NAC の設定

この章では、Cisco NX-OS デバイス上で Network Admission Control（NAC）を設定する手順を説明します。

この章は、次の項で構成されています。

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

NAC の概要

NACを使用すると、エンドポイント装置のネットワーク アクセスを許可する前に、エンドポイント装置のセキュリティ適合性と脆弱性をチェックできます。このセキュリティ適合性のチェックのことを、ポスチャ検証といいます。ポスチャ検証により、ワーム、ウイルス、およびその他の不正アプリケーションがネットワーク全体に拡散することを防止できます。

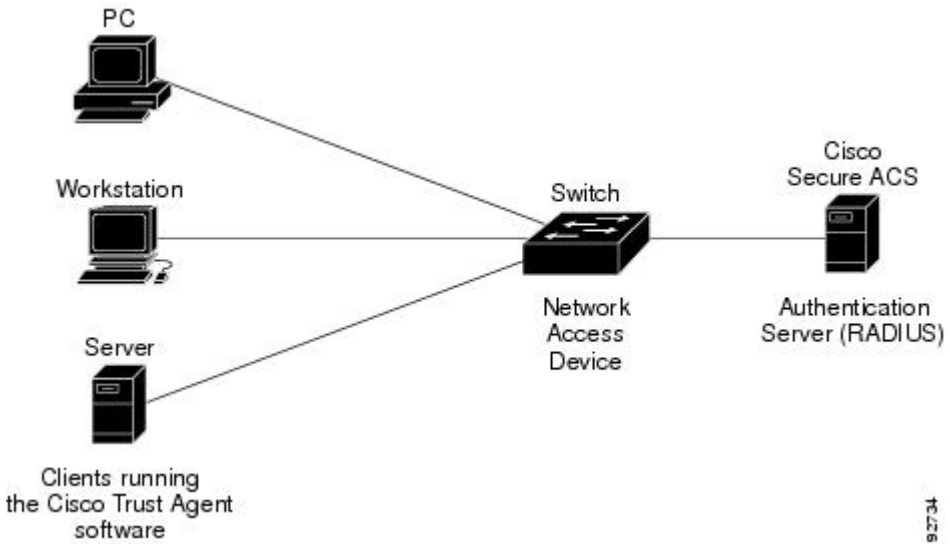
NACは、エンドポイント装置がネットワークの保護された領域にアクセス可能になる前に、エンドポイント装置のポスチャ（状態）がセキュリティ ポリシーに適合しているかどうかを検証します。セキュリティ ポリシーに適合する場合は、ネットワークの保護されたサービスにアクセスすることが許可されます。デバイスがセキュリティ ポリシーに適合しない場合は、修復専用のネットワークにアクセスが許可されます。修復ネットワークではデバイスのポスチャが再度チェックされます。

NAC デバイスのロール

NAC は、ネットワーク上の各デバイスにロールを割り当てます。

次の図に、NAC デバイスのロールを設定したネットワークの例を示します。

図 *1*：ポスチャ検証デバイス



NAC は、次のネットワーク デバイスのロールをサポートしています。

エンドポイント装置

Cisco NX-OS デバイスのアクセス ポートに直接接続される PC、ワークステーション、またはサーバなどのネットワークのシステムまたはクライアントです。エンドポイント装置では Cisco Trust Agent（CTA）ソフトウェアが稼働し、LAN およびスイッチのサービスへのアクセスを要求し、スイッチからの要求に応答します。エンドポイント装置はウイルスの感染源である可能性があり、NAC はエンドポイント装置にネットワーク アクセスを許可する前に、アンチウイルス ステータスを検証する必要があります。

（注） Cisco Trust Agent ソフトウェアは、ポスチャ エージェントまたはアンチウイルス クライアントとも呼ばれます。Cisco Trust Agent ソフトウェアの詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

ネットワーク アクセス デバイス（NAD）

ネットワーク エッジで検証サービスの提供およびとポリシーの適用、クライアントのアクセス ポリシーに基づいてネットワークへの物理アクセスを制御する Cisco NX-OS デバイスです。NAD は、エンドポイントと認証サーバの間で拡張認証プロトコル（EAP）メッセージをリレーします。
NAD は、ネットワークに対する新しい接続を検出すると、ポスチャ クレデンシャルを照会します。エンドポイント装置にポスチャ エージェント（PA）がインストールされている場合は、インバンド ポスチャ検証を実行します。NAD は、エンドポイント装置と AAA サーバとの間で、ポスチャ検証情報の交換に関するすべてのメッセージのリレー エージェントとして動作します。PA が見つからない場合は、監査サーバを介してアウトオブバンド ポスチャ検証を実行します。

NAD は、ネットワークに対する新しい接続を検出すると、ポスチャ クレデンシャルを照会します。エンドポイント装置にポスチャ エージェント（PA）がインストールされている場合は、インバンド ポスチャ検証を実行します。NAD は、エンドポイント装置と AAA サーバとの間で、ポスチャ検証情報の交換に関するすべてのメッセージのリレー エージェントとして動作します。PA が見つからない場合は、監査サーバを介してアウトオブバンド ポスチャ検証を実行します。

（インバンドかアウトバンドかにかかわらず）ポスチャ検証情報の交換が完了すると、NAD はどのホストが NAD デバイスを経由してネットワークの宛先にアクセスできるかを、AAA サーバから受信したネットワーク アクセス プロファイルに基づいて制御します。ネットワーク アクセス プロファイルは、次のいずれかの形式をとります。

- VLAN またはプライベート VLAN。
- アクセス コントロール リスト（ACL）は、NAC プロセスとは無関係にすべてのホストに付与されるデフォルト アクセス（DHCP サーバ、修復サーバ、監査サーバなどへのアクセス）に加えて、このホストが到達可能な宛先とそのトラフィック タイプを指定します。

NAD は、次のタイミングでポスチャ検証プロセスをトリガーします。

- 新しいセッションの開始
- 再検証タイマーの期限切れ
- システム管理者コマンドの入力
- PA によるポスチャの変更の通知（PA を備えるエンドポイント装置のみ対象）

Cisco NX-OS デバイスの場合、EAP メッセージのカプセル化の情報はユーザ データグラム プロトコル（UDP）に基づいています。UDP は、EAP over UDP（EAPoUDP または EoU）フレームの形で使用されます。

認証サーバ

実際のクライアント認証を行うサーバのことです。認証サーバはクライアントのアンチウイルス ステータスを検証し、アクセス ポリシーを確定し、LAN および NAD サービスへのアクセスをクライアントに許可するかどうかを NAD に通知します。NAD はプロキシとして動作するため、NAD と認証サーバの間の EAP メッセージ交換は、NAD に対しては透過的に行われます。

Cisco NX-OS デバイスは、RADIUS、認証、許可、アカウンティング（AAA）、および EAP 拡張機能を備えた Cisco Secure Access Control Server（ACS）Version 4.0 以降をサポートします。

