NPS、ワイヤレス LAN コントローラ、ワイヤレス ネットワークの設定例

目次

概要

このドキュメントでは、RADIUS サーバに Microsoft Network Policy Server（NPS）を使用した Cisco Unified Wireless Network で Microsoft Challenge Handshake Authentication Protocol（MS-CHAP）バージョン 2 認証を使用した Protected Extensible Authentication Protocol（PEAP）を設定する際の設定例を紹介しています。

前提条件

要件

この設定を試す前に、次のことに精通していることを確認してください。

- 基本的な Windows 2008 インストールの知識
- シスコ コントローラ インストールの知識

この設定を試す前に、次の要件が満たされていることを確認してください。

- テスト ラボのそれぞれのサーバに Microsoft Windows Server 2008 オペレーティング システムがインストールされていること。
- すべてのサービス パックが更新されていること。
- コントローラと Lightweight アクセス ポイント（LAP）がインストールされていること。
- 最新ソフトウェア更新が設定されていること。

Cisco 5508 シリーズ ワイヤレス コントローラの初期インストールと設定については、『Cisco 5500 シリーズ ワイヤレス コントローラ インストレーション ガイド』を参照してください。

注: この資料が読者に PEAP-MS-CHAP 認証に Microsoft サーバで必要な設定の例を与えるように意図されています。 このドキュメントで示す Microsoft Windows サーバの設定はラボでテスト済みで、期待通りに動作することが確認されています。 設定で問題が発生した場合は、Microsoft に支援を求めてください。 Cisco Technical Assistance Center（TAC）では Microsoft Windows サーバの設定をサポートしません。

Microsoft Windows 2008 のインストール ガイドと設定ガイドは Microsoft Tech Net にあります。

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。

- ファームウェア バージョン 7.4 が稼働する Cisco 5508 ワイヤレス コントローラ
- Lightweight アクセス ポイント プロトコル（LWAPP）を含む Cisco Aironet 3602 アクセス ポイント（AP）
- NPS、認証局（CA）、Dynamic Host Control Protocol（DHCP）、ドメイン ネーム システム（DNS）サービスがインストールされている Windows 2008 Enterprise Server
- Microsoft Windows 7 クライアント PC
- Cisco Catalyst 3560 シリーズ スイッチ

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

PEAP の概要

PEAP では、Transport Level Security（TLS）を使用して、ワイヤレス ラップトップなど認証対象の PEAP クライアントと Microsoft NPS や任意の RADIUS サーバなどの PEAP オーセンティケータとの間に暗号化チャネルを作成します。 PEAP では認証方式は指定されませんが、PEAP により提供される TLS-encrypted 暗号化チャネルで動作できる EAP-MS-CHAP v2 などの他の Extensible Authentication Protocol（EAP）認証プロトコルに対してセキュリティが付加されます。 PEAP の認証プロセスは、主に 2 つのフェーズで構成されます。

PEAP フェーズ 1： TLS-Encrypted チャネル

ワイヤレス クライアントで AP とのアソシエーションが確立されます。 IEEE 802.11 ベースのアソシエーションでは、クライアントとアクセス ポイントでセキュアなアソシエーションが確立される前に、オープン システムや共有秘密鍵による認証が提供されます。 クライアントとアクセス ポイントの間に IEEE 802.11 ベースのアソシエーションが確立されると、AP との TLS セッションがネゴシエートされます。 ワイヤレス クライアントと NPS の間での認証が完了すると、クライアントと NPS の間で TLS セッションがネゴシエートされます。 このネゴシエーションで生成された鍵が、後続のすべての通信の暗号化に使用されます。

PEAP フェーズ 2： EAP 認証による通信

PEAP 認証プロセスの最初の段階で PEAP が作成した TLS チャネルで、EAP ネゴシエーションを含む EAP 通信が発生します。 NPS では、EAP-MS-CHAP v2 でワイヤレス クライアントの認証が行われます。 LAP とコントローラでは、ワイヤレス クライアントと RADIUS サーバの間でのメッセージの転送だけが行われます。 このワイヤレス LAN コントローラ（WLC）と LAP は TLS のエンド ポイントではないため、これらのメッセージの復号化はできません。

