

오프라인 VBond/VSmart의 사용자 이름 및 비밀번호 재설정

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[기본 개념](#)

[시스코택 사용자 액세스](#)

[솔루션](#)

[1단계. ciscotacrw를 사용하여 SSH 로그인을 통해 vBond/vSmart에 액세스합니다.](#)

[2단계. 기존 사용자 비밀번호 재설정](#)

[3단계. 새 Netadmin 사용자 추가\(선택 사항\)](#)

[4단계. 잠긴 계정 잠금 해제\(해당되는 경우\)](#)

[5단계. 컨피그레이션 확인](#)

[관련 정보](#)

소개

이 문서에서는 SD-WAN 오프라인 vBond/vSmart의 사용자 이름 및 비밀번호를 재설정하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco SD-WAN(Software-defined Wide Area Network).

사용되는 구성 요소

이 문서의 정보는 Cisco vManager 버전 20.9.4를 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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

vBonds 및 vSmarts에 대한 액세스가 손실되었습니다. 이는 자격 증명을 알지 못하거나 기억하지 못하는 경우 또는 두 인터페이스에 로그인을 시도했으나 성공하지 못한 후 액세스가 잠긴 경우에 발생합니다. 이와 동시에 vManage, vSmarts 및 vBond 간의 제어 연결이 중단됩니다. 오프라인 vbond 및 vsmart는 vmanage GUI를 통해 작동할 수 없습니다.

기본 개념

시스코택 사용자 액세스

Cisco Edge 소프트웨어는 두 명의 사용자(ciscotacro 및 ciscotacrw)를 제공하며 이는 Cisco 지원 팀에서만 사용할 수 있습니다. 이러한 사용자는 클라우드 및 온프레미스 설치 모두에서 사용할 수 있습니다. 모든 새 로그인 세션에 대해 새 토큰이 필요한 동의 토큰 챌린지 및 토큰 응답 인증에서 작동합니다. ciscotacro 및 ciscotacrw 사용자는 이 토큰을 사용하여 Cisco SD-WAN Manager 웹 서버 및 Cisco SD-WAN Manager의 SSH 터미널에 로그인할 수 있습니다. 이러한 사용자는 Cisco SD-WAN Manager의 SSH 터미널을 사용하여 Cisco SD-WAN Validator, Cisco SD-WAN Controller 및 Cisco vEdge 디바이스에 액세스할 수도 있습니다.

기본 CLI 템플릿에는 ciscotacro 및 ciscotacrw 사용자 컨피그레이션이 포함됩니다. 이러한 사용자는 기본적으로 활성화되어 있습니다. 그러나 필요한 경우를 사용하여 이러한 사용자를 비활성화할 수 있습니다.

- ciscotacro 사용자: 이 사용자는 읽기 전용 권한만 있는 운영자 사용자 그룹의 일부입니다. 이 사용자는 컨피그레이션을 모니터링할 수만 있으며, 네트워크의 컨피그레이션을 수정하는 작업은 수행할 수 없습니다.
- ciscotacrw 사용자: 이 사용자는 읽기/쓰기 권한이 있는 netadmin 사용자 그룹의 일부입니다. 이 사용자는 네트워크 컨피그레이션을 수정할 수 있습니다. 또한 이 사용자만 동의 토큰을 사용하여 루트 셸에 액세스할 수 있습니다.

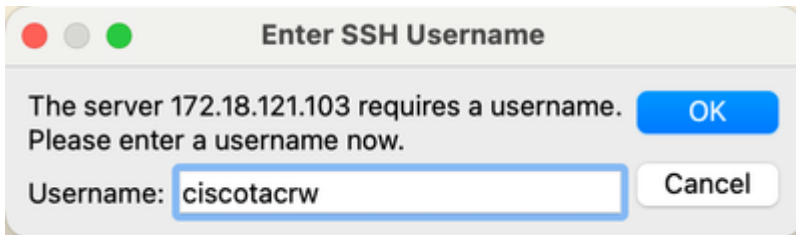


참고: "ciscotac" 사용자 계정이 도입되었으며 기본적으로 버전 20.x와 관련된 Cisco SD-WAN 소프트웨어 릴리스부터 포함됩니다.

