Catalyst 스위치에서 TACACS+, RADIUS 및 Kerberos 구성

목차

소개

Cisco Catalyst 스위치 제품군(Catalyst 4000, Catalyst 5000 및 CatOS를 실행하는 Catalyst 6000)은 2.2 코드에서 시작되는 일부 인증 유형을 지원합니다. 이후 버전에서 향상된 기능이 추가되었습니다. 인증, 권한 부여 및 계정 관리(AAA)를 위한 XTACACS UDP(User Datagram Protocol) 포트 49가 아닌 TACACS+ TCP 포트 49, RADIUS 또는 Kerberos 서버 사용자 설정은 라우터 사용자와 동일합니다. 이 문서에는 이러한 기능을 활성화하는 데 필요한 최소 명령의 예가 포함되어 있습니다. 해당 버전의 스위치 설명서에서 추가 옵션을 사용할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

배경 정보

이후 버전의 코드에서는 추가 옵션을 지원하므로 스위치의 코드 버전을 확인하려면 **show version** 명령을 실행해야 합니다. 스위치에서 사용되는 코드의 버전을 결정한 후에는 이 표를 사용하여 장비에서 사용할 수 있는 옵션과 구성할 옵션을 결정합니다.

인증 및 권한 부여를 추가할 때 항상 스위치에 유지됩니다. 실수로 잠기지 않도록 다른 창에서 컨피그레이션을 테스트합니다.

메서드(최소)	**Cat 버전 2.2 ~ 5.1**	**Cat 버전 5.1 ~ 5.4.1**	**Cat 버전 5.4.1 ~ 7.5.1**	**Cat 버전 7.5.1 이상**
TACACS+ 인증 또는	단계 A	단계 A	단계 A	단계 A
RADIUS 인증 또는	해당 없음	B단계	B단계	B단계
Kerberos 인증 또는	해당 없음	해당 없음	K단계	K단계
로컬 사용자 이름 인증/권한 부여	해당 없음	해당 없음	해당 없음	단계 C
더하기(옵션)				
TACACS+ 명령어 권한 부여	해당 없음	해당 없음	단계 D	단계 D
TACACS+ EXEC 권한 부여	해당 없음	해당 없음	E단계	E단계
RADIUS EXEC 권한 부여	해당 없음	해당 없음	F단계	F단계
계정 관리 - TACACS+ 또는 RADIUS	해당 없음	해당 없음	단계 G	단계 G
TACACS+ 권한 부여 사용	H단계	H단계	H단계	H단계
RADIUS 권한 부여 사용	해당 없음	1단계	1단계	1단계
TACACS+ 권한 부여 사용	해당 없음	해당 없음	단계 J	단계 J

구성 단계

A단계 - TACACS+ 인증

이전 버전의 코드에서 명령은 일부 이후 버전만큼 복잡하지 않습니다. 스위치에서 최신 버전의 추가 옵션을 사용할 수 있습니다.

1. 서버가 다운된 경우 스위치에 백도어가 있는지 확인하려면 **set authentication login local enable** 명령을 실행합니다.
2. TACACS+ 인증을 **활성화하려면 set authentication login tacacs enable** 명령을 실행합니다.
3. **set tacacs server #.#.#.#** 명령을 실행하여 서버를 정의합니다.
4. set tacacs **key *your_key* 명령**을 실행하여 TACACS+에서 선택적인 서버 키를 정의하면 스위치-서버 데이터가 암호화됩니다. 사용하는 경우 서버와 일치해야 합니다.**참고:** Cisco Catalyst OS 소프트웨어에서는 키 또는 비밀번호의 일부로 물음표(**?**)를 허용하지 **않습니다**. 물음표는 명령 구문에 대한 도움말에 명시적으로 사용됩니다.

B 단계 - RADIUS 인증

이전 버전의 코드에서 명령은 일부 이후 버전만큼 복잡하지 않습니다. 스위치에서 최신 버전의 추가 옵션을 사용할 수 있습니다.

1. 서버가 다운된 경우 스위치에 백도어가 있는지 확인하려면 **set authentication login local enable** 명령을 실행합니다.
2. RADIUS **인증을 활성화하려면 set authentication login radius enable** 명령을 실행합니다.
3. 서버를 정의합니다. 다른 모든 Cisco 장비에서 기본 RADIUS 포트는 1645/1646(인증/어카운팅)입니다.Catalyst에서 기본 포트는 1812/1813입니다. Cisco Secure 또는 다른 Cisco 장비와 통신하는 서버를 사용하는 경우 1645/1646 포트를 사용합니다. **set radius server #.#.#.# auth-port 1645 acct-port 1646 primary** 명령을 실행하여 Cisco IOS에서 서버를 정의하고 이에 상응하는 명령을 **radius-server source-ports 1645-1646으로** 정의합니다.
4. 서버 키를 정의합니다.이는 RADIUS 인증/권한 부여 RFC 2865 및 RADIUS 어카운팅 RFC 2866 에서와 같이 스위치-서버 비밀번호를 암호화하도록 하기 때문에 필수 사항입니다. 사용하는 경우 서버와 일치해야 합니다. set radius **key *your_key* 명령을 실행합니다**.