正常な認証（ユーザが PEAP-MS-CHAP v2 でパスワードベースの有効なクレデンシャルを入力した場合）の RADIUS メッセージ シーケンスは次のとおりです。

1. NPS がクライアントに ID 要求メッセージ EAP-Request/Identity を送信します。
2. クライアントが ID 応答メッセージ EAP-Response/Identity で応答します。
3. NPS が MS-CHAP v2 チャレンジ メッセージ EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge) を送信します。
4. クライアントが MS-CHAP v2 チャレンジと応答 EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response) で応答します。
5. サーバがクライアントを正常に認証すると、NPS は MS-CHAP v2 成功パケット EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success) を返送します。
6. クライアントがサーバを正常に認証すると、クライアントは MS-CHAP v2 成功パケット EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success) で応答します。
7. NPS が認証の成功を示す EAP-type-length-value（TLV）を送信します。
8. クライアントが EAP-TLV ステータスの成功メッセージを返します。
9. サーバが認証を完了し、EAP-Success メッセージをプレーン テキストで送信します。 クライアントの分離に VLAN が展開されている場合は、このメッセージに VLAN の属性が含まれています。

設定

このセクションでは、PEAP-MS-CHAP v2 の設定について説明します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

この設定では、次のネットワーク設定を使用します。

この設定では、Microsoft Windows 2008 Server は次の役割を果たします。

- ドメイン wireless.com のドメイン コントローラ
- DHCP/DNS サーバ
- CA サーバ
- NPS か。 無線ユーザを認証するため
- アクティブ ディレクトリか。 ユーザデータベースを維持するため

サーバは、図のようにレイヤ 2 スイッチを介して有線ネットワークに接続します。 WLC と登録済み LAP もレイヤ 2 スイッチを介してネットワークに接続しています。

ワイヤレス クライアントは Wi-Fi Protected Access 2（WPA2）- PEAP-MS-CHAP v2 認証を使用してワイヤレス ネットワークに接続します。

設定

この例の目標は、PEAP-MS-CHAP v2 認証でワイヤレス クライアントを認証するように、Microsoft 2008 Server、Wireless LAN Controller、および Light Weight AP を設定することです。このプロセスには、次の 3 つの主なステップがあります。

1. Microsoft Windows 2008 Server の設定
2. WLC と Light Weight AP の設定
3. ワイヤレス クライアントの設定

Microsoft Windows 2008 Server の設定

この例では、Microsoft Windows 2008 Server の完全な設定に次のステップが含まれます。

1. サーバをドメイン コントローラとして設定する
2. DHCP サービスをインストールして設定する
3. CA サーバとしてサーバをインストールして設定する
4. クライアントをドメインに接続する
5. NPS をインストールする
6. 証明書をインストールする
7. PEAP 認証のために NPS を設定する
8. Active Directory にユーザを追加する

ドメイン コントローラとしての Microsoft Windows 2008 Server の設定

Microsoft Windows 2008 Server をドメイン コントローラとして設定するには、次の手順を実行します。

1. [Start] > [Server Manager] の順にクリックします。

2. [Roles] > [Add Roles] の順にクリックします。

3. [Next] をクリックします。

4. サービス [Active Directory Domain Services] を選択し、[Next] をクリックします。

5. 「Introduction to Active Directory Domain Services」に目を通し、[Next] をクリックします。

6. [Install] をクリックして、インストール プロセスを開始します。

   インストールが進んで完了します。

7. [Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)] をクリックし、Active Directory のインストールと設定を続けます。

