Cisco NexusデバイスのOxized or RANCID Network Device Configuration Backup ToolsのユーザRBACの設定

内容

概要

このドキュメントでは、Cisco Nexusデバイスでローカルユーザアカウントを設定し、OxizedまたはRANCIDネットワークデバイス設定バックアップツールで使用されるコマンドに制限されるロールベースアクセスコントロール(RBAC)ロールを使用する方法について説明します。

前提条件

要件

他のローカルユーザアカウントおよびRBACロールを作成できるユーザアカウントを少なくとも1つ持っている必要があります。通常、このユーザアカウントはデフォルトの「network-admin」ロールを保持しますが、該当するロールは特定のネットワーク環境と設定で異なる場合があります。

次の項目に関する知識があることが推奨されます。

- NX-OSでのユーザアカウントの設定方法
- NX-OSでのRBACロールの設定方法
- ネットワークデバイス設定バックアップツールの設定方法

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Nexus 9000プラットフォームNX-OSリリース7.0(3)I7(1)以降

このドキュメントの情報では、次のネットワークデバイス設定バックアップツールについて説明

します。

- 酸化v0.26.3
- RANCID v3.9

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

このセクションでは、Oxized and RANCIDネットワークデバイス設定バックアップツールの設定手順について説明します。

> **注**：別のネットワークデバイス設定バックアップツールを使用する場合は、例としてOxizedおよびRANCID手順を使用し、状況に応じて手順を変更します。

Oxizedのユーザアカウントとロールの設定

OxizedのNX-OSモデルに示されているように、OxizedはNX-OSを実行するすべてのCisco Nexusデバイス上で、次のコマンドのリストをデフォルトで実行します。

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

これらのコマンドだけを実行できるユーザアカウントを設定するには、次の手順を実行します。

1. これらのコマンドを許可するRBACロールを設定します。次の例では、「酸化」がロール名として定義されています。

```
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#
```

> **注意**：上記の例に示すように、**terminal length 0**コマンドを許可するルールを必ず追加してください。このコマンドが許可されていない場合、**terminal length 0**コマンドを実行すると、Oxyedユーザーアカウントに「% Permission denied for the role 」というエラーメッセージが表示されます。Oxizedによって実行されたコマンドの出力がデフォルトのターミナル長24を超えると、Oxizedは"—More—"プロンプト（以下に示す）を正常に処理せず、デバイスでコマンドを実行した後に"Timeout::Error with msg 'execution expired'"警告syslogをします。

```
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. ステップ1で設定したロールを継承する新しいユーザーアカウントを構成します。次の例では、このユーザーアカウントの名前は「oxized」で、パスワードは「oxized!123」です。

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

3. 新しいOxizedユーザアカウントを使用してNexusデバイスに手動でログインし、必要なすべてのコマンドを問題なく実行できることを確認します。
4. Oxizedの入力データソースを変更して、新しいOxizedユーザアカウントのアカウント認証情報を受け入れます。5台のNexusデバイスを使用したCSVソースの出力例を次に示します。

```
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
```

上記のCSVソースに関連するOxized source設定を次に示します。

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

5. コンフィギュレーションファイルとデータソースに対してOxizedを実行し、すべてのコマンドの出力が設定されたデータ出力に表示されることを確認します。これを行うための具体的なコマンドは、Oxizedの実装とインストールによって異なります。

RANCIDのユーザアカウントとロールの設定

RANCIDのNX-OSモデルに示されているように、RANCIDはNX-OSを実行する任意のCisco Nexusデバイス上で次のコマンドのリストをデフォルトで実行します。

- 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 volatile:
- show module
- show module xbar
- show inventory
- 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

このリストの一部のコマンドは、network-adminユーザロールを持つユーザアカウントによってのみ実行できます。カスタムユーザーロールによってコマンドが明示的に許可されている場合でも、そのロールを持つユーザーアカウントはコマンドを実行できず、「%Permission denied for the role」エラーメッセージが返される可能性があります。この制限は、各Nexusプラットフォームのセキュリティ構成ガイドの「ユーザーアカウントとRBACの構成」の章に記載されています。

> *「ユーザロールに設定されている読み取り/書き込みルールに関係なく、一部のコマンドは、事前定義されたnetwork-admin口ールによってのみ実行できます。」*

この制限の結果、RANCIDのデフォルトのコマンドリストでは、「network-admin」ロールがRANCIDで使用されるNX-OSユーザアカウントに割り当てられている必要があります。このユーザアカウントを設定するには、次の手順を実行します。

1. 新しいユーザアカウントを「network-admin」ロールで設定します。次の例では、このユー

ザアカウントの名前は「rancid」で、パスワードは「rancid!123」です。

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

2. 新しいRANCIDユーザアカウントを使用してNexusデバイスに手動でログインし、必要なすべてのコマンドを問題なく実行できることを確認します。
3. 新しいユーザアカウントを使用するようにRANCIDのログイン設定ファイルを変更します。ログイン設定ファイルを変更する手順は、環境によって異なるため、ここでは詳細は説明しません。 **注**：RANCIDのログイン設定ファイルの名前は通常**.cloginrc**です。ただし、RANCIDの展開で別の名前を使用する場合があります。
4. 単一のNexusデバイスまたはデバイスのセットに対してRANCIDを実行し、すべてのコマンドが正常に実行されることを確認します。これを行うための具体的なコマンドは、RANCIDの実装とインストールによって異なります。

注：RANCIDが使用するNexusユーザアカウントがセキュリティ上の理由で「network-admin」ロールを保持できない場合、およびこのロールを必要とする関連コマンドが環境に必要ない場合は、RANCIDによって実行されるリストからコマンドを手動で削除できます。まず、上記のコマンドの実行のみが許可されているNexusユーザアカウントから、上記のコマンドの完全なリストを実行します。「network-admin」ロールを必要とするコマンドでは、「%Permission denied for the role」エラーメッセージが返されます。その後、RANCIDによって実行されたコマンドのリストから、エラーメッセージを返したコマンドを手動で削除できます。これらのコマンドを削除する正確な手順は、このドキュメントの範囲外です。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- 酸化GitHubプロジェクト
- RANCID(Really Asome New Cisco Conflg Differ)ホームページ

- 『Cisco Nexus 9000 Series NX-OS Security Configuration Guide:
  - リリース9.3(x)
  - リリース9.2(x)
  - リリース7.x
  - リリース6.x
- 『Cisco Nexus 7000 Series NX-OS Security Configuration Guide:
  - リリース8.x
  - リリース7.x
  - リリース6.x
- 『Cisco Nexus 6000 Series NX-OS System Management Configuration Guide』の「

Configuring User Accounts and RBAC」の章
  - リリース7.x
  - リリース6.x
- 『Cisco Nexus 5600 Series NX-OS System Management Configuration Guide』の「Configuring User Accounts and RBAC」の章
  - リリース7.x
- 『Cisco Nexus 5500 Series NX-OS System Management Configuration Guide』の「Configuring User Accounts and RBAC」の章
  - リリース7.x
  - リリース6.x
- テクニカル サポートとドキュメント – Cisco Systems