Nexus N5500、5600 および N6000 ロールの Base アクセスコントロール（RBAC）

目次

概要

この資料に Nexus 5500 にアクセスするためにユーザを制限する方法を Nexus 5600 記述され、ロールを使用して Nexus 6000 スイッチはアクセスコントロール（RBAC）を基づかせています。

RBAC はスイッチ管理 オペレーションにアクセスできるユーザの許可を制限する割り当てられたユーザの役割のためのルールを定義することを可能にします。

作成し、ユーザアカウントを管理し、Nexus 5500、Nexus 5600 および Nexus 6000 スイッチにアクセスを制限するロールを割り当てることができます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Nexus 5500、Nexus 5600、Nexus 6000 スイッチ CLI 設定コマンド
- Cisco Fabric Services （ CFS ）。

使用するコンポーネント

この文書に記載されている情報は NXOS 5.2(1)N1(9) 7.3(1)N1(1) が稼働している Nexus 5500、Nexus 5600 および Nexus 6000 スイッチに基づいています。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

ユーザの要求

これらは達成される必要のいくつかのユーザの要求です:

- ネットワーク Admin ロールのユーザだけロールを作成できます。
- ネットワーク Admin ロールのユーザだけ**示しますロールを**出力をの表示できます。
- すべての show コマンドを実行することがユーザができてもこれらのユーザ ネットワーク Admin 役割が割り当てられなければ、**示します役割**出力を表示することができません。
- ユーザアカウントは少なくとも 1 つのユーザの役割がなければなりません。

ユーザ ロール

各ロールは複数のユーザに割り当て、各ユーザは複数のロールの一部である場合もあります。

たとえば、役割 A ユーザは show コマンドを発行することができ、役割 B ユーザはコンフィギュレーション変更を行なうことができます。

ユーザが役割 A および役割両方 B に割り当てられる場合、このユーザは表示コマンドを発行し、設定への変更を行なうことができます。

割り当てアクセス コマンドは拒否アクセス コマンド上の優先順位を奪取 します。

たとえば、拒否が設定コマンドにアクセスするロールに属する場合。

ただし、また設定コマンドにアクセスできるロールに属すれば、設定コマンドにそれからアクセスがあります。

5 つのデフォルトユーザ ロールがあります:

- ネットワーク Admin -全体のスイッチに読み書きアクセスを完了して下さい。
- ネットワーク オペレータ-全体のスイッチに読み取り アクセスを完了して下さい。
- vdc Admin - VDC に制限される読み書きアクセス
- vdc オペレータ- VDC に制限される読み取り アクセス
- サン Admin - SAN 管理者に読み書きアクセスを完了して下さい。

注: /削除デフォルトユーザ ロール修正できません。

注: コマンド **ロールが**スイッチで利用可能 なロールを表示することを**示して下さい**

ルール ユーザの役割の

ルールはロールの基本的な要素です。

ルールはどんなオペレーションを行うことをロールがユーザが可能にするか定義します。

これらのパラメータのためのルールを適用できます:

- コマンドの Command-a 正規表現で定義されるコマンドかグループ。
- 機能に適用する NX-OS ソフトウェアによって提供される機能コマンド。
- 機能の機能グループ デフォルトかユーザが定義するグループ。

これらのパラメータは階層関係をつくます。 ほとんどの BC モード パラメータはコマンドです。

次の制御 パラメータは機能と関連付けられるすべてのコマンドを表す機能です。

最後の制御 パラメータは機能 グループです。 関連する機能 グループ結合は特色にし、容易にルールを管理することを可能にします。

ユーザが指定するルール数はルールが適用する順序を判別します。

ルールは降順で適用されます。

たとえば、ルール 1 はルール 3 の前に適用するルール 2 の前に等適用します。

rule コマンドは特定の役割によって実行されたことができるオペレーションを規定 します。 各ルールはルール数で、規則の種類構成されています（割り当てか拒否）、

コマンドの種類（たとえば、設定は、exec、デバッグ示します）、および選択機構名前（たとえば、FCOE、HSRP、VTP、インターフェイス）。

ディストリビューション ユーザの役割の

役割ベース コンフィギュレーション 使用効率的なデータベース 管理を有効に し、ネットワークの設定の一点を提供する Cisco Fabric Services （CFS）インフラストラクチャ。

デバイスの機能のための CFS ディストリビューションを有効に するとき、デバイスはまた機能の CFS ディストリビューションのために有効に した ネットワークでその他のデバイスが含まれている CFS 領域に属します。 機能 ユーザの役割ののための CFS ディストリビューションはデフォルトでディセーブルにされます。

コンフィギュレーション変更を配りたいと思う各デバイスのユーザの役割のための CFS を有効にして下さい。

スイッチのユーザの役割のための CFS ディストリビューションを有効に した後、これらの処置をとるために原因をスイッチ NX-OS ソフトウェア入力する最初のユーザの役割の設定コマンド:

1. スイッチの CFS セッションを作成します。
2. 機能 ユーザの役割ののために有効に なる CFS の CFS 領域のすべてのスイッチの設定 ユーザの役割のロックします。
3. スイッチで一時バッファのコンフィギュレーション変更 ユーザの役割の保存します。

変更はスイッチの一時バッファに明示的に CFS 領域のデバイスに配られるべきそれらを託すまでとどまります。

変更を保存するとき、NX-OS ソフトウェアはこれらの処置をとります:

