EEMscripts gebruiken om intermitterende RADIUS-serverfouten op te lossen

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met een RADIUS-server die is gemarkeerd als mislukt in ASA en hoe dit storingen kan veroorzaken voor de clientinfrastructuur.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis bewustzijn voor EM-scripting op Cisco ASA

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

RADIUS-servers worden in Cisco ASA als mislukt/dood gemarkeerd. Het probleem is intermitterend maar veroorzaakt stroomstoringen voor de cliëntinfrastructuur. TAC moet onderscheiden of dit een ASA-, Data Path- of Radius Server-kwestie is. Als een opname wordt gemaakt op het moment van mislukking, sluit het Cisco ASA uit omdat het onderkent of de ASA de pakketten naar de RADIUS-server stuurt en of ze als tegenprestatie worden ontvangen.

Topologie

Dit is bijvoorbeeld de topologie die wordt gebruikt:

Voer de volgende stappen uit om dit probleem op te lossen.

Stap 1: Configureer pakketvastlegging en toepasbare toegangslijsten om pakketten tussen servers op te nemen

De eerste stap is het configureren van Packet Capture en toepasbare toegangslijsten om pakketten tussen de ASA- en RADIUS-servers op te nemen.

Als u hulp nodig hebt bij Packet Capture, raadpleegt u de Packet Capture Config-generator en -analyzer.

access-list TAC uitgebreide vergunning ip host 10.20.20.180 host 10.10.10.150

access-list TAC uitgebreide vergunning ip host 10.10.10.150 host 10.20.20.180

access-list TAC uitgebreide vergunning ip host 10.20.20.180 host 10.10.20.150

access-list TAC uitgebreide vergunning ip host 10.10.20.150host 10.20.20.180

Capture RADIUS-type onbewerkte gegevens-toegangslijst TAC-buffer 30000000 interface binnen circulaire-buffer

> **Opmerking**: u moet de buffergrootte controleren om te verzekeren dat deze niet overvult en de gegevens doet. Een buffergrootte van 1000000 is voldoende. Merk op dat onze

voorbeeldbuffer 3000000 is.

Stap 2: EM-script configureren

Configureer vervolgens het EEM-script.

Dit voorbeeld gebruikt de Syslog ID van 113022 en u kunt EEM activeren op vele andere Syslog-berichten:

De berichttypen voor ASA zijn te vinden op Cisco Secure Firewall ASA Series Syslog-berichten.

De trigger in dit scenario is:

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

Het ASA heeft een verificatie-, autorisatie- of accountingverzoek aan de AAA-server geprobeerd en heeft geen antwoord ontvangen binnen het geconfigureerde time-outvenster. De AAA-server wordt vervolgens gemarkeerd als mislukt en uit de service verwijderd.

```
Event Manager applet ISE_Radius_Check
 gebeurtenis syslog id 113022
 actie 0 cli, opdracht "Toon klok"
 actie 1 cli opdracht "aaa-server ISE tonen"
 actie 2 cli opdracht "aaa-server ISE active host 10.10.10.150"
 actie 3 cli opdracht "aaa-server ISE active host 10.10.20.150"
 actie 4 cli opdracht "aaa-server ISE tonen"
 actie 5 cli commando "show Capture radius decode dump"
 uitvoerbestand toegevoegd op schijf0:/ISE_Recover_With_Cap.txt
```

EEMScript-uitleg

Event Manager applet ISE_Radius_Check. —*Je noemt je emscript.*

event syslog id 113022 —*Uw trigger: (zie eerdere uitleg)*

actie 0 cli opdracht "toon klok" —*best practices om nauwkeurige tijdstempels te vastleggen terwijl het probleemoplossing om te vergelijken met andere logbestanden die de client kan hebben.*

actie 1 cli commando "toon aaa-server ISE" — *Dit toont de status van onze aaa-server groep. In dit geval heet die groep ISE.*

actie 2 cli opdracht "aaa-server ISE active host 10.10.10.150" — *Deze opdracht is om de aaa-server met die IP "terug te brengen". Dit stelt u in staat om te blijven proberen radius pakketten om datapath fouten te bepalen.*

actie 3 cli opdracht "aaa-server ISE active host 10.10.20.150" *—Zie vorige opdrachtuitleg.*

actie 4 cli opdracht "toon aaa-server ISE". *--Deze opdracht controleert of de servers back-up hebben gemaakt.*

actie 5 cli opdracht "show Capture radius decode dump" *—u decodeert/dump nu uw pakketopname.*

uitvoerbestand voegt disk0:/ISE_Recover_With_Cap.txt toe *—deze opname wordt nu opgeslagen in een tekstbestand op de ASA en er worden nieuwe resultaten toegevoegd aan het einde.*

Laatste stappen

Tot slot kunt u deze informatie vervolgens uploaden naar een Cisco TAC-case of de informatie gebruiken om de nieuwste pakketten in de stroom te analyseren en uit te zoeken waarom de RADIUS-servers zijn gemarkeerd als mislukt.

Het tekstbestand kan worden gedecodeerd en in een pcap worden omgezet bij de eerder genoemde Packet Capture Config-generator en -analyzer.

voorbeeld uit de echte wereld

In het volgende voorbeeld wordt de opname voor RADIUS-verkeer gefilterd. U ziet dat ASA het apparaat is dat in .180 eindigt en dat de RADIUS-server in .21 eindigt

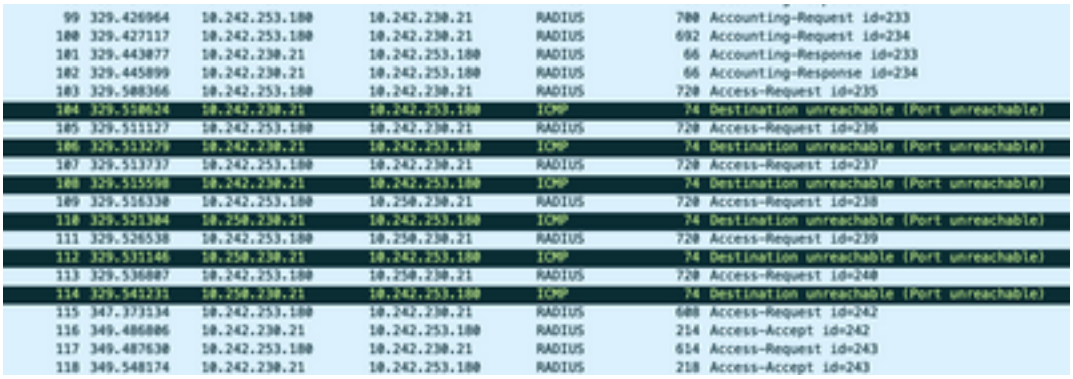
In dit voorbeeld geven *beide* RADIUS-servers een "poort onbereikbaar" terug, 3 keer achter elkaar. Dit brengt ASA ertoe om *beide* servers van de RADIUS binnen milliseconden dood van elkaar te merken.

Het resultaat

Elk .21 adres in dit voorbeeld was een F5 VIP adres. Dat betekent dat achter de VIPS clusters van Cisco ISE-knooppunten in de PSN-persona lagen.

De F5 keerde "port unreach" terug vanwege een F5 defect.

In dit voorbeeld heeft het Cisco TAC-team met succes bewezen dat de ASA heeft gewerkt zoals verwacht. Dat wil zeggen, het verstuurde radiuspakketten en ontving 3 poorten die voordien onbereikbaar waren, en voerde de Radius Server gemarkeerd mislukte:



Gerelateerde informatie

- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.