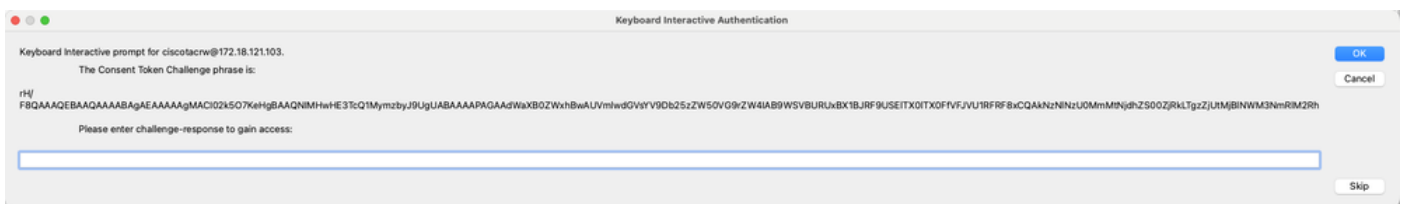
솔루션

1단계. ciscotacrw를 사용하여 SSH 로그인을 통해 vBond 또는 vSmart에 액세스합니다.

- 사용자 이름으로 ciscotacrw를 입력합니다.



- OK(확인)를 클릭하면 Consent Token Challenge(동의 토큰 챌린지) 구문이 그에 따라 생성됩니다.



- SR 케이스를 통해 TAC에 "Consent Token Challenge phrase"를 제공해야 합니다. 그런 다음 TAC는 해당 "sdwanchallenge-response 토큰"을 반환합니다.
- "sdwanchallenge-response token" 입력

2단계. 기존 사용자 비밀번호 재설정

ciscotacrw 계정을 통해 오프라인 vBond/vSmart에 로그인한 후(인증에 consent-token 사용) 사용자 이름과 비밀번호를 복원하거나 재설정할 수 있습니다.

- 컨피그레이션 모드를 시작하고 기존 사용자(예: admin)의 비밀번호를 재설정합니다.

```
vBond# config terminal
vBond(config)# system aaa user admin password <new password>
vBond(config)# commit
```



참고: 제출 후 시스템은 자동으로 일반 텍스트 비밀번호를 암호화합니다.

3단계. 새 Netadmin 사용자 추가(선택 사항)

새 관리자 계정을 만들어야 하는 경우:

```
vBond(config)# system aaa user <new username> password <new password>
vBond(config)# system aaa user <new username> group netadmin
vBond(config)# commit
```

4단계. 잠긴 계정 잠금 해제(해당되는 경우)

여러 번 실패한 로그인으로 인해 계정이 잠긴 경우 다음 명령을 사용하여 잠금을 해제할 수 있습니다.

```
request aaa unlock-user <username>
```

5단계. 컨피그레이션 확인

- show running-config system aaa 명령을 사용하여 사용자 컨피그레이션이 올바르게 적용되었는지 확인합니다.
- 성공적인 복구를 확인하기 위해 새 자격 증명으로 로그인을 시도합니다.



참고: vBond는 오프라인 상태(vManage와 연결되지 않았거나 연결이 끊어진 상태)이므로 vManage에서 템플릿을 발급하는 대신 CLI를 통해 직접 컨피그레이션을 완료하는 것이 좋습니다.



경고: 완료 후 vManage와의 관리 연결을 다시 설정해야 하는 경우 자격 증명이 vManage의 컨피그레이션과 일치하는지 확인하십시오.

관련 정보

- [제어 연결이 설정된 경우 SD-WAN vSmart 및 vBond 액세스 복구](#)

- [시스코택 사용자 액세스](#)

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.