用して、エンドポイントの接続先NASポートをシャット ダウンできます。

シャットダウンでは、MAC アドレスに対して指定された IP アドレスに基づいて NAS ポートを閉じることが可能です。また、手動でポートを復元して、エンドポイントをネットワークに戻す必要があります。これは、有線メディアで接続されたエンドポイントのみに有効です。

シャットダウンはすべてのデバイスでサポートされているわけではありません。ただし、大部分のスイッチでシャットダウン コマンドがサポートされています。getResult() コマンドを使用すると、シャットダウンが正常に実行されたかどうかを確認できます。

この図は、 ANC のシャットダウンのフローを示しています。図のクライアント デバイスでは、このクライアント デバイスがネットワークにアクセスするために使用する NAS でシャットダウン操作が実行されます。

図 *2 : ANC* のシャットダウン フロー

エンドポイントの消去の設定

[管理（Administration）] > [ID の管理（Identity Management）] > [設定（Settings）] > [エンドポイント消去（Endpoint Purge）] を使用して、ID グループおよび他の条件に基づいて、設定ルールによってエンドポイント パージ ポリシーを定義できます。指定したエンドポイントを消去しないことや、選択したプロファイリング条件に基づいてエンドポイントを消去することを選択できます。

エンドポイント消去ジョブをスケジュールできます。このエンドポイント消去スケジュールはデフォルトで有効です。Cisco ISE はデフォルトで、30 日よりも古い登録デバイスとエンドポイントを削除します。消去ジョブは、プライマリ PAN で設定された時間帯に基づいて毎日午前 1 時に実行されます。

エンドポイントの消去では、3 分ごとに 5000 エンドポイントが削除されます。

次に、エンドポイントの消去に使用できる条件と例の一部を示します。

- InactivityDays：エンドポイントでの最後のプロファイリング アクティビティまたは更新からの日数。
  - この条件によって、時間の経過に伴って蓄積した古いデバイス（一般的には一時的なゲストやパーソナルデバイス）、または廃止されたデバイスが消去されます。これらのエンドポイントは、ネットワーク上でアクティブでないか、近い将来に使用される可能性が低いため、ほとんどの展開でノイズを表す傾向があります。それらが再度接続した場合は、必要に応じて再検出、プロファイリング、登録などが行われます。
  - エンドポイントから更新が発生すると、InactivityDaysはプロファイリングが有効である場合にのみ 0 にリセットされます。
- ElapsedDays：オブジェクトが作成されてからの日数。
  - この条件は、ゲストまたは請負業者のエンドポイント、ネットワーク アクセスにWebAuthを利用する従業員などの、未認証アクセスまたは条件付きアクセスが一定期間認められたエンドポイントに使用できます。許可された接続猶予期間が経過した後、それらは完全に再認証および登録される必要があります。
- PurgeDate：エンドポイントを消去する日付。
  - このオプションは、作成または開始時間に関係なく一定期間のアクセスを許可する、特別なイベントやグループに使用できます。このオプションでは、すべてのエンドポイントを同時に消去できます。たとえば、展示会、会議、または毎週メンバーが入れ替わる週ごとのトレーニング クラスでは、絶対的な日/週/月ではなく、特定の週や月にアクセスを許可する場合に使用します。