8. [Next] をクリックして Active Directory Domain Services Installation Wizard を実行します。

9. 「Operating System Compatbilty」の情報に目を通し、[Next] をクリックします。

10. **新しいフォレストの新しいドメインを > 次に**新しいドメインを作成するために『Create』をクリック して下さい。

11. 新しいドメイン（この例**の** wireless.com）の完全な DNS名を入力し、『Next』 をクリック して下さい。

12. ドメインのフォレスト機能レベルを選択し、[Next] をクリックします。

13. ドメインのドメイン機能レベルを選択し、[Next] をクリックします。

14. DNS が選択されていることを確認し、[Next] をクリックします。

15. [Yes] をクリックします。インストール ウィザードが DNS でドメイン用に新しいゾーンを作成します。

16. Active Directory がファイルに使用するフォルダを選択し、[Next] をクリックします。

17. 管理者パスワードを入力し、[Next] をクリックします。

18. 選択内容を確認し、[Next] をクリックします。

    インストールが続行されます。

19. [Finish] をクリックしてウィザードを終了します。

20. サーバを再起動して変更を有効にします。

Microsoft Windows 2008 Server での DHCP サービスのインストールと設定

Microsoft 2008 Server 上の DHCP サービスは、ワイヤレス クライアントに IP アドレスを提供するために使用されます。 DHCP サービスをインストールして設定するには、次の手順を実行します。

1. [Start] > [Server Manager] の順にクリックします。

2. [Roles] > [Add Roles] の順にクリックします。

3. [Next] をクリックします。

4. サービス [DHCP Server] を選択し、[Next] をクリックします。

5. 「Introduction to DHCP Server」に目を通し、[Next] をクリックします。

6. DHCP サーバが要求を監視するインターフェイスを選択し、[Next] をクリックします。

7. DHCP サーバがクライアントに提供するデフォルト DNS 設定を構成し、[Next] をクリックします。

8. ネットワークで WINS をサポートする場合は、WINS を設定します。

9. ウィザードを使用して DHCP スコープを作成するには [Add] をクリックし、DHCP スコープを後で作成するには [Next] をクリックします。 [Next] をクリックして処理を続けます。

10. サーバでの DHCPv6 のサポートを有効または無効にして、[Next] をクリックします。

11. 前の手順で DHCPv6 を有効にした場合は、IPv6 DNS 設定を構成します。 [Next] をクリックして処理を続けます。

12. Active Directory で DHCP サーバを認可するドメイン管理者クレデンシャルを指定し、[Next] をクリックします。

13. 確認ページの設定を確認し、[Install] をクリックしてインストールを完了します。

    インストールが続行されます。

14. [Close] をクリックし、ウィザードを閉じます。

これで、DHCP サーバがインストールされました。

15. > **DHCP サービスを設定する管理ツール > DHCP** 『Start』 をクリック して下さい。

16. DHCP サーバ（この例では win-mvz9z2umms.wireless.com）を展開し、[IPv4] を右クリックして [New Scope] を選択して DHCP スコープを作成します。

17. New Scope Wizard で新しいスコープを設定するには、[Next] をクリックします。

18. 新しいスコープの名前（この例では Wireless Clients）を指定し、[Next] をクリックします。

19. DHCP リースに使用できる IP アドレスの範囲を入力します。 [Next] をクリックして次に進みます。

20. 除外するアドレスのリスト（任意指定）を作成します。 [Next] をクリックして次に進みます。

21. リース時間を設定し、[Next] をクリックします。

22. [Yes, I want to configure these options now] をクリックしてから [Next] をクリックします。

23. このスコープのデフォルト ゲートウェイの IP アドレスを入力し、[Add] > [Next] の順にクリックします。

24. クライアントが使用する DNS ドメイン名と DNS サーバを設定します。 [Next] をクリック

して次に進みます。

25. ネットワークで WINS をサポートする場合は、このスコープの WINS 情報を入力します。[Next] をクリックして次に進みます。

26. このスコープをアクティブにするには、[Yes, I want to activate this scope now] > [Next] の順にクリックします。

27. [Finish] をクリックします。ウィザードが終了します。

Microsoft Windows 2008 Server の CA サーバとしてのインストールと設定

EAP-MS-CHAP v2 を使用する PEAP は、サーバにある証明書に基づいて RADIUS サーバの検証を行います。 また、クライアント コンピュータの信頼するパブリックな CA がサーバ証明書を発行する必要があります (つまり、パブリックな CA 証明書がクライアント コンピュータの証明書ストアの Trusted Root Certification Authority フォルダにすでに存在する必要があります)。