ポスチャ検証サーバ

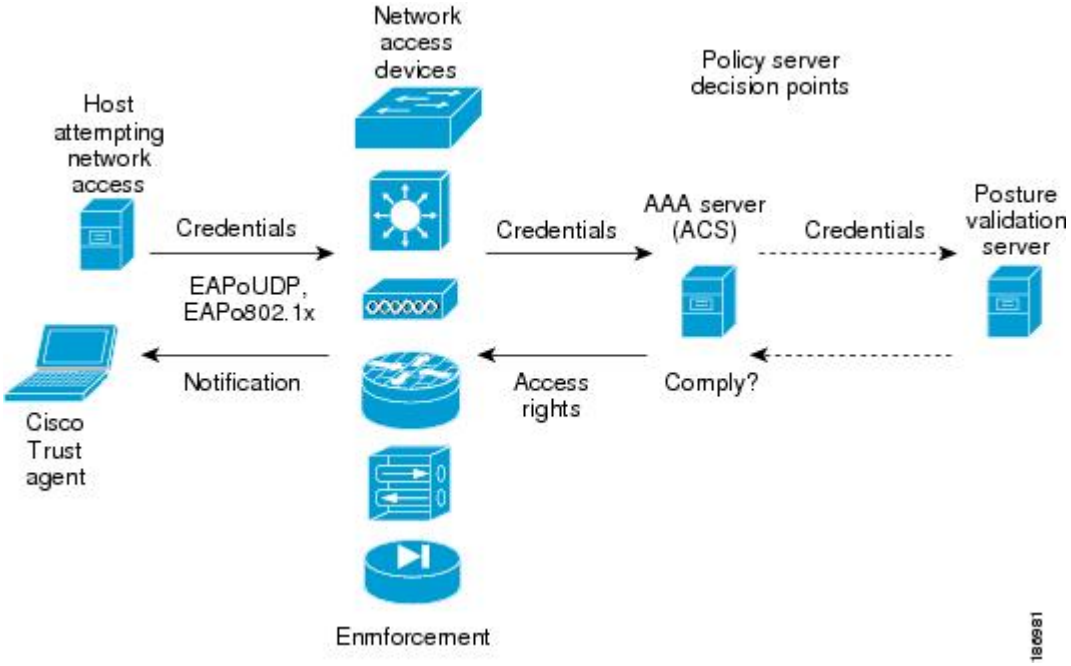
ポスチャ クレデンシャル セットをポリシー ルール セットに照らして許可する際に、NAC においてアプリケーション固有のポリシー デシジョン ポイントとして動作するサードパーティ製のサーバです。ポスチャ検証サーバは、認証サーバから要求を受信します。

NAC のポスチャ検証

ポスチャ検証は、ネットワーク リソースへの接続または使用を試みるエンドポイント装置を NAC 対応の NAD が検出したときに行われます。新しいエンドポイント装置を検出すると、NAD はエンドポイント装置のネットワーク アクセス プロファイルを AAA サーバ（Cisco Secure ACS など）に要求します。

次の図に、NAC によるエンドポイント装置のポスチャ検証プロセスを示します。

図 *2*：*NAC* によるエンドポイント装置のポスチャ検証



AAA サーバは、エンドポイント装置にポスチャ エージェントがインストールされているかどうかを確認します。エンドポイント装置にポスチャ エージェント（Cisco Trust Agent など）が存在すれば、AAA サーバは NAD を経由してエンドポイント装置にポスチャ情報を要求します。エンドポイント装置は、AAA サーバにポスチャ クレデンシャル セットを使用して応答します。AAA サーバは、このポスチャ情報をローカルで検証するか、あるいは 1 つまたは複数の外部ポスチャ検証サーバにポスチャ検証処理を任せます。

エンドポイント装置にポスチャ エージェントが存在しなければ、AAA サーバは監査サーバに別な手段（フィンガープリントやポート スキャンなど）でポスチャ情報を収集するように要求できます。また、AAA サーバは監査サーバに、収集した情報を検証しポスチャ検証結果を返すように要求することもできます。

AAA サーバは、これらのソースからのポスチャ検証結果を集約し、エンドポイント装置がネットワーク ポリシーに準拠しているかどうかを基に許可の判定を行います。AAA サーバは、エンドポイント装置のネットワーク アクセス プロファイルを確定すると、そのプロファイルを NAD に送信してエンドポイント装置の許可を適用できるようにします。

AAA サーバによるエンドポイント装置のクレデンシャルの検査では、1 つまたは複数のアプリケーション ポスチャ トークン（APT）が作成されます。APT は、ベンダー アプリケーションの適合性チェックを表しています。AAA サーバは、各ポスチャ検証サーバからすべての APT を集約し 1 つのシステム ポスチャ トークン（SPT）にまとめます。この SPT は、エンドポイント装置の総合適合性を表しています。SPT の値は、APT セットの中の最も不良な APT に基づいています。APT および SPT は、どちらも次の既定のトークンを使用して表されます。

Healthy

エンドポイント装置はポスチャ ポリシーに適合しており、この装置に課せられる規制はありません。

Checkup

エンドポイント装置はポリシーの範囲内にありますが、最新のソフトウェアが使用されていないため、アップデートを推奨します。

Transition

エンドポイント装置はポスチャの検証を受けている途中であり、その検証結果が出るまで暫定的にアクセスが許可されています。transitionは、ホストがブート中のため完全なポスチャ情報を入手できない、または完全な監査結果が得られない場合の状態です。

Quarantine

エンドポイント装置はポリシーに適合していません。この装置を検疫ネットワークに規制して修復する必要があります。他のエンドポイント装置にただちに脅威となるわけではありませんが、この装置は攻撃やウイルス感染に脆弱であり、できるだけ早急にアップデートする必要があります。

感染している

エンドポイント装置は他のエンドポイント装置に実際の脅威となっています。ネットワーク アクセスを厳格に規制し、この装置に修復処置を施すか、この装置へのすべてのネットワーク アクセスを禁止する必要があります。

不明（Unknown）

AAA サーバは、エンドポイント装置のポスチャ クレデンシャルを確認できません。適切なポスチャ クレデンシャルを取得しネットワーク アクセス許可の評価ができるように、エンドポイント装置の完全性を確認する必要があります。

IP デバイス トラッキング

IP デバイス トラッキングを使用すると、AAA サーバが使用できない場合でも、エンドポイント装置を引き続いてネットワークに接続できます。NAC の一般的な導入では、Cisco Secure ACS を使用してクライアントの状態（ポスチャ）が検証され、ポリシーが NAD に返されます。

IP デバイス トラッキングには、次の利点があります。

- AAAが使用できない間、エンドポイント装置は制限があるにしても、ネットワークへの接続は維持されます。
- AAA サーバが再び使用可能になると、ユーザは再検証を受けることができ、ACS からユーザのポリシーをダウンロードできます。

（注） AAA サーバの停止時は、ホストに既存のポリシーが関連付けられていない場合にだけ、NAD は IP デバイス トラッキング ポリシーを適用します。通常、再検証中に AAA サーバが停止した場合は、NAD はエンドポイント装置に使用されている現行のポリシーを保持します。

NAC LPIP

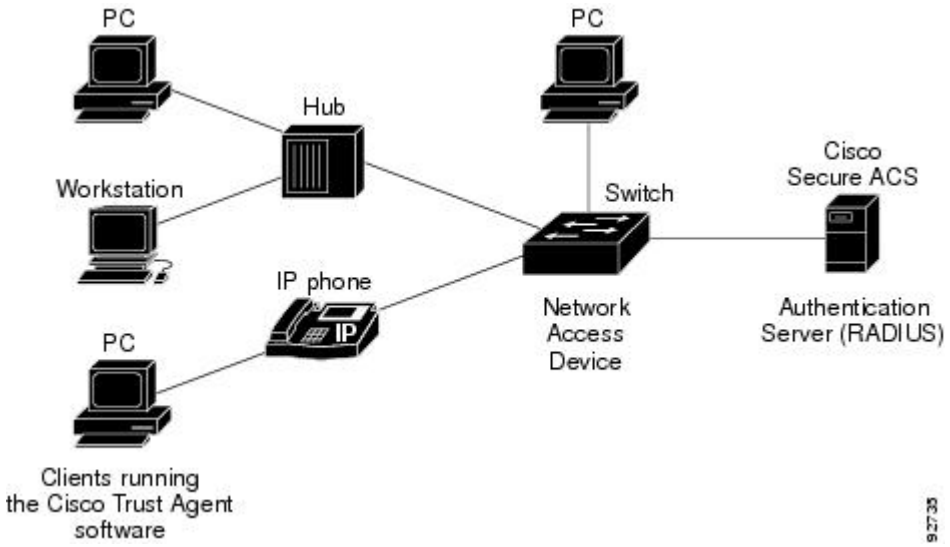
NAC LAN Port IP（LPIP）検証では、レイヤ 3 トランスポート EAPoUDP を使用してポスチャ検証情報が伝送されます。LPIP 検証には、次の特徴があります。

- レイヤ 2 ポート上でだけ動作し、レイヤ 3 ポート上では動作できません。
- ポート上で IP トラフィックを送信するすべてのホストがポスチャ検証の対象になります。

LPIP 検証では、DHCP メッセージまたはアドレス解決プロトコル（ARP）メッセージのスヌーピングによりアドミッション コントロールをトリガーします。データ パスでの IP パケットの代行受信は使用されません。LPIP 検証ではアクセス コントロール リスト（ACL）を使用してポリシーを適用します。

