무선 LAN 컨트롤러에서 RADIUS 서버 대체 기능 구성

목차

소개

이 문서에서는 WLC(Wireless LAN Controller)를 사용하여 RADIUS 서버 폴백 기능을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAP(Lightweight Access Point) 및 Cisco WLC의 구성에 대한 기본 지식
- CAPWAP(무선 액세스 포인트 프로토콜)의 제어 및 프로비저닝에 대한 기본 지식
- 무선 보안 솔루션에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 Cisco 5508/5520 컨트롤러를 기반으로 합니다.

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

배경 정보

RADIUS 서버 대체 기능

5.0 이전의 WLC 소프트웨어 버전은 RADIUS 서버 대체 메커니즘을 지원하지 않습니다.기본 RADIUS 서버를 사용할 수 없게 되면 WLC는 다음 활성 백업 RADIUS 서버로 장애 조치됩니다.기본 서버가 사용 가능한 경우에도 WLC는 계속해서 보조 RADIUS 서버를 계속 사용합니다.일반적으로 기본 서버는 높은 성능과 기본 서버입니다.

WLC 5.0 이상 버전에서는 WLC가 RADIUS 서버 대체 기능을 지원합니다.이 기능을 사용하면 WLC를 구성하여 기본 서버가 사용 가능한지 확인하고 사용 가능한 경우 기본 RADIUS 서버로 다시 전환할 수 있습니다.이를 위해 WLC는 RADIUS 서버의 상태를 확인하기 위해 패시브 및 액티브 두 가지 새 모드를 지원합니다.WLC는 지정된 시간 초과 값 이후에 가장 바람직한 서버로 돌아갑니다.

대체 모드

활성 모드

활성 모드에서 서버가 WLC 인증 요청에 응답하지 않을 경우 WLC는 서버를 Dead로 표시한 다음 서버를 비활성 서버 풀로 이동하고 서버가 응답할 때까지 주기적으로 프로브 메시지를 보내기 시작합니다.서버가 응답하면 WLC는 데드 서버를 활성 풀로 이동하고 프로브 메시지 전송을 중지합니다.이 모드에서 인증 요청이 오면 WLC는 항상 RADIUS 서버의 활성 풀에서 가장 낮은 인덱스(가장 높은 우선순위) 서버를 선택합니다.

WLC는 서버가 이전에 응답하지 않을 경우 서버 상태를 확인하기 위해 시간 초과 후 프로브 패킷(기본값은 300초)을 전송합니다.

수동 모드

패시브 모드에서 서버가 WLC 인증 요청에 응답하지 않을 경우 WLC는 서버를 비활성 대기열로 이동하고 타이머를 설정합니다.타이머가 만료되면 WLC는 서버의 실제 상태에 관계없이 서버를 활성 대기열로 이동합니다.인증 요청이 수신되면 WLC는 활성 대기열에서 가장 낮은 인덱스(가장 높은 우선 순위) 서버(비활성 서버가 포함될 수 있음)를 선택합니다. 서버가 응답하지 않으면 WLC는 비활성 상태로 표시하고 타이머를 설정하고 다음으로 우선 순위가 높은 서버로 이동합니다.이 프로세스는 WLC가 활성 RADIUS 서버를 찾거나 활성 서버 풀이 모두 소모될 때까지 계속됩니다.

WLC는 서버가 이전에 응답하지 않을 경우 시간 초과 후 서버가 활성(기본값은 300초)이라고 가정합니다.여전히 응답하지 않는 경우 WLC는 다른 시간 제한을 기다렸다가 인증 요청이 들어올 때 다시 시도합니다.

끄기 모드

오프 모드에서는 WLC가 장애 조치만 지원합니다.즉, 폴백이 비활성화됩니다.기본 RADIUS 서버가 다운되면 WLC는 다음 활성 백업 RADIUS 서버로 장애 조치됩니다.기본 서버를 사용할 수 있는 경우에도 WLC는 계속해서 보조 RADIUS 서버를 계속 사용합니다.

구성

CLI를 사용하여 RADIUS 서버 대체 기능 구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

WLC에서 RADIUS 서버 대체 기능을 활성화하려면 WLC CLI에서 다음 명령을 사용합니다.

