EEM-Skript zur Fehlerbehebung bei unregelmäßigen RADIUS-Serverausfällen verwenden

Inhalt

Einleitung

Dieses Dokument beschreibt die Fehlerbehebung bei einem RADIUS-Server, der in ASA als ausgefallen markiert wurde, und erläutert, wie dies zu Ausfällen in der Client-Infrastruktur führen kann.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Bewusstsein für EEM-Scripting auf der Cisco ASA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

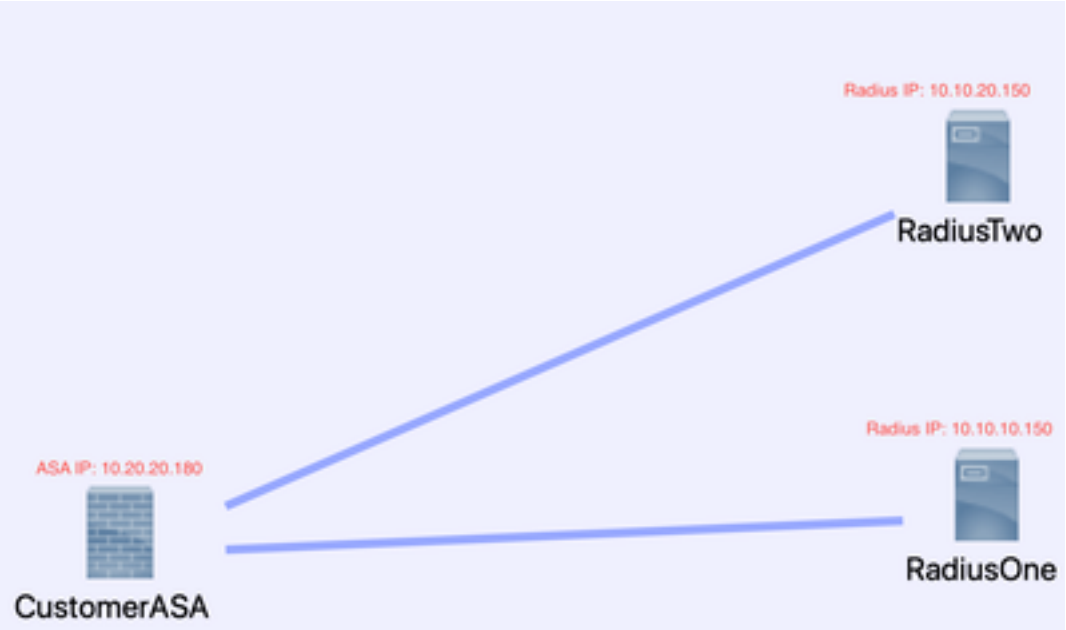
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Problem

RADIUS-Server werden in der Cisco ASA als ausgefallen/ausgefallen markiert. Das Problem tritt nur gelegentlich auf, verursacht jedoch Ausfälle in der Client-Infrastruktur. Das TAC muss unterscheiden, ob es sich um ein ASA-, Data Path- oder Radius Server-Problem handelt. Wenn eine Erfassung zum Zeitpunkt des Ausfalls durchgeführt wird, schließt dies die Cisco ASA aus, da sie erkennt, ob die ASA die Pakete an den RADIUS-Server sendet und ob sie im Gegenzug empfangen werden.

Topologie

In diesem Beispiel wird die folgende Topologie verwendet:



Führen Sie die folgenden Schritte aus, um dieses Problem zu beheben.

Schritt 1: Konfigurieren der Paketerfassung und der anwendbaren Zugriffslisten, um Pakete zwischen Servern zu erfassen

Der erste Schritt besteht in der Konfiguration der Paketerfassung und anwendbarer Zugriffslisten, um Pakete zwischen ASA- und RADIUS-Servern zu erfassen.

Wenn Sie Hilfe bei der Paketerfassung benötigen, lesen Sie den Abschnitt Paketerfassungs-Konfigurationsgenerator und -analysator.

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

Erfassen der RADIUS-Typ-RAW-Daten-Zugriffsliste TAC-Puffer 30000000-Schnittstelle im

Ringpuffer

> **Hinweis**: Sie müssen die Puffergröße überprüfen, um sicherzustellen, dass sie nicht überfüllt wird und die Daten nicht überfüllt werden. Eine Puffergröße von 1000000 ist ausreichend. Beachten Sie, dass unser Beispielpuffer 3000000 ist.

Schritt 2: EEM-Skript konfigurieren

Konfigurieren Sie anschließend das EEM-Skript.

In diesem Beispiel wird die Syslog-ID 113022 verwendet. Sie können EEM auch für viele andere Syslog-Meldungen auslösen:

Die Meldungsarten für ASA finden Sie unter Cisco Secure Firewall ASA Series Syslog Messages (Syslog-Meldungen der ASA-Serie).

Der Auslöser in diesem Szenario ist:

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

Die Fehlermeldung ASA hat eine Authentifizierungs-, Autorisierungs- oder Accounting-Anfrage an den AAA-Server gesendet und innerhalb des konfigurierten Zeitüberschreitungsfensters keine Antwort erhalten. Der AAA-Server wird dann als ausgefallen markiert und aus dem Dienst entfernt.

