

Document ID: 118703

Updated: 2015 年 1 月 05 日

アーロン レオナルド、Shankar Ramanathan、および Jesse Dubois によって貢献される、Cisco TAC エンジニア。



[PDF のダウンロード](#)



[印刷](#)

[\[+\] フィードバック](#)

## 関連製品

- [ワイヤレス LAN \( WLAN \)](#)
- [802.1X](#)

## 目次

### [概要](#)

#### [観察される現象](#)

1. [RADIUS パフォーマンスを監視して下さい](#)
2. [WLC は Msglogs の RADIUS キューを十分に見ます](#)
3. [デバッグ AAA](#)
4. [RADIUSサーバは余りに使用中で、応答しません](#)

#### [最良の方法調整](#)

#### [WLC 側調整](#)

#### [Cisco サポート コミュニティ - 特集対話](#)

## 概要

この資料は AireOS ワイヤレス LAN コントローラ ( WLC ) のような大規模なワイヤレス配備に Cisco Identity Services Engine ( ISE ) または Cisco Secure Access Control Server ( ACS ) を RADIUS を基本設定ガイドラインの簡潔な概要に与えたものです。この資料はすばらしい技術的詳細が付いている他の文書を参照します。

## 観察される現象

通常大学環境はこの認証、許可、アカウントिंग ( AAA ) 溶解状態に出会います。このセクションはこの環境で目撃される通常現象/ログを記述します。

## 1. RADIUS パフォーマンスを監視して下さい

Dotx クライアントに認証を受ける多くの再試行を用いる大きい遅延が生じます。

コマンドを表示します半径 auth 統計情報 ( GUI を使用して下さい: [モニタ > 統計情報 > RADIUSサーバ](#) ) 問題を探すため。具体的には多数の再試行、リジェクトおよびタイムアウトを探して下さい。次に例を示します。

次を調査します。

- 高い再試行: 最初要求 比率 ( 10% 以下あるはず )
- 高いリジェクト: 比率を受け入れて下さい
- 高いタイムアウト: 最初要求 比率 ( 5% 以下あるはず )

問題がある場合、をチェックして下さい:

- 不適切に設定されたクライアント
- WLC と RADIUSサーバ間のネットワークの到達可能性問題
- 、Active Directory ( AD ) とのような使用中なら RADIUSサーバとバックエンド データベース間の問題、

## 2. WLC は Msglogs の RADIUS キューを十分に見ます

WLC は RADIUS キューについてのこのメッセージを受け取ります:

## 3.デバッグ AAA

AAA のデバッグはこのメッセージを表示します:

AAA のデバッグは AAA エラー タイムアウトを戻します ( -5 ) モバイルデバイスのために。AAAサーバは到達不能で、クライアント deauthorization に先行しています。

## 4. RADIUSサーバは余りに使用中で、応答しません

ログ システムの時刻 トラップはここにあります:

## 最良の方法調整

### WLC 側調整

- Extensible Authentication Protocol ( EAP ) - 802.1X クライアント 除外作業を作して下さい。

802.1X のためのクライアント 除外をグローバルに有効にして下さい。

少なくとも 120 秒に 802.1X ワイヤレス LAN ( WLAN ) のクライアント 除外を設定して下さい

さい。

[AireOS WLC 技術情報の 802.1X クライアント 除外](#)に記述されているように EAP タイマーを設定して下さい。

- 少なくとも 5 秒に RADIUS 再送信タイムアウトを設定して下さい。
- 少なくとも 8 時間にセッション タイムアウトを設定して下さい。
- 積極的なフェールオーバーをディセーブルにして下さい、単一不品行な振舞いをうサブリカントが WLC が RADIUSサーバの間で失敗しませんしない。
- クライアントのための高速セキュアローミングを設定して下さい。

Microsoft Windows EAP クライアント 使用 Wi-Fi によって保護されるアクセス 2 ことを確かめて下さい ( WPA2)/Advanced 暗号化 規格 ( AES ) そう彼らは日和見主義キー キャッシング ( OKC を使用できます ) 。