証明書を NPS に発行する CA サーバとして Microsoft Windows 2008 Server を設定するには、次の手順を実行します。

1. [Start] > [Server Manager] の順にクリックします。

2. [Roles] > [Add Roles] の順にクリックします。

3. [Next] をクリックします。

4. サービス [Active Directory Certificate Services] を選択し、[Next] をクリックします。

5. 「Introduction to Active Directory Certificate Services」に目を通し、[Next] をクリックします。

6. [Certificate Authority] を選択し、[Next] をクリックします。

7. [Enterprise] を選択し、[Next] をクリックします。

8. [Root CA] を選択し、[Next] をクリックします。

9. [Create a new private key] を選択し、[Next] をクリックします。

10. 「Configuring Cryptography for CA」で [Next] をクリックします。

11. [Next] をクリックし、この CA のデフォルトの通常名を受け入れます。

12. この CA 証明書が有効である時間を選択し、[Next] をクリックします。

13. [Next] をクリックし、証明書データベースのデフォルトの場所を受け入れます。

14. 設定を見直し、[Install] をクリックします。Active Directory Certificate Service が開始されます。

15. インストールが完了したら、[Close] をクリックします。

ドメインへのクライアントの接続

クライアントを有線ネットワークに接続し、ドメイン固有の情報を新しいドメインからダウンロードするには、次の手順を実行します。

1. ストレート型のイーサネット ケーブルでクライアントを有線ネットワークに接続します。
2. クライアントをブートし、クライアントのユーザ名とパスワードでログインします。
3. Start > Run の順にクリック し、**cmd を**入力し、『OK』 をクリック して下さい。

4. コマンド プロンプトで「**ipconfig**」と入力し、[Enter] をクリックして、DHCP が正常に動作しクライアントが DHCP サーバから IP アドレスを受け取ったことを確認します。
5. クライアントをドメインに加入させるには、[Start] をクリックして[Computer] を右クリックし、[Properties] を選択して右下の [Change Settings] を選択します。
6. [Change] をクリックします。
7. [Domain] をクリックして「**wireless.com**」と入力し、[OK] をクリックします。

8. ユーザ名「**Administrator**」を入力し、クライアントが参加するドメインのパスワードを入力します。 これはサーバ上での Active Directory の管理者アカウントです。

9. [OK] をクリックし、さらに [OK] をクリックします。

10. > **コンピュータを再起動する再始動今**『Close』 をクリック して下さい。
11. コンピュータが再起動したら、次の情報を使用してログインします。 ユーザ名 = Administrator パスワード = <ドメイン パスワード> ドメイン = wireless
12. [Start] をクリックして [Computer] を右クリックし、[Properties] を選択して右下の [Change Settings] を選択します。wireless.com ドメインにいることを確認してください。
13. 次の手順では、クライアントがサーバから CA 証明書（信頼）を受信したことを確認します。

14. [Start] をクリックして「**mmc**」と入力し、**Enter** キーを押します。
15. [File] をクリックし、[Add/Remove] スナップインをクリックします。
16. [Certificates] を選択して、[Add] をクリックします。

17. [Computer account]、[Next] の順にクリックします。

18. [Local Computer]、[Next] の順にクリックします。

19. [OK] をクリックします。
20. [Certificates (Local Computer)] と [Trusted Root Certification Authorities] フォルダを展開し、[Certificates] をクリックします。 リストから [wireless domain CA cert] を探します。 この例の CA 証明書は wireless-WIN-MVZ9Z2UMNMS-CA です。

21. 別のクライアントをさらにドメインに追加するには、この手順を繰り返します。

Microsoft Windows 2008 Server でのネットワーク ポリシー サーバのインストール

この設定では、PEAP 認証を使用してワイヤレス クライアントを認証するために、NPS を RADIUS サーバとして使用します。 Microsoft WIndows 2008 Server で NPS をインストールして設定するには、次の手順を実行します。

