ONS 15454 버전 6.0의 RADIUS 인증 문제

목차

소개

이 문서에서는 Cisco ONS 15454 환경의 ONS 15454 버전 6.0에서 RADIUS(Remote Authentication Dial-In User Service) 서버 인증에 대해 알려진 몇 가지 문제에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ONS 15454
- RADIUS 서버

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ONS 15454 버전 6.0

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

RADIUS는 네트워크 및 네트워크 서비스에 대한 원격 액세스를 무단 액세스로부터 보호하는 분산 보안 시스템입니다. RADIUS는 다음 세 가지 구성 요소로 구성됩니다.

- UDP(User Datagram Protocol)/IP를 사용하는 프레임 형식의 프로토콜
- 서버
- 클라이언트

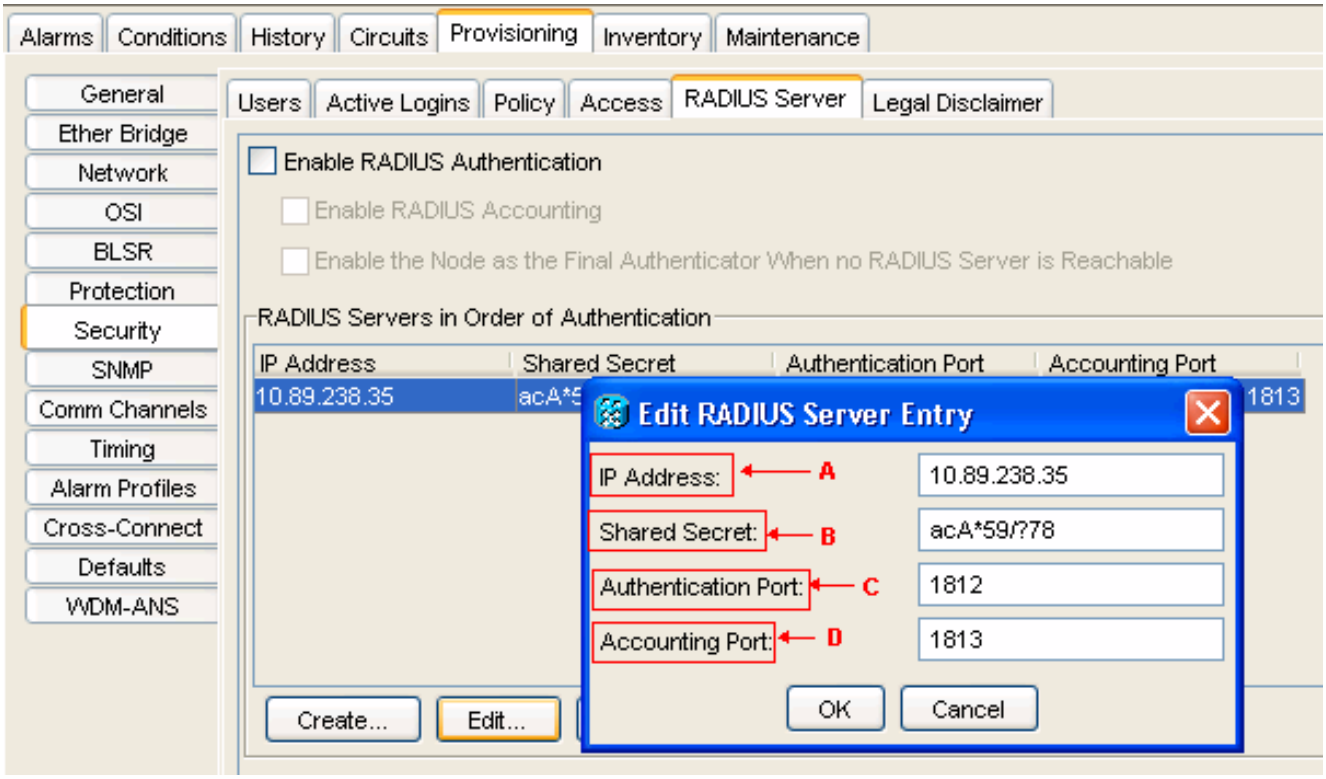
ONS 15454 노드는 RADIUS의 클라이언트로 작동합니다. 클라이언트는 사용자 정보를 지정된 RADIUS 서버로 전달한 다음 응답에 대해 작동합니다. RADIUS 서버는 사용자 연결 요청을 받고 사용자를 인증하며 클라이언트가 사용자에게 서비스를 제공하는 데 필요한 모든 구성 정보를 반환합니다.