C 단계 - 로컬 사용자 이름 인증/권한 부여

CatOS 버전 7.5.1부터 로컬 사용자 인증이 가능합니다. 예를 들어, 로컬 비밀번호로 인증하는 대신 Catalyst에 저장된 사용자 이름과 비밀번호를 사용하여 인증/권한 부여를 수행할 수 있습니다.

로컬 사용자 인증에는 두 가지 권한 레벨(0 또는 15)만 있습니다. 레벨 0은 비권한 exec 레벨입니다. 레벨 15는 특별 권한 활성화 레벨입니다.

이 예에서 이 명령을 추가하면 사용자 `poweruser` 텔넷 또는 콘솔의 enable 모드로 스위치에 도착하고 사용자가 `nonenable`을 지원하지 않는 사용자가 텔넷 또는 콘솔의 exec 모드로 스위치에 도착합니다.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

참고: 사용자가 `enable` 비밀번호 **설정**을 있으면 해당 사용자는 모드를 계속 활성화할 수 있습니다.

컨피그레이션 후에는 비밀번호가 암호화됩니다.

로컬 사용자 이름 인증은 원격 TACACS+ exec, 명령 어카운팅 또는 원격 RADIUS exec 어카운팅과 함께 사용할 수 있습니다. 또한 원격 TACACS+ exec 또는 명령 권한 부여와 함께 사용할 수도 있지만, 사용자 이름을 TACACS+ 서버 및 로컬 스위치에 모두 저장해야 하므로 이 방법을 사용하는 것은 적절하지 않습니다.

D단계 - TACACS+ 명령 권한 부여

이 예에서 스위치에는 TACACS+를 사용하는 컨피그레이션 명령에만 권한 부여가 필요하다는 메시지가 표시됩니다. TACACS+ 서버가 다운된 경우 인증은 none입니다. 이는 콘솔 포트 및 텔넷 세션 모두에 적용됩니다. 다음 명령을 실행합니다.

authorization 명령 enable config tacacs none 모두 설정

이 예에서는 다음 매개변수를 설정할 때 허용하도록 TACACS+ 서버를 구성할 수 있습니다.

```
command=set
arguments (permit)=port 2/12
```

set port enable 2/12 명령이 확인을 위해 TACACS+ 서버로 전송됩니다.

참고: 명령 권한 부여가 활성화된 경우 enable이 명령으로 간주되지 않는 라우터와는 달리 enable을 시도하면 스위치에서 enable 명령을 서버로 전송합니다. 서버가 enable 명령을 허용하도록 구성되어 있는지 **확인합니다**.

E단계 - TACACS+ Exec 인증

이 예에서는 스위치가 TACACS+를 사용하는 exec 세션에 대한 권한 부여를 필요로 합니다. TACACS+ 서버가 다운된 경우 권한 부여는 none입니다. 이는 콘솔 포트와 텔넷 세션 모두에 적용됩니다. set authorization exec enable tacacs**+ none both** 명령**을 실행합니다.**

인증 요청 외에도 스위치에서 TACACS+ 서버에 별도의 권한 부여 요청을 보냅니다. 사용자 프로필이 TACACS+ 서버에서 shell/exec에 대해 구성된 경우 해당 사용자는 스위치에 액세스할 수 있습니다.

이렇게 하면 PPP 사용자와 같이 서버에 구성된 셸/exec 서비스가 없는 사용자가 스위치에 로그인할 수 없습니다. `Exec` 를 읽는 메시지 얻을 수 있습니다. 사용자에 대한 EXEC 모드를 허용/거부하는 것 외에도, 서버에 할당된 권한 수준 15를 사용하여 시작할 때 활성화 모드를 강제로 사용할 수 있습니다. Cisco 버그 ID CSCdr51314(등록된 고객만 해당)가 고정된 코드를 실행해야 합니다.

F 단계 - RADIUS Exec 권한 부여

RADIUS exec 권한 부여를 활성화하는 명령이 없습니다. 또는 RADIUS 서버에서 Service-Type(RADIUS 특성 6)을 Administrative(관리)로 설정하여 사용자를 RADIUS 서버에서 활성화 모드로 실행하는 것이 좋습니다. 1-login, 7-shell 또는 2-framed와 같이 6-administrative 이외의 항목에 대해 service-type이 설정된 경우 사용자는 enable 프롬프트가 아니라 switch exec 프롬프트에 도착합니다.

인증 및 권한 부여를 위해 스위치에 다음 명령을 추가합니다.