1. [Start] > [Server Manager] の順にクリックします。

2. [Roles] > [Add Roles] の順にクリックします。

3. [Next] をクリックします。

4. サービス [Network Policy and Access Services] を選択し、[Next] をクリックします。

5. 「Introduction to Network Policy and Access Services」に目を通し、[Next] をクリックします。

6. [Network PolicyServer] を選択し、[Next] をクリックします。

7. 確認事項を見直し、[Install] をクリックします。

   インストールの完了後、次のような画面が表示されます。

8. [Close] をクリックします。

証明書のインストール

コンピュータ証明書を NPS にインストールするには、次の手順を実行します。

1. [Start] をクリックして「**mmc**」と入力し、**Enter** キーを押します。
2. [File] > [Add/Remove Snap-in] の順にクリックします。
3. [Certificates] を選択して、[Add] をクリックします。

4. **Computer account** を選択し、**Next** をクリックします。

5. [Localcomputer] を選択し、[Finish] をクリックします。

6. [OK] をクリックし、Microsoft 管理コンソール（MMC）に戻ります。

7. [Certificates (Local Computer)] と [Personal] フォルダを展開し、[Certificates] をクリックします。

8. CA 証明書の下の空白領域を右クリックし、[All Tasks] > [Request New Certificate] の順に選択します。

9. [Next] をクリックします。

10. [Domain Controller] を選択し、[Enroll] をクリックします。

11. 証明書がインストールされたら、[Finish] をクリックします。

    これで、NPS 証明書がインストールされました。

12. 証明書の [Intended Purpose] が「**Client Authentication, Server Authentication**」になっていることを確認します。

PEAP-MS-CHAP v2 認証のネットワーク ポリシー サーバ サービスの設定

認証用に NPS を設定するには、次の手順を実行します。

1. [Start] > [Administrative Tools] > [Network Policy Server] の順にクリックします。
2. [NPS (Local)]を右クリックし、[Register server in Active Directory] を選択します。

3. [OK] をクリックします。

4. [OK] をクリックします。

5. NPS の認証、許可、アカウンティング（AAA）クライアントとしてワイヤレス LAN コントローラを追加します。
6. [RADIUS Clients and Servers] を展開します。 [RADIUS Clients] を右クリックし、[New RADIUS Client] を選択します。

7. フレンドリ名（この例では WLC）、WLC の管理 IP アドレス（この例では 192.168.162.248）、共有秘密を入力します。 WLC の設定には同じ共有秘密を使用します。

8. [OK] をクリックして、前の画面に戻ります。

9. 新しいネットワーク ポリシーをワイヤレス ユーザ用に作成します。 [Policies] を展開して [NetworkPolicies] を右クリックし、[New] を選択します。

10. このルールのポリシー名（この例では Wireless PEAP）を入力し、[Next] をクリックします。

11. このポリシーでワイヤレス ドメイン ユーザのみを許可するには、次の 3 つの条件を追加して [Next] をクリックします。

    - Windows グループ：Domain Users
    - NAS ポート タイプ：Wireless - IEEE 802.11
    - 認証タイプ：EAP

12. このポリシーと一致する接続を許可するには、[Access granted] をクリックし、[Next] をクリックします。

13. [Less secure authentication methods] の下ですべての認証方式を無効にします。

14. [Add] をクリックして [PEAP] を選択し、[OK] をクリックして PEAP を有効にします。

15. [Microsoft: Protected EAP (PEAP)] を選択し、[Edit] をクリックします。 以前作成したドメイン コントローラ証明書が [Certificate issued] ドロップダウン リストで選択されていることを確認し、[Ok] をクリックします。

16. [Next] をクリックします。

17. [Next] をクリックします。

18. [Next] をクリックします。

19. **[Finish] をクリックします。**

Active Directory へのユーザの追加

この例では、Active Directory にユーザ データベースが維持されます。 次の手順を実行して、Active Directory データベースにユーザを追加します。

