# 防止大规模无线RADIUS网络崩溃

## 目录

[简介](#)
[观察到的症状](#)
[1.监控RADIUS性能](#)
[2. WLC看到Msglogs上的RADIUS队列已满](#)
[3.调试AAA](#)
[4. RADIUS服务器太忙，没有响应](#)
[最佳实践调整](#)
[WLC端调整](#)

## 简介

本文档简要概述大规模无线部署的基本配置指南，例如配备思科身份服务引擎(ISE)或思科安全访问控制服务器(ACS)的AireOS无线局域网控制器(WLC)与RADIUS。 本文档参考了具有更详细技术细节的其他文档。

## 观察到的症状

通常，大学环境会遇到这种身份验证、授权和记帐(AAA)崩溃状态。本部分介绍在此环境中看到的常见症状/日志。

### 1.监控RADIUS性能

Dotx客户端在多次尝试进行身份验证时遇到了较大的延迟。

使用命令show radius auth statistics(GUI:Monitor > Statistics > RADIUS Servers)以查找问题。特别要查找大量重试、拒绝和超时。例如：

```
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
```

查找：

- 高重试：第一个请求比率（不应超过10%）
- 高拒绝：接受比率
- 高超时：第一个请求比率（不应超过5%）

如果存在问题，请检查：

- 客户端配置错误
- WLC和RADIUS服务器之间的网络连通性问题
- RADIUS服务器和后端数据库之间的问题（如果使用），例如使用Active Directory(AD)

## 2. WLC看到Msglogs上的RADIUS队列已满

WLC收到有关RADIUS队列的以下消息：

```
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.调试AAA

AAA调试显示以下消息：

```
*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的调试返回移动设备的AAA错误超时(-5)。无法访问AAA服务器，然后进行客户端取消授权。

## 4. RADIUS服务器太忙，没有响应

以下是日志系统时间陷阱：

```
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
```

# 最佳实践调整

## WLC端调整

- 可扩展身份验证协议(EAP) — 使802.1X客户端排除正常工作。
    - 为802.1X全局启用客户端排除。
    - 将802.1X无线LAN(WLAN)上的客户端排除设置为至少120秒。
    - 按照AireOS WLC上的802.1X客户端排除文章中的说明设置EAP计时器。

- 将RADIUS重新传输超时设置为至少五秒。
- 将Session-Timeout设置为至少八小时。
- 禁用主动故障转移，它不允许单个行为不当的请求方导致RADIUS服务器之间的WLC失败。
- 为客户端配置快速安全漫游。
    - 确保Microsoft Windows EAP客户端使用Wi-Fi保护访问2(WPA2)/高级加密标准(AES)，以便可以使用机会密钥缓存(OKC)。
    - 如果可以将Apple iOS客户端隔离到其自己的WLAN，则可以在该WLAN上启用802.11r。
    - 为支持792x电话的任何WLAN启用思科集中密钥管理(CCKM)(但不要在支持Microsoft Windows或Android客户端的任何服务集标识符(SSID)上启用CCKM，因为它们的CCKM实施往往存在问题)。
    - 为支持Macintosh操作系统(MAC OS)X和/或Android客户端的任何EAP WLAN启用粘滞密钥缓存(SKC)。

有关详细信息，请参阅802.11 WLAN漫游和CUWN上的快速安全漫游。

---

注意： 使用show pmk-cache all命令在峰值时间监控WLC成对主密钥(PMK)缓存的使用情况。如果您达到最大PMK缓存大小或接近该大小，则可能必须禁用SKC。

---

- 如果将ISE用于分析，则使用WLC端DHCP/HTTP分析。这会将分析数据封装到可轻松进行负载均衡的RADIUS记帐数据包中，从而确保终端的所有数据都到达同一公共服务网络(PSN)。
- 确保临时记账处于关闭状态，除非您对基于字节的计费服务需要临时记账。否则，临时会计将只会增加负荷，而不会增加额外收益。
- 运行最佳WLC代码。

## RADIUS服务器端调整

- 降低日志记录速率。大多数RADIUS服务器可配置它们将存储的日志记录。如果使用ACS或ISE，管理员可以选择将哪些类别记录到监控数据库。例如，如果从RADIUS服务器发送记账数据，并使用其他应用程序（如SYSLOG）进行查看，则不要在本地将数据写入数据库。在ISE上，确保日志抑制始终保持启用状态。如果出于故障排除目的必须禁用此功能，请转至Administration > System > Logging > Collection Filters，并使用Bypass Suppression选项以禁用单个终端或用户上的抑制。在ISE版本1.3及更高版本中，可以在实时身份验证日志中右击终端，以禁用抑制。
- 确保后端身份验证延迟较低(AD、轻量级目录访问协议(LDAP)、Rivest、Shamir、Adleman(RSA))。 如果使用ACS或ISE，可以运行身份验证摘要报告，以监控每台服务器的平均延迟和峰值延迟。处理请求的时间越长，ACS或ISE可以处理的身份验证速率越低。95%的情况下，由于后端数据库的响应缓慢，导致延迟较高。
- 禁用受保护的可扩展身份验证协议(PEAP)密码重试。大多数设备不支持在PEAP隧道内重试密码，因此EAP服务器的重试会导致设备停止响应并使用新的EAP会话重新启动。这会导致EAP超时而不是拒绝，这意味着客户端排除不会受到影响。
- 禁用未使用的EAP协议。这并不是关键因素，但确实会提高EAP交换的效率，并确保客户端无法使用较弱或无意的EAP方法。
- 启用PEAP会话恢复和快速重新连接。
- 如果不需要，请勿将MAC身份验证发送到AD。这是一种常见的配置错误，会增加ISE进行身份验证的域控制器上的负载。这通常会导致耗时的负面搜索并增加平均延迟。

- 使用设备传感器（如果适用）（特定于ISE）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。