次の図に、NAD ポートに接続されたシングル ホスト、または同一 NAD ポートに接続されたマルチ ホストの LPIP 検証プロセスを示します。

図 *3*：*LPIP* 検証を使用するネットワーク



LPIP 検証をイネーブルにすると、EAPoUDP は IPv4 トラフィックだけをサポートします。NAD はエンドポイント装置またはクライアントのアンチウイルス ステータスをチェックして、アクセス コントロール ポリシーを適用します。

ポスチャ検証

1 つまたは複数のエンドポイント装置が接続されるポートで LPIP 検証をイネーブルにすると、Cisco NX-OS デバイスは DHCP スヌーピングおよび ARP スヌーピングを使用して、接続されたホストを識別します。Cisco NX-OS デバイスは、ARP パケットを受信した後、または DHCP スヌーピングのバインディング エントリを作成した後にポスチャ検証を開始します。デフォルトでは、接続されたホストの検出には ARP スヌーピングが使用されます。DHCP スヌーピング バインディング エントリが作成されたときに NAD にホストを検出させるには、DHCP スヌーピングをイネーブルにする必要があります。

ポスチャ検証のトリガー

LPIP 検証では、ARP スヌーピングを使用して、ダイナミックに取得した IP アドレスを持つホストまたはスタティックに設定された IP アドレスを持つホストを検出します。NAD が未知のホストからの ARP 要求を受信すると、ポスチャ検証をトリガーします。インターフェイスで DHCP スヌーピングがイネーブルになっている場合には、NAD に DHCP バインディング エントリが作成されるとポスチャ検証がトリガーされます。DHCP パケットは ARP 要求が送信される前に交換されるので、DHCP スヌーピングのほうがわずかに早く応答します。ARP スヌーピングと DHCP スヌーピングの両方が、同じホストのポスチャ検証をトリガーすることがあります。その場合、DHCP スヌーピング バインディングの作成によって起動されたトリガーが、ARP スヌーピングに優先します。

（注） DHCP スヌーピングと ARP スヌーピングを使用してホストの存在を検出する場合、悪意あるホストがスタティック ARP テーブルを設定してポスチャ検証をバイパスする可能性があります。この種の脅威から保護するために、ポートで IP ソース ガードをイネーブルにします。IP ソース ガードを使用すると、未認証のホストによるネットワークへのアクセスを防ぐことができます。

ポスチャ検証の方法

ホストのポスチャ検証がトリガーされると、次のいずれかの方法を使用してホストに適用するポリシーを指定できます。

- 例外リスト
- EAPoUDP

例外リスト

例外リストには、ローカル プロファイルとポリシー設定が含まれます。IP アドレスまたは MAC アドレスに基づいてデバイスをスタティックに許可または検証する場合は、アイデンティティ プロファイルを使用します。アイデンティティ プロファイルはローカル ポリシーに関連付けし、ローカル ポリシーにアクセス コントロール属性を指定できます。

例外リストを使用すると、特定のエンドポイント装置のポスチャ検証をバイパスして、スタティックに設定したポリシーを適用できます。ポスチャ検証がトリガーされると、NADは例外リストのホスト情報をチェックします。例外リストと一致した場合、NADはそのエンドポイント装置用に設定されたポリシーを適用します。

EAPoUDP

エンドポイント装置が例外リストと一致しなかった場合、NAD は EAPoUDP パケットを送信してポスチャ検証を開始します。ポスチャ検証の実行中、NADはデフォルトのアクセスポリシーを適用します。NAD が EAPoUDP メッセージをホストに送信し、ホストがこのアンチウイルス状態要求メッセージに応答すると、NAD は受信した EAPoUDP 応答を Cisco Secure ACS に転送します。NADが所定の回数試行してもホストから応答が得られない場合、このホストを非応答として分類します。ACS がクレデンシャルを検証すると、認証サーバが Access-Accept または Access-Reject メッセージを NAD に返します。NAD は EAPoUDP セッション テーブルを更新し、アクセス制限事項を適用します。これにより不適切なポスチャのエンドポイント装置は、隔離され検疫されるか、ネットワーク アクセスを拒否されます。

（注） Access-Reject メッセージは、EAPoUDP 情報の交換が失敗したことを意味します。これは、エンドポイント装置のポスチャが不適切であるという意味ではありません。

Access-Accept メッセージの場合は、NAD は Policy-based ACL（PACL）名を含むポリシーを適用し、EAP 再検証タイマーとステータス クエリー タイマーを開始します。

Access-Preject メッセージの場合は、NADはホストの適用ポリシーをすべて削除し、エンドポイント装置を既定の時間（ホールドタイマー）、Held ステートにします。ホールドタイマーの期限が切れると、エンドポイント装置は再検証されます。

（注） エンドポイント装置の DHCP スヌーピング バインディング エントリを削除すると、NAD はセッション テーブルからこのクライアントのエントリを削除します。これ以降、このクライアントは認証されません。

関連トピック

ACL を使用したポリシーの適用, （10 ページ）

ACL を使用したポリシーの適用

LPIP 検証では、ポリシーの適用に PACL を使用します。

NAD は、ポリシー検証に失敗（AAA サーバが Accept-Reject メッセージを送信）すると PACL を適用します。デフォルト ポリシーでは、ポートに適用されるアクティブな MAC ACL が使用されます（Port ACL（PACL）とも呼ばれます）。アクティブ MAC ACL には、スタティックに設定された PACL、または 802.1X 認証に基づいた AAA サーバ指定の PACL を使用できます。

PACL には、エンドポイント装置の IP アドレスのリストに展開されるグループを定義します。通常、PACL にはエンドポイント装置の IP アドレスを含みます。NAD は特定のグループを使用してエンドポイント装置を分類すると、そのエンドポイント装置に対応する IP アドレスを該当するグループに追加します。これにより、ポリシーがエンドポイント装置に適用されます。

NAD ポートの LPIP 検証を定義する場合は、その NAD ポートにデフォルトの PACL も定義する必要があります。また、そのデフォルト ACL を、ポスチャ検証が未完了のホストの IP トラフィックに適用するようにしてください。

NAD にデフォルト ACL が設定されていて、Cisco Secure ACS がホストのアクセス ポリシーを NAD に送信した場合、NAD は NAD ポートに接続されているそのホストからのトラフィックにこのポリシーを適用します。ポリシーがトラフィックに適用される場合、NAD はそのトラフィックを転送します。ポリシーが適用されない場合、NAD はデフォルトの ACL を適用します。ただし、NAD が Cisco Secure ACS からエンドポイント装置のアクセス ポリシーを取得しても、デフォルト ACL が設定されていないと、LPIP 検証の設定は有効になりません。

（注） DHCP スヌーピングと ARP スヌーピングは、どちらも VLAN 単位でイネーブルになります。ただし、NAC レイヤ 2 ポスチャ検証によりダウンロードされるセキュリティ ACL は、ポート単位で適用されます。その結果、これらの機能がいずれかの VLAN でイネーブルになると、DHCP パケットと ARP パケットはすべて代行受信されます。

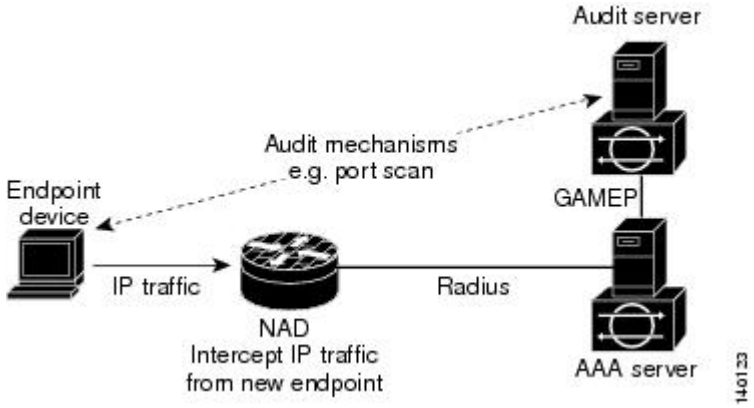
監査サーバおよび非応答ホスト

ポスチャ エージェント（Cisco Trust Agent）が稼働していないエンドポイント装置は、NAD から要求されてもクレデンシャルを提供できません。このようなデバイスを、エージェントレスまたは非応答と表現します。

