Configuración de RBAC de Usuario para las Herramientas de Respaldo de Configuración de Dispositivos de Red Oxidadas o RANCID en los Dispositivos Cisco Nexus

Contenido

Introducción

Este documento describe cómo configurar cuentas de usuario locales en dispositivos Cisco Nexus para utilizar funciones de control de acceso basado en roles (RBAC) que están restringidas a los comandos utilizados por las herramientas de copia de seguridad de configuración de dispositivos de red Oxidadas o RANCID.

Prerequisites

Requirements

Debe tener acceso al menos a una cuenta de usuario que pueda crear otras cuentas de usuario locales y funciones de RBAC. Normalmente, esta cuenta de usuario tiene la función predeterminada de "administrador de red", pero la función aplicable puede ser diferente para su configuración y entorno de red concretos.

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar cuentas de usuario en NX-OS
- Cómo configurar las funciones de RBAC en NX-OS
- Cómo configurar la herramienta de copia de seguridad de la configuración del dispositivo de red

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Plataforma Nexus 9000 NX-OS versión 7.0(3)I7(1) o posterior

La información en este documento cubre estas herramientas de backup de configuración del dispositivo de red:

- Oxidized v0.26.3
- RANCID v3.9

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio 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 sección proporciona instrucciones de configuración para las herramientas de respaldo de configuración de dispositivos de red Oxidized y RANCID.

> **Nota:** Si utiliza una herramienta de copia de seguridad de configuración de dispositivo de red diferente, utilice los procedimientos Oxidized y RANCID como ejemplos y modifique las instrucciones según corresponda según su situación.

Configuración de la cuenta de usuario y la función para Oxidiated

Como se ve en el modelo NX-OS de Oxidized, Oxidized ejecuta esta lista de comandos de forma predeterminada en cualquier dispositivo Cisco Nexus que ejecute NX-OS:

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

Para configurar una cuenta de usuario que sólo puede ejecutar esos comandos, lleve a cabo este procedimiento:

1. Configure un rol RBAC que permita esos comandos. En el siguiente ejemplo, "oxidado" se define como el nombre de rol.

```
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#
```

> **Precaución:** No olvide agregar una regla que permita el comando **terminal length 0** como se muestra en el ejemplo anterior. Si no se permite este comando, la cuenta de usuario Oxidada recibirá un mensaje de error "% Permission denied for the role" cuando ejecute el

comando **terminal length 0**. Si el resultado de un comando ejecutado por Oxidized supera la longitud de terminal predeterminada de 24, Oxidized no manejará correctamente el mensaje "—More—" (mostrado a continuación) y generará un syslog de advertencia "Timeout::Error con msg 'execute expiró'" después de ejecutar los comandos en el 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 una nueva cuenta de usuario que herede la función configurada en el paso 1. En el siguiente ejemplo, esta cuenta de usuario se denomina "oxidized" y tiene una contraseña de "¡oxidized!123".

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

3. Inicie sesión manualmente en el dispositivo Nexus con la nueva cuenta de usuario optimizada y verifique que pueda ejecutar todos los comandos necesarios sin problemas.
4. Modifique el origen de datos de entrada de Oxidized para aceptar las credenciales de cuenta de la nueva cuenta de usuario Oxidized. A continuación se muestra un ejemplo de salida de un origen CSV con 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 continuación se muestra la configuración de origen optimizada correspondiente al origen CSV anterior.

```
---
source:
  default: csv
  csv:
    file: "/filepath/to/router.db"
    delimiter: !ruby/regexp /:/
    map:
```

```
name: 0
ip: 1
model: 2
username: 3
password: 4
```

5. Ejecute Oxidized con el archivo de configuración y el origen de datos y verifique que el resultado de todos los comandos aparezca en el resultado de datos configurado. El comando específico para hacer esto dependerá de su implementación e instalación de Oxidized.

