

# Configurar o RBAC do usuário para as ferramentas de backup de configuração de dispositivos de rede oxidados ou RANCID em dispositivos Cisco Nexus

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configurar conta de usuário e função para Oxidado](#)

[Configurar conta de usuário e função para RANCID](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como configurar contas de usuário locais em dispositivos Cisco Nexus para usar funções RBAC (Role-Based Access Control, Controle de Acesso Baseado em Função) que são restritas aos comandos usados pelas ferramentas de backup de configuração de dispositivos de rede Oxidized ou RANCID.

## Prerequisites

### Requirements

Você deve ter acesso a pelo menos uma conta de usuário que possa criar outras contas de usuário local e funções de RBAC. Normalmente, essa conta de usuário tem a função padrão de "administrador de rede", mas a função aplicável pode ser diferente para o ambiente e a configuração de rede específicos.

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar contas de usuário no NX-OS
- Como configurar funções de RBAC no NX-OS
- Como configurar sua ferramenta de backup de configuração de dispositivo de rede

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Plataforma NX-OS Nexus 9000 versão 7.0(3)I7(1) ou posterior

As informações neste documento abrangem estas ferramentas de backup de configuração de dispositivos de rede:

- Oxidado v0.26.3
- RANCID v3.9

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configurar

Esta seção fornece instruções de configuração para as ferramentas de backup de configuração de dispositivos de rede Oxidized e RANCID.

**Note:** Se você usar uma ferramenta de backup de configuração de dispositivo de rede diferente, use os procedimentos Oxidized e RANCID como exemplos e modifique as instruções conforme apropriado para sua situação.

### Configurar conta de usuário e função para Oxidado

Como visto no [modelo NX-OS da Oxidized](#), a Oxidized executa essa lista de comandos por padrão em qualquer dispositivo Cisco Nexus que execute o NX-OS:

- terminal length 0
- show version
- show inventário
- show running-config

Para configurar uma conta de usuário com permissão para executar apenas esses comandos, execute este procedimento:

1. Configure uma função RBAC que permita esses comandos. No exemplo abaixo, "oxidado" é definido como o nome da função.

```
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#
```

**Caution:** Não se esqueça de adicionar uma regra que permita o comando **terminal length 0** como mostrado no exemplo acima. Se esse comando não for permitido, a conta de usuário Oxidized receberá uma mensagem de erro "% Permission Denuncia for the role" quando executar o comando **terminal length 0**. Se a saída de um comando executado pela Oxidized exceder o comprimento de terminal padrão de 24, a Oxidized não lidará com o prompt "—More—" (demonstrado abaixo) e criará um syslog de aviso "Timeout::Error with msg

'execution expired'" após executar comandos no dispositivo.

```
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. Configure uma nova conta de usuário que herde a função configurada na etapa 1. No exemplo abaixo, esta conta de usuário é denominada "oxidada" e tem uma senha "oxidada!123".

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

3. Faça login manualmente no dispositivo Nexus com a nova conta de usuário Oxidized e verifique se você pode executar todos os comandos necessários sem problemas.
4. Modificar a fonte de dados de entrada da Oxidized para aceitar as credenciais de conta da nova conta de usuário Oxidized. A saída de exemplo de uma fonte CSV é mostrada abaixo com cinco dispositivos Nexus.

```
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
```

A configuração de origem oxidada relevante para a fonte CSV acima é mostrada abaixo.

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

5. Execute o Oxidized no arquivo de configuração e na fonte de dados e verifique se a saída de todos os comandos aparece na saída de dados configurada. O comando específico para fazer isso dependerá da implementação e instalação da Oxidized.

## Configurar conta de usuário e função para RANCID

Como visto no [modelo NX-OS da RANCID](#), a RANCID executa essa lista de comandos por padrão em qualquer dispositivo Cisco Nexus que executa o NX-OS:

- terminal no monitor-force
- show version
- show version build-info all
- show license
- show license usage
- show license host-id
- show system redundancy status
- show environment clock
- show environment fan
- show environment fex all fan
- show environment temperature
- show environment power
- show boot
- dir bootflash:
- dir debug:
- dir logflash:
- dir slot0:
- dir usb1:
- dir usb2:
- dir volátil:
- show module
- show module xbar
- show inventário
- show interface transceiver
- show vtp status
- show vlan
- show debug
- show cores vdc-all
- show processes log vdc-all
- show module fex
- show fex
- show running-config

Alguns dos comandos dessa lista podem ser executados somente por contas de usuário que contêm a função de usuário network-admin. Mesmo que o comando seja explicitamente permitido por uma função de usuário personalizada, as contas de usuário que contêm essa função podem não ser capazes de executar o comando e retornarão uma mensagem de erro "%Permissão negada para a função". Essa limitação está documentada no capítulo "Configurando Contas de Usuário e RBAC" de cada [Guia de Configuração de Segurança da plataforma Nexus](#):

*"Independente da regra de leitura/gravação configurada para uma função de usuário, alguns comandos podem ser executados somente por meio da função predefinida network-admin."*

Como resultado dessa limitação, a lista de comandos padrão da RANCID exige que a função "network-admin" seja atribuída à conta de usuário do NX-OS usada por RANCID. Para configurar esta conta de usuário, execute este procedimento:

1. Configure uma nova conta de usuário com a função "network-admin". No exemplo abaixo, essa conta de usuário é chamada "rancid" e tem uma senha "rancid!123".

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

2. Faça login manualmente no dispositivo Nexus com a nova conta de usuário RANCID e verifique se você pode executar todos os comandos necessários sem problemas.
3. Modifique o arquivo de configuração de login da RANCID para usar a nova conta de usuário. O procedimento para modificar o arquivo de configuração de login varia de um ambiente para outro, portanto, os detalhes não são fornecidos aqui. **Note:** O arquivo de configuração de login da RANCID é normalmente chamado `.loginrc`, mas sua implantação de RANCID pode usar um nome diferente.
4. Execute o RANCID em um único dispositivo Nexus ou conjunto de dispositivos e verifique se todos os comandos foram executados com êxito. O comando específico para fazer isso depende da implementação e instalação do RANCID.

**Note:** Se a conta de usuário do Nexus usada pela RANCID não puder conter a função "network-admin" por motivos de segurança e se os comandos relevantes que exigem essa função não forem necessários em seu ambiente, você poderá remover manualmente esses comandos da lista executada pela RANCID. Primeiro, execute a lista completa de comandos mostrados acima a partir de uma conta de usuário do Nexus que só tem permissão para executar os comandos acima. Os comandos que requerem a função "network-admin" retornarão uma mensagem de erro "%Permission Negado para a função". Você pode, então, remover manualmente os comandos que retornaram a mensagem de erro da lista de comandos executados por RANCID. O procedimento exato para remover esses comandos está fora do escopo deste documento.

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Projeto GitHub Oxidado](#)

- [Página inicial do RANCID \(Realmente incrível, novo Cisco Conflg Differ\)](#)
- Capítulo "Configurando Contas de Usuário e RBAC" do Guia de Configuração de Segurança do Cisco Nexus 9000 Series NX-OS:
  - [Versão 9.3\(x\)](#)
  - [Versão 9.2\(x\)](#)
  - [Versão 7.x](#)
  - [Versão 6.x](#)
- Capítulo "Configurando Contas de Usuário e RBAC" do Guia de Configuração de Segurança do Cisco Nexus 7000 Series NX-OS:
  - [Versão 8.x](#)
  - [Versão 7.x](#)
  - [Versão 6.x](#)
- Capítulo "Configurando Contas de Usuário e RBAC" do Guia de Configuração de Gerenciamento do Sistema NX-OS do Cisco Nexus 6000 Series
  - [Versão 7.x](#)
  - [Versão 6.x](#)
- Capítulo "Configurando Contas de Usuário e RBAC" do Guia de Configuração de Gerenciamento do Sistema NX-OS do Cisco Nexus 5600 Series
  - [Versão 7.x](#)
- Capítulo "Configurando Contas de Usuário e RBAC" do Guia de Configuração de Gerenciamento do Sistema NX-OS do Cisco Nexus 5500 Series
  - [Versão 7.x](#)
  - [Versão 6.x](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)