Event Manager-Applet ISE_Radius_Check

Ereignis-Syslog-ID **113022**

action 0 cli-Befehl "show clock"

action 1 cli-Befehl "show aaaa-server ISE"

action 2 cli-Befehl "aaa-server ISE active host 10,10.10,150"

action 3 cli-Befehl "aaa-server ISE active host 10,10.20,150"

action 4 cli-Befehl "show aaaa-server ISE"

action 5 cli-Befehl "show capture radius decode dump"

Ausgabedatei anhängen disk0:/ISE_Recover_With_Cap.txt

EEM-Skript - Erläuterung

Event Manager-Applet ISE_Radius_Check. - *Sie nennen Ihr EEM-Skript.*

event syslog id **113022** - *Ihr Auslöser: (siehe vorherige Erklärung)*

action 0 cli-Befehl "show clock*": Best Practices zur Erfassung genauer Zeitstempel bei der Fehlerbehebung, um Vergleiche mit anderen Protokollen anzustellen, die der Client haben kann.*

action 1 cli-Befehl "show aaa-server ISE" - *Zeigt den Status unserer aaa-server-Gruppe an. In diesem Fall heißt diese Gruppe ISE.*

action 2 cli-Befehl "aaa-server ISE active host 10.10.10.150" - *Mit diesem Befehl wird der aaa-server mit dieser IP wieder aktiviert. Auf diese Weise können Sie weiterhin versuchen, RADIUS-Pakete zur Ermittlung von Datenpfadfehlern zu verwenden.*

action 3 cli-Befehl "aaa-server ISE active host 10.10.20.150" - *Siehe vorherige Befehlsbeschreibung.*

action 4 cli-Befehl "show aaa-server ISE". --*Mit diesem Befehl wird überprüft, ob die Server wieder aktiviert wurden.*

action 5 cli-Befehl "show capture radius decode dump*": Decodierung/Dump der Paketerfassung*

Ausgabedatei anhängen disk0:/ISE_Recover_With_Cap.txt - *Diese Erfassung wird jetzt in einer Textdatei auf der ASA gespeichert und neue Ergebnisse werden an das Ende angehängt.*

Abschließende Schritte

Schließlich können Sie diese Informationen in ein Cisco TAC-Ticket hochladen oder die Informationen verwenden, um die neuesten Pakete im Datenfluss zu analysieren und herauszufinden, warum die RADIUS-Server als ausgefallen markiert sind.

Die Textdatei kann mit dem zuvor erwähnten Packet Capture Config Generator und Analyzer entschlüsselt und in ein pcap umgewandelt werden.

Beispiel aus der Praxis

Im nächsten Beispiel wird die Erfassung für RADIUS-Datenverkehr herausgefiltert. Wie Sie sehen, endet die ASA mit .180 und der RADIUS-Server mit .21.

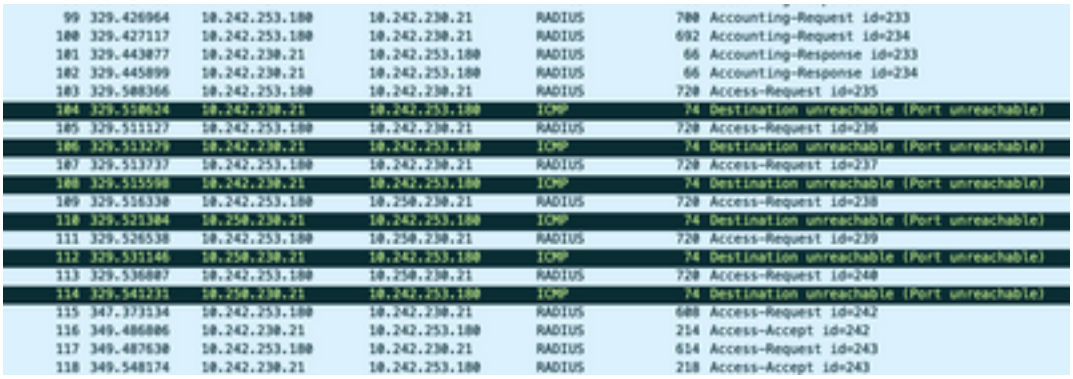
In diesem Beispiel geben *beide* RADIUS-Server dreimal hintereinander den Ausdruck "port unreachable" (Port nicht erreichbar) zurück. Dadurch wird die ASA veranlasst, *beide* RADIUS-Server innerhalb von Millisekunden als ausgefallen zu markieren.

Ergebnis

Jede .21-Adresse in diesem Beispiel war eine F5-VIP-Adresse. Das bedeutet, dass sich hinter dem VIPS Cluster von Cisco ISE-Knoten in der PSN-Rolle befanden.

Die F5 gab aufgrund eines F5-Defekts "port unreachable" (Port nicht erreichbar) zurück.

In diesem Beispiel hat das Cisco TAC-Team erfolgreich bewiesen, dass die ASA wie erwartet funktioniert. Dies bedeutet, dass RADIUS-Pakete gesendet und 3 Ports empfangen wurden, die zuvor nicht erreichbar waren, und dass der als fehlerhaft markierte RADIUS-Server ausgelöst wurde:



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

Zugehörige Informationen

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.