낮은 권한 수준의 사용자에 대해 전체 "show running-config"를 표시하도록 IOS-XE를 구성합니다.

목차

소개

이 문서에서는 낮은 권한 수준의 라우터에 로그인한 사용자의 전체 실행 중인 컨피그레이션을 표시하는 방법에 대한 컨피그레이션 단계를 설명합니다. 아래의 문제를 이해하고 이를 해결하려면 특권 수준을 이해하는 것이 필요하다. 사용 가능한 권한 수준은 0~15이며, 관리자가 어떤 권한 수준에서 어떤 명령을 사용할 수 있는지 사용자 지정할 수 있습니다. 기본적으로 라우터의 세 가지 권한 레벨은 다음과 같습니다.

- 레벨 0 - 기본 명령만 포함합니다(disable, enable, exit, help, logout).
- 레벨 1 - 사용자 EXEC 명령 모드에서 사용 가능한 모든 명령을 포함합니다.
- 레벨 15 - 특별 권한 EXEC 명령 모드에서 사용 가능한 모든 명령을 포함합니다.

이러한 최소 수준과 최대 수준 사이의 나머지 수준은 관리자가 명령 및/또는 사용자를 할당할 때까지 정의되지 않습니다. 따라서 관리자는 이러한 최소 및 최대 권한 레벨 사이에서 사용자에게 서로 다른 권한 레벨을 할당하여 서로 다른 사용자가 액세스할 수 있는 권한을 구분할 수 있습니다. 그런 다음 관리자는 개별 권한 레벨에 개별 명령(및 다양한 기타 옵션)을 할당하여 이 레벨의 모든 사용자가 사용할 수 있도록 할 수 있습니다. 예를 들면 다음과 같습니다.

```
Router(config)# 사용자 이름 user1  권한 7 비밀번호 P@ssw0rD1
Router(config)# 권한 exec  level 7 show access-lists
```

이 컨피그레이션에서는 라우터에 'user1'이 연결되면 'show access-lists' 명령 및/또는 해당 권한 수준에서 활성화된 다른 명령을 실행할 수 있습니다. 그러나 'show running-config' 명령을 활성화한 경우에도 동일하게 설명할 수 없습니다. 이에 대해서는 아래에서 문제 설명과 함께 설명합니다.

사전 요구 사항

요구 사항

이 문서를 이해하려면 cisco 권한 수준에 대한 기본적인 이해가 필요하며, 위 소개에서는 필요한 권한 수준에 대한 이해를 설명하기에 충분합니다.

사용되는 구성 요소

이 문서의 구성 예제에 사용된 구성 요소는 ASR1006이지만 모든 IOS/IOS-XE 장치는 비슷합니다.

"이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다."

컨피그레이션 문제

각기 다른 사용자를 위해 라우터에 서로 다른 액세스 레벨을 구성하는 경우, 네트워크 관리자가 특정 사용자에게 'show' 명령에만 액세스할 수 있도록 지정하고 'configuration' 명령에는 액세스할 수 없도록 지정하는 것이 일반적인 애플리케이션입니다. 이는 대부분의 show 명령에 대한 간단한 작업으로, 다음과 같이 간단한 컨피그레이션을 통해 액세스 권한을 부여할 수 있습니다.

```
Router(config)# 사용자 이름 test_user  권한 10 비밀번호 testP@ssw0rD
Router(config)# 권한 exec  레벨 10 표시
Router(config)# 권한 exec  레벨 10 show running-config
```

이 예제 컨피그레이션에서는 두 번째 행에서 'test_user'가 일반적으로 이 권한 수준에서는 사용할 수 없는 다양한 show 관련 명령에 액세스할 수 있습니다. 그러나 show running-config 명령은 대부분의 show 명령과 다르게 처리됩니다. 예제 코드의 세 번째 줄에서도 해당 명령이 올바른 권한 수준에서 지정되었음에도 불구하고 생략되거나 축약된 'show running-config'만 사용자에게 표시됩니다.

```
사용자 액세스 확인

사용자 이름: test_user
암호:
라우터 번호
Router#show  권한
현재 권한 레벨은 10입니다.
라우터 번호
Router#show running-config
구성을 빌드하는 중...

현재 컨피그레이션: 121바이트
!
! 21:10:08 UTC Mon Aug 28 2017의 마지막 구성 변경
!
부팅 시작 마커
부트 끝 표식
!
!
!
끝

라우터 번호
```

보시다시피 이 출력에는 컨피그레이션이 표시되지 않으며, 라우터 컨피그레이션에 대한 정보를 수집하려는 사용자에게 도움이 되지 않습니다. 이는 show running-config 명령은 사용자가 현재 권한 수준에서 수정할 수 있는 모든 명령만 표시하기 때문입니다. 이는 사용자가 현재 권한 수준 이상에

서 구성된 명령에 액세스할 수 없도록 하는 보안 컨피그레이션으로 설계되었습니다. 이는 'show running-config'가 엔지니어가 트러블슈팅 시 초기에 수집할 수 있는 표준 명령이기 때문에 show 명령에 액세스할 수 있는 사용자를 생성하려고 할 때 발생하는 문제입니다.

