

ワイヤレス LAN コントローラの RADIUSサーバ フォールバック 機能を設定して下さい

TAC

Document ID: 106258

Updated: 2008 年 4 月 30 日

Contributed by Nicolas Darchis, Cisco TAC Engineer.



[PDF のダウンロード](#)

[印刷](#)

[フィードバック](#)

関連製品

- [Cisco 4400 シリーズ ワイヤレス LAN コントローラ](#)
- [Cisco 2100 シリーズ ワイヤレス LAN コントローラ](#)
- [Cisco Catalyst 3750 シリーズ統合型ワイヤレス LAN コントローラ](#)
- [Cisco Catalyst 6500 シリーズ/7600 シリーズ ワイヤレス サービス モジュール \(WiSM \)](#)
- [Cisco 2000 シリーズ ワイヤレス LAN コントローラ](#)
- [Cisco ワイヤレス LAN コントローラ モジュール](#)
- [Cisco 4100 シリーズ ワイヤレス LAN コントローラ](#)
- [+ 詳細情報](#)

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[RADIUS サーバ フォールバック機能](#)

[フォールバック モード](#)

[アクティブ モード](#)

[パッシブ モード](#)

[オフ モード](#)

[設定](#)

[CLI で RADIUSサーバ フォールバック 機能を設定して下さい](#)

[GUI で RADIUSサーバ フォールバック 機能を設定して下さい](#)

[確認](#)

[トラブルシューティング](#)

概要

この資料にワイヤレス LAN コントローラ (WLCs) で RADIUSサーバ フォールバック 機能を設定する方法を記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Lightweight アクセスポイント (LAP) および Cisco WLCs の設定の基本的な知識。
- コントロールの基本的な知識およびワイヤレスアクセスポイント プロトコル (CAPWAP) のプロビジョニング。
- ワイヤレスセキュリティ ソリューションの基本的な知識。

使用するコンポーネント

ファームウェアリリース 5.0 を実行するこの文書に記載されている情報は Cisco に 4400 WLC 基づいています。

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。

背景説明

RADIUS サーバ フォールバック機能

WLC ソフトウェア バージョンは先により 5.0 RADIUSサーバ 代替機構をサポートしません。プライマリ RADIUS サーバが使用不能になると、WLC は次にアクティブなバックアップ RADIUS サーバにフェールオーバーします。WLC は、プライマリ サーバが使用可能になっても、永続的にセカンダリ RADIUS サーバを使用し続けます。通常、プライマリ サーバはパフォーマンスが高く、優先サーバとなっています。

WLC 5.0 および それ以降 バージョンでは、WLC は RADIUSサーバ フォールバック 機能をサポートします。この機能を使用すると、プライマリ サーバが使用可能かどうかを確認し、プライマリ RADIUS サーバが使用可能になったらプライマリ サーバに切り替わるように、WLC を設定できます。これをするために WLC は RADIUSサーバのステータスをチェックするために 2 つの新しいモードを、受動態およびアクティブ、サポートします。WLC は、指定されたタイムアウト

値を過ぎると、最も優先度の高いサーバに切り替わります。

フォールバック モード

アクティブ モード

アクティブ モードでは、サーバが WLC 認証要求に応答しないとき、WLC はサーバをと同時に死者示し、次に非活動的なサーバプールにサーバを移動し、そのサーバが応答するまでプローブメッセージを定期的に送信し始める。サーバが応答する場合、WLC はアクティブなプールにデッドサーバを移動し、プローブメッセージを送信することを止めます。このモードでは、認証要求を受信すると、WLC は RADIUS サーバのアクティブなプールから最も低いインデックス (最優先) のサーバを常に選択します。

WLC はサーバが無理解なより早かったらサーバステータスを判別するためにプローブパケットを後タイムアウト (デフォルトは 300 秒です) 送信しました。

パッシブ モード

パッシブモードでは、サーバが WLC 認証要求に応答しなければ、WLC は非アクティブキューにサーバを移動し、タイマーを設定します。タイマーが切れるとき、WLC はサーバの実際のステータスに関係なくアクティブなキューにサーバを移動します。認証要求を受信すると、WLC はアクティブキューから最も低いインデックス (最優先) のサーバを選択します (この際、アクティブキューには非アクティブなサーバが含まれている場合があります)。サーバが応答しなければ WLC は非アクティブとしてそれを示し、タイマーを設定し、次の高優先順位サーバに移動します。このプロセスは、WLC がアクティブな RADIUS サーバを見つけるか、アクティブなサーバプールがなくなるまで続行されます。

WLC はサーバが無理解なより早かったらサーバがアクティブ後タイムアウトだったことを仮定します (デフォルトは 300 秒です)。それでもまだ応答がない場合、認証要求を受信すると、WLC は次のタイムアウトまで待機して再試行します。

オフ モード

オフモードでは、WLC はフェールオーバーのみサポートします。つまり、フォールバックが無効化されます。プライマリ RADIUS サーバがダウンすると、WLC は次にアクティブなバックアップ RADIUS サーバにフェールオーバーします。WLC はプライマリサーバが利用できてセカンダリ RADIUS サーバを永久に使用し続けます。

設定

CLI で RADIUSサーバ フォールバック 機能を設定して下さい

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。

WLC の RADIUSサーバ フォールバック 機能を有効にするために WLC CLI からのこれらのコマンドを使用して下さい。

最初の手順では、RADIUS サーバ フォールバックのモードを選択します。すでに述べたように、WLC ではアクティブ モードとパッシブ モードのフォールバックをサポートしています。

フォールバックのモードを選択するために、このコマンドを入力して下さい:

```
WLC1 > config radius fallback-test mode {active/passive/off}
```

- アクティブ-デッド サーバにプローブをステータスをテストするために送信します。
- 受動-最後のトランザクションに基づいてサーバステータスを設定します。
- 以外サーバ フォールバック テスト (デフォルト) をディセーブルにします。

次の手順では、アクティブ モードのプローブ間隔またはパッシブ動作モードの非アクティブ時間を指定する間隔を選択します。

間隔を設定するために、このコマンドを入力して下さい:

```
WLC1 > config radius fallback-test mode interval {180 - 3600}
```

<180 への 3600> -秒にプローブ 間隔が非アクティブ時間に入って下さい (デフォルトは 300 秒です)。

間隔は、アクティブ モード フォールバックの場合はプローブ間隔を、パッシブ モード フォールバックの場合は非アクティブ時間を指定します。

アクティブな動作モードに関しては、RADIUSサーバに送信された プローブ 要求で使用されるユーザ名を設定する必要があります。

ユーザ名を設定するために、このコマンドを入力して下さい:

```
WLC1 >config radius fallback-test username {username}
```

<username> - 16 の英数字まで名前を入力して下さい (デフォルトは Cisco プローブです)。

注: 独自のユーザ名を入力しても、デフォルトのままにしておいてもかまいません。デフォルトのユーザ名は「Cisco プローブ」です。プローブ メッセージを送信するのにこのユーザ名が使用されているのでパスワードを設定する必要はありません。

GUI で RADIUSサーバ フォールバック 機能を設定して下さい

GUI で WLC を設定するためにこれらのステップを完了して下さい:

1. RADIUSサーバ フォールバックのモードを設定して下さい。これをするために、WLC GUI から **> RADIUS > フォールバック 『Security』** を選択して下さい。[RADIUS] > [Fallback Parameters] ページが表示されます。
2. フォールバック モード ドロップダウン リストから、フォールバックのモードを選択して下さい。利用可能な オプションはアクティブが、受動態、含まれ。アクティブなフォールバック モードの設定のためのスクリーン ショット例はここにあります

:



3. アクティブ動作モードの場合、[Username] フィールドにユーザ名を入力します。
4. プローブ間隔値を [Interval in sec.] フィールドにフィールドの URL のみが置換されます。
5. [Apply] をクリックします。

積極的なフェールオーバー機能が WLC で有効になる場合、WLC は "not responding" として AAA サーバを示すには余りにも積極的です。AAA サーバが可能性のあるその特定のクライアントにだけ敏感ではないのでこれがどんなにすべきではなくても、無声廃棄をする場合。有効な証明書を持つ他の有効なクライアントへの応答である可能性があります。WLC はまだ "not responding" として「」機能 AAA サーバを示し。

これを解決するには、アグレッシブ フェールオーバー機能を無効にします。これを行うためにコントローラ GUI から **config 半径積極的フェールオーバー disable** コマンドを入力して下さい。この機能を無効にすると、コントローラは、連続して 3 つのクライアントが RADIUS サーバからの応答の受信に失敗した場合にのみ、次の AAA サーバにフェールオーバーします。

確認

ここでは、設定が正常に動作していることを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の **show** コマンドがサポートされています。OIT を使用して、**show** コマンド出力の解析を表示できます。

フォールバック設定を確認するために **show radius summary** コマンドを入力して下さい。次に例を示します。

```
WLC1 >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Type..... IP Address
Aggressive Failover..... Enabled
Keywrap..... Disabled
```

```
Fallback Test:
```

```
Test Mode..... Active
Probe User Name..... testaccount
Interval (in seconds)..... 180
```

```
Authentication Servers
```

```
Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
-----
1 NM 10.1.1.12 1812 Enabled 2 Disabled Disabled-none/unknown/group-0/0 none/none
```

```
Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
-----
1 N 10.1.1.12 1813 Enabled 2 N/A Disabled-none/unknown/group-0/0 none/nonen
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

注: [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- デバッグして下さい dot1x イベント イネーブル- 802.1X イベントのデバッグを設定します。
- デバッグ AAA イベント イネーブル-すべての AAA イベントのデバッグを設定します。

関連情報

- [WLAN Controller \(WLC \) での EAP 認証の設定例](#)
- [Wireless LAN Controller \(WLC \) への Lightweight AP \(LAP \) の登録](#)
- [セキュリティ ソリューションの設定](#)
- [RADIUS LAN VLAN 設定例](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)

このドキュメントは有用でしたか。 [はい いいえ](#)

フィードバックいただき、ありがとうございました。

[サポート ケースのオープン](#) ([シスコ サービス契約 < ts generic='1' nval='P%1,2%%'が必要ですよ](#))。

Cisco サポート コミュニティ - 特集対話

[Cisco サポート コミュニティ](#)では、フォーラムに参加して情報交換することができます。

このドキュメントで使用されている表記法の詳細は、『[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。

Updated: 2008 年 4 月 30 日

Document ID: 106258