Cisco Nexus 디바이스에서 Oxized 또는 RANCID 네트워크 디바이스 컨피그레이션 백업 도구에 대한 사용자 RBAC 구성

목차

소개

이 문서에서는 Cisco Nexus 디바이스에서 로컬 사용자 계정을 구성하여 Oxized 또는 RANCID 네트워크 디바이스 컨피그레이션 백업 툴에서 사용하는 명령으로 제한되는 RBAC(Role-Based Access Control) 역할을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다른 로컬 사용자 계정 및 RBAC 역할을 만들 수 있는 사용자 계정을 하나 이상 액세스할 수 있어야 합니다.일반적으로 이 사용자 계정에는 기본 "network-admin" 역할이 있지만 해당 역할은 특정 네트워크 환경 및 구성에 따라 다를 수 있습니다.

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- NX-OS에서 사용자 계정을 구성하는 방법
- NX-OS에서 RBAC 역할을 구성하는 방법
- 네트워크 디바이스 컨피그레이션 백업 툴을 구성하는 방법

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Nexus 9000 플랫폼 NX-OS 릴리스 7.0(3)I7(1) 이상

이 문서의 정보는 다음 네트워크 디바이스 컨피그레이션 백업 툴을 다룹니다.

- 산화된 v0.26.3
- RANCID v3.9

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 Oxized 및 RANCID 네트워크 디바이스 컨피그레이션 백업 도구에 대한 컨피그레이션 지침을 제공합니다.

> **참고:**다른 네트워크 디바이스 컨피그레이션 백업 툴을 사용하는 경우 Oxized 및 RANCID 절차를 예로 사용하고 상황에 맞게 지침을 수정합니다.

산화된 사용자 계정 및 역할 구성

Oxdized의 NX-OS 모델에서 볼 수 있듯이, Oxized는 NX-OS를 실행하는 모든 Cisco Nexus 디바이스에서 기본적으로 이 명령 목록을 실행합니다.

- 터미널 길이 0
- 버전 표시
- 인벤토리 표시
- show running-config

이러한 명령만 실행할 수 있는 사용자 계정을 구성하려면 다음 절차를 수행합니다.

1. 이러한 명령을 허용하는 RBAC 역할을 구성합니다.아래 예에서는 "산화됨"이 역할 이름으로 정의됩니다.

```
Nexus# configure terminal
Nexus(config)# role name oxidized
Nexus(config-role)# description Role for Oxidized network device configuration backup tool
Nexus(config-role)# rule 1 permit command terminal length 0
Nexus(config-role)# rule 2 permit command show version
Nexus(config-role)# rule 3 permit command show inventory
Nexus(config-role)# rule 4 permit command show running-config
Nexus(config-role)# end
Nexus#
```

> **주의:**위 예와 같이 **terminal length 0** 명령을 허용하는 규칙을 추가하는 것을 잊지 마십시오.이 명령을 사용할 수 없는 경우, **터미널 길이 0** 명령을 실행할 때 Oxized 사용자 계정에는 "% Permission denied for the role" 오류 메시지가 표시됩니다.Oxdized에서 실행하는 명령의 출력이 기본 터미널 길이인 24를 초과하면 Oxdized가 "—More—" 프롬프트(아래에 설명)를 정상적으로 처리하지 않고 디바이스에서 명령을 실행한 후 "Timeout::Error with msg 'execution expired' 경고 syslog를 생성합니다.

```
Nexus# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
```

```
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.35
  NXOS: version 7.0(3)I7(6)
--More--    <<<
```

2. 1단계에서 구성한 역할을 상속받는 새 사용자 계정을 구성합니다. 아래 예에서는 이 사용자 계정의 이름이 "산화됨"이고 암호가 "산화됨!123"입니다.

```
Nexus# configure terminal
Nexus(config)# username oxidized role oxidized password oxidized!123
Nexus(config)# end
Nexus#
```

3. 새 산화된 사용자 계정으로 Nexus 디바이스에 수동으로 로그인하고 문제 없이 필요한 모든 명령을 실행할 수 있는지 확인합니다.
4. Oxized의 입력 데이터 소스를 수정하여 새로운 Oxized 사용자 계정의 계정 자격 증명을 수락합니다.CSV 소스의 샘플 출력은 5개의 Nexus 디바이스와 함께 아래에 나와 있습니다.

```
nexus01.local:192.0.2.1:nxos:oxidized:oxidized!123
nexus02.local:192.0.2.2:nxos:oxidized:oxidized!123
nexus03.local:192.0.2.3:nxos:oxidized:oxidized!123
nexus04.local:192.0.2.4:nxos:oxidized:oxidized!123
nexus05.local:192.0.2.5:nxos:oxidized:oxidized!123
```

   위의 CSV 소스에 대한 관련 Oxed source 컨피그레이션이 아래에 나와 있습니다.

```
---
source:
  default: csv
  csv:
    file: "/filepath/to/router.db"
    delimiter: !ruby/regexp /:/
    map:
      name: 0
      ip: 1
      model: 2
      username: 3
      password: 4
```

5. 구성 파일 및 데이터 소스에 대해 산화됨 을 실행하고 구성된 데이터 출력에 모든 명령의 출력이 나타나는지 확인합니다.이 작업을 수행하는 특정 명령은 Oxdized의 구현 및 설치에 따라 달라집니다.