첫 번째 단계는 RADIUS 서버 폴백 모드를 선택하는 것입니다.앞에서 언급한 대로, WLC는 활성 및 수동 대체 모드를 지원합니다.

대체 모드를 선택하려면 다음 명령을 입력합니다.

```
WLC1 > config radius fallback-test mode {active/passive/off}
```

- active - 상태를 테스트하기 위해 Dead 서버에 프로브를 보냅니다.
- passive - 마지막 트랜잭션을 기반으로 서버 상태를 설정합니다.
- off - 서버 대체 테스트를 비활성화합니다(기본값).

다음 단계는 액티브 모드의 프로브 간격 또는 수동 작업 모드의 비활성 시간을 지정하는 간격을 선택하는 것입니다.

간격을 설정하려면 다음 명령을 입력합니다.

```
WLC1 > config radius fallback-test mode interval {180 - 3600}
```

<180~3600> - 프로브 간격 또는 비활성 시간을 초 단위로 입력합니다(기본값은 300초).

이 간격은 액티브 모드 폴백 또는 패시브 모드 폴백 시 비활성 시간의 프로브 간격을 지정합니다.

활성 작동 모드의 경우 RADIUS 서버로 전송된 프로브 요청에 사용될 사용자 이름을 구성해야 합니다.

사용자 이름을 구성하려면 다음 명령을 입력합니다.

```
WLC1 >config radius fallback-test username {username}
```

<username> - 최대 16자의 영숫자 문자를 입력합니다(기본값은 cisco-probe임).

> **참고:**사용자 이름을 직접 입력하거나 기본값으로 둘 수 있습니다.기본 사용자 이름은 "cisco-probe"입니다. 이 사용자 이름은 프로브 메시지를 보내는 데 사용되므로 비밀번호를 구성할 필요가 없습니다.

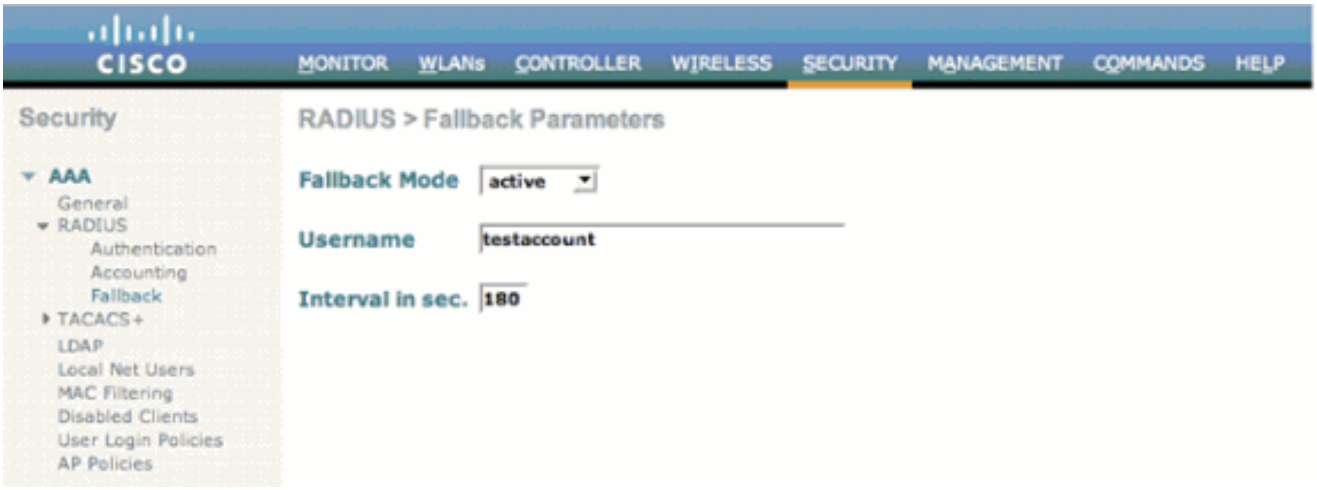
GUI를 사용하여 RADIUS 서버 대체 기능 구성

GUI를 사용하여 WLC를 구성하려면 다음 단계를 완료합니다.

1. RADIUS 서버 폴백 모드를 구성합니다.이렇게 하려면 WLC GUI에서 **보안 > RADIUS > 대체**

를 선택합니다. **RADIUS > 대체 매개변수** 페이지가 나타납니다.

