使用EEM指令碼診斷間歇性RADIUS伺服器故障

目錄

簡介

本文檔介紹如何對ASA中標籤為失敗的RADIUS伺服器進行故障排除，以及這如何導致客戶端基礎設施中斷。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA上的基本感知或EEM指令碼

採用元件

本文件所述內容不限於特定軟體和硬體版本。

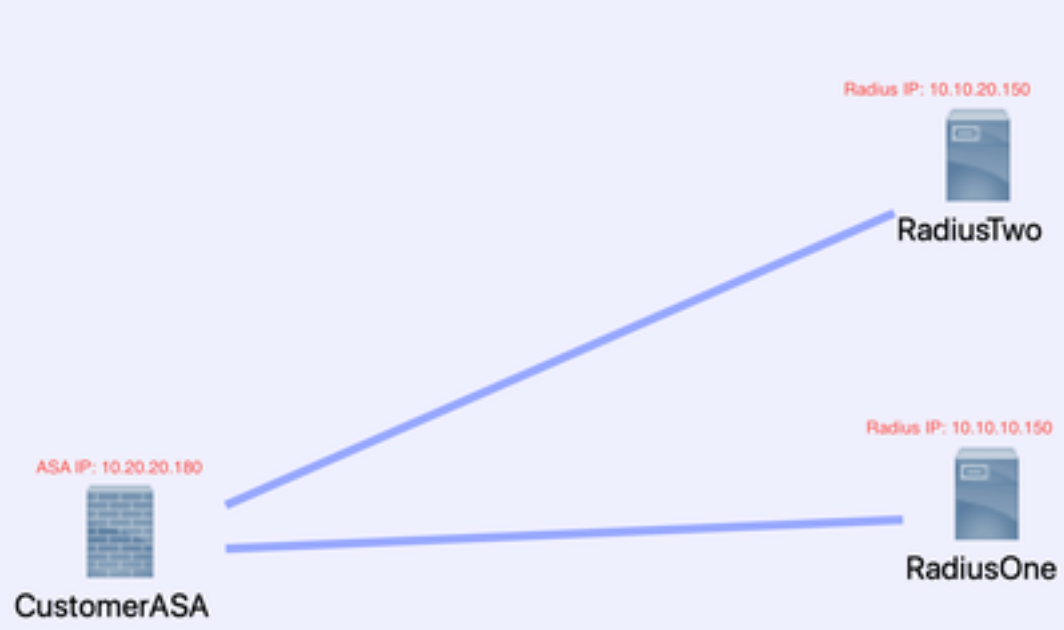
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

在Cisco ASA中，RADIUS伺服器標籤為失敗/失效。問題是間歇性的，但會導致客戶端基礎架構中斷。TAC必須區分這是ASA問題、資料路徑問題還是Radius伺服器問題。如果在發生故障時捕獲資料包，它會排除Cisco ASA，因為它會判斷ASA是否將資料包傳送到RADIUS伺服器，以及是否收到這些資料包。

拓撲

在本例中，這是使用的拓撲：



要解決此問題，請執行以下步驟。

第1步：配置資料包捕獲和應用訪問清單以捕獲伺服器之間的資料包

第一步是配置資料包捕獲和適用的訪問清單，以捕獲ASA和RADIUS伺服器之間的資料包。

如需封包擷取方面的協助，請參閱封包擷取組態產生器和分析器。

access-list TAC extended permit ip host 10.20.20.180 host 10.10.10.150

access-list TAC extended permit ip host 10.10.10.150 host 10.20.20.180

access-list TAC extended permit ip host 10.20.20.180 host 10.10.20.150

access-list TAC extended permit ip host 10.10.20.150host 10.20.20.180

capture RADIUS type raw-data access-list TAC buffer 30000000 interface inside circular-buffer

> **註**：您需要檢查緩衝區大小，以確保它不會過滿，並且不會產生過多的資料。緩衝區大小1000000足夠。請注意，示例緩衝為3000000。

第2步：配置EEM指令碼

接下來，配置EEM指令碼。

此示例使用113022的系統日誌ID，並且可以在許多其他系統日誌消息中觸發EEM:

