EEM 스크립트를 사용하여 간헐적인 RADIUS 서버 장애 문제 해결

목차

소개

이 문서에서는 ASA에서 장애가 발생한 것으로 표시된 RADIUS 서버의 문제를 해결하는 방법 및 클라이언트 인프라에 중단을 일으킬 수 있는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA에서 기본 인식 또는 EEM 스크립팅

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

RADIUS 서버는 Cisco ASA에서 실패/죽은 것으로 표시됩니다. 이 문제는 간헐적이지만 클라이언

트 인프라에 중단을 초래합니다. TAC에서는 이 문제가 ASA 문제인지, 데이터 경로 문제인지, RADIUS 서버 문제인지 구별해야 합니다. 장애 발생 시 캡처가 이루어지는 경우, ASA가 RADIUS 서버로 패킷을 전송하는지 여부와 그 대가로 패킷을 수신하는지 여부를 판별하므로 Cisco ASA를 배제합니다.

토폴로지

이 예에서는 다음 토폴로지가 사용됩니다.

이 문제를 해결하려면 다음 단계를 수행하십시오.

1단계: 패킷 캡처 및 적용 가능한 액세스 목록을 구성하여 서버 간 패킷 캡처

첫 번째 단계는 ASA와 RADIUS 서버 간의 패킷을 캡처하도록 패킷 캡처 및 적용 가능한 액세스 목록을 구성하는 것입니다.

패킷 캡처에 대한 지원이 필요한 경우 Packet Capture Config Generator and Analyzer를 참조하십시오.

access-list TAC 확장 허용 ip 호스트 10.20.20.180 호스트 10.10.10.150

access-list TAC 확장 허용 ip 호스트 10.10.10.150 호스트 10.20.20.180

access-list TAC 확장 허용 ip 호스트 10.20.20.180 호스트 10.10.20.150

access-list TAC 확장 허용 ip 호스트 10.10.20.150호스트 10.20.20.180

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

> **참고**: 버퍼 크기를 확인하여 데이터가 과도하게 채워지지 않도록 해야 합니다. 버퍼 크기 1000000 충분합니다. 예제 버퍼는 3000000입니다.

2단계: EEM 스크립트 구성

다음으로, EEM 스크립트를 구성합니다.

이 예에서는 Syslog ID인 113022을 사용하며, 다른 여러 Syslog 메시지에서 EEM을 트리거할 수 있습니다.

ASA의 메시지 유형은 Cisco Secure Firewall ASA Series Syslog Messages에 있습니다.

이 시나리오의 트리거는 다음과 같습니다.

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

이 ASA 에서 AAA 서버에 대한 인증, 권한 부여 또는 계정 관리 요청을 시도했으나 구성된 시간 제한 기간 내에 응답을 받지 못했습니다. 그런 다음 AAA 서버가 실패한 것으로 표시되고 서비스에서 제거됩니다.

이벤트 관리자 애플릿 ISE_Radius_Check

이벤트 syslog id **113022**

action 0 cli 명령 "show clock"

action 1 cli 명령 "show aaa-server ISE"

action 2 cli 명령 "aaa-server ISE active host 10.10.150"

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

action 4 cli 명령 "show aaa-server ISE"

action 5 cli 명령 "show capture radius decode dump"

출력 파일 append disk0:/ISE_Recover_With_Cap.txt

EEM 스크립트 설명

이벤트 관리자 애플릿 ISE_Radius_Check. - *eem 스크립트의 이름을 지정합니다.*

event syslog id **113022** - *트리거: (이전 설명 참조)*

action 0 cli 명령 "show clock" - *클라이언트가 가질 수 있는 다른 로그와 비교하기 위해 문제를 해결하는 동안 정확한 타임스탬프를 캡처하는 모범 사례입니다.*

action 1 cli 명령 "show aaa-server ISE" — *aaa-server 그룹의 상태를 표시합니다. 이 경우에는 해당 그룹을 ISE라고 합니다.*

