防止大规模无线RADIUS网络熔毁

目录

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

简介

本文档简要概述大型无线部署的基本配置指南，如带RADIUS的AireOS无线局域网控制器(WLC)和思科身份服务引擎(ISE)或思科安全访问控制服务器(ACS)。 本文档引用了具有更详细技术细节的其他文档。

观察到的症状

通常，大学环境会遇到此身份验证、授权和记帐(AAA)崩溃状态。本节介绍此环境中出现的常见症状/日志。

1.监控RADIUS性能

Dotx客户体验大延迟，多次重试进行验证。

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

```
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：

- 高重试次数：第一个请求比率（不应超过10%）
- 高拒绝：接受率
- 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服务器之间的网络可达性问题
- RADIUS服务器与后端数据库（如果使用）之间的问题，例如与Active Directory(AD)

2. WLC在Msglogs上看到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)。AAA服务器无法访问，随后客户端取消授权。

4. RADIUS服务器太忙，无法响应

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。

  全局启用802.1X的客户端排除。
  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”文章中所述设置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。

- 禁用主动故障切换，这不允许单个行为不正的请求方导致WLC在RADIUS服务器之间发生故障。

- 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)，以便他们可以使用机会密钥缓存(OKC)。

  如果可以将Apple iOS客户端分离到其自己的WLAN，则可以在该WLAN上启用802.11r。

  为任何支持792x电话的WLAN启用思科集中密钥管理(CCKM)(但不在任何支持Microsoft Windows或Android客户端的服务集标识符(SSID)上启用CCKM，因为CCKM实施往往有问题)。

  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CUWN上的802.11 WLAN漫游和快速安全漫游。

  注意： 使用show pmk-cache all命令在高峰时段监控WLC成对主密钥(PMK)**缓存的使**用情况。如果达到最大PMK缓存大小，或接近它，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易于负载平衡的

RADIUS记帐数据包中，从而确保终端的所有数据都到达相同的公共服务网络(PSN)。

确保临时记帐处于关闭状态，除非您需要它来提供基于字节的计费服务。否则，临时会计只增加负载，无额外收益。

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服务器都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，如果记帐数据从RADIUS服务器发送并通过其他应用（如SYSLOG）查看，则不要将数据写入本地数据库。在ISE上，确保日志抑制始终处于启用状态。如果必须为故障排除目的禁用它，请转到**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%的时间，高延迟是由于后端数据库响应缓慢所致。

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PEAP隧道内的密码重试，因此，从EAP服务器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被命中。

禁用未使用的EAP协议。这并不重要，但会为EAP交换增加一些效率，并确保客户端不能使用弱或非预期的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。这是常见的错误配置，增加了ISE对其进行身份验证的域控制器上的负载。这通常导致负搜索耗时并增加平均延迟。

如果适用，使用设备传感器（ISE特定）。