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

G 단계 - 계정 관리 - TACACS+ 또는 RADIUS

TACACS+ 어카운팅을 활성화하려면

1. 스위치 프롬프트가 표시되면 set accounting exec enable start-**stop tacacs+** 명령**을** 실행합니다.
2. 스위치에서 텔넷이 실행되는 사용자는 **set accounting connect enable start-stop tacacs+** 명령을 실행합니다.
3. 스위치를 재부팅하는 경우 set accounting system enable start-stop tacacs**+** 명령**을** 실행합니다.
4. 명령을 수행하는 사용자는 set accounting **명령을 실행하여 모든 start-stop tacacs+** 명령을 활성화합니다.
5. 예를 들어, 사용자가 여전히 로그인되어 있음을 보여주기 위해 1분에 한 번 레코드를 업데이트하려면 set accounting update periodic **1** 명령**을 실행합니다**.

RADIUS 어카운팅을 활성화하려면

1. 스위치 프롬프트를 가져오는 사용자는 set accounting exec enable start-stop radius 명령**을** 실행합니다.
2. 스위치에서 텔넷하는 사용자는 set accounting connect enable start-stop radius 명령**을** 실행합니다.
3. 스위치를 재부팅할 때 set **accounting system enable start-stop radius** 명령**을** 실행합니다.
4. 예를 들어, 사용자가 여전히 로그인되어 있음을 보여주기 위해 1분에 한 번 레코드를 업데이트하려면 set accounting update periodic **1** 명령**을** 실행합니다.

TACACS+ 프리웨어 레코드

이 출력은 레코드가 서버에 표시되는 방법의 예입니다.

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

UNIX의 RADIUS 레코드 출력

이 출력은 레코드가 서버에 표시되는 방법의 예입니다.

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

H단계 - TACACS+ 인증 활성화

다음 단계를 완료하십시오.

1. 서버가 다운된 경우 백 도어가 있는지 확인하려면 set authentication enable local enable 명령을 실행합니다.
2. 스위치가 활성화 요청을 서버로 전송하도록 **지시하려면 set authentication enable tacacs enable** 명령을 실행합니다.

1단계 - RADIUS 인증 활성화

스위치를 RADIUS 서버에 사용자 이름 `$enab15$`를 전송하도록 하려면 다음 명령을 추가합니다. 일부 RADIUS 서버는 이러한 유형의 사용자 이름을 지원하지 않습니다. 다른 대체는 E단계를 참조하

십시오. 예를 들어 개별 사용자를 활성화 모드로 실행하는 서비스 유형 [RADIUS attribute 6 - Administrative]를 설정한 경우.

1. 서버가 다운된 경우 백도어가 있는지 확인하려면 set authentication enable local enable 명령을 실행합니다.
2. RADIUS 서버가 $enab15$ 사용자 이름을 지원하는 경우 스위치에서 서버에 enable 요청을 보내도록 하려면 set authentication enable radius enable 명령을 실행합니다.

J 단계 - TACACS+ 권한 부여 사용

이 명령을 추가하면 사용자가 활성화하려고 할 때 스위치가 enable을 서버에 전송합니다. 서버에서 enable 명령을 **허용해야** 합니다. 이 예에서는 서버가 다운된 경우 none으로 페일오버가 수행됩니다.

author enable tacacs+ none 모두 설정

K단계 - Kerberos 인증

스위치에 Kerberos를 설정하는 방법에 대한 자세한 내용은 Control and Monitoring Access to the Switch Using Authentication, Authorization, and Accounting을 참조하십시오.

비밀번호 복구

비밀번호 복구 절차에 대한 자세한 내용은 비밀번호 복구 프로시저를 참조하십시오.

이 페이지는 Cisco 제품에 대한 비밀번호 복구 절차의 인덱스입니다.

추가 보안을 위한 ip permit 명령

추가 보안을 위해 **ip permit** 명령을 통해 텔넷 액세스를 제어하도록 Catalyst를 구성할 수 있습니다.

ip permit enable telnet 설정

ip permit *범위 마스크|host 설정*

이렇게 하면 스위치에 텔넷에 지정된 범위나 호스트만 허용됩니다.

Catalyst에서 디버그

Catalyst에서 디버깅을 활성화하기 전에 서버 로그에서 실패 원인을 확인합니다. 따라서 스위치의 운영이 더욱 쉽고 간단해집니다. 이전 스위치 버전에서는 **디버그**가 엔지니어링 모드에서 수행되었습니다. 다음 코드의 이후 버전에서 **debug** 명령을 실행하기 위해 엔지니어링 모드에 액세스할 필요가 없습니다.

추적 tacacs|radius|kerberos 4 설정

참고: set trace tacacs|radius|kerberos 0 명령은 Catalyst를 no-tracing 모드로 반환합니다.

멀티레이어 LAN 스위치에 대한 자세한 내용은 스위치 제품 지원 페이지를 참조하십시오.

관련 정보

- TACACS+ 및 RADIUS 비교
- Cisco IOS 설명서의 RADIUS, TACACS+ 및 Kerberos
- RADIUS 지원 페이지
- TACACS/TACACS+ 지원 페이지
- Kerberos 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems