액세스 서버에서 기본 AAA 구성

목차

소개

이 문서에서는 Radius 또는 TACACS+ 프로토콜을 사용하는 Cisco 라우터에서

AAA(Authentication, Authorization, and Accounting)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

표기 규칙

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

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® 소프트웨어 릴리스 12 기본 행을 기준으로 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

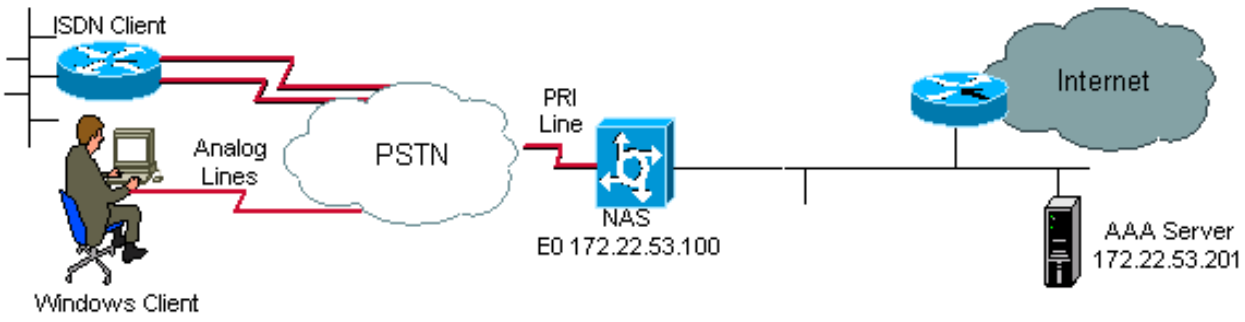
배경 정보

이 문서에서는 Radius 또는 TACACS+ 프로토콜을 사용하는 Cisco 라우터에서 AAA(Authentication, Authorization, and Accounting)를 구성하는 방법에 대해 설명합니다. 이 문서의 목적은 모든 AAA 기능을 다루는 것이 아니라 기본 명령을 설명하고 몇 가지 예와 지침을 제공하는 것입니다.

> **참고:** Cisco IOS 컨피그레이션을 진행하기 전에 General AAA Configuration(일반 AAA 컨피그레이션)의 섹션을 읽어 보십시오. 이렇게 하지 않으면 컨피그레이션이 잘못되어 이후에 잠길 수 있습니다.

자세한 내용은 인증, 권한 부여 및 계정 관리 컨피그레이션 가이드를 참조하십시오.

네트워크 다이어그램



네트워크 다이어그램

일반 AAA 컨피그레이션

AAA 활성화

AAA를 활성화하려면 전역 컨피그레이션에서 **aaa new-model** 명령을 구성해야 합니다.

> **참고:** 이 명령이 활성화될 때까지 다른 모든 AAA 명령은 숨겨집니다.

> **경고:** aaa **new-model 명령은** 모든 회선 및 인터페이스에 로컬 인증을 즉시 적용합니다(콘솔 회선 **con 0 제외**). 이 명령이 활성화된 후 텔넷 세션이 라우터에 열리면(또는 연결 시간이 초과되어 다시 연결해야 하는 경우) 사용자는 라우터의 로컬 데이터베이스를 사용하여 인증해야 합니다. AAA 컨피그레이션을 시작하기 전에 액세스 서버에서 사용자 이름과 비밀번호를 정의하는 것이 좋습니다. 그러면 라우터에서 잠기지 않습니다. 다음 코드 예제를 참조하십시오.

```
Router(config)#username xxx password yyy
```

> **팁:** AAA 명령을 구성하기 전에 save 구성합니다. 다음을 수행할 수 있습니다. save aaa 컨피그레이션을 완료한 후에만 컨피그레이션을 다시 수행할 수 있습니다(그리고 올바르게 작동한다는 점에 만족함). 이렇게 하면 라우터를 다시 로드하여 변경 사항을 롤백할 수 있으므로 예기치 않은 잠금이 발생하는 경우에도 복구할 수 있습니다.

외부 AAA 서버 지정

전역 컨피그레이션에서 AAA(Radius, TACACS+)와 함께 사용되는 보안 프로토콜을 정의합니다. 이 두 프로토콜 중 하나를 사용하지 않으려면 라우터의 로컬 데이터베이스를 사용할 수 있습니다.

TACACS+를 사용하는 경우 tacacs-**server host <AAA 서버의 IP address> <key> 명령을** 사용합니다.

Radius를 사용하는 경우 radius-**server host <AAA 서버의 IP address> <key> 명령을** 사용합니다.

AAA 서버 컨피그레이션

AAA 서버에서 다음 매개변수를 구성합니다.

- 액세스 서버의 이름입니다.
- 액세스 서버가 AAA 서버와 통신하는 데 사용하는 IP 주소.**참고:** 두 디바이스가 동일한 이더넷 네트워크에 있는 경우 기본적으로 액세스 서버는 AAA 패킷을 전송할 때 이더넷 인터페이스에 정의된 IP 주소를 사용합니다. 라우터에 여러 인터페이스가 있는 경우(따라서 주소가 여러 개인 경우) 이 문제가 중요합니다.
- 액세스 서버에 **구성된** 동일한 키 **<key>**입니다.**참고:** 키는 대/소문자를 구분합니다.
- 액세스 서버에서 사용하는 프로토콜(TACACS+ 또는 Radius).

이전 매개변수를 구성하는 데 사용되는 정확한 절차는 AAA 서버 설명서를 참조하십시오. AAA 서버가 올바르게 구성되지 않은 경우 NAS의 AAA 요청을 AAA 서버에서 무시할 수 있으며 연결이 실패할 수 있습니다.

AAA 서버는 액세스 서버에서 IP에 연결할 수 있어야 합니다(연결을 확인하기 위해 **ping** 테스트 수행).

인증 구성

인증은 네트워크 및 네트워크 서비스에 대한 액세스가 허용되기 전에 사용자를 확인합니다(권한 부여로 확인됨).

AAA 인증을 구성하려면

1. 먼저 (글로벌 컨피그레이션 모드에서) 인증 방법의 명명된 목록을 정의합니다.
2. 하나 이상의 인터페이스에 목록을 적용합니다(인터페이스 컨피그레이션 모드).

유일한 예외는 default 메서드 목록(default라는 이름)입니다. 기본 메서드 목록은 명시적으로 정의된 명명된 메서드 목록이 있는 인터페이스를 제외한 모든 인터페이스에 자동으로 적용됩니다. 정의된 메서드 목록이 기본 메서드 목록을 재정의합니다.

이러한 인증 예에서는 Radius, 로그인 및 PPP(Point-to-Point Protocol) 인증을 사용하여 메서드 및 명명된 목록과 같은 개념을 설명합니다. 모든 예에서 TACACS+는 Radius 또는 로컬 인증을 대신할 수 있습니다.

Cisco IOS 소프트웨어는 나열된 첫 번째 방법을 사용하여 사용자를 인증합니다. 해당 방법이 응답하지 않을 경우(오류로 표시됨) Cisco IOS 소프트웨어는 방법 목록에 나열된 다음 인증 방법을 선택합니다. 이 프로세스는 나열된 인증 방법과의 통신에 성공하거나 방법 목록에 정의된 모든 방법이 소진될 때까지 계속됩니다.

Cisco IOS Software는 이전 방법의 응답이 없을 때만 나열된 다음 인증 방법으로 인증을 시도합니다. 이 주기의 어느 시점에서든 인증이 실패하면, 즉 AAA 서버 또는 로컬 사용자 이름 데이터베이스 응답이 사용자 액세스를 거부하면(FAIL로 표시됨) 인증 프로세스가 중지되고 다른 인증 방법이 시도되지 않습니다.

사용자 인증을 허용하려면 AAA 서버에서 사용자 이름과 비밀번호를 구성해야 합니다.