RANCID에 대한 사용자 계정 및 역할 구성

RANCID의 NX-OS 모델에서 볼 수 있듯이, RANCID는 NX-OS를 실행하는 모든 Cisco Nexus 디바이스에서 기본적으로 이 명령 목록을 실행합니다.

- 터미널 no monitor force
- 버전 표시
- show version build-info all
- 라이센스 표시
- 라이센스 사용 표시
- show license host id
- 시스템 이중화 상태 표시
- 환경 시계 표시
- 환경 팬 표시
- 환경 fex 모든 팬 표시
- 환경 온도 표시
- 환경 전원 표시
- 부팅 표시
- 디렉토리 부트 플래시:
- 디렉터리 디버그:
- dir logflash:
- dir 슬롯 0:
- dir usb1:
- dir usb2:
- dir volatile:
- 모듈 표시
- 모듈 xbar 표시
- 인벤토리 표시
- 인터페이스 트렌시버 표시
- vtp 상태 표시
- vlan 표시
- 디버그 표시
- show cores vdc-all
- show processes log vdc-all
- 모듈 fex 표시
- fex 표시
- show running-config

이 목록의 일부 명령은 네트워크 관리자 사용자 역할을 보유한 사용자 계정에서만 실행할 수 있습니다.사용자 지정 사용자 역할에서 명령이 명시적으로 허용된 경우에도 해당 역할을 보유한 사용자 계정은 명령을 실행할 수 없으며 "%Permission denied for the role" 오류 메시지를 반환합니다.이 제한 사항은 각 Nexus 플랫폼의 보안 컨피그레이션 가이드의 "사용자 계정 및 RBAC 구성" 장에 설명되어 있습니다.

> *"사용자 역할에 대해 구성된 읽기-쓰기 규칙과 상관없이 일부 명령은 미리 정의된 네트워크 관리자 역할을 통해서만 실행할 수 있습니다."*

이러한 제한 때문에 RANCID의 기본 명령 목록을 사용하려면 RANCID에서 사용하는 NX-OS 사용자 계정에 "network-admin" 역할이 할당되어야 합니다.이 사용자 계정을 구성하려면 다음 절차를 수행합니다.

1. "network-admin" 역할로 새 사용자 계정을 구성합니다.아래 예에서 이 사용자 계정의 이름은 "rancid"이며 비밀번호는 "rancid!123"입니다.

```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
```

```
Nexus(config)# end
Nexus#
```

2. 새 RANCID 사용자 계정으로 Nexus 디바이스에 수동으로 로그인하고 문제 없이 필요한 모든 명령을 실행할 수 있는지 확인합니다.
3. 새 사용자 계정을 사용하도록 RANCID의 로그인 구성 파일을 수정합니다.로그인 컨피그레이션 파일을 수정하는 절차는 한 환경에 따라 다르므로 여기에 세부 정보가 제공되지 않습니다. **참고:**RANCID의 로그인 컨피그레이션 파일은 일반적으로 **.cloginrc**로 명명되지만 RANCID의 구축에서는 다른 이름을 사용할 수 있습니다.
4. 단일 Nexus 디바이스 또는 디바이스 세트에 대해 RANCID를 실행하고 모든 명령이 성공적으로 실행되는지 확인합니다.이 작업을 수행하는 특정 명령은 RANCID의 구현 및 설치에 따라 달라집니다.

   참고:RANCID에서 사용하는 Nexus 사용자 계정이 보안상의 이유로 "network-admin" 역할을 절대 가질 수 없고 이 역할이 필요한 관련 명령이 사용자 환경에서 필요하지 않은 경우 RANCID에서 실행하는 목록에서 해당 명령을 수동으로 제거할 수 있습니다.먼저 앞서 설명한 명령만 실행할 수 있는 Nexus 사용자 계정에서 위에 표시된 명령의 전체 목록을 실행합니다 ."network-admin" 역할이 필요한 명령은 "%Permission denied for the role" 오류 메시지를 반환합니다.그런 다음 RANCID에서 실행한 명령 목록에서 오류 메시지를 반환한 명령을 수동으로 제거할 수 있습니다.이러한 명령을 제거하는 정확한 절차는 이 문서의 범위를 벗어납니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 산화된 GitHub 프로젝트
- RANCID(Really Awesome New Cisco Conflg Different) 홈페이지
- Cisco Nexus 9000 Series NX-OS 보안 컨피그레이션 가이드의 "사용자 계정 및 RBAC 구성" 장 :
  - 릴리스 9.3(x)
  - 릴리스 9.2(x)
  - 릴리스 7.x
  - 릴리스 6.x
- Cisco Nexus 7000 Series NX-OS 보안 컨피그레이션 가이드의 "사용자 계정 및 RBAC 구성" 장 :
  - 릴리스 8.x
  - 릴리스 7.x
  - 릴리스 6.x
- Cisco Nexus 6000 Series NX-OS 시스템 관리 컨피그레이션 가이드의 "사용자 계정 및 RBAC 구성" 장

    - 릴리스 7.x
    - 릴리스 6.x
- Cisco Nexus 5600 Series NX-OS 시스템 관리 컨피그레이션 가이드의 "사용자 계정 및 RBAC 구성" 장
    - 릴리스 7.x
- Cisco Nexus 5500 Series NX-OS 시스템 관리 컨피그레이션 가이드의 "사용자 계정 및 RBAC 구성" 장
    - 릴리스 7.x
    - 릴리스 6.x
- 기술 지원 및 문서 – Cisco Systems