防止大规模无线RADIUS网络融解下来

目录

简介

本文为大规模无线部署提供基本配置指南简要概述例如AireOS无线局域网控制器(WLC) RADIUS以思科身份服务引擎(ISE)或思科安全访问控制服务器(ACS)。本文参考与更加了不起的技术详细资料的其他文档。

被观察的症状

典型地大学环境遇到此验证、授权和统计(AAA)熔毁状态。此部分描述在此环境/日志目击的通常症状。

1. 箴言报RADIUS性能

Dotx客户端体验大延迟以许多重试次数验证。

请使用show radius命令**验证统计信息**(GUI ：**监视器>统计信息> RADIUS服务器**)为了寻找问题。特别地请寻找很大数量的重试次数、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：第一请求比率(应该是不大于10%)
- 高拒绝：接受比率
- 高超时：第一请求比率(应该是不大于5%)

如果有问题，请检查：

- 不正确的配置的客户端
- 在WLC和RADIUS服务器之间的网络可达性问题
- 在RADIUS服务器和后端数据库之间的问题，如果在使用中，例如与激活目录(AD)

2. WLC看到RADIUS队列全双工在Msglogs

WLC收到关于RADIUS队列的此消息：

```
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. Debug aaa

AAA调试表示此消息：

```
*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调试返回AAA错误**超时(-5)**移动设备的。AAA服务器是不可得到的和由客户端deauthorization跟随。

4. RADIUS服务器太忙碌，并且不回应

这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旁拉调整

- 可扩展的认证协议(EAP) -做802.1X客户端排除工作。

  启用客户端排除全局802.1X的。
  设置在802.1X无线LAN (WLAN)的客户端排除为至少120秒。
  设置EAP计时器正如在AireOS WLC条款的802.1X客户端排除所描述。

- 设置RADIUS重新传输超时为至少五秒。

- 设置Session-timeout为至少八个小时。

- 禁用积极的故障切换，不允许单个行为不端的请求方造成WLC失效在RADIUS服务器之间。

- 配置法塞特安全漫游您的客户端的。

  确保Microsoft Windows EAP wi-fi客户端使用受保护的访问2 (WPA2)/Advanced加密标准(AES)他们能如此使用机会主义的关键高速缓冲存储(OKC)。

  如果能分离苹果公司iOS客户端到他们自己的WLAN，则您能启用在该WLAN的802.11r。

  启用所有WLAN的Cisco Centralized Key Management (CCKM)支持792x打电话(但是请勿启用在支持Microsoft Windows或机器人客户端的任何服务集标识(SSID)的CCKM，因为他们倾向于有有问题的CCKM实施)。

  启用粘贴关键高速缓冲存储(SKC)支持麦金塔操作系统的所有EAP WLAN的(MAC OS) X并且/或者机器人客户端。

  参考漫游和法塞特安全漫游在CUWN的802.11 WLAN欲知更多信息。

  Note: 成对地监控您的WLC主密钥(PMK)缓存使用情况在高峰时间用**all命令显示的PMK缓存**。
  如果到达您的最大PMK缓存大小或者获得接近它，则您很可能将必须禁用SKC。
  如果以描出使用ISE，则请使用WLC旁拉DHCP/HTTP描出。这包裹配置文件数据到容易地负载

平衡，保证的RADIUS认为的数据包所有数据为终端到达同一公共服务网络(PSN)。

确保临时核算关闭，除非为基于字节的发单的服务需要它。否则临时认为只添加负载没有其它好处。

运行最好的WLC代码。

RADIUS服务器端的调整减少记录日志速率。多数RADIUS服务器是可配置关于什么记录日志他们将存储。如果使用ACS或ISE，管理员能选择什么类别被记录对监听数据库。一示例也许是，如果帐户数据发送RADIUS服务器并且查看与另一应用程序例如SYSLOG，然后不写数据对数据库本地。在ISE，请保证日志抑制依然是一直启用。如果必须禁用它为了实现故障排除目的，则去**管理>System >记录日志>集过滤**并且使用旁路抑制选项为了禁用在一个单个终端或用户的抑制。在ISE版本1.3和以上，终端可以按实际认证登录顺序禁用抑制用鼠标右键单击。

保证后端身份验证延迟低(AD，轻量级目录访问协议(LDAP)， Rivest，沙米尔， Adleman (RSA))。如果使用ACS或ISE，验证汇总报告可以送为了监控根据一个每服务器基本类型的延迟为平均值和高峰延迟。越很多时间它花费请求处理，更低认证速率ACS或ISE能处理。95%时间，高延迟归结于从一个后端数据库的一慢作用。

禁用Protected Extensible Authentication Protocol (PEAP)密码重试次数。多数设备不支持密码重试次数在PEAP通道里面，因此从EAP服务器的重试次数促成设备停止与一新的EAP会话的响应和重新启动。这导致EAP超时而不是拒绝，因此意味着客户端排除不会点击。

禁用未使用EAP协议。这不是关键，而是添加若干效率到EAP交换并且保证客户端不能使用一个弱或不愿意的EAP方法。

Enable (event) PEAP会话恢复和法塞特重新连接。

请勿发送MAC验证对AD，如果没需要。这是增加在域控制器的负载ISE验证的一普通的误配置。这些经常导致费时的负搜索并且增加平均时延。

请使用设备传感器哪里可适用(ISE特定)。