EEMスクリプトを使用した断続的なRADIUSサーバ障害のトラブルシューティング

内容

概要

このドキュメントでは、ASAで障害が発生したとマークされたRADIUSサーバをトラブルシューティングする方法と、これがクライアントインフラストラクチャの停止を引き起こす方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco ASAでの基本的な認識またはEEMスクリプト

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

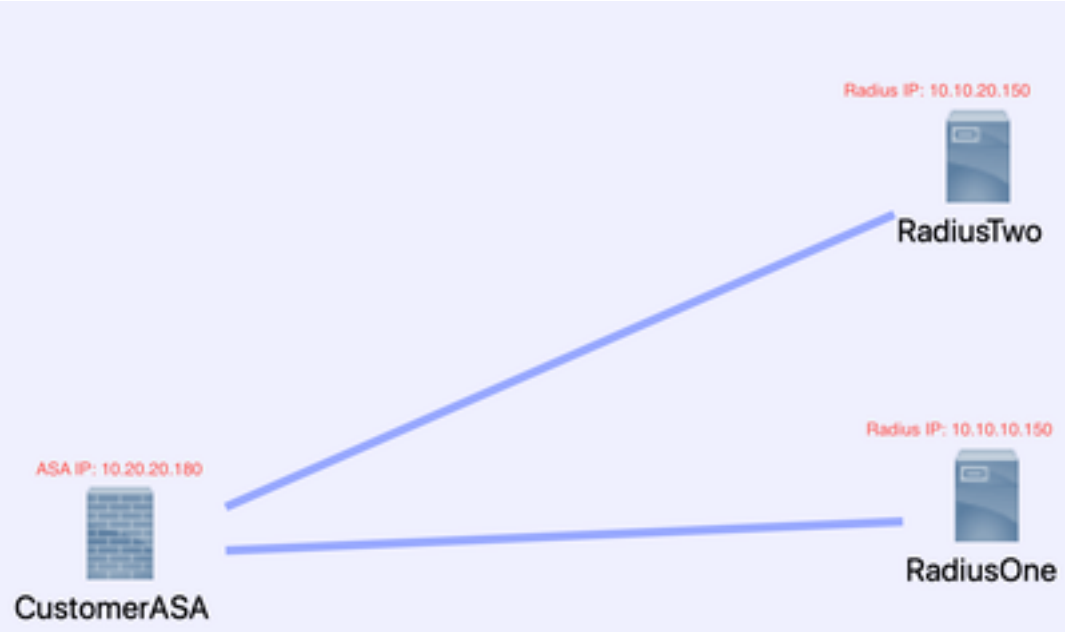
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

RADIUSサーバは、Cisco ASAで障害が発生したか停止したとしてマークされます。この問題は断続的に発生しますが、クライアントインフラストラクチャの停止を引き起こします。TACは、これがASAの問題、データパスの問題、またはRADIUSサーバの問題のいずれであるかを区別する必要があります。障害発生時にキャプチャが行われると、ASAがパケットをRADIUSサーバに送信するかどうかと、そのパケットが受信されたかによって、Cisco ASAは除外されます。

トポロジ

この例では、次のトポロジが使用されます。



この問題を解決するには、次の手順を実行します。

ステップ1：サーバ間のパケットをキャプチャするためのパケットキャプチャと適用可能なアクセスリストの設定

最初のステップでは、ASAサーバとRADIUSサーバの間のパケットをキャプチャするように、パケットキャプチャと適用可能なアクセスリストを設定します。

パケットキャプチャに関するサポートが必要な場合は、『パケットキャプチャ設定ジェネレータとアナライザ』を参照してください。

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

注：バッファサイズをチェックして、バッファサイズが過充填されておらず、データが処理されていることを確認する必要があります。バッファサイズは1000000で十分です。この例のバッファは3000000であることに注意してください。

ステップ2:EEMスクリプトの設定

次に、EEMスクリプトを設定します。

この例では、Syslog IDとして113022を使用しており、他の多くのSyslogメッセージでEEMをトリガーできます。

ASAのメッセージタイプについては、『Cisco Secure Firewall ASAシリーズsyslogメッセージ』を参照してください。

このシナリオのトリガーは次のとおりです。

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

「 ASA はAAAサーバに対して認証、認可、またはアカウンティング要求を試行しましたが、設定されたタイムアウトウィンドウ内に応答を受信しませんでした。その後、AAAサーバは障害としてマークされ、サービスから削除されます。