NAC アーキテクチャは監査サーバをサポートしており、これを使用してエージェントレス エンドポイント装置を検証します。監査サーバは、エンドポイント装置にポスチャ エージェントがない場合でもそのセキュリティ適合性を調査、スキャン、および判別できるサードパーティ製サーバです。監査サーバの検査結果をアクセス サーバに反映させることができるので、エンドポイント装置固有のネットワーク アクセス ポリシーの適用が可能になり、すべての非応答エンドポイント装置に共通の制限ポリシーを適用する必要がありません。任意のサードパーティ製監査処理を NAC アーキテクチャに統合することで、より堅牢なホスト監査および検査機能を構築できます。

次の図に、一般的なトポロジに監査サーバを組み込む方法を示します。

図 *4*：*NAC* デバイスのロール



NACは、監査サーバが到達可能になっていて、エンドポイント装置が監査サーバと通信できることを前提としています。ポスチャ検証が設定されたNADを経由してエンドポイント装置がネットワーク アクセスを行うと、NAD は AAA サーバ（Cisco Secure ACS）に、このホストに適用するアクセス ポリシーを要求します。AAAサーバは、外部の監査サーバによるホストのスキャンをトリガーするように設定できます。監査サーバによるスキャンは非同期に行われ、完了までに数秒かかります。スキャンの実行中、AAAサーバは、適用を行う最小限の制限セキュリティ ポリシーと短時間のポーリング タイマー（セッション タイムアウト）を NAD に伝送します。監査サーバから結果が返されるまで、NADは所定の時間間隔でAAAサーバをポーリングします。AAAサーバは監査結果を受け取ると、監査結果に基づいてアクセス ポリシーを計算し、NADからの次の要求で、適用に必要なこのポリシーを NAD に送信します。

NAC タイマー

ここでは、NAC タイマーについて説明します。

ホールド タイマー

ホールド タイマーは、EAPoUDP セッションの失敗を検証する試みのあとに、次の新規セッションがすぐに開始されないように抑制します。NAC はこのタイマーを、Cisco Secure ACS が Accept-Reject メッセージを NAD に送信した場合にだけ使用します。ホールド タイマーのデフォルト値は 180 秒（3 分）です。

EAPoUDPセッションの検証が失敗するのは、ホストのポスチャ検証が失敗した場合、セッションタイマーの期限が切れた場合、NAD または Cisco Secure ACS が無効なメッセージを受信した場合などです。NADまたは認証サーバが無効なメッセージを連続して受信する場合は、悪意あるユーザが DoS 攻撃（サービス拒絶攻撃）を仕掛けようとしている可能性もあります。

AAA タイマー

AAA タイマーは、ポスチャ検証の実行中、NAD が要求を再送信する前に AAA サーバからの応答を待機する時間を制御します。再送信タイマーのデフォルト値は 60 秒です。

（注） このタイマーの設定値が低すぎると、不必要な再送信が行われる可能性があり、設定値が高すぎると、応答時間が長くなる可能性があります。

再送信タイマー

再送信タイマーは、ポスチャ検証の実行中、NAD が要求を再送信する前にクライアントからの応答を待機する時間を制御します。再送信タイマーのデフォルト値は 3 秒です。

（注） このタイマーの設定値が低すぎると、不必要な再送信が行われる可能性があり、設定値が高すぎると、応答時間が長くなる可能性があります。

再検証タイマー

再検証タイマーは、ポスチャ検証の実行中に EAPoUDP メッセージを使用していたエンドポイント装置に対し、NAD が NAC ポリシーを適用する期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。ホストが再検証されると、このタイマーはリセットされます。再検証タイマーのデフォルト値は 36000 秒（10 時間）です。

Cisco NX-OS ソフトウェアの再検証タイマーは、AAA サーバ（Cisco Secure ACS）からの Access-Accept メッセージに含まれる Session-Timeout RADIUS 属性（Attribute [27]）、および Termination-Action RADIUS-REQUEST 属性（Attribute [29]）に基づいて動作します。NAD が Session-Timeout 値を受信した場合、この値は NAD の再検証タイマー値に優先します。

再検証タイマーが満了した場合の NAD のアクションは、次の Termination-Action 属性の値に応じて異なります。

- Termination-Action RADIUS 属性の値がデフォルト値の場合は、セッションは終了します。
- NAD が受信した Termination-Action 属性の値がデフォルト以外の場合は、ポスチャ検証の実行中、EAPoUDP セッションおよび現在のアクセス ポリシーは有効な状態を維持します。
- Termination-Action 属性の値が RADIUS の場合は、NAD はクライアントを再検証します。
- サーバからのパケットに Termination-Action 属性が含まれない場合は、EAPoUDP セッションは終了します。

ステータス クエリー タイマー

ステータスクエリータイマーは、以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、NAD の待機時間を制御します。EAPoUDP メッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。ステータス クエリー タイマーのデフォルト値は 300 秒（5 分）です。

ホストが再認証されると、このタイマーはリセットされます。このタイマーが満了すると、NAD はホストに Status-Query メッセージを送信して、ホストのポスチャ検証の状態を確認します。ポスチャが変更されたことを示すメッセージをホストが NAD に送信すると、NAD はホストのポスチャを再検証します。

NAC ポスチャ検証および冗長スーパーバイザ モジュール

スイッチオーバーが発生した場合、Cisco NX-OS デバイスはエンドポイント装置と現在の PACL アプリケーションに関する情報を保持しますが、各 EAPoUDP セッションの現在のステートは失われます。Cisco NX-OS デバイスは、現在の PACL アプリケーションを削除し、ポスチャ検証を再開します。

LPIP 検証および他のセキュリティ機能

ここでは、LPIP 検証と Cisco NX-OS デバイス上の他のセキュリティ機能との相互作用について説明します。

802.1X

ポートに 802.1X と LPIP の両方を設定した場合、802.1X 認証によるソース MAC チェックに合格しないトラフィックは、ポスチャ検証をトリガーしません。ポートに 802.1X を設定した場合、接続されているホストが 802.1X により認証されるまでは、ポートはトラフィック（EAP over LAN（EAPOL）を除く）の送信および受信ができません。このメカニズムにより、ホストが認証されるまでは、ホストからの IP トラフィックがポスチャ検証をトリガーしないようになっています。

ポート セキュリティ

NAD は、ソース MAC アドレスをポート セキュリティの MAC アドレスと照合し、照合されなかった場合はそのエンドポイント装置をドロップします。NAD は、ポートセキュリティで検証された MAC アドレスにだけポスチャ検証を許可します。ポート セキュリティ違反が発生し、ポートがシャットダウンした場合は、Cisco NX-OS ソフトウェアはそのポートの LPIP ステートを削除します。

DHCP スヌーピング

DHCP によってバインディング エントリが作成されるまでは、ポスチャ検証は実行されません。DHCP スヌーピングと LPIP をイネーブルにした場合、DHCP を使用して IP アドレスを取得するホストのバインディング エントリを DHCP が作成したときに、Cisco NX-OS ソフトウェアがそのホストのポスチャ検証をトリガーします。

ダイナミック ARP インスペクション

インターフェイス上で LPIP 検証をイネーブルにすると、パケットがダイナミック ARP インスペクション（DAI）に合格した場合だけ、ポスチャ検証がトリガーされます。DAI をイネーブルにしないと、すべての ARP パケット（有効な MAC/IP ペアの場合）でポスチャ検証がトリガーされます。

（注） ARP スヌーピングは、ホストの検出に使用されるデフォルトのメカニズムです。ただし、ARP スヌーピングと DAI は同じものではありません。LPIP 検証をイネーブルにすると、Cisco NX-OS ソフトウェアは ARP パケットを LPIP 検証に渡します。DAI をイネーブルにすると、Cisco NX-OS ソフトウェアは ARP パケットを DAI に渡します。

（注） DHCP スヌーピングがイネーブルになっている場合、Cisco NX-OS ソフトウェアは DAI をバイパスします。

IP ソース ガード

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- DHCP スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP と MAC アドレス バインディングに基づいてフィルタリングするので、有効なホストの IP アドレスのスプーフィングを使用した攻撃の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