로그인 인증

aaa authentication login 명령을 사용하여 액세스 서버(tty, vty, console 및 aux)에 exec 액세스를 원하는 사용자를 인증할 수 있습니다.

예 1: Radius로 Exec 액세스, Local(로컬)

```
Router(config)#aaa authentication login default group radius local
```

이전 명령에서 다음을 수행합니다.

- 명명된 목록은 기본 목록입니다(기본값).
- 두 가지 인증 방법(그룹 RADIUS 및 로컬)이 있습니다.

모든 사용자는 Radius 서버로 인증됩니다(첫 번째 방법). Radius 서버가 응답하지 않으면 라우터 로컬 데이터베이스가 사용됩니다(두 번째 방법). 로컬 인증의 경우 사용자 이름 및 비밀번호를 정의합니다.

```
Router(config)#username xxx password yyy
```

aaa authentication login 명령의 목록 기본값이 사용되므로 모든 로그인 연결(예: tty, vty, console 및

aux)에 대해 로그인 인증이 자동으로 적용됩니다.

참고: AAA 서버에 액세스 서버가 올바르게 정의되지 않았거나 AAA 서버가 액세스 서버에 올바르게 정의되지 않은 경우, IP 연결이 없는 경우 서버(Radius 또는 TACACS+)는 액세스 서버가 보낸 **aaa 인증 요청**에 응답할 수 없습니다.

참고: 이전 예를 local 키워드 없이 사용할 경우 **결과**는 다음과 같습니다.

```
Router(config)#aaa authentication login default group radius
```

참고: AAA 서버가 인증 요청에 응답하지 않을 경우, (라우터에 시도할 대체 방법이 없으므로) 인증이 실패합니다.

참고: group **키워드**는 현재 서버 호스트를 그룹화하는 방법을 제공합니다. 이 기능을 사용하면 구성된 서버 호스트의 하위 집합을 선택하여 특정 서비스에 사용할 수 있습니다.

예 2: 회선 암호와 함께 사용되는 콘솔 액세스

콘솔 로그인이 라인 con 0에 설정된 비밀번호로만 인증되도록 Example 1에서 컨피그레이션을 확장합니다.

목록 CONSOLE이 정의된 다음 행 0에 적용됩니다.

설정:

```
Router(config)#aaa authentication login CONSOLE line
```

이전 명령에서 다음을 수행합니다.

- 명명된 목록은 CONSOLE입니다.
- 인증 방법(라인)은 하나뿐입니다.

이름이 지정된 목록(이 예에서는 CONSOLE)을 만들 경우 실행하기 전에 라인이나 인터페이스에 적용해야 합니다. 이 작업은 login authentication 명령을 사용합니다:

```
Router(config)#line con 0
Router(config-line)#exec-timeout 0 0
Router(config-line)#password cisco
Router(config-line)#login authentication CONSOLE
```

CONSOLE 목록은 라인 con 0의 기본 방법 목록**을 재정의합니다**. 라인 con 0에서 이 구성을 수행한 후에는 비밀번호 **cisco**를 입력하여 콘솔 액세스를 가져와야 합니다. 기본 목록은 tty, vty 및 aux에서 계속 사용됩니다.

참고: 로컬 사용자 이름 및 비밀번호로 콘솔 액세스를 인증하려면 다음 코드 예를 사용합니다.

```
Router(config)#aaa authentication login CONSOLE local
```

이 경우 라우터의 로컬 데이터베이스에 사용자 이름과 비밀번호를 구성해야 합니다. 목록도 회선 또는 인터페이스에 적용해야 합니다.

참고: 인증을 사용하지 않으려면 다음 코드 예를 사용합니다.

```
Router(config)#aaa authentication login CONSOLE none
```

이 경우 콘솔 액세스에 대한 인증이 없습니다. 목록도 회선 또는 인터페이스에 적용해야 합니다.