1. [Active Directory Users and Computers] を開きます。 [Start] > [Administrative Tools] > [Active Directory Users and Computers] の順にクリックします。
2. [Active Directory Users and Computers] のコンソール ツリーでドメインを展開し、[Users] > [New] の順に右クリックし、[User] を選択します。
3. [New Object - User] ダイアログ ボックスでワイヤレス ユーザの名前を入力します。 この例では、[First name] フィールドに [Client1]、[User logon name] フィールドに [Client1] という

名前を使用しています。 [Next] をクリックします。

4. [New Object - User] ダイアログボックスの [Password] フィールドと [Confirm password] フィールドに任意のパスワードを入力します。 [User must change password at next logon] チェック ボックスをオフにして、[Next] をクリックします。

5. [New Object - User] ダイアログボックスで [Finish] をクリックします。

6. 追加のユーザ アカウントを作成するには、ステップ 2 ~ 4 を繰り返します。

ワイヤレス LAN コントローラと LAP の設定

この設定のワイヤレス デバイス (ワイヤレス LAN コントローラと LAP) を構成します。

RADIUS 認証の WLC の設定

NPS を認証サーバに使用するように WLC を設定します。 ユーザ クレデンシャルを外部 RADIUS サーバに転送するには、WLC を設定する必要があります。 そうすると、外部 RADIUS サーバは、ユーザのクレデンシャルを検証し、ワイヤレス クライアントにアクセス権を付与します。

セキュリティの RADIUSサーバとして NPS を追加するためにこれらのステップを **> Radius Authentication ページ**完了して下さい:

1. RADIUS認証サーバ ページを表示する コントローラ インターフェイスから **> RADIUS > 認証** 『Security』 を選択 して下さい。 [New] をクリックして、RADIUS サーバを定義します。

2. RADIUS サーバ パラメータを定義します。 RADIUS サーバ IP アドレス、共有秘密、ポート番号、サーバ ステータスなどのパラメータがあります。 [Network User] チェックボックスと [Management] チェックボックスでは、管理ユーザとネットワーク (ワイヤレス) ユーザに RADIUS ベースの認証を適用するかどうかを指定します。 この例では、IP アドレスが 192.168.162.12 である RADIUS サーバとして NPS を使用します。 [Apply] をクリックします。

WLAN でのクライアントの設定

ワイヤレス クライアントが接続するサービス セット ID (SSID) (WLAN) を設定します。 この例では、PEAP という名前の SSID を作成します。

クライアントが EAP ベースの認証（この例では PEAP-MS-CHAP v2）を実行して、暗号化メカニズムとして高度暗号化規格（AES）を使用するように、レイヤ 2 認証を WPA2 として定義します。 他の値はすべてデフォルトのままにします。

注: このドキュメントでは、WLAN を管理インターフェイスにバインドしています。 ネットワークに複数の VLAN がある場合、独立した VLAN を作成してそれを SSID にバインドすることができます。 WLC に VLAN を設定する方法については、『無線 LAN コントローラでの VLAN の設定例』を参照してください。

WLC で WLAN を設定するには、次の手順を実行します。

1. コントローラのインターフェイスで [WLANs] をクリックして、[WLANs] ページを表示します。 このページには、コントローラに存在する WLAN の一覧が表示されます。
2. 新しい WLAN を作成するには、[New] をクリックします。 WLAN の WLAN ID と WLAN SSID を入力し、[Apply] をクリックします。

3. 802.1x の SSID を設定するには、次の手順を実行します。 [General] タブをクリックし、WLAN を有効にします。

   [Security] [Layer 2] の順にタブをクリックしてレイヤ 2 セキュリティを [WPA + WPA2] に設定し、[WPA+WPA2 Parameters] の必要なチェックボックス（[WPA2 AES] など）をオンにして、認証キー管理として [802.1x] をクリックします。

   [Security] > [AAA Servers] の順にタブをクリックし、NPS の IP アドレスを [Server 1] ドロップダウン リストから選択し、[Apply] をクリックします。

