防止大規模無線RADIUS網路崩潰

目錄

簡介

本檔案簡要概述大規模無線部署的基本配置原則，例如使用思科身分識別服務引擎(ISE)或思科安全存取控制伺服器(ACS)且具有RADIUS的AireOS無線LAN控制器(WLC)。 本檔案會以更多技術詳細資訊引用其他檔案。

觀察到的症狀

通常大學環境會遇到這種身份驗證、授權和記帳(AAA)崩潰狀態。本節介紹在此環境中遇到的常見症狀/日誌。

1.監控RADIUS效能

Dotx客戶端在進行多次身份驗證重試後遇到較大的延遲。

使用命令**show radius auth statistics**(GUI:**Monitor > Statistics > RADIUS Servers**)以尋找問題。特別要查詢大量重試、拒絕和超時。以下是範例：

```
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
```
尋找：

- 高重試：第一個請求比率（不應超過10%）
- 高拒絕：接受比率
- 高超時：第一個請求比率（不應超過5%）

如果有問題，請檢查：

- 客戶端配置錯誤
- WLC和RADIUS伺服器之間的網路連線問題
- RADIUS伺服器和後端資料庫之間出現問題（如果使用），例如使用Active Directory(AD)

2. WLC看到Msglogs上的RADIUS佇列已滿

WLC收到有關RADIUS佇列的以下訊息：

```
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.調試AAA

AAA的偵錯顯示以下訊息：

```
*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的調試返回移動設**備的AAA錯誤超**時(-5)。AAA伺服器無法連線，接著進行使用者端解除授權。

4. RADIUS伺服器太忙，沒有響應

以下是日誌系統時間陷阱：

```
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
```

最佳實踐調整

WLC端調諧

- 可擴展身份驗證協定(EAP) — 使802.1X客戶端排除起作用。

  為802.1X全域性啟用客戶端排除。
  將802.1X無線LAN(WLAN)上的客戶端排除設定至少為120秒。
  按照AireOS WLC文章上的802.1X客戶端排除中的說明設定EAP計時器。

- 將RADIUS重新傳輸超時設定為至少五秒。

- 將Session-Timeout設定為至少8小時。

- 禁用主動故障轉移，它不允許單個行為不當的請求方導致RADIUS伺服器之間的WLC失敗。

- 為客戶端配置快速安全漫遊。

  確保Microsoft Windows EAP客戶端使用Wi-Fi保護訪問2(WPA2)/高級加密標準(AES)，以便可以使用機會金鑰快取(OKC)。

  如果您可以將Apple iOS客戶端隔離到其自己的WLAN，則可以在該WLAN上啟用802.11r。

  為支援792x電話的任何WLAN啟用Cisco集中金鑰管理(CCKM)(但不要在支援Microsoft Windows或Android客戶端的任何服務集識別符號(SSID)上啟用**CCKM，因為它們的CCKM實施往往有問題)。**

  為支援Macintosh作業系統(MAC OS)X和/或Android客戶端的任何EAP WLAN啟用粘滯金鑰快取(SKC)。

  如需詳細資訊，請參閱802.11 WLAN漫遊和CUWN上的快速安全漫遊。

  附註： 使用**show pmk-cache all**命令，在高峰時間監控WLC成對主金鑰(PMK)快取使用情況。如果您達到最大PMK快取大小或接近該大小，則可能必須禁用SKC。
  如果將ISE用於分析，則使用WLC端DHCP/HTTP分析。這會將分析資料封裝到易於負載平衡的RADIUS記帳資料包中，從而確保終端的所有資料都到達相同的公共服務網路(PSN)。

確保臨時記帳處於關閉狀態，除非您對基於位元組的計費服務需要臨時記帳。否則，臨時會計處理只會增加負荷，而不會增加額外收益。

執行最佳的WLC代碼。

RADIUS伺服器端調整降低日誌記錄速率。大多數RADIUS伺服器可配置它們要儲存的日誌記錄。如果使用ACS或ISE，管理員可以選擇記錄到監控資料庫的類別。例如，如果從RADIUS伺服器傳送記帳資料，並使用另一個應用程式（如SYSLOG）進行檢視，則不要在本地將資料寫入資料庫。在ISE上，確保日誌抑制始終處於啟用狀態。如果出於故障排除目的必須禁用此功能，請轉至**Administration > System > Logging > Collection Filters**，並使用Bypass Suppression選項禁用單個終端或使用者上的抑制。在ISE版本1.3及更高版本中，可以在即時身份驗證日誌中按一下右鍵一個終端以禁用抑制。

確保後端身份驗證延遲較低(AD、輕量級目錄訪問協定(LDAP)、Rivest、Shamir、Adleman(RSA))。 如果使用ACS或ISE，可以運行身份驗證摘要報告，以便按伺服器監控平均延遲和峰值延遲。處理請求的時間越長，ACS或ISE可以處理的身份驗證速率越低。95%的情況下，由於後端資料庫的響應緩慢，導致出現高延遲。

禁用受保護的可擴展身份驗證協定(PEAP)密碼重試。大多數裝置不支援在PEAP隧道內進行密碼重試，因此EAP伺服器的重試會導致裝置停止響應，並使用新的EAP會話重新啟動。這會導致EAP超時而不是拒絕，這意味著客戶端排除將不會被命中。

禁用未使用的EAP協定。這並不是關鍵，但確實會為EAP交換增加一些效率，並確保客戶端無法使用弱或無意的EAP方法。

啟用PEAP會話恢復和快速重新連線。

如果不需要，請勿將MAC身份驗證傳送到AD。這是一種常見的配置錯誤，會增加ISE進行身份驗證的域控制器上的負載。這通常會導致耗時的負搜尋並增加平均延遲。

使用裝置感測器（如果適用）（特定於ISE）。