自身の WLAN に Apple iOS クライアントを分離できる場合その WLAN の 802.11r を有効にすることができます。

問題となる CCKM 実装がありがちであるので )、792x 電話をサポートするあらゆる WLAN のための Cisco Centralized Key Management ( CCKM ) を有効にして下さい ( しかし Microsoft Windows または Android クライアントをサポートするあらゆる Service Set Identifier ( SSID ) の CCKM を有効にしないで下さい。

マッキントッシュ オペレーティング システム ( MAC OS ) X をや Android クライアント サポートするあらゆる EAP WLAN のためのスティッキ キー キャッシング ( SKC ) を有効にして下さい。

詳細については [CUWN の 802.11 WLAN ローミングおよび高速セキュアローミング](#)を参照して下さい。

注のピーク時に WLC マスタ鍵 ( PMK ) キャッシュ 使用方法を**すべての**コマンド一対に監視して下さい。 最大 PMK キャッシュ サイズに達するか、またはその近くで得れば、おそらく SKC をディセーブルにしなければなりません。

プロファイルと ISE を使用する場合、WLC 側 DHCP/HTTP プロファイルを使用して下さい。これは RADIUS 説明パケットに容易に負荷バランシングされるプロファイリング データをラップします、エンドポイントのすべてのデータは同じ公共事業 ネットワーク ( PSN ) にアクセスするようにする。

バイト ベースの請求サービスのためにそれを必要としなかったら中間アカウントリングが消えていることを確かめて下さい。 さもなければ中間アカウントリングは追加の 利点無しだけでロードを追加します。

推奨 WLC コードを実行して下さい。

**RADIUS サーバ側の調整**ロギング比率を減らして下さい。ほとんどの RADIUSサーバはどんなロギングを保存するかについて設定可能です。 ACS が ISE が使用される場合、管理

者はどんなカテゴリーが監視データベースに記録されるか選択できます。1つの例はデータベースに、ローカルで書き込みませんデータをアカウント データが RADIUSサーバの送信され、SYSLOG のような別のアプリケーションと表示されればであるかもしれません。ISE で、ログ抑制がいつも有効にされて残ることを確認して下さい。それがトラブルシューティングを行うのにディセーブルにする必要がある場合 Administration > システム > ログイン > 収集へ行くことはバイパス抑制オプションをフィルタリングし、個々のエンドポイントまたはユーザの抑制をディセーブルにするために使用します。ISE バージョン 1.3 および それ以降では抑制をまたディセーブルにするために、エンドポイントはライブ認証ログイン順序で右クリックすることができます。

バックエンド認証 レイテンシーを低いです確認して下さい ( AD、Lightweight Directory Access Protocol ( LDAP )、Rivest、シャミール、Adleman ( RSA ) )。ACS か ISE を使用する場合両方の平均およびピーク レイテンシーのためのサーバごとの基礎のレイテンシーを監視するために、認証 要約レポートは送ることができます。が処理されるべき要求に時間がかかれば下部の 認証 レート ACS または ISE は処理できます。時間の 95% は、高いレイテンシー バックエンド データベースからの遅い応答が原因です。

ディセーブル Protected Extensible Authentication Protocol ( PEAP ) パスワード再試行。ほとんどのデバイスは PEAP トンネルの中のパスワード再試行をサポートしません、従って EAP サーバからの再試行によりデバイスは応答することを止め、新しい EAP セッションで再起動します。これによりリジェクトの代わりに EAP タイムアウトを引き起こします、つまりクライアント 除外が見つからないことを意味します。

ディセーブル未使用 EAP プロトコル。これは重要でし、EAP 交換に効率を追加し、クライアントが弱くか故意ではない EAP 方式を使用できないようにします。

イネーブル PEAP セッション レジュームおよびファーストは再接続します。

必要とされない AD に MAC 認証を送信しないで下さい。これは ISE が認証するドメイン コントローラのロードを増加するよくあるミスコンフィギュレーションです。これらは頻繁に時間のかかる原因となり、平均 待ち時間を高めます否定的な検索の。

適当ところでデバイス センサーを使用して下さい ( ISE 仕様 ) 。

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 ) 。

## 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: 2015 年 1 月 05 日

Document ID: 118703