예 3: 외부 AAA 서버와 함께 사용되는 모드 액세스 활성화

enable 모드(권한 15)에 대한 인증을 수행할 수 있습니다.

설정:

```
Router(config)#aaa authentication enable default group radius enable
```

비밀번호만 요청할 수 있으며 사용자 이름은 $enab15$입니다. 따라서 사용자 이름 $enab15$는 AAA 서버에서 정의되어야 합니다.

Radius 서버가 응답하지 않으면 라우터에 로컬로 구성된 enable 비밀번호를 입력해야 합니다.

PPP 인증

aaa **authentication ppp** 명령은 PPP 연결을 인증하는 데 사용됩니다. 일반적으로 액세스 서버를 통해 인터넷이나 중앙 사무실에 액세스하려는 ISDN 또는 아날로그 원격 사용자를 인증하는 데 사용됩니다.

예 1: 모든 사용자를 위한 단일 PPP 인증 방법

액세스 서버에는 PPP 전화 접속 클라이언트를 허용하도록 구성된 ISDN 인터페이스가 있습니다. 다이얼러 **로터리 그룹 0을 사용하지만**, 컨피그레이션은 기본 인터페이스 또는 다이얼러 프로파일 인터페이스에서 수행할 수 있습니다.

설정:

```
Router(config)#aaa authentication ppp default group radius local
```

이 명령은 Radius를 사용하는 모든 PPP 사용자를 인증합니다. Radius 서버가 응답하지 않으면 로컬 데이터베이스가 사용됩니다.

예 2: 특정 목록과 함께 사용되는 PPP 인증

기본 목록 대신 명명된 목록을 사용하려면 다음 명령을 구성합니다.

```
Router(config)#aaa authentication ppp ISDN_USER group radius

Router(config)#interface dialer 0
Router(config-if)#ppp authentication chap ISDN_USER
```

이 예에서는 목록이 ISDN_USER이고 방법이 Radius입니다.

예 3: 문자 모드 세션 내에서 PPP 실행

액세스 서버에는 내부 모뎀 카드(Mica, Microcom 또는 Next Port)가 있습니다. **aaa authentication login** 및 **aaa authentication ppp 명령**이 모두 구성되어 있다고 가정합니다.

모뎀 사용자가 처음으로 문자 모드 실행 세션을 통해 라우터에 액세스하는 경우(예: 다이얼 후 터미널 창 사용), 사용자는 tty 회선에서 인증됩니다. 패킷 모드 세션으로 시작하려면 사용자가 ppp default 또는 **ppp를** 입력해야 합니다. PPP 인증이 명시적으로 구성되기 때문에(**aaa authentication ppp**) 사용자는 PPP 레벨에서 다시 인증됩니다.

이 두 번째 인증을 방지하려면 **if-needed 키워드를** 사용합니다.

```
Router(config)#aaa authentication login default group radius local
Router(config)#aaa authentication ppp default group radius local if-needed
```

> **참고:** 클라이언트가 PPP 세션을 직접 시작하면 액세스 서버에 대한 로그인 액세스가 없으므로 PPP 인증이 직접 수행됩니다.

권한 부여 구성

권한 부여는 사용자가 수행할 수 있는 작업을 제어할 수 있는 프로세스입니다.

AAA 권한 부여에는 인증과 동일한 규칙이 있습니다.

1. 먼저 권한 부여 방법의 명명된 목록을 정의합니다.
2. 그런 다음 하나 이상의 인터페이스에 해당 목록을 적용합니다(기본 방법 목록 제외).
3. 나열된 첫 번째 방법이 사용됩니다. 대응하지 못하면 두 번째를 사용하는 등.

메서드 목록은 요청된 권한 부여 유형에 따라 다릅니다. 이 문서에서는 Exec 및 네트워크 권한 부여 유형에 중점을 둡니다.

다른 권한 부여 유형에 대한 자세한 내용은 Cisco IOS 보안 컨피그레이션 가이드를 참조하십시오.

