为Cisco Nexus设备上的已氧化或RANCID网络设备配置备份工具配置用户RBAC

目录

简介

本文档介绍如何在Cisco Nexus设备上配置本地用户帐户以使用基于角色的访问控制(RBAC)角色，这些角色仅限于Oxicoded或RANCID网络设备配置备份工具使用的命令。

先决条件

要求

您必须至少拥有一个用户帐户的访问权限，该用户帐户可以创建其他本地用户帐户和RBAC角色。通常，此用户帐户具有默认的“network-admin”角色，但适用的角色可能与您的特定网络环境和配置不同。

Cisco 建议您了解以下主题：

- 如何在NX-OS中配置用户帐户
- 如何在NX-OS中配置RBAC角色
- 如何配置网络设备配置备份工具

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Nexus 9000平台NX-OS版本7.0(3)I7(1)或更高版本

本文档中的信息包括以下网络设备配置备份工具：

- 氧化v0.26.3
- RANCID v3.9

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认

）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

本节提供Oxiced和RANCID网络设备配置备份工具的配置说明。

> **注意**：如果您使用不同的网络设备配置备份工具，请使用Oxicoded和RANCID过程作为示例，并根据您的情况修改说明。

配置用户帐户和角色以进行氧化

如Oxicated的NX-OS型号所示,Oxicaded在运行NX-OS的任何Cisco Nexus设备上默认执行以下命令列表：

- 终端长度0
- show version
- show inventory
- show running-config

要配置仅允许执行这些命令的用户帐户，请执行以下步骤：

1. 配置允许这些命令的RBAC角色。在以下示例中，“oxicated”定义为角色名称。

```
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#
```

> **警告**：不要忘记添加允许terminal length 0命**令的规**则，如上例所示。如果此命令不被允许，则Oxined用户帐户在执行terminal length 0命令时将收到“拒绝角色的%权限”**错误**消息。如果Oxicated执行的命令的输出超过默认终端长度24,Oxicated将无法正常处理“ — More — ”提示符（如下所示），并在设备上执行命令后引发“Timeout::Error with msg 'execution expired'”警告系统日志。

```
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. 配置一个新用户帐户，该用户帐户继承您在步骤1中配置的角色。在以下示例中，此用户帐户名为“oxicated”，密码为“oxicated!123”。

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

3. 使用新的Oxinated用户帐户手动登录Nexus设备，并验证您是否可以执行所有必要的命令，而不会出现问题。
4. 修改Oxiconed的输入数据源以接受新Oxiconed用户帐户的帐户凭证。CSV源的输出示例如下所示，其中包含五台Nexus设备。

```
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
```

   上述CSV源的相关氧化源配置如下所示。

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

5. 对配置文件和数据源执行Oxicated，并验证所有命令的输出是否显示在配置的数据输出中。执行此操作的具体命令将取决于您实施和安装Oxicoded。

配置RANCID的用户帐户和角色

如RANCID的NX-OS模型所示,RANCID默认在运行NX-OS的任何Cisco Nexus设备上执行以下命令列表：

- 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
- 显示环境温度
- 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 inventory
- show interface transever
- show vtp status
- show vlan
- show debug
- show cores vdc-all
- show processes log vdc-all
- show module fex
- show fex
- show running-config

此列表中的某些命令只能由持有network-admin用户角色的用户帐户执行。即使该命令被自定义用户角色明确允许，承担该角色的用户帐户也可能无法执行该命令，并将返回“拒绝该角色的%权限”错误消息。此限制记录在每个Nexus平台安全配置指南的“配置用户帐户和RBAC”一章中:

"无论为用户角色配置的读写规则如何，某些命令只能通过预定义的网络管理员角色执行。"

由于此限制，RANCID的默认命令列表要求将“network-admin”角色分配给RANCID使用的NX-OS用户帐户。要配置此用户帐户，请执行以下步骤：

1. 使用“network-admin”角色配置新用户帐户。在以下示例中，此用户帐户名为“rancid”，密码为“rancid!123”。

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

2. 使用新的RANCID用户帐户手动登录Nexus设备，并验证您可以执行所有必要的命令，而不会发出任何问题。
3. 修改RANCID的登录配置文件以使用新用户帐户。修改登录配置文件的过程因环境而异，因此此处不提供详细信息。 **注意：**RANCID的登录配置文件通常命名为**.cloginrc**，但RANCID的部署可能使用其他名称。
4. 对单个Nexus设备或一组设备执行RANCID，并检验所有命令是否都成功执行。执行此操作的具体命令取决于RANCID的实施和安装。

注意：如果RANCID使用的Nexus用户帐户出于安全原因绝对不能保留“network-admin”角色，并且如果在您的环境中不需要要求此角色的相关命令，您可以手动从RANCID执行的列表中

删除这些命令。首先，从仅允许运行上述命令的Nexus用户帐户执行上面显示的命令的完整列表。需要“network-admin”角色的命令将返回“%拒绝该角色的权限”错误消息。然后，可以从RANCID执行的命令列表中手动删除返回错误消息的命令。删除这些命令的确切步骤不在本文档的讨论范围之内。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 氧化GitHub项目
- RANCID(Really Weasome New Cisco Conflg Differect)主页
- Cisco Nexus 9000系列NX-OS安全配置指南的“配置用户帐户和RBAC”一章：
  - 版本9.3(x)
  - 版本9.2(x)
  - 版本7.x
  - 6.x 版
- Cisco Nexus 7000系列NX-OS安全配置指南的“配置用户帐户和RBAC”一章：
  - 版本8.x
  - 版本7.x
  - 6.x 版
- Cisco Nexus 6000系列NX-OS系统管理配置指南的“配置用户帐户和RBAC”一章
  - 版本7.x
  - 6.x 版
- Cisco Nexus 5600系列NX-OS系统管理配置指南的“配置用户帐户和RBAC”一章
  - 版本7.x
- Cisco Nexus 5500系列NX-OS系统管理配置指南的“配置用户帐户和RBAC”一章
  - 版本7.x
  - 6.x 版
- 技术支持和文档 - Cisco Systems