action 2 cli 명령 "aaa-server ISE active host 10.10.10.150" — *이 명령은 해당 IP를 사용하여 aaa-server를 "다시 시작"하는 것입니다. 그러면 radius 패킷을 계속 시도하여 데이터 경로 오류를 확인할 수 있습니다.*

action 3 cli 명령 "aaa-server ISE active host 10.10.20.150" - *이전 명령 설명을 참조하십시오.*

action 4 cli 명령 "show aaa-server ISE" - *이 명령은 서버가 백업되었는지 확인합니다.*

action 5 cli 명령 "show capture radius decode dump" - *이제 패킷 캡처를 디코딩/덤프합니다.*

output file append disk0:/ISE_Recover_With_Cap.txt —*이 캡처는 이제 ASA의 텍스트 파일에 저장되며 새 결과가 끝에 추가됩니다.*

최종 단계

마지막으로 이 정보를 Cisco TAC 케이스에 업로드하거나 이 정보를 사용하여 플로우의 최신 패킷을 분석하고 RADIUS 서버가 실패한 것으로 표시된 이유를 파악할 수 있습니다.

텍스트 파일은 앞서 언급한 Packet Capture Config Generator and Analyzer에서 디코딩하고 pcap로 변환할 수 있습니다.

실세계의 예

다음 예에서는 RADIUS 트래픽에 대한 캡처가 필터링됩니다. ASA는 .180으로 끝나는 디바이스이고 RADIUS 서버는 .21로 끝나는 디바이스입니다

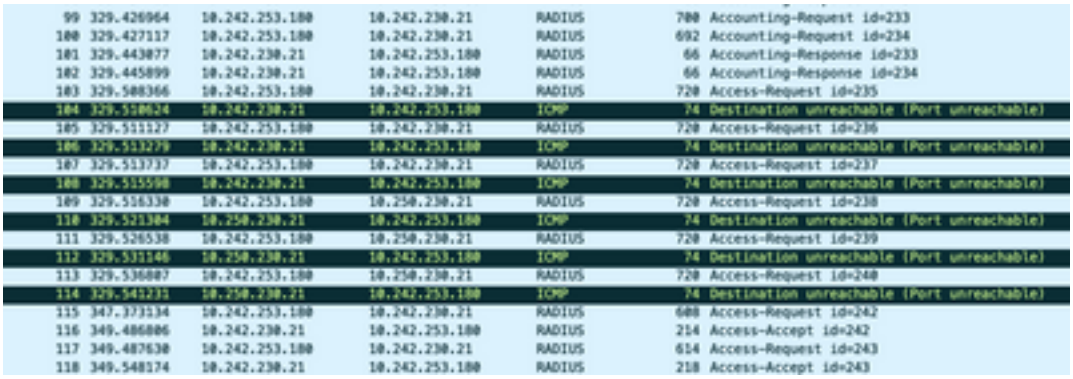
이 예에서 *두 RADIUS* 서버는 각각 한 행에서 3번 "포트 도달 불가"를 반환합니다. 이렇게 하면 ASA가 *두* RADIUS *서버*를 서로 밀리초 이내에 dead로 표시하도록 트리거됩니다.

결과

이 예에서 각 .21 주소는 F5 VIP 주소입니다. 이는 VIP 뒤에 PSN 페르소나의 Cisco ISE 노드 클러스터가 있었다는 것을 의미합니다.

F5에서 F5 결함으로 인해 "port unreachable"을 반환했습니다.

이 예에서 Cisco TAC 팀은 ASA가 예상대로 작동한다는 것을 입증했습니다. 즉, RADIUS 패킷을 전송하고 이전에 연결할 수 없는 3개의 포트를 받았으며, 실패한 것으로 표시된 RADIUS 서버에 영향을 주었습니다.



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	329.443077	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	329.510024	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	329.521304	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	329.543231	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	349.486886	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

관련 정보

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.