ASA的消息型別可在Cisco Secure Firewall ASA Series Syslog Messages中找到。

此案例中的觸發因素為：

Error Message %ASA-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED

其 ASA 已嘗試向AAA伺服器發出身份驗證、授權或記帳請求，並且在配置的超時視窗中未收到響應。然後，AAA伺服器被標籤為發生故障，並從服務中刪除。

事件管理器小程式ISE_Radius_Check

事件系統日誌id 113022

action 0 cli命令"show clock"

action 1 cli命令"show aaa-server ISE"

action 2 cli命令"aaa-server ISE active host 10.10.10.150"

action 3 cli命令"aaa-server ISE active host 10.10.20.150"

action 4 cli命令"show aaa-server ISE"

操作5 cli命令「show capture radius decode dump」

輸出檔案附加disk0:/ISE_Recover_With_Cap.txt

EEM指令碼說明

事件管理器小程式ISE_Radius_Check。 — *您為eem指令碼命名。*

event syslog id 113022 — *您的觸發器：（參見先前說明）*

action 0 cli命令"show clock" — *在故障排除時捕獲準確時間戳的最佳實踐，以便與客戶端可以具有的其他日誌進行比較。*

action 1 cli命令"show aaa-server ISE" — *此命令顯示aaa-server組的狀態。在這種情況下，該組稱為ISE。*

action 2 cli command "aaa-server ISE active host 10.10.10.150" — *此命令使用該IP「恢復」aaa伺服器。這麼做可讓您繼續嘗試radius封包以確定資料路徑錯誤。*

action 3 cli command "aaa-server ISE active host 10.10.20.150" — *參見上一命令說明。*

action 4 cli命令「show aaa-server ISE」。 - — *此命令驗證伺服器是否恢復。*

action 5 cli命令"show capture radius decode dump" — *現在可對資料包捕獲進行解碼/轉儲。*

輸出檔案append disk0:/ISE_Recover_With_Cap.txt — *此捕獲現在儲存在ASA上的文本檔案中，新結果將附加到結尾。*

最終步驟

最後，您可以將此資訊上傳到Cisco TAC案例，或使用該資訊來分析流量中的最新封包，並弄清楚

RADIUS伺服器標籤為失敗的原因。

文本檔案可以解碼，並在前面提到的封包擷取組態產生器和分析器上轉為pcap。

真實世界示例

在下一個範例中，RADIUS流量的擷取會過濾掉。您會看到ASA是以。180結尾的裝置，而RADIUS伺服器以。21結尾

在本範例中，*兩個RADIUS*伺服器都傳回「連線埠無法連線」，一列中的每一台傳回3次。這將觸發ASA將兩個*RADIUS服*務器標籤為彼此在毫秒內的停機。

結果

本示例中的每個。21地址都是F5 VIP地址。這意味著VIPS後面是PSN角色中的思科ISE節點集群。

由於F5缺陷，F5返回「埠無法訪問」。

在本示例中，Cisco TAC團隊成功證明了ASA工作正常。也就是說，它傳送了radius資料包並接收了3個之前無法訪問的埠，並影響了Radius伺服器標籤為失敗：

99	329.426964	10.242.253.180	10.242.230.21	RADIUS	700	Accounting-Request id=233
100	329.427117	10.242.253.180	10.242.230.21	RADIUS	692	Accounting-Request id=234
101	329.443877	10.242.230.21	10.242.253.180	RADIUS	66	Accounting-Response id=233
102	329.445899	10.242.230.21	10.242.253.180	RADIUS	66	Accounting-Response id=234
103	329.508366	10.242.253.180	10.242.230.21	RADIUS	720	Access-Request id=235
104	329.510624	10.242.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
105	329.511527	10.242.253.180	10.242.230.21	RADIUS	720	Access-Request id=236
106	329.513279	10.242.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
107	329.513737	10.242.253.180	10.242.230.21	RADIUS	720	Access-Request id=237
108	329.515598	10.242.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
109	329.516330	10.242.253.180	10.250.230.21	RADIUS	720	Access-Request id=238
110	329.521304	10.250.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
111	329.526538	10.242.253.180	10.250.230.21	RADIUS	720	Access-Request id=239
112	329.531146	10.250.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
113	329.536807	10.242.253.180	10.250.230.21	RADIUS	720	Access-Request id=240
114	329.541231	10.250.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
115	347.373134	10.242.253.180	10.242.230.21	RADIUS	688	Access-Request id=242
116	349.486086	10.242.230.21	10.242.253.180	RADIUS	214	Access-Accept id=242
117	349.487630	10.242.253.180	10.242.230.21	RADIUS	614	Access-Request id=243
118	349.548174	10.242.230.21	10.242.253.180	RADIUS	218	Access-Accept id=243

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。