대규모 무선 RADIUS 네트워크 녹음을 방지

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine) 또는 Cisco ACS(Secure Access Control Server)를 사용하여 RADIUS를 사용하는 WLC(AireOS Wireless LAN Controller) 같은 대규모 무선 구축에 대한 기본 컨피그레이션 지침을 간략하게 소개합니다. 이 문서는 더 자세한 기술적 세부 정보를 가진 다른 문서를 참조합니다.

관찰된 증상

일반적으로 대학에서는 AAA(Authentication, Authorization, and Accounting) 붕괴 상태가 발생합니다.이 섹션에서는 이 환경에서 목격되는 일반적인 증상/로그에 대해 설명합니다.

1. RADIUS 성능 모니터링

Dotx 클라이언트는 많은 인증 재시도와 함께 많은 지연을 경험합니다.

show radius auth **statistics** 명령(GUI:**Monitor(모니터링) > Statistics(통계) > RADIUS Servers(RADIUS 서버)**)에서 문제를 확인합니다.특히 Retries, Rejects 및 Timeouts의 수가 많습니다.예를 들면 다음과 같습니다.

```
Server Index..................................... 2
Server Address................................... 192.168.88.1
Msg Round Trip Time.............................. 3 (msec)
First Requests................................... 1256
Retry Requests................................... 5688
Accept Responses................................. 22
Reject Responses................................. 1
Challenge Responses.............................. 96
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
```

```
Pending Requests.............................. 1
Timeout Requests.............................. 6824
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```
대상:

- 높은 재시도:첫 번째 요청 비율(10% 이하여야 함)
- 높은 거부:허용 비율
- 높은 시간 초과:첫 번째 요청 비율(5% 이하여야 함)

문제가 있는 경우 다음을 확인하십시오.

- 잘못 구성된 클라이언트
- WLC와 RADIUS 서버 간의 네트워크 연결 문제
- AD(Active Directory)와 같이 사용 중인 경우 RADIUS 서버와 백엔드 데이터베이스 간의 문제

2. WLC는 MSGLOGS에서 RADIUS 대기열이 꽉 찬 것으로 인식합니다.

WLC는 RADIUS 대기열에 대한 다음 메시지를 받습니다.

```
Univ-WISM2-02: *aaa QueueReader: Dec 02 14:25:31.565: #AAA-3-3TXQUEUE_ADD_FAILED:
radius_db.c:889 Transmission queue full. Que name: Radius queue. Dropping
sessionpackets.
host = x.x.x.x.
```

3. 디버그 AAA

AAA의 디버그는 다음 메시지를 표시합니다.

```
*aaaQueueReader: Dec 02 21 09:19:52.198: xx:xx:xx:xx:xx:xx Returning AAA Error
'Out of Memory' (-2) for mobile xx:xx:xx:xx:xx:xx
```
AAA의 디버그는 모바일 디바이스에 대한 AAA Error **Timeout(-5)**을 반환합니다.AAA 서버에 연결할 수 없으며 클라이언트 권한 부여가 그 뒤에 옵니다.

4. RADIUS 서버가 사용 중이어서 응답하지 않습니다.

로그 시스템 시간 트랩은 다음과 같습니다.

```
0 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
1 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
2 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
3 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
4 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 unavailable
5 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 22) for client 68:96:7b:0e:46:7f / user 'user1@univ1.edu'
6 Wed Aug 20 15:29:57 2014 User Larry_Dull_231730 logged Out. Client MAC:84:a6:c8:
87:13:9c, Client IP:198.21.137.22, AP MAC:c0:7b:bc:cf:af:40, AP Name:Dot1x-AP
7 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 183) for client 48:d7:05:7d:93:a5 / user ' user2@univ2.edu '
8 Wed Aug 20 15:28:42 2014 RADIUS auth-server x.x.x.x:1812 unavailable
9 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 154) for client 40:0e:85:76:00:68 / user ' user1@univ1.edu '
```

```
10 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 available
11 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 unavailable
12 Wed Aug 20 15:28:41 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 99) for client 50:2e:5c:ea:e4:ba / user ' user3@univ3.edu '
13 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
14 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
15 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 30) for client b4:18:d1:60:6b:51 / user ' user1@univ1.edu '
16 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
17 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
18 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
19 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
```

모범 사례 튜닝

WLC 측 조정

- EAP(Extensible Authentication Protocol) - 802.1X 클라이언트 제외 작업을 활성화합니다.

  802.1X에 대해 전역적으로 클라이언트 제외를 활성화합니다.
  802.1X WLAN(무선 LAN)에서 클라이언트 제외를 최소 120초로 설정합니다.
  AireOS WLC 기사에서 802.1X 클라이언트 제외에 설명된 대로 EAP 타이머를 설정합니다.

- RADIUS 재전송 시간 제한을 최소 5초로 설정합니다.

- Session-Timeout을 최소 8시간으로 설정합니다.

- Disable Aggressive Failover(적극적인 장애 조치 비활성화) - 잘못된 단일 신청자가 RADIUS 서버 간에 WLC가 실패하도록 허용하지 않습니다.

- 클라이언트에 대해 빠른 보안 로밍을 구성합니다.

  Microsoft Windows EAP 클라이언트가 OKC(Opportunistic Key Caching)를 사용할 수 있도록 WPA2(Wi-Fi Protected Access 2)/AES(Advanced Encryption Standard)를 사용해야 합니다.

  Apple iOS 클라이언트를 자체 WLAN으로 분리할 수 있는 경우 해당 WLAN에서 802.11r을 활성화할 수 있습니다.

  792x 폰을 지원하는 모든 WLAN에 대해 Cisco CCKM(Centralized Key Management)을 활성화합니다(그러나 Microsoft Windows 또는 Android 클라이언트를 지원하는 SSID(Service Set Identifier)에서는 CCKM을 활성화하지 **않음**). CCKM은 CCKM 구현에 문제가 있는 경향이 있기 때문입니다.

  MAC OS(Macintosh Operating System) X 및/또는 Android 클라이언트를 지원하는 EAP WLAN에 대해 SKC(Sticky Key Caching)를 활성화합니다.

자세한 내용은 CUWN의 802.11 WLAN 로밍 및 고속 보안 로밍을 참조하십시오.

참고: show pmk-cache all 명령을 사용하여 피크 시간에 WLC PMK(Pairwise Master Key) 캐시 사용량을 모니터링합니다.최대 PMK 캐시 크기에 도달하거나 근접하게 되면 SKC를 비활성화해야 할 수 있습니다.
프로파일링에 ISE를 사용하는 경우 WLC 측 DHCP/HTTP 프로파일링을 사용합니다.이렇게 하면 프로파일링 데이터가 쉽게 로드 밸런싱되는 RADIUS 어카운팅 패킷에 래핑되므로 엔드포인트의 모든 데이터가 동일한 PSN(Public Services Network)에 도달합니다.

바이트 기반 청구 서비스에 중간 어카운팅이 필요하지 않은 경우 해당 어카운트가 꺼져 있는지 확인합니다.그렇지 않은 경우 중간 어카운팅은 추가 혜택 없이 부하를 추가합니다.

최상의 WLC 코드를 실행합니다.

RADIUS 서버측 조정로깅 속도를 줄입니다.대부분의 RADIUS 서버는 저장할 로깅에 대해 구성할 수 있습니다.ACS 또는 ISE를 사용하는 경우 관리자는 모니터링 데이터베이스에 로깅되는 범주를 선택할 수 있습니다.예를 들어 계정 데이터를 RADIUS 서버에서 보내고 SYSLOG와 같은 다른 애플리케이션과 함께 보고 데이터베이스에 로컬로 데이터를 쓰지 않는 경우가 있습니다.ISE에서 로그 억제가 항상 활성화되어 있는지 확인합니다.문제 해결을 위해 비활성화해야 하는 경우 Administration(관리) > System(**시스템) > Logging(로깅) > Collection Filters(컬렉션 필터)로 이동하여** 개별 엔드포인트 또는 사용자에 대한 억제를 비활성화하려면 Bypass Suppression(숨김) 옵션을 사용합니다.ISE 버전 1.3 이상에서는 실시간 인증 로그에서 엔드포인트를 마우스 오른쪽 버튼으로 클릭하여 삭제를 비활성화할 수도 있습니다.

백엔드 인증 레이턴시가 낮은지 확인합니다(AD, LDAP(Lightweight Directory Access Protocol), Rivest, Shamir, Adleman(RSA)). ACS 또는 ISE를 사용하는 경우 평균 및 피크 대기 시간 모두에 대해 서버별로 대기 시간을 모니터링하기 위해 인증 요약 보고서를 실행할 수 있습니다.요청을 처리하는 데 시간이 오래 걸수록 ACS 또는 ISE가 처리할 수 있는 인증 비율이 낮아집니다.시간의 95%, 지연 시간이 높은 이유는 백엔드 데이터베이스의 응답이 느리기 때문입니다.

PEAP(Protected Extensible Authentication Protocol) 비밀번호 재시도를 비활성화합니다.대부분의 디바이스는 PEAP 터널 내에서 비밀번호 재시도를 지원하지 않으므로 EAP 서버로부터의 재시도는 디바이스가 응답을 중지하고 새 EAP 세션을 사용하여 재시작합니다.그러면 거부 대신 EAP 시간 초과가 발생하며, 이는 클라이언트 제외가 적중되지 않음을 의미합니다.

사용하지 않는 EAP 프로토콜을 비활성화합니다.이는 중요하지는 않지만 EAP 교환에 일부 효율성을 추가하고 클라이언트가 취약하거나 의도하지 않은 EAP 방법을 사용할 수 없도록 합니다.

PEAP 세션 재시작 및 빠른 재연결을 활성화합니다.

필요 없는 경우 AD에 MAC 인증을 전송하지 마십시오.이는 ISE가 인증하는 도메인 컨트롤러의 로드를 증가시키는 일반적인 컨피그레이션입니다.이렇게 하면 시간이 많이 소요되고 평균 레이턴시가 증가하는 부정적인 검색이 발생하는 경우가 많습니다.

해당하는 경우 Device Sensor(디바이스 센서)를 사용합니다(ISE에만 해당).