공유 암호는 RADIUS 클라이언트와 서버 간의 트랜잭션을 인증합니다. 공유 암호는 네트워크를 통해 전송되지 않습니다. 또한 모든 사용자 비밀번호는 클라이언트와 RADIUS 서버 간에 교환될 때 암호화됩니다. 암호화 프로세스를 사용하면 안전하지 않은 네트워크를 모니터링하여 사용자의 비밀번호를 확인할 가능성이 없습니다.

공유 암호

공유 암호는 ONS15454 RADIUS 클라이언트와 RADIUS 서버 간의 비밀번호 역할을 하는 텍스트 문자열입니다. 공유 암호를 만들려면 다음 단계를 완료하십시오.

1. CTC(Cisco Transport Controller)에 로그인합니다.
2. 네트워크 보기로 이동합니다.
3. Shelf 보기로 이동하려면 특정 ONS 15454를 선택합니다.
4. Provisioning **> Security > RADIUS Server를 클릭합니다**.
5. IP Address 필드에 RADIUS 서버의 IP 주소를 입력합니다(그림 1의 화살표 A 참조).
6. 공유 암호 필드에 공유 암호를 입력합니다. 공유 비밀은 RADIUS 클라이언트와 RADIUS 서버 간에 비밀번호로 사용되는 텍스트 문자열입니다(그림 1의 화살표 B 참조).
7. Authentication Port(인증 포트) 필드에 RADIUS 인증 포트 번호를 입력합니다(그림 1의 화살표 C 참조).기본 인증 포트 번호는 1812입니다. 노드가 ENE인 경우 인증 포트를 1860 및 1869 범위의 숫자로 설정합니다.
8. Accounting Port 필드에 RADIUS 어카운팅 포트 번호를 입력합니다(그림 1의 화살표 D 참조).기본 어카운팅 포트 번호는 1813입니다. 노드가 ENE인 경우 어카운팅 포트를 1870 및 1879 범위의 숫자로 설정합니다.**그림 1 - 보안: RADIUS 서버**



공유 암호를 사용하여 동일한 공유 암호로 구성한 RADIUS 지원 디바이스가 액세스 요청 메시지를 제외한 모든 RADIUS 메시지를 전송하도록 합니다.

공유 암호는 RADIUS 메시지가 전송 중에 수정되지 않도록 합니다. 즉, 공유 비밀은 메시지 무결성을 유지합니다. 공유 암호는 일부 RADIUS 특성을 암호화합니다(예: User-Password 및 Tunnel-Password).

ONS 15454 버전 6.0은 공유 비밀의 길이를 16자로 제한합니다. 그러나 ONS 15454 버전 6.2부터는 최대 길이를 128자로 늘릴 계획입니다. 자세한 내용은 Cisco 버그 ID CSCsc16614(등록된 고객만 해당)를 참조하십시오.

공유 암호 문자 그룹은 다음을 지원합니다.

- 문자(대문자 및 소문자)(예: A, B, a 및 b).
- 숫자(예: 1, 2, 3)입니다.
- 기호 - 문자 또는 숫자로 정의되지 않은 모든 문자를 나타냅니다(예: >, (, *).

사용자 보안 그룹 매핑

AV(attribute-value) 쌍은 변수 및 변수가 보유할 수 있는 값 중 하나를 나타냅니다. ONS 15454 내에서 사용자는 Cisco AV 쌍을 기반으로 서로 다른 보안 그룹에 매핑됩니다. 예를 들면 다음과 같습니다.

"shell:priv-lvl=X" 여기서 X는 0~3의 값이 될 수 있습니다.

- 0은 RTRV를 나타냅니다.
- 1은 PROV를 나타냅니다.
- 2는 MAINT를 나타냅니다.
- 3은 SUPER를 나타냅니다.

비밀번호

RADIUS 서버 및 클라이언트는 비밀번호에 사용하는 문자를 제한하지 않습니다. 그러나 CTC에는 한계가 있습니다. ONS 15454 버전 6.0의 경우 CTC가 지원하는 문자는 다음과 같습니다.

- 문자(대문자 및 소문자)(예: A, B, a 및 b).
- 숫자(예: 1, 2, 3)입니다.
- #, % 및 + 특수 기호만 사용할 수 있습니다.

Cisco는 이후 버전의 ONS 15454에서 특수 기호의 제한을 제거할 계획입니다. 자세한 내용은 Cisco 버그 ID CSCsc16604(등록된 고객만 해당)를 참조하십시오.

관련 정보

- 기술 지원 및 문서 – Cisco Systems