컨피그레이션 솔루션 및 확인

이러한 딜레마에 대한 해결 방법으로, 이 명령의 제한을 우회하는 기존의 show run 명령의 다른 버전이 있습니다.

```
Router(config)# show running-config view full
Router(config)# 권한 exec 레벨 10 show running-config view full
```

명령에 'view full'을 추가하면(그리고 사용자가 명령에 액세스할 수 있도록 명령의 권한 레벨을 변경할 수 있음) 이제 사용자는 생략된 명령 없이 전체 show running-config를 볼 수 있습니다.

```
사용자 이름: test_user
암호:
라우터 번호
Router#show 권한
현재 권한 레벨은 10입니다.
라우터 번호
Router#show running-config view full

구성을 빌드하는 중...

현재 컨피그레이션: 2664바이트
!
! 21:25:45 UTC Mon Aug 28 2017의 마지막 구성 변경
!
버전 15.4
서비스 타임스탬프 디버그 datetime msec
서비스 타임스탬프 로그 datetime msec
플랫폼 punt-keepalive disable-kernel-core 없음
!
호스트 이름 라우터
!
부팅 시작 마커
부트 시스템 플래시 bootflash:packages.conf
부트 시스템 플래시 부트플래시:asr1000rp1-adventerprisek9.03.13.06a.S.154-
3.S6a-ext.bin
부트 끝 표식
!
vrf 정의 관리-intf
 !
 주소군 ipv4
 출구 주소군
 !
```

```
 주소군 ipv6
 출구 주소군
!
enable 비밀번호 <생략>
!
aaa 신규 모델 없음
!
ip 도메인 조회 없음
!
가입자 템플릿
!
multilink bundle-name 인증
!
스패닝 트리 확장 시스템 ID
!
사용자 이름 test_user 권한 10 비밀번호 0 testP@ssw0rD
!
이중화
 모드 sso
!
cdp 실행
!
인터페이스 GigabitEthernet0/2/0
 ip 주소 없음
 셧다운
 자동 협상
!
인터페이스 GigabitEthernet0/2/1
 ip 주소 없음
 셧다운
 자동 협상
!
인터페이스 GigabitEthernet0
 vrf 포워딩 관리-intf
 IP 주소 <생략>
 자동 협상
 cdp 활성화
!
ip 전달 프로토콜 nd
!
제어 평면
!
!
권한 exec 레벨 10 show running-config view full
alias exec show-running-config show running-config view full
!
```

```
라인 con 0
 정지 비트 1
보조 0
 exec-timeout 0 1
 실행 안 함
 전송 출력 없음
 정지 비트 1
라인 vty 0 4
로컬 로그인
!
끝
라우터 번호
```

그러나 이렇게 하면 이 버전의 명령에 대한 사용자 액세스 권한을 제공함으로써 문제가 발생하지만, 이는 생략된 버전을 설계하여 해결하려고 했던 초기 보안 위험을 높이지 않습니까?

솔루션에 대한 해결 방법으로 그리고 보안 네트워크 설계에서 일관성을 보장하기 위해, 아래에 표시된 것처럼 사용자에게 액세스/지식을 제공하지 않고 show running-config 명령의 전체 버전을 실행할 사용자의 별칭을 생성할 수 있습니다.

```
Router(config)# alias exec show-running-config show running-config
view full
```

이 예에서 'show-running-config'는 별칭 이름이며, 사용자가 라우터에 로그인하면 명령 대신 이 별칭 이름을 입력하고 실행 중인 실제 명령을 알지 못한 채 필요한 출력을 받을 수 있습니다.

참고: 16.X 버전에서는 플랫폼에 따라 "(config)#file privilege <level>" 명령을 사용하여 파일에 권한을 추가해야 합니다.

결론

결론적으로, 이는 여러 레벨에서 사용자 권한 액세스를 관리적으로 생성할 때 더 많은 제어 권한을 갖는 방법의 한 예에 불과합니다. 다양한 권한 레벨을 생성하고 서로 다른 명령에 액세스할 수 있는 옵션이 많습니다. 'show-only' 사용자가 컨피그레이션 명령에 액세스할 수 없을 때 여전히 전체 running-config에 액세스할 수 있도록 하는 방법을 보여주는 예입니다.

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.