실행 권한 부여

aaa **authorization exec 명령**은 사용자가 EXEC 셸을 실행할 수 있는지 여부를 결정합니다. 이 기능은 자동 명령 정보, 유휴 시간 제한, 세션 시간 제한, 액세스 목록 및 권한 및 기타 사용자별 요소와 같은 사용자 프로필 정보를 반환할 수 있습니다.

EXEC 권한 부여는 vty 및 tty 행에서만 수행됩니다.

다음 예에서는 Radius를 사용합니다.

예 1: 모든 사용자에 대해 동일한 Exec 인증 방법

인증할 때:

```
Router(config)#aaa authentication login default group radius local
```

액세스 서버에 로그인하려는 모든 사용자는 Radius(첫 번째 방법) 또는 로컬 데이터베이스(두 번째 방법)를 통해 권한을 부여받아야 합니다.

설정:

```
Router(config)#aaa authorization exec default group radius local
```

> **참고:** AAA 서버에서 Service-Type=1(login)을 선택해야 합니다.

> **참고:** 이 예에서는 local 키워드**가** 포함되지 않고 AAA 서버가 응답하지 않으면 권한 부여가 불가능하고 연결이 실패할 수 있습니다.

> **참고:** 다음 예 2 및 3에서는 라우터에 어떤 명령도 추가할 필요가 없습니다. 액세스 서버에서 프로파일만 구성하면 됩니다.

예 2: AAA 서버에서 Exec 권한 레벨 할당

예 1을 기반으로 사용자가 액세스 서버에 로그인하고 활성화 모드를 직접 시작할 수 있도록 AAA 서버에서 다음 Cisco AV 쌍을 구성합니다.

```
shell:priv-lvl=15
```

이제 사용자가 활성화 모드로 직접 이동할 수 있습니다.

> **참고:** 첫 번째 방법이 응답하지 않으면 로컬 데이터베이스가 사용됩니다. 그러나 사용자는 enable 모드로 직접 이동할 수 없지만 enable 명령을 입력하고 enable 비밀번호를 **제공해야** 합니다.

예 3: AAA 서버에서 Idle-Timeout 할당

유휴 시간 제한을 구성하려면(유휴 시간 제한 후 트래픽이 없을 경우 세션 연결이 끊어지도록) IETF Radius 특성 28을 사용합니다. 사용자 프로필의 유휴 시간 제한입니다.

네트워크 권한 부여

이 aaa authorization network 이 명령은 PPP, SLIP 및 ARAP와 같은 모든 네트워크 관련 서비스 요청에 대한 권한 부여를 실행합니다. 이 절에서는 가장 일반적으로 사용되는 PPP를 중점적으로 살펴본다

.

AAA 서버는 클라이언트에 의한 PPP 세션이 허용되는지 확인합니다. 또한 클라이언트가 PPP 옵션을 요청할 수 있습니다. 콜백, 압축, IP 주소 등 이러한 옵션은 AAA 서버의 사용자 프로필에서 구성해야 합니다. 또한 특정 클라이언트에 대해 AAA 프로필은 유휴 시간 제한, 액세스 목록 및 Cisco IOS 소프트웨어가 다운로드하고 이 클라이언트에 적용할 수 있는 기타 사용자별 특성을 포함할 수 있습니다.

다음 예에서는 Radius를 통한 권한 부여를 보여줍니다.

예 1: 모든 사용자에 대해 동일한 네트워크 인증 방법

액세스 서버는 PPP 전화 접속 연결을 수락하는 데 사용됩니다.

다음과 같이 사용자가 인증됩니다(이전에 구성된 대로).

```
Router(config)#aaa authentication ppp default group radius local
```

다음 명령을 사용하여 사용자에게 권한을 부여합니다.

```
Router(config)#aaa authorization network default group radius local
```

참고: AAA 서버에서 다음을 구성합니다. Service-Type=7(프레임) 및 Framed-Protocol=PPP.