2. Fallback **Mode** 드롭다운 목록에서 대체 모드를 선택합니다.사용 가능한 옵션에는 active, passive 및 off가 포함됩니다.다음은 이미지에 표시된 대로 활성 폴백 모드 컨피그레이션에 대한 예제 스크린샷입니다.



3. 활성 작동 모드의 경우 사용자 이름 필드에 사용자 이름을 입력합니다.
4. 간격(초)에 프로브 간격 값을 입력합니다.필드.
5. Apply를 **클릭합니다**.

WLC에서 적극적인 장애 조치 기능이 활성화된 경우 WLC는 AAA 서버를 "응답하지 않음"으로 표시할 수 없습니다. 그러나 AAA 서버가 무음 폐기 시 해당 특정 클라이언트에만 응답하지 않을 수 있으므로 이 작업은 수행하지 마십시오.유효한 인증서가 있는 다른 유효한 클라이언트에 대한 응답일 수 있습니다.WLC는 여전히 AAA 서버를 "응답하지 않음" 및 "작동하지 않음"으로 표시할 수 있습니다.

이를 해결하려면 적극적인 장애 조치 기능을 비활성화합니다.컨트롤러 GUI에서 **config radius aggressive-failover disable** 명령을 입력하여 이를 수행합니다.이 기능이 비활성화된 경우, RADIUS 서버로부터 응답을 받지 못한 연속된 세 개의 클라이언트가 있는 경우 컨트롤러는 다음 AAA 서버로 장애 조치됩니다.

> **참고:**릴리스 8.5.140,8.8.100,8.10.105 이상에서 도입된 기능 변경:컨트롤러에 대한 RADIUS 적극적인 장애 조치가 비활성화된 경우:클라이언트에서 중단되지 않는 한 패킷은 6번 재시도됩니다.RADIUS 서버(AUTH와 ACCT 모두)는 여러 클라이언트(이전의 정확히 세 개의 클라이언트에서)에서 세 개의 시간 초과 이벤트(18번의 연속 재시도)가 발생한 후 도달 불가 상태로 표시됩니다. 컨트롤러에 대한 RADIUS 적극적인 장애 조치가 활성화된 경우:클라이언트에서 중단되지 않는 한 패킷은 6번 재시도됩니다.RADIUS 서버(AUTH 및 ACCT 모두)는 여러 클라이언트(이전의 정확히 하나의 클라이언트에서)에서 하나의 시간 초과 이벤트(6회 연속 재시도)가 발생한 후 도달 불가 상태로 표시됩니다. 이는 RADIUS 서버당 18번의 연속 재시도(AUTH 또는 ACCT)가 여러 클라이언트에서 발생할 수 있음을 의미합니다.따라서 각 패킷이 6회 재시도된다는 것이 항상 보장되지는 않습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 OIT를 사용합니다.

폴백 컨피그레이션을 확인하려면 show radius **summary** 명령을 입력합니다.예를 들면 다음과 같습니다.

```
WLC1 >show radius summary

Vendor Id Backward Compatibility..................... Disabled
Call Station Id Type.............................. IP Address
Aggressive Failover............................... Enabled
Keywrap........................................... Disabled

Fallback Test:
Test Mode..................................... Active
Probe User Name............................... testaccount
Interval (in seconds)......................... 180

Authentication Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------------
1 NM 10.1.1.12 1812 Enabled 2 Disabled Disabled-none/unknown/group-0/0 none/none

Accounting Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------
1 N 10.1.1.12 1813 Enabled 2 N/A Disabled-none/unknown/group-0/0 none/nonen
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

> **참고:debug** 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug dot1x events enable** - 802.1X 이벤트의 디버그를 구성합니다.
- **debug aaa events enable -** 모든 AAA 이벤트의 디버그를 구성합니다.

관련 정보

- WLAN 컨트롤러(WLC)를 사용한 EAP 인증 컨피그레이션 예
- WLC(Wireless LAN Controller)에 LAP(Lightweight AP) 등록
- 보안 솔루션 구성
- RADIUS 서버 및 무선 LAN 컨트롤러 구성을 통한 동적 VLAN 할당 예
- 기술 지원 및 문서 – Cisco Systems