event manager applet ISE_Radius_Check

event syslog id **113022**

action 0 cliコマンド「show clock」

アクション1 cliコマンド「show aaa-server ISE」

アクション2 cliコマンド「aaa-server ISE active host 10.10.10.150」

アクション3 cliコマンド「aaa-server ISE active host 10.10.20.150」

アクション4 cliコマンド「show aaa-server ISE」

アクション5 cliコマンド「show capture radius decode dump」

出力ファイルappend disk0:/ISE_Recover_With_Cap.txt

EEMスクリプトの説明

イベントマネージャアプレットISE_Radius_Check。*— eemスクリプトに名前を付けます。*

event syslog id **113022**：トリガー：（前の説明を参照）

action 0 cliコマンド「show clock」*：クライアントが保持できる他のログと比較するためにトラブルシューティングを行う際に、正確なタイムスタンプをキャプチャするためのベストプラクティスです。*

アクション1 cliコマンド「show aaa-server ISE」*:aaa-serverグループのステータスを表示します。この場合、そのグループはISEと呼ばれます。*

アクション2 cliコマンド「aaa-server ISE active host 10.10.10.150」*：このコマンドは、その IPを使用してaaaサーバを「起動」することです。これにより、引き続きRADIUSパケットを試行してデータパスエラーを判別できます。*

アクション3 cliコマンド「aaa-server ISE active host 10.10.20.150」*：前のコマンドの説明を参照してください。*

アクション4 cliコマンド「show aaa-server ISE」。 – このコマンドは、サーバがバックアップされたかどうかを確認します。

アクション5 cliコマンド「show capture radius decode dump」*：パケットキャプチャをデコード/ダンプします。*

output file append disk0:/ISE_Recover_With_Cap.txt*：このキャプチャはASA上のテキストファイルに保存され、新しい結果が末尾に追加されます。*

最後の段階

最後に、この情報をCisco TACケースにアップロードするか、この情報を使用してフロー内の最新パケットを分析し、RADIUSサーバが障害としてマークされている理由を突き止めることができます。

テキストファイルは、前述のPacket Capture Config Generator and Analyzerでデコードしてpcapに変換できます。

実際の例

次の例では、RADIUSトラフィックのキャプチャをフィルタリングして除外します。ASAは。180で終わるデバイスで、RADIUSサーバは。21で終わることがわかります

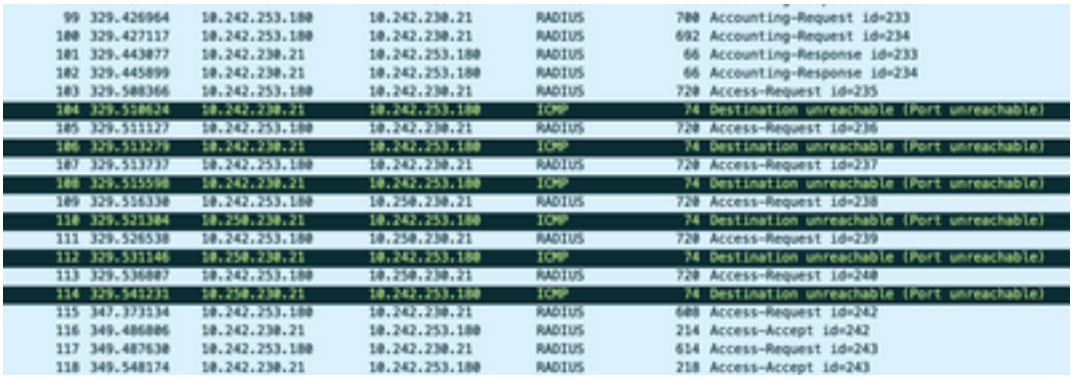
この例では、*両方*のRADIUSサーバが「port unreachable」を返します。これは、各サーバに対して3回連続して返されます。これにより、ASAがトリガーされ、両方のRADIUSサーバが*dead*として相互にミリ秒以内にマークされます。

結果

この例の各。21アドレスはF5 VIPアドレスです。つまり、VIPの背後には、PSNペルソナ内のCisco ISEノードのクラスタが存在します。

F5は、F5ポートが原因で「ポート到達不能」を返しました(F5不具合)。

この例では、Cisco TACチームはASAが期待どおりに動作していることを正しく証明しました。つまり、RADIUSパケットを送信し、以前に到達不能だった3つのポートを受信し、「failed」とマークされたRADIUSサーバに影響を与えました。



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	329.511127	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	329.521384	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	608	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

関連情報

- [シスコテクニカルサポートおよびダウンロード]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。