関連トピック

IP ソース ガードの設定

ポスチャのホスト固有 ACE

Cisco NX-OS ソフトウェアは、パケットが拒否条件と一致する場合はパケットをドロップし、パケットが許可条件と一致する場合はアクティブ PACL をスキップします。ACE の最後まで明示的な拒否がなく、一致もなかった場合、Cisco NX-OS ソフトウェアはパケットをアクティブ PACL と照合します。

（注） DHCP スヌーピングまたは DAI をイネーブルにすると、NAD はポスチャのホスト固有 ACE を処理しません。

アクティブ PACL

アクティブ PACL は、スタティックに設定された PACL の場合と、802.1X 認証に基づいた AAA サーバ指定の PACL の場合があります。パケットは、いずれかの拒否条件に一致するとドロップされ、許可条件に一致すると次のステップに進みます。

（注） DHCP スヌーピングまたは DAI がイネーブルになっている場合、NAD はアクティブ PACL を処理しません。

VACL

Cisco NX-OS ソフトウェアは、拒否条件と一致するパケットをすべてドロップします。

（注） DHCP スヌーピングまたは DAI がイネーブルになっている場合、NAD は VACL をバイパスします。

NAC のバーチャライゼーション サポート

NAC の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。

VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

NAC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	NACにはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

NAC の前提条件

NAC の前提条件は次のとおりです。

- NAD と各エンドポイント装置との間にレイヤ 3 ルートが存在していること

NAC の注意事項と制約事項

NAC に関する注意事項と制約事項は次のとおりです。

- EAPoUDP バイパスと AAA ダウン ポリシーはサポートされません。
- NAC は、認証に RADIUS だけを使用します。

LPIP の制約事項

LPIP 検証に関する制約事項は次のとおりです。

- LPIP 検証が許可されるのは、アクセス ポートだけです。
- LPIP 検証をトランク ポートまたはポート チャネル上でイネーブルできません。
- LPIP 検証は、スパンの終点であるポート上では許可されません。
- LPIP 検証は、プライベート VLAN に属するポート上では許可されません。
- LPIP 検証は、IPv6 をサポートしていません。
- LPIP 検証が許可されるのは、NAD に直接接続されたエンドポイント装置上だけです。
- NAD とエンドポイント装置との間にレイヤ 3 ルートがないと LPIP 検証を使用できません。

NAC のデフォルト設定

次の表に、NAC パラメータのデフォルト設定を示します。

表 *1*：*NAC* パラメータのデフォルト設定

パラメータ（Parameters）	デフォルト
EAPoUDP	ディセーブル
EAP UDP ポート番号	21862（0x5566）
クライアントレス ホストの使用	ディセーブル
定期的な自動再検証	イネーブル
再検証タイムアウト間隔	36000 秒（10 時間）
再送信タイムアウト間隔	3 秒
ステータス クエリー タイムアウト間隔	300 秒（5 分）
ホールド タイムアウト間隔	180 秒（3 分）
AAA タイムアウト間隔	60 秒（1 分）
最大リトライ回数	3.
EAPoUDP レート制限最大数	20 同時セッション
EAPoUDP ロギング	ディセーブル
IP デバイス トラッキング	イネーブル

NAC の設定

ここでは、NAC の設定方法について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

NAC の設定プロセス

NAC の設定には、次の作業を行います。

手順の概要

1. EAPoUDP をイネーブルにします。
2. AAA サーバへの接続を設定します。
3. エンドポイント装置と接続するインターフェイスに PACL を適用します。
4. エンドポイント装置と接続するインターフェイス上で NAC をイネーブルにします。

手順の詳細

ステップ 1 EAPoUDP をイネーブルにします。
ステップ 2 AAA サーバへの接続を設定します。
ステップ 3 エンドポイント装置と接続するインターフェイスに PACL を適用します。
ステップ 4 エンドポイント装置と接続するインターフェイス上で NAC をイネーブルにします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）
EAPoUDP のデフォルト AAA 認証方式のイネーブル化, （20 ページ）
インターフェイスへの PACL の適用, （22 ページ）
インターフェイスでの NAC のイネーブル化, （23 ページ）

EAPoUDP のイネーブル化

Cisco NX-OS デバイスは、エンドポイントと認証サーバの間で拡張認証プロトコル（EAP）メッセージをリレーします。NAC を設定する前に、Cisco NX-OS デバイス上で EAP over UDP（EAPoUDP）をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature eou**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**feature eou** 例： `switch(config)# feature eou`	EAPoUDP をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

EAPoUDP のデフォルト AAA 認証方式のイネーブル化

EAPoUDP のデフォルト AAA 認証方式をイネーブルにする必要があります。

（注） LPIP は認証に RADIUS だけを使用できます。

はじめる前に

EAPoUDP をイネーブルにします。

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa authentication eou default group***group-list*
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**aaa authentication eou default group***group-list* 例： `switch(config)# aaa authentication eou default group RadServer`	EAPoUDP のデフォルト AAA 認証方式として、1 つまたは複数の RADIUS サーバ グループのリストを設定します。*group-list* 引数には、グループをスペースで区切ったリストを指定します。グループ名は次のとおりです。 • **radius** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：RADIUS サーバの名前付きサブセットを認証に使用します。 デフォルトでは、認証方式は設定されていません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） デフォルトの AAA 認証方式を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）
AAA の設定
RADIUS の設定

インターフェイスへの PACL の適用

AAA サーバから PACL を入手できない場合は、NAD 上の LPIP ポスチャ検証を実行するアクセス インターフェイスに PACL を適用する必要があります。

はじめる前に

MAC ACL を作成します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **mac access-group***access-list*
4. **exit**
5. （任意） **show running-config interface**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス 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	**mac access-group***access-list* 例： `switch(config-if)# mac access-group acl-01`	指定の方向に流れるトラフィックを対象に、PACL をインターフェイスに適用します。 （注） インターフェイスは、PACL を 1 つだけ保有できます。インターフェイス上の PACL を交換する場合は、新しい PACL 名でこのコマンドを再度入力します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	**show running-config interface** 例： `switch(config)# show running-config interface`	（任意） インターフェイスの PACL 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの NAC のイネーブル化

ポスチャ検証を行うには、インターフェイス上で NAC をイネーブルにする必要があります。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **switchport**
4. **switchport mode access**
5. **nac enalbe**
6. **exit**
7. （任意） **show running-config interface**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス 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	**switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 スイッチング インターフェイスとして設定します。デフォルトでは、すべてのポートがレイヤ 3 ポートです。
ステップ 4	**switchport mode access** 例： `switch(config-if)# switchport mode access`	ポート モードをアクセスとして設定します。
ステップ 5	**nac enalbe** 例： `switch(config-if)# nac enable`	インターフェイスで NAC をイネーブルにします。

ステップ 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 7	**show running-config interface** 例： `switch(config)# show running-config interface`	（任意） インターフェイスの PACL 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

アイデンティティ ポリシーおよびアイデンティティ プロファイル エントリの設定

アイデンティティ プロファイルを使用して LPIP ポスチャ検証の例外を設定できます。アイデンティティ プロファイルには、LPIP 検証の際に対象外とするエンドポイント装置のエントリも含め

ます。オプションとして、アイデンティティプロファイルごとにアイデンティティポリシーを設定し、そのポリシーにNX-OSデバイスがエンドポイント装置に適用するPACLを指定することができます。デフォルトのアイデンティティ ポリシーは、インターフェイスのPACLです。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **identity policy***policy-name*
3. **object-group***access-list*
4. （任意） **description "***text***"**
5. **exit**
6. （任意） **show identity policy**
7. **identity profile eapoudp**
8. **device** {**authenticate** | **not-authenticate**} {**ip-address***ipv4-address* [*ipv4-subnet-mask*] | **mac-address***mac-address* [*mac-subnet-mask*]} **policy***name*
9. **exit**
10. （任意） **show identity profile eapoudp**
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**identity policy***policy-name*
	
	例：
	`switch(config)# identity policy AccType1`
	`switch(config-id-policy)#`
		アイデンティティ ポリシー名を指定し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。最大 1024 のアイデンティティ ポリシーを作成できます。名前の最大長は 100 文字です。

ステップ 3	**object-group***access-list* 例： `switch(config-id-policy)# object-group maxaclx`	ポリシーの IP ACP または MAC ACL を指定します。

	コマンドまたはアクション	目的
ステップ 4	**description "***text***"** 例： `switch(config-id-policy)# description "This policy prevents endpoint device without a PA"`	（任意） アイデンティティ ポリシーの説明を記します。最大長は 100 文字です。

ステップ 5	**exit**
	
	例：
	`switch(config-id-policy)# exit`
	`switch(config)#`
		アイデンティティ ポリシー コンフィギュレーション モードを終了します。

ステップ 6	**show identity policy** 例： `switch(config)# show identity policy`	（任意） アイデンティティ ポリシーの設定を表示します。

ステップ 7	**identity profile eapoudp**
	
	例：
	`switch(config)# identity profile eapoudp`
	`switch(config-id-prof)#`
		EAPoUDP のアイデンティティ プロファイル コンフィギュレーション モードを開始します。

ステップ 8	**device** {**authenticate** | **not-authenticate**} {**ip-address***ipv4-address* [*ipv4-subnet-mask*] | **mac-address***mac-address* [*mac-subnet-mask*]} **policy***name* 例： `switch(config-id-prof)# device authenticate ip-address 10.10.2.2 policy AccType1`	例外エントリを指定します。エントリの最大数は 5000 です。

ステップ 9	**exit**
	
	例：
	`switch(config-id-prof)# exit`
	`switch(config)#`
		アイデンティティ プロファイル コンフィギュレーション モードを終了します。

ステップ 10	**show identity profile eapoudp** 例： `switch(config)# show identity profile eapoudp`	（任意） アイデンティティ プロファイルの設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

クライアントレス エンドポイント装置の検証

ネットワーク内の PA 未搭載（クライアントレス）のエンドポイント装置に対してポスチャ検証を実行できます。このポスチャ検証は、エンドポイント装置にアクセスできる監査サーバが実行します。

はじめる前に

EAPoUDP をイネーブルにします。

AAA サーバとクライアントレス エンドポイント装置が監査サーバにアクセスできることを確認します。

手順の概要

1. **configure terminal**
2. **eou allow clientless**
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou allow clientless** 例： `switch(config)# eou allow clientless`	クライアントレス エンドポイント装置のポスチャ検証を可能にします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

EAPoUDP のロギングのイネーブル化

EAPoUDPイベント メッセージのロギングをイネーブルにできます。EAPoUDPイベントには、エラーやステータスの変化などが含まれます。これらのイベント メッセージは、設定されている syslog に送られます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou logging**
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou logging** 例： `switch(config)# eou logging`	EAPoUDP ロギングをイネーブルにします。デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch)# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

EAPoUDP のグローバル最大リトライ回数の変更

EAPoUDP のグローバル最大リトライ回数を変更できます。デフォルト値は 3 です。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou max-retry***count*
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou max-retry***count* 例： `switch(config)# eou max-retry 2`	EAPoUDP の最大リトライ回数を変更します。デフォルトは 3 です。有効な範囲は 1 ～ 3 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（19 ページ）
個別インターフェイスの EAPoUDP 最大リトライ回数の変更，（30 ページ）

個別インターフェイスの EAPoUDP 最大リトライ回数の変更

個別インターフェイスの EAPoUDP 最大リトライ回数を変更できます。デフォルト値は 3 です。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **eou max-retry***count*
4. **exit**
5. （任意） **show eou**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス 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	**eou max-retry***count* 例： `switch(config-if)# eou max-retry 2`	EAPoUDP の最大リトライ回数を変更します。デフォルトは 3 です。有効な範囲は 1 ～ 3 です。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show eou** 例： `switch(config)# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（19 ページ）

EAPoUDP のグローバル最大リトライ回数の変更，（29 ページ）
インターフェイスでの NAC のイネーブル化，（23 ページ）

EAPoUDP の UDP ポートの変更

EAPoUDP で使用される UDP ポートを変更できます。デフォルト ポートは 21862 です。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou port***udp-port*
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou port***udp-port* 例： `switch(config)# eou port 27180`	EAPoUDP で使用される UDP ポートを変更します。デフォルトは 21862 です。有効な範囲は 1 ～ 65535 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

EAPoUDPポスチャ検証の同時セッション数に関するレート制限の設定

EAPoUDP ポスチャ検証の同時セッション数を制御するレート制限を設定できます。EAPoUDP ポスチャ検証の最大同時セッション数を制御するレート制限値を変更できます。デフォルト値は 20 です。ゼロ（0）に設定すると、レート制限はディセーブルになります。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou ratelimit***number-of-sessions*
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou ratelimit***number-of-sessions* 例： `switch(config)# eou ratelimit 15`	EAPoUDP ポスチャ検証の同時セッション数を設定します。デフォルトは 20 です。範囲は 0 ～ 200 です。 （注） ゼロ（0）に設定すると、レート制限はディセーブルになります。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

グローバル自動ポスチャ再検証の設定

Cisco NX-OS ソフトウェアは、設定された間隔で Cisco NX-OS デバイスのエンドポイント装置のポスチャを自動的に再検証します。デフォルトの間隔は 36,000 秒（10 時間）です。再検証をディセーブルにしたり、再検証の間隔を変更することができます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **eou revalidate**
3. （任意） **eou timeout revalidation***seconds*
4. **exit**
5. （任意） **show eou**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的
ステップ 2	**eou revalidate** 例： `switch(config)# eou revalidate`	（任意） 自動ポスチャ検証をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 3	**eou timeout revalidation***seconds* 例： `switch(config)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。 自動ポスチャ検証をディセーブルにするには、**no eou revalidate** コマンドを使用します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）
個別インターフェイスでの自動ポスチャ再検証の設定, （35 ページ）

個別インターフェイスでの自動ポスチャ再検証の設定

Cisco NX-OS ソフトウェアは、設定された間隔で Cisco NX-OS デバイスのエンドポイント装置のポスチャを自動的に再検証します。デフォルトの間隔は 36,000 秒（10 時間）です。再検証をディセーブルにしたり、再検証の間隔を変更することができます。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. （任意） **eou revalidate**
4. （任意） **eou timeout revalidation***seconds*
5. **exit**
6. （任意） **show eou**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネットインターフェイスを指定し、インターフェイス 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	**eou revalidate** 例： `switch(config-if)# eou revalidate`	（任意） 自動ポスチャ検証をイネーブルにします。デフォルトではイネーブルになっています。 自動ポスチャ検証をディセーブルにするには、**no eou revalidate** コマンドを使用します。
ステップ 4	**eou timeout revalidation***seconds* 例： `switch(config-if)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	**show eou** 例： `switch(config)# show eou`	（任意） EAPoUDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（19 ページ）
グローバル自動ポスチャ再検証の設定，（34 ページ）
インターフェイスでの NAC のイネーブル化，（23 ページ）

EAPoUDP グローバル タイマーの変更

Cisco NX-OS ソフトウェアは、EAPoUDP の次のグローバル タイマーをサポートしています。

AAA

ポスチャ検証の実行中に、NAD が要求を再送信する前に AAA サーバからの応答を待機する時間を制御します。

ホールド時間

EAPoUDP セッションの失敗を検証する試みのあとに、すぐに次の新規セッションが開始されないように抑制します。NAC はこのタイマーを、Cisco Secure ACS が Accept-Reject メッセージを NAD に送信した場合にだけ使用します。

Retransmit

ポスチャ検証の実行中に、NAD が要求を再送信する前にクライアントからの応答を待機する時間を制御します。

再検証

ポスチャ検証の実行中に EAPoUDP メッセージを使用していたエンドポイント装置に対し、NAD が NAC ポリシーを適用する期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。