예 2: 사용자별 특성 적용

AAA 서버를 사용하여 IP 주소, 콜백 번호, 다이얼러 유휴 시간 제한 값 또는 액세스 목록 등과 같은 사용자별 특성을 할당할 수 있습니다. 이러한 구현에서 NAS는 AAA 서버 사용자 프로필에서 적절한 특성을 다운로드합니다.

예 3: 특정 목록의 PPP 권한 부여

인증과 마찬가지로 기본 목록 이름이 아닌 목록 이름을 구성합니다.

```
Router(config)#aaa authorization network ISDN_USER group radius local
```

그런 다음 이 목록을 인터페이스에 적용합니다.

```
Router(config)#interface dialer 0
Router(config-if)#ppp authorization ISDN_USER
```

계정 구성

AAA 어카운팅 기능을 사용하면 사용자가 액세스하는 서비스 및 사용자가 사용하는 네트워크 리소스의 양을 추적할 수 있습니다.

AAA 어카운팅에는 인증 및 권한 부여와 동일한 규칙이 있습니다.

1. 먼저 이름이 지정된 회계 방법 목록을 정의해야 합니다.
2. 그런 다음 하나 이상의 인터페이스에 해당 목록을 적용합니다(기본 방법 목록 제외).
3. 첫 번째 나열된 방법이 사용되는데, 응답하지 못하면 두 번째 나열된 방법이 사용됩니다.

- 네트워크 어카운팅은 모든 PPP, Slip 및 AppleTalk ARAP(Remote Access Protocol) 세션에 대한 정보를 제공합니다. 패킷 수, 옥텟 수, 세션 시간, 시작 및 중지 시간.
- Exec 어카운팅은 네트워크 액세스 서버의 사용자 EXEC 터미널 세션(예를 들어 텔넷 세션)에 대한 정보를 제공합니다. 세션 시간, 시작 및 중지 시간.

다음 예에서는 AAA 서버로 정보를 전송하는 방법에 중점을 둡니다.

어카운팅 컨피그레이션 예

예 1: 시작 및 중지 계정 레코드 생성

모든 다이얼인 PPP 세션에서 클라이언트가 인증되고 연결이 끊어진 후 **start-stop 키워드**를 사용하여 어카운팅 정보가 AAA 서버로 전송됩니다.

```
Router(config)#aaa accounting network default start-stop group radius local
```

예 2: 계정 관리 중지만 생성

클라이언트의 연결이 끊긴 후에만 계정 정보를 전송해야 하는 경우 stop 키워드를 사용하여 다음 **줄**을 구성합니다.

```
Router(config)#aaa accounting network default stop group radius local
```

예 3: 인증 및 협상 실패에 대한 리소스 레코드 생성

이 시점까지 AAA 어카운팅은 사용자 인증을 통과한 통화에 대한 시작 및 중지 레코드 지원을 제공합니다.

인증 또는 PPP 협상이 실패하면 인증 기록이 없습니다.

해결 방법은 AAA 리소스 오류 계정 정지를 사용하는 것입니다.

```
Router(config)#aaa accounting send stop-record authentication failure
```

AAA 서버에 중지 레코드가 전송됩니다.

예 4: 전체 자원 계정 관리 사용

통화 설정 시 시작 레코드 및 통화 종료 시 중지 레코드를 모두 생성하는 전체 리소스 어카운팅을 활성화하려면 다음을 구성합니다.

```
Router(config)#aaa accounting resource start-stop
```

이 명령은 Cisco IOS Software 릴리스 12.1(3)T에서 도입되었습니다.

이 명령을 사용하면 통화 설정 및 통화 연결 끊기 시작-중지 어카운팅 레코드가 디바이스에 대한 리소스 연결의 진행률을 추적합니다. 별도의 사용자 인증 시작-중지 계정 관리 레코드는 사용자 관리 진행률을 추적합니다. 이 두 어카운팅 레코드 세트는 통화에 대한 고유한 세션 ID와 상호 연결됩니다.

관련 정보

- Technical Support - Cisco Systems

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.