RADIUS NAC サポートの設定

- RADIUS NAC サポートについて，1 ページ
- RADIUS NAC サポートの制約事項，2 ページ
- RADIUS NAC サポートの設定（GUI），4 ページ
- RADIUS NAC サポートの設定（CLI），4 ページ

RADIUS NAC サポートについて

Cisco Identity Services Engine（ISE）は、次世代のコンテキストベース アクセス コントロール ソリューションで、Cisco Secure Access Control System（ACS）と Cisco Network Admission Control（NAC）の機能を 1 つの統合されたプラットフォームで提供します。

ISE は Cisco Unified Wireless Network のリリース 7.0.116.0 で導入されています。 ISE を使用して、配備されたネットワークで高度なセキュリティを実現できます。 ISE は、コントローラ上で設定できる認証サーバです。 RADIUS NAC 対応の WLAN 上のコントローラにクライアントがアソシエートされると、コントローラは ISE サーバに要求を転送します。

ISE サーバはデータベースでユーザを検証し、認証が正常に完了すると、URL と事前認証 ACL がクライアントに送信されます。 このときクライアントは Posture Required 状態になり、ISE サーバから返された URL にリダイレクトされます。

（注） ISE サーバから返された URL にキーワード「**cwa**」が含まれる場合、クライアントは、Central Web Authentication の状態になります。

クライアントの NAC エージェントによって、ポスチャ検証プロセスがトリガーされます。 ISE サーバによるポスチャ検証が正常に完了すると、クライアントは RUN 状態になります。

（注） RADIUS NAC による Flex ローカル スイッチングは、リリース 7.2.110.0 で追加されました。これは、7.0 リリースおよび 7.2 リリースではサポートされていません。 RADIUS NAC 対応の WLAN 機能が動作するよう再設定するには、7.2.110.0 以降のリリースを 7.2 または 7.0 リリースにダウングレードする必要があります。

デバイス登録

デバイス登録を行うと、RADIUS NAC を使用して WLAN の新しいデバイスの認証とプロビジョニングを行えるようになります。 デバイスを WLAN に登録すると、設定されている ACL に基づいてネットワークを使用できるようになります。

中央 Web 認証

中央 Web 認証（CWA）の場合、Web 認証は ISE サーバで行われます。 ISE サーバの Web ポータルに、クライアント用のログイン ページが表示されます。 ISE サーバで資格情報が検証されると、クライアントがプロビジョニングされます。 CoA が適用されるまで、クライアントは POSTURE_REQD 状態のままです。 資格情報と ACL が ISE サーバから送信されます。

ローカル Web 認証

ローカル Web 認証は、RADIUS NAC でサポートされていません。

次の表に、一般的な ISE でのデバイス登録、CWA、および LWA の有効な組み合わせを示します。

表 *1*：*ISE* ネットワーク認証フロー

WLAN の設定	CWA	LWA	デバイス登録
RADIUS NAC 対応	Yes	No	Yes
L2 なし	No	PSK、Static WEP、CKIP	No
L3 なし	該当なし	内部/外部	該当なし
MAC フィルタリング対応	Yes	No	Yes

RADIUS NAC サポートの制約事項

- RADIUS NAC 対応の WLAN は、オープン認証と MAC フィルタリングをサポートしています。

- 設定されたアカウンティング サーバが認証（ISE）サーバではない場合、RADIUS NAC は機能しません。 ISE 機能を使用する場合は、認証およびアカウンティング サーバと同じサーバを設定する必要があります。 ISE を ACS 機能専用にする場合は、アカウンティング サーバを柔軟に設定できます。
- 認証またはアカウンティング RADIUS サーバに障害が発生した場合、認証またはアカウンティング サーバのリスト内の該当するサーバが起動しなくなります。 これは、クライアント認証およびアカウンティングが同じ IP 認証およびアカウンティング サーバで実行されていることを意味しています。 ただし、認証およびアカウンティング サーバを連携させる場合、RADIUS サーバの設定時にこれらのサーバを同じ順序で追加する必要があります。
- クライアントがある WLAN から別の WLAN へ移動し、アイドル タイムアウトが発生する前に元の WLAN に戻った場合、コントローラはそのクライアントの監査セッション ID を保持しています。 したがって、アイドル タイムアウト セッションの期限が切れる前にクライアントがコントローラに join すると、それらのクライアントはただちに RUN 状態になります。 セッションがタイムアウトしてから、クライアントがコントローラに再アソシエートされているかどうかが検証されます。
- たとえば 2 つの WLAN があり、1 台のコントローラに WLAN 1 が設定され（WLC1）、もう 1 台のコントローラに WLAN2 が設定され（WLC2）、その両方が RADIUS NAC 対応であるとします。 クライアントはまず WLC1 に接続し、ポスチャ検証のあと RUN 状態になります。 次にこのクライアントは、WLC2 に移動するとします。 WLC1 内のこのクライアントに対する PMK の期限が切れる前に、クライアントが WLC1 に再接続した場合、このクライアントに対するポスチャ検証は省略されます。 クライアントはポスチャ検証を省略してただちに RUN 状態になります。これは、コントローラがこのクライアントの古い監査セッション ID を保持し、ISE がその ID をすでに認識しているからです。
- ワイヤレス ネットワークに RADIUS NAC を導入する場合は、プライマリおよびセカンダリ ISE サーバを設定しないでください。 代わりに、2 つの ISE サーバ間に HA を設定することをお勧めします。 プライマリおよびセカンダリ ISE を設定すると、クライアントが RUN 状態に移行する前に、ポスチャ検証が必要になります。 HA を設定すると、クライアントはフォールバック ISE サーバで自動的に RUN 状態に移行します。
- RADIUS NAC が設定されたコントローラ ソフトウェアは、サービス ポートでの認可変更（CoA）をサポートしません。
- アクティブなネットワーク内で AAA サーバ インデックスを入れ替えないでください。クライアントが切断され、RADIUS サーバへの再接続が必要になる可能性があります。それによって、ISE サーバ ログにログ メッセージが追加される場合があります。
- RADIUS NAC を使用するには、WLAN 上で AAA Override を有効にする必要があります。
- WLAN 上で WPA および WPA2 または dot1X を有効にする必要があります。
- 低速なローミング中に、クライアントのポスチャ検証が行われます。
- ゲストのトンネリング モビリティは、ISE NAC 対応の WLAN でサポートされます。
- VLAN Select はサポートされません。
- ワークグループ ブリッジはサポートされません。

- AP Group over NAC は RADIUS NAC ではサポートされません。
- RADIUS NAC を有効にすると、RADIUS サーバの上書きインターフェイスはサポートされません。
- クライアントとサーバ間の DHCP 通信。 DHCP プロファイルは一度だけ解析されます。 これは一度だけ ISE サーバに送信されます。
- AAAの `url-redirect-acl` および `url-redirect` 属性を AAA サーバが要求する場合、AAA Override 機能をコントローラで有効にする必要があります。

RADIUS NAC サポートの設定（GUI）

ステップ 1 [WLANs] タブを選択します。

ステップ 2 ISE を有効にする WLAN の WLAN ID をクリックします。
[WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [NAC State] ドロップダウン リストから [Radius NAC] を選択します。

- [SNMP NAC]：WLAN に SNMP NAC を使用します。
- [Radius NAC]：WLAN に Radius NAC を使用します。

（注） WLAN 上で RADIUS NAC を使用すると、自動的に AAA Override が有効になります。

ステップ 5 [Apply] をクリックします。

RADIUS NAC サポートの設定（CLI）

次のコマンドを入力します。

config wlan nac radius { **enable** | **disable**} *wlan_id*