ステータス クエリー

以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、NAD の待機時間を制御します。EAPoUDP メッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **eou timeout aaa***seconds*
3. （任意） **eou timeout hold-period***seconds*
4. （任意） **eou timeout retransmit***seconds*
5. （任意） **eou timeout revalidation***seconds*
6. （任意） **eou timeout status-query***seconds*
7. **exit**
8. （任意） **show eou**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou timeout aaa***seconds* 例： `switch(config)# eou timeout aaa 30`	（任意） AAA タイムアウト間隔を変更します。デフォルト値は 60 秒（1 分）です。有効な範囲は 0 ～ 60 秒です。
ステップ 3	**eou timeout hold-period***seconds* 例： `switch(config)# eou timeout hold-period 300`	（任意） ホールド時間タイムアウト間隔を変更します。デフォルト値は 180 秒（3 分）です。範囲は 60 ～ 86400 秒です。
ステップ 4	**eou timeout retransmit***seconds* 例： `switch(config)# eou timeout retransmit 10`	（任意） 再送信タイムアウト間隔を変更します。デフォルトは 3 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 5	**eou timeout revalidation***seconds* 例： `switch(config)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。

	コマンドまたはアクション	目的
ステップ 6	**eou timeout status-query***seconds* 例： `switch(config)# eou timeout status-query 360`	（任意） ステータス クエリー タイムアウト間隔を変更します。デフォルトは 300 秒（5 分）です。有効な範囲は 10 ～ 1800 秒です。

ステップ 7	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 8	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 9	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（19 ページ）
個別インターフェイスでの EAPoUDP タイマーの変更，（39 ページ）
NAC タイマー，（12 ページ）

個別インターフェイスでの EAPoUDP タイマーの変更

Cisco NX-OS ソフトウェアは、NAC がイネーブルになっている各インターフェイスで、EAPoUDP に関する次のタイマーをサポートしています。

AAA

ポスチャ検証の実行中に、NAD が要求を再送信する前に AAA サーバからの応答を待機する時間を制御します。

ホールド時間

EAPoUDP セッションの失敗を検証する試みのあとに、すぐに次の新規セッションが開始されないように抑制します。NAC はこのタイマーを、Cisco Secure ACS が Accept-Reject メッセージを NAD に送信した場合にだけ使用します。

Retransmit

ポスチャ検証の実行中に、NAD が要求を再送信する前にクライアントからの応答を待機する時間を制御します。

再検証

ポスチャ検証の実行中にEAPoUDPメッセージを使用していたエンドポイント装置に対し、NADがNACポリシーを適用する期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。

ステータス クエリー

以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、NADの待機時間を制御します。EAPoUDPメッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. （任意） **eou timeout aaa***seconds*
4. （任意） **eou timeout hold-period***seconds*
5. （任意） **eou timeout retransmit***seconds*
6. （任意） **eou timeout revalidation***seconds*
7. （任意） **eou timeout status-query***seconds*
8. **exit**
9. （任意） **show eou**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネットインターフェイスを指定し、インターフェイス 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	**eou timeout aaa***seconds* 例： `switch(config-if)# eou timeout aaa 50`	（任意） AAA タイムアウト間隔を変更します。デフォルト値は 60 秒（1 分）です。有効な範囲は 0 ～ 60 秒です。
ステップ 4	**eou timeout hold-period***seconds* 例： `switch(config-if)# eou timeout hold-period 300`	（任意） ホールド時間タイムアウト間隔を変更します。デフォルト値は 180 秒（3 分）です。範囲は 60 ～ 86400 秒です。
ステップ 5	**eou timeout retransmit***seconds* 例： `switch(config-if)# eou timeout retransmit 10`	（任意） 再送信タイムアウト間隔を変更します。デフォルトは 3 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 6	**eou timeout revalidation***seconds* 例： `switch(config-if)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。
ステップ 7	**eou timeout status-query***seconds* 例： `switch(config-if)# eou timeout status-query 360`	（任意） ステータス クエリー タイムアウト間隔を変更します。デフォルトは 300 秒（5 分）です。有効な範囲は 10 ～ 1800 秒です。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show eou** 例： `switch(config)# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）
EAPoUDP グローバル タイマーの変更, （37 ページ）
NAC タイマー, （12 ページ）
インターフェイスでの NAC のイネーブル化, （23 ページ）

EAPoUPD グローバル設定のデフォルト値へのリセット

EAPoUDP グローバル設定をデフォルト値にリセットできます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou default**
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**eou default** 例： `switch(config)# eou default`	EAPoUDP 設定をデフォルト値にリセットします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（19 ページ）
EAPoUPD インターフェイス設定のデフォルト値へのリセット，（43 ページ）

EAPoUPD インターフェイス設定のデフォルト値へのリセット

インターフェイスの EAPoUDP 設定をデフォルト値にリセットできます。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **eou default**
4. **exit**
5. （任意） **show eou interface ethernet** *slot*/*port*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネットインターフェイスを指定し、インターフェイス 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	**eou default** 例： `switch(config-if)# eou default`	インターフェイスの EAPoUDP 設定をデフォルト値にリセットします。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show eou interface ethernet** *slot/port* 例： `switch(config)# show eou interface ethernet 2/1`	（任意） EAPoUDP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（19 ページ）
EAPoUPD グローバル設定のデフォルト値へのリセット，（42 ページ）
インターフェイスでの NAC のイネーブル化，（23 ページ）

IP デバイス トラッキングの設定

IP デバイス トラッキングを設定できます。AAA サーバに対する IP デバイス トラッキングの処理は、次のようになります。

- Cisco NX-OS デバイスが新しいセッションを検出します。
- ポスチャ検証のトリガー前に AAA サーバが到達不能であれば、Cisco NX-OS デバイスは IP デバイス トラッキング ポリシーを適用し、セッションのステートを AAA DOWN にします。
- AAA サーバが再度使用可能になると、ホストの再検証が実行されます。

（注） AAA サーバの停止時は、エンドポイント装置に他の既存のポリシーが関連付けられていない場合だけ、Cisco NX-OS デバイスが IP トラッキング ポリシーを適用します。再検証中に AAA サーバが停止した場合は、Cisco NX-OS デバイスはエンドポイント装置に使用されているポリシーを保持します。

手順の概要

1. **configure terminal**
2. **ip device tracking enable**
3. （任意） **ip device tracking probe** {**count***count* | **interval***seconds*}
4. （任意） **radius-server host** {*hostname* | *ip-address*} **test** [**username***username* [**password***password*]] [**idle-time***minutes*]
5. **exit**
6. （任意） **show ip device tracking all**
7. （任意） **show radius-server** {*hostname* | *ip-address*}
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**ip device tracking enable** 例： `switch(config)# ip device tracking enable`	IP デバイス トラッキングをイネーブルにします。デフォルトの状態はイネーブルです。
ステップ 3	**ip device tracking probe** {**count***count* | **interval***seconds*} 例： `switch(config)# ip device tracking probe count 4`	（任意） IP デバイス トラッキング テーブルに対し、次のパラメータを設定します。 **count** Cisco NX-OS デバイスが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。

	コマンドまたはアクション	目的
		間隔 Cisco NX-OS デバイスが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効な範囲は 1 ～ 302300 秒です。デフォルトは 30 秒です。
ステップ 4	**radius-server host** {*hostname* | *ip-address*} **test** [**username***username* [**password***password*]] [**idle-time***minutes*] 例： `switch(config)# radius-server host 10.10.1.1 test username User2 password G1r2D37&k idle-time 5`	（任意） RADIUS サーバのテスト パケットのパラメータを設定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。 **idle-time** パラメータには、サーバの動作ステータスを確認するために行うサーバテストの実行頻度を設定します。RADIUS サーバへのトラフィックがない場合は、NAD はこのアイドル タイマーの値に基づき、RADIUS サーバにダミーのパケットを送信します。アイドル タイマーのデフォルト値は 0 分です（ディセーブル）。 複数の RADIUS サーバがある場合は、このコマンドを再度入力します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	**show ip device tracking all** 例： `switch# show ip device tracking all`	（任意） IP デバイス トラッキングの情報を表示します。
ステップ 7	**show radius-server** {*hostname* | *ip-address*} 例： `switch# show radius-server 10.10.1.1`	（任意） RADIUS サーバ情報を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