ワイヤレス クライアントでの PEAP-MS-CHAP v2 認証の設定

PEAP WLAN に接続するように、Windows Zero Config ツールでワイヤレス クライアントを設定するには、次の手順を実行します。

1. タスク バーの [Network] アイコンをクリックします。 [PEAP] SSID をクリックし、[Connect] をクリックします。

2. クライアントはネットワークに接続します。

3. 接続できない場合は、WLAN に接続しなおしてみてください。 問題が解決しない場合は、トラブルシューティングのセクションを参照してください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

クライアントが WLAN に接続しない場合は、このセクションの情報を利用して設定をトラブルシューティングしてください。

802.1x 認証の障害の診断には、 **debug client** コマンドおよび Windows の [Event Viewer] という 2 つのツールを使用できます。

WLC からクライアントをデバッグしても、リソースはそれほど使用されないので、サービスには影響しません。 デバッグ セッションを開始するには、WLC のコマンドライン インターフェイス（CLI）を開き、「**debug client** *mac address*」と入力します。mac address は、接続できないワイヤレス クライアントのワイヤレス MAC アドレスです。 このデバッグの実行中に、クライアントの接続を試します。 WLC の CLI に次のように表示されます。

これは、設定の誤りによって発生する可能性がある問題の例です。 ここでは、WLC が認証状態に移行したことが WLC デバッグに示されています。つまり、WLC は NPS からの応答を待機しています。 これは一般的に、WLC または NPS で共有秘密が誤っていることを示します。 これは Windows Server Event Viewer で確認できます。 ログが見つからない場合は、NPS に要求がなされていません。

WLC デバッグから見つかる別の例はアクセス拒否です。 アクセス拒否は、NPS がクライアント クレデンシャルを受信して拒否したことを示します。 以下は、クライアントがアクセス拒否を受けた例です。

アクセス拒否を確認したら、Windows Server のイベント ログのログを確認し、NPS がクライアントにアクセス拒否で応答した理由を判断します。

認証が正常である場合は、次の例のようにクライアント デバッグでアクセス容認が表示されます。

アクセス拒否と応答タイムアウトのトラブルシューティングには、RADIUS サーバへのアクセスが必要です。 WLC はオーセンティケータとして動作し、クライアントと RADIUS サーバとの間で EAP メッセージを渡します。 アクセス拒否または応答タイムアウトで応答する RADIUS サーバは、RADIUS サービスのメーカーが検討して診断する必要があります。

注: TAC は、サードパーティ RADIUS サーバのテクニカル サポートを行いません。 ただし、一般的には RADIUS サーバのログから、クライアント要求が拒否されたり無視されたりした理由が分かります。

NPS からのアクセス拒否と応答タイムアウトをトラブルシューティングするには、サーバの Windows Event Viewer で NPS ログを見直します。

1. >イベント ビューアを開始し、**NPS ログを見る管理者 Tools > Event Viewer** 『Start』 をクリック して下さい。
2. [Custom Views] [Server Roles] > [Network Policy and Access] を展開します。

Event Viewer のこのセクションには、正常な認証とエラーになった認証の口グがあります。 このログを検討し、クライアントが認証でエラーになった理由をトラブルシューティングします。 正常な認証とエラーになった認証は、両方とも情報として表示されます。 口グをスクロールし、WLC デバッグによると認証がエラーになってアクセス拒否を受けたユーザ名を探します。

以下は、NPS がユーザ アクセスを拒否している例です。

Event Viewer で拒否の文を確認するときは、[Authentication Details] セクションを検討します。この例では、ユーザ名が誤っているために NPS がユーザ アクセスを拒否したことが分かります。

WLC が NPS から応答を受けていない場合は、NPS の Event Viewer もトラブルシューティングに役立ちます。 一般的には、NPS と WLC との間で共有秘密が誤っているために発生します。

この例では、共有秘密が誤っているため、NPS は WLC からの要求を破棄しました。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems