対規模なワイヤレス RADIUS ネットワークのメルトダウンを防止する

目次

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、アカウンティング（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。

```
Server Index..................................... 2
Server Address................................... 192.168.88.1
Msg Round Trip Time.............................. 3 (msec)
First Requests................................... 1256
Retry Requests................................... 5688
Accept Responses................................. 22
Reject Responses................................. 1
Challenge Responses.............................. 96
```

```
Malformed Msgs.................................. 0
Bad Authenticator Msgs.......................... 0
Pending Requests................................ 1
Timeout Requests................................ 6824
Unknowntype Msgs................................ 0
Other Drops..................................... 0
```
次を調査します。

- 高い再試行: 最初要求比率（10% 以下あるはずです）
- 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% 以下あるはずです）

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:

```
Univ-WISM2-02: *aaa QueueReader: Dec 02 14:25:31.565: #AAA-3-3TXQUEUE_ADD_FAILED:
radius_db.c:889 Transmission queue full. Que name: Radius queue. Dropping
sessionpackets.
host = x.x.x.x.
```

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:

```
*aaaQueueReader: Dec 02 21 09:19:52.198: xx:xx:xx:xx:xx:xx Returning AAA Error
'Out of Memory' (-2) for mobile xx:xx:xx:xx:xx:xx
```
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:

```
0 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
1 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
2 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
3 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
4 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 unavailable
5 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 22) for client 68:96:7b:0e:46:7f / user 'user1@univ1.edu'
6 Wed Aug 20 15:29:57 2014 User Larry_Dull_231730 logged Out. Client MAC:84:a6:c8:
87:13:9c, Client IP:198.21.137.22, AP MAC:c0:7b:bc:cf:af:40, AP Name:Dot1x-AP
7 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
```

```
(ID 183) for client 48:d7:05:7d:93:a5 / user ' user2@univ2.edu '
8 Wed Aug 20 15:28:42 2014 RADIUS auth-server x.x.x.x:1812 unavailable
9 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 154) for client 40:0e:85:76:00:68 / user ' user1@univ1.edu '
10 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 available
11 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 unavailable
12 Wed Aug 20 15:28:41 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 99) for client 50:2e:5c:ea:e4:ba / user ' user3@univ3.edu '
13 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
14 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
15 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 30) for client b4:18:d1:60:6b:51 / user ' user1@univ1.edu '
16 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
17 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
18 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
19 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
```

最良の方法調整

WLC 側調整

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

  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。
  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要求元が WLC が RADIUSサーバの間で失敗しますことを可能にしない。

- 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 Protected Access （ WPA ） 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 ）をイネーブルにして下さい（ 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 をイネーブルにしないで下さい。

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。

802.11 詳細については CUWN の WLAN をローミングおよび高速セキュアローミング参照して下さい。

注: 提示 pmk キャッシュのピーク時に 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、またはそれの近くで得れば、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。 これは容易に負荷バランシングされる RADIUS 説明パケットにプロファイリング 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ティ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ティ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 レートを減らして下さい。 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 か ISE が使用される場合、管理者はどんなカテゴリ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、ログ抑制がいつもイネーブル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 > ロギング > 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 を使用する場合平均およびピーク レイテンシー両方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 レジュームは速く再接続し。

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）。