IP デバイス トラッキングのクリア

AAA サーバの IP トラッキング情報をクリアできます。

手順の概要

1. （任意） **clear ip device tracking all**
2. （任意） **clear ip device tracking interface ethernet***slot*/*port*
3. （任意） **clear ip device tracking ip-address***ipv4-address*
4. （任意） **clear ip device tracking mac-address***mac-address*
5. （任意） **show ip device tracking all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ip device tracking all** 例： `switch# clear ip device tracking all`	（任意） すべてのEAPoUDPセッションをクリアします。
ステップ 2	**clear ip device tracking interface ethernet***slot*/*port* 例： `switch# clear ip device tracking interface ethernet 2/1`	（任意） 指定のインターフェイス上のEAPoUDPセッションをクリアします。
ステップ 3	**clear ip device tracking ip-address***ipv4-address* 例： `switch# clear ip device tracking ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレス（A.B.C.D 形式）の EAPoUDP セッションをクリアします。
ステップ 4	**clear ip device tracking mac-address***mac-address* 例： `switch# clear ip device tracking mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレス（XXXX.XXXX.XXXX 形式）の EAPoUDP セッションをクリアします。
ステップ 5	**show ip device tracking all** 例： `switch# show ip device tracking all`	（任意） IP デバイス トラッキングの情報を表示します。

手動による EAPoUDP セッションの初期化

手動で EAPoUDP セッションを初期化できます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. （任意） **eou initialize all**
2. （任意） **eou initialize authentication** {**clientless** | **eap** | **static**}
3. （任意） **eou initialize interface ethernet***slot*/*port*
4. （任意） **eou initialize ip-address***ipv4-address*
5. （任意） **eou initialize mac-address***mac-address*
6. （任意） **eou initialize posturetoken***name*
7. （任意） **show eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**eou initialize all** 例： `switch# eou initialize all`	（任意） すべての EAPoUDP セッションを初期化します。
ステップ 2	**eou initialize authentication** {**clientless** | **eap** | **static**} 例： `switch# eou initialize authentication static`	（任意） 指定の認証タイプの EAPoUDP セッションを初期化します。
ステップ 3	**eou initialize interface ethernet***slot*/*port* 例： `switch# eou initialize interface ethernet 2/1`	（任意） 指定のインターフェイス上の EAPoUDP セッションを初期化します。
ステップ 4	**eou initialize ip-address***ipv4-address* 例： `switch# eou initialize ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレス（A.B.C.D 形式）の EAPoUDP セッションを初期化します。

	コマンドまたはアクション	目的
ステップ 5	**eou initialize mac-address***mac-address* 例： `switch# eou initialize mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレス（XXXX.XXXX.XXXX 形式）の EAPoUDP セッションを初期化します。
ステップ 6	**eou initialize posturetoken***name* 例： `switch# eou initialize posturetoken Healthy`	（任意） 指定のポスチャ トークン名の EAPoUDP セッションを初期化します。 （注） トークン名を表示する場合は、**show eou all** コマンドを使用します。
ステップ 7	**show eou all** 例： `switch# show eou all`	（任意） EAPoUDP セッションの設定を表示します。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

手動による EAPoUDP セッションの再検証

手動で EAPoUDP セッションを再検証できます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. （任意） **eou revalidate all**
2. （任意） **eou revalidate authentication** {**clientless** | **eap** | **static**}
3. （任意） **eou revalidate interface ethernet***slot*/*port*
4. （任意） **eou revalidate ip-address***ipv4-address*
5. （任意） **eou revalidate mac-address***mac-address*
6. （任意） **eou revalidate posturetoken***name*
7. （任意） **show eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**eou revalidate all** 例： `switch# eou revalidate all`	（任意） すべての EAPoUDP セッションを再検証します。
ステップ 2	**eou revalidate authentication** {**clientless** | **eap** | **static**} 例： `switch# eou revalidate authentication static`	（任意） 指定の認証タイプの EAPoUDP セッションを再検証します。
ステップ 3	**eou revalidate interface ethernet***slot/port* 例： `switch# eou revalidate interface ethernet 2/1`	（任意） 指定のインターフェイス上の EAPoUDP セッションを再検証します。
ステップ 4	**eou revalidate ip-address***ipv4-address* 例： `switch# eou revalidate ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレスの EAPoUDP セッションを再検証します。
ステップ 5	**eou revalidate mac-address***mac-address* 例： `switch# eou revalidate mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレスの EAPoUDP セッションを再検証します。
ステップ 6	**eou revalidate posturetoken***name* 例： `switch# eou revalidate posturetoken Healthy`	（任意） 指定のポスチャ トークン名の EAPoUDP セッションを再検証します。 （注）　トークン名を表示する場合は、**show eou all** コマンドを使用します。
ステップ 7	**show eou all** 例： `switch# show eou all`	（任意） EAPoUDP セッションの設定を表示します。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

EAPoUDP セッションのクリア

EAPoUDP セッションを Cisco NX-OS デバイスからクリアできます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. （任意） **clear eou all**
2. （任意） **clear eou authentication** {**clientless** | **eap** | **static**}
3. （任意） **clear eou interface ethernet***slot*/*port*
4. （任意） **clear eou ip-address***ipv4-address*
5. （任意） **clear eou mac-address***mac-address*
6. （任意） **clear eou posturetoken***name*
7. （任意） **show eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear eou all** 例： `switch# clear eou all`	（任意） すべての EAPoUDP セッションをクリアします。
ステップ 2	**clear eou authentication** {**clientless** | **eap** | **static**} 例： `switch# clear eou authentication static`	（任意） 指定の認証タイプの EAPoUDP セッションをクリアします。
ステップ 3	**clear eou interface ethernet***slot*/*port* 例： `switch# clear eou interface ethernet 2/1`	（任意） 指定のインターフェイス上の EAPoUDP セッションをクリアします。
ステップ 4	**clear eou ip-address***ipv4-address* 例： `switch# clear eou ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレスの EAPoUDP セッションをクリアします。
ステップ 5	**clear eou mac-address***mac-address* 例： `switch# clear eou mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレスの EAPoUDP セッションをクリアします。

	コマンドまたはアクション	目的
ステップ 6	**clear eou posturetoken***name* 例： `switch# clear eou posturetoken Healthy`	（任意） 指定のポスチャ トークン名の EAPoUDP セッションをクリアします。 （注） トークン名を表示する場合は、**show eou all** コマンドを使用します。
ステップ 7	**show eou all** 例： `switch# show eou all`	（任意） EAPoUDP セッションの設定を表示します。

関連トピック

EAPoUDP のイネーブル化, （19 ページ）

EAPoUDP 機能のディセーブル化

Cisco NX-OS デバイス上の EAPoUDP 機能をディセーブルにできます。

注意 EAPoUDP をディセーブルにすると、Cisco NX-OS デバイスからすべての EAPoUDP 設定が削除されます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **no feature eou**
3. **exit**
4. （任意） **show feature**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**no feature eou** 例： `switch(config)# no feature eou`	EAPoUDP をディセーブルにします。 **注意** EAPoUDP 機能をディセーブルにすると、すべての EAPoUDP 設定が削除されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show feature** 例： `switch# show feature`	（任意） Cisco NX-OS 機能のイネーブルまたはディセーブル ステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NAC の設定の確認

NAC の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show eou [**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet***slot*/*port* | **ip-address***ipv4-address* | **mac-address***mac-address* | **posturetoken***name*]	EAPoUDP の設定を表示します。
show ip device tracking [**all** | **interface ethernet***slot*/*port* | **ip-address***ipv4-address* | **mac-address***mac-address*]	IP デバイス トラッキングの情報を表示します。
show running-config eou [**all**]	実行コンフィギュレーション内の EAPoUDP 設定を表示します。

コマンド	目的
show startup-config eou	スタートアップ コンフィギュレーション内の EAPoUDP 設定を表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

NAC の設定例

次に、NAC を設定する例を示します。

```
feature eou
aaa authentication eou default group radius
mac access-list macacl-01
  10 permit any any 0x100
interface Ethernet8/1
  mac access-group macacl-01
```

NAC に関する追加情報

ここでは、NAC に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

NAC の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2* : *NAC* の機能の履歴

機能名	リリース	機能情報
NAC	6.0(1)	Release 5.2 以降、変更はありません。

機能名	リリース	機能情報
NAC	5.2(1)	Release 5.1 以降、変更はありません。
NAC	5.1(1)	Release 5.0 以降、変更はありません。
NAC	5.0(2)	Release 4.2 以降、変更はありません。