大規模なワイヤレス RADIUS ネットワークのメルトダウンを防止する

内容

[概要](#)
[観測された症状](#)
[1. RADIUSパフォーマンスの監視](#)
[2. WLCがMsglogsのRADIUSキューがいっぱいであることを確認する](#)
[3. AAA のデバッグ](#)
[4. RADIUSサーバがビジー状態で応答しない](#)
[チューニングのベスト プラクティス](#)
[WLC 側のチューニング](#)

概要

このドキュメントでは、大規模なワイヤレス導入環境（AireOS ワイヤレス LAN コントローラ（WLC）と RADIUS および Cisco Identity Services Engine（ISE）または Cisco Secure Access Control Server（ACS）など）の基本設定ガイドラインについて概説します。 このドキュメントでは、技術的な詳細情報については他のドキュメントを参照しています。

観測された症状

通常、認証、許可、アカウンティング（AAA ）メルトダウン状態は大学環境で発生します。このセクションでは、この環境で観測されることがよくある症状/ログについて説明します。

1. RADIUSパフォーマンスの監視

Dotx クライアントでは、認証再試行回数が多いと大幅な遅延が発生します。

問題を調べるには、**show radius auth statistics（GUI：[Monitor] > [Statistics] > [RADIUS Servers]）を使用します。**具体的には、回数の多い再試行、拒否、およびタイムアウトを検索します。以下が一例です。

```
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
```
チェック ポイント：

- 回数の多い再試行：最初の要求率（10% 以下であること）
- 回数の多い拒否：承認率
- 回数の多いタイムアウト：最初の要求率（5% 以下であること）

問題がある場合は、次の点を確認します。

- クライアントの不良構成
- WLC と RADIUS サーバ間のネットワーク到達可能性の問題
- Active Directory（AD）での場合のように、バックエンド データベースが使用されているとしたら、RADIUS サーバとバックエンド データベース間の問題

2. WLCがMsglogsのRADIUSキューがいっぱいであることを確認する

WLC で、RADIUS キューに関する次のメッセージを受信することがあります。

```
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. AAA のデバッグ

AAA のデバッグで次のメッセージが表示されることがあります。

```
*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
```
モバイル デバイスの場合、AAA をデバッグすると AAA エラー Timeout (-5) が返されることがあります。AAA サーバが到達不能になると、続いてクライアント認証が解除されます。

4. RADIUSサーバがビジー状態で応答しない

ログ システム時刻トラップは次のとおりです。

```
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
```

チューニングのベスト プラクティス

WLC 側のチューニング

- Extensible Authentication Protocol（EAP）：802.1X のクライアント除外を有効にします。

  802.1X に対してクライアント除外をグローバルに有効にします。
  802.1X ワイヤレス LAN（WLAN）で、クライアント除外を 120 秒以上に設定します。
  AireOS WLC での 802.1X クライアント除外に関する記事の説明に従って EAP タイマーを設定します。

- RADIUS 再送信タイムアウトを 5 秒以上に設定します。

- セッション タイムアウトを 8 時間以上に設定します。

- アグレッシブ フェールオーバーを無効にします。アグレッシブ フェールオーバーでは、RADIUS サーバ間の WLC 障害の原因となるサプリカントの誤動作は一切許容されません。

- クライアントの高速セキュア ローミングを設定します。

  Microsoft Windows EAP クライアントが Wi-Fi Protected Access 2（WPA2）/Advanced Encryption Standard（AES）を使用していて、Opportunistic Key Caching（OKC）を使用できることを確認します。

  Apple iOS クライアントを専用 WLAN に分離できる場合は、その WLAN で 802.11r を有効にすることができます。

  792x フォンをサポートするすべての WLAN に対して Cisco Centralized Key Management（CCKM）を有効にします。（ただし、Microsoft Windows または Android クライアントをサポートするサービス セット識別子（SSID）では CCKM を**有効にしないでください。有効にすると、CCKM 実装で問題が発生する傾向があります）。**

Macintosh オペレーティング システム（MAC OS）X や Android クライアントをサポートするすべての EAP WLAN に対して Sticky Key Caching（SKC）を有効にします。

詳細については、CUWN での 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ください。

注： show pmk-cache all コマンドを使用して、ピーク時の WLC ペアワイズ マスター キー（PMK）キャッシュ使用状況をモニタします。最大 PMK キャッシュ サイズに達した場合、またはそれに近くなった場合は、おそらく SKC を無効にする必要があります。
プロファイルで ISE を使用する場合は、WLC 側の DHCP/HTTP プロファイルを使用します。これにより、簡単にロード バランシングできる RADIUS アカウンティング パケット内にプロファイル データがまとめられるため、エンドポイントのすべてのデータが同じ Public Services Network（PSN）に到達することになります。

バイト ベースの課金サービスが必要でない限り、中間アカウンティングをオフにしてください。そうでないと、中間アカウンティングが負荷を追加するだけで、メリットはありません。

最適な WLC コードを実行します。

RADIUS サーバ側のチューニングロギング レートを低くします。ほとんどの RADIUS サーバは、保存するロギングについて設定することができます。ACS または ISE が使用されている場合、管理者はモニタリング データベースに記録するログのカテゴリを選択できます。一例として、アカウンティング データを RADIUS サーバに送信して、そのデータを SYSLOG などの別のアプリケーションで表示する場合は、ローカルでデータをデータベースに書き込まないでください。ISE では、ログ抑制が常に有効な状態を維持することを確認します。トラブルシューティングのために無効にしなければならない場合は、[Administration] > [System] > [Logging] > [Collection Filters]に移動して、[Bypass Suppression] オプションを使用して個々のエンドポイントまたはユーザで抑制を無効にします。ISE バージョン 1.3 以降では、ライブ認証ログでエンドポイントを右クリックすることで、抑制を無効にすることもできます。

バックエンド認証遅延が低いこと（AD、Lightweight Directory Access Protocol（LDAP）、Rivest、Shamir、Adleman（RSA））を確認します。 ACS または ISE を使用する場合、サーバごとに平均遅延とピーク遅延の両方をモニタするために認証サマリ レポートを実行できます。要求の処理にかかる時間が長いほど、ACS または ISE による認証処理率が低くなります。処理時間の 95% を占める遅延の原因は、バックエンド データベースからの応答が遅いことにあります。

Protected Extensible Authentication Protocol（PEAP）パスワード再試行を無効にします。ほ

とんどのデバイスは PEAP トンネル内でのパスワード再試行をサポートしないため、EAP サーバから再試行すると、デバイスが応答を停止し、新しい EAP セッションを再開します。これにより、拒否されるのではなく EAP がタイムアウトになるため、クライアント除外は有効になりません。

未使用の EAP プロトコルを無効にします。これは必須ではありませんが、EAP 交換をある程度効率化し、クライアントが弱い、または意図されていない EAP 方式を使用できないようになります。

PEAP セッション再開および高速再接続を有効にします。

必要がなければ、MAC 認証を AD に送信しないでください。これはよくある不良構成で、ISE で認証に使用するドメイン コントローラの負荷が増加することになります。これにより、検索に時間がかかり、平均遅延が増加する場合もよくあります。

該当する場合（ISE 固有）は、デバイス センサを使用します。