Configuración de la cuenta de usuario y la función para RANCID

Como se ve en el modelo NX-OS de RANCID, RANCID ejecuta esta lista de comandos de forma predeterminada en cualquier dispositivo Cisco Nexus que ejecute 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 temperatura
- show environment power
- show boot
- dir bootflash:
- dir debug:
- dir logflash:
- dir slot0:
- dir usb1:
- dir usb2:
- dir volatile:
- show module
- show module xbar
- show inventario
- 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

Algunos de los comandos de esta lista sólo pueden ser ejecutados por cuentas de usuario que tengan la función de usuario administrador de red. Incluso si un rol de usuario personalizado

permite explícitamente el comando, es posible que las cuentas de usuario que tienen ese rol no puedan ejecutar el comando y devuelvan un mensaje de error "%Permission denied for the role". Esta limitación se documenta en el capítulo "Configuración de cuentas de usuario y RBAC" de la Guía de Configuración de Seguridad de cada plataforma Nexus:

> *"Independientemente de la regla de lectura y escritura configurada para una función de usuario, algunos comandos sólo se pueden ejecutar a través de la función de administrador de red predefinida".*

Como resultado de esta limitación, la lista de comandos predeterminada de RANCID requiere que la función "administrador de red" se asigne a la cuenta de usuario de NX-OS utilizada por RANCID. Para configurar esta cuenta de usuario, lleve a cabo este procedimiento:

1. Configure una nueva cuenta de usuario con la función "network-admin". En el siguiente ejemplo, esta cuenta de usuario se denomina "rancid" y tiene una contraseña de "¡rancid!123".
```
Nexus# configure terminal
Nexus(config)# username rancid role network-admin password rancid!123
Nexus(config)# end
Nexus#
```
2. Inicie sesión manualmente en el dispositivo Nexus con la nueva cuenta de usuario RANCID y verifique que pueda ejecutar todos los comandos necesarios sin problemas.
3. Modifique el archivo de configuración de inicio de sesión de RANCID para utilizar la nueva cuenta de usuario. El procedimiento para modificar el archivo de configuración de inicio de sesión varía de un entorno a otro, por lo que no se proporcionan detalles aquí. **Nota:** El archivo de configuración de inicio de sesión de RANCID se denomina normalmente **.cloginrc**, pero su implementación de RANCID puede utilizar un nombre diferente.
4. Ejecute RANCID contra un único dispositivo Nexus o conjunto de dispositivos y verifique que todos los comandos se ejecuten correctamente. El comando específico para hacer esto depende de la implementación e instalación de RANCID.

   Nota: Si la cuenta de usuario de Nexus utilizada por RANCID no puede mantener la función "administrador de red" por razones de seguridad y si los comandos relevantes que requieren esta función no son necesarios en su entorno, puede quitar manualmente esos comandos de la lista que ejecuta RANCID. Primero, ejecute la lista completa de comandos mostrada arriba desde una cuenta de usuario de Nexus que sólo está permitida para ejecutar los comandos mencionados anteriormente. Los comandos que requieren la función "network-admin" devolverán un mensaje de error "%Permission denied for the role" (Permiso denegado para la función). A continuación, puede quitar manualmente los comandos que devolvieron el mensaje de error de la lista de comandos ejecutados por RANCID. El procedimiento exacto para quitar esos comandos está fuera del alcance de este documento.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Resolución de problemas

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Proyecto GitHub optimizado
- Página de inicio de RANCID (realmente asombrosa nueva diferencia de Cisco Conflg)

- Capítulo "Configuración de cuentas de usuario y RBAC" de la guía de configuración de seguridad de Cisco Nexus serie 9000 NX-OS:
  - Versión 9.3(x)
  - Versión 9.2(x)
  - Versión 7.x
  - Versión 6.x
- Capítulo "Configuración de cuentas de usuario y RBAC" de la guía de configuración de seguridad de Cisco Nexus serie 7000 NX-OS:
  - Versión 8.x
  - Versión 7.x
  - Versión 6.x
- Capítulo "Configuración de cuentas de usuario y RBAC" de la guía de configuración de administración del sistema NX-OS de Cisco Nexus serie 6000
  - Versión 7.x
  - Versión 6.x
- Capítulo "Configuración de cuentas de usuario y RBAC" de la guía de configuración de administración del sistema NX-OS de Cisco Nexus serie 5600
  - Versión 7.x
- Capítulo "Configuración de cuentas de usuario y RBAC" de la guía de configuración de administración del sistema NX-OS de Cisco Nexus serie 5500
  - Versión 7.x
  - Versión 6.x
- Soporte Técnico y Documentación - Cisco Systems