1. スイッチの実行コンフィギュレーションへの変更を加えます。
2. CFS 領域の他のスイッチに設定更新済ユーザの役割の配ります。
3. CFS 領域のデバイスの設定 ユーザの役割のロック解除します。
4. CFS セッションを終了します。

これらのコンフィギュレーションは配られます:

- ロール名および説明
- ロールのためのルールのリスト

設定と show コマンド

	コマンド	目的
ステップ 1：	**configure terminal** 例： switch# **configure terminal** switch (config) #	グローバル コンフィギュレーション モードを開始します
呼び出します。	**ロール名***ロール名* 例： switch (config) # **ロール名ウセラ** スイッチ (構成ロール) #	ユーザの役割を規定 し、コンフィギュレーションモード ロ ます。
ステップ 3	**VLAN方針拒否** 例： スイッチ (構成ロール) # **VLAN方針拒否** スイッチ (構成ロール VLAN) #	コンフィギュレーションモード ロールの VLAN方針入力し
ステップ 4	**割り当て VLAN** vlan-id 例： スイッチ (構成ロール VLAN) **#割り当て VLAN 1**	アクセス ロールができる VLAN を規定 します。 必要に応じて多くの VLAN のためのこのコマンドを繰り返 さい。
ステップ 5	**exit** 例： スイッチ (構成ロール VLAN) **#終了** スイッチ (構成ロール) #	コンフィギュレーションモード ロールの VLAN方針終了し
ステップ 6	**ロールを示して下さい** 例： スイッチ (構成ロール) は **#ロールを示します**	(オプションの) 設定ロールの表示する。
ステップ 7	**ロールを示して下さい{保留中の | 保留中 diff}** 例： スイッチ (構成ロール) は **#保留中のロールを示します**	(オプションの) ディストリビューションのために保留中 の役割の表示する
ステップ 8	**ロールは託します** 例： スイッチ (構成ロール) は	(オプションの) 機能 ユーザの役割ののための CFS 設定 ューションを有効に する場合一時データベースのコンフィ ン変更 ユーザの役割の実行コンフィギュレーションに適用

	#ロール託します **copy running-config startup-config**	swithces に設定 ユーザの役割の配ります。
ステップ 9	例： switch# **copy running-config startup-config**	（オプション）スタートアップ コンフィギュレーションにギュレーションをコピーします。

これらのステップはディストリビューション ロールの設定 有効に します:

	コマンド	**目的**
ステップ 1：	switch# **config t** switch（config）#	コンフィギュレーションモードを開始します。
呼び出します。	switch（config）# **ロールは配ります** switch（config）#no **ロールは配ります**	ディストリビューション ロールの設定 有効に します 無効ロールの設定 ディストリビューション（デフト）。

これらのステップはコンフィギュレーション変更ロールの託します:

	コマンド	**目的**
ステップ 1	Nexus# **config t** Nexus（config）#	コンフィギュレーションモードを開始します。
ステップ 2	Nexus（config）# **ロールは託します**	コンフィギュレーション変更ロールの託します。

これらのステップはコンフィギュレーション変更ロールの廃棄します:

	コマンド	**目的**
ステップ 1	Nexus# **config t** Nexus（config）#	コンフィギュレーションモードを開始します。
ステップ 2	Nexus（config）# **打ち切る ロールの**	コンフィギュレーション変更ロールの廃棄し、保留中の設定 データベースをクリアします。

ユーザアカウントおよび RBAC 構成情報を表示するために、これらのタスクの 1 つを行って下さい:

コマンド	**目的**
ロールを示して下さい	設定 ユーザの役割の表示する。
機能ロールの示して下さい	機能リストを表示する。
機能グループ ロールの示して下さい	機能 グループ設定を表示します。

セッション ユーザの役割のディストリビューション クリアして下さい

進行中の Cisco Fabric Services ディストリビューション セッションを（もしあれば）解決し、機能 ユーザの役割ののためのファブリックをロック解除することができます。

注意： このコマンドを発行する場合保留中のデータベースのどの変更でも失われます。

	コマンド	**目的**
ステップ 1	switch# **セッション クリア ロールの** **例：** switch# セッション クリア ロールの	セッションを解決し、ファブリックをロック解除しま
ステップ 2	**セッションステータス ロールの示して下さい**	（オプションの）セッションステータス ユーザの役割 CFS 表示する。

例：
switch# はセッションステータス ロール
の示します

設定例

この例では、アクセス 権これらのでユーザアカウント TAC を作成しようと思っています:

- clear コマンドへのアクセス
- 設定コマンドへのアクセス
- debug コマンドへのアクセス
- EXEC コマンドへのアクセス
- 表示コマンドへのアクセス
- VLAN 1-10 へのアクセスのみ

```
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z
C5548P-1(config)# role name Cisco
C5548P-1(config-role)# rule 1 permit command clear
C5548P-1(config-role)# rule 2 permit command config
C5548P-1(config-role)# rule 3 permit command debug
C5548P-1(config-role)# rule 4 permit command exec
C5548P-1(config-role)# rule 5 permit command show
C5548P-1(config-role)# vlan policy deny
C5548P-1(config-role-vlan)# permit vlan 1-10
C5548P-1(config-role-vlan)# end

C5548P-1# show role name Cisco

Role: Cisco
  Description: new role
  vsan policy: permit (default)
  Vlan policy: deny
  Permitted vlans: 1-10
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------
  5       permit  command                         show
  4       permit  command                         exec
  3       permit  command                         debug
  2       permit  command                         config
  1       permit  command                         clear


C5548P-1#
C5548P-1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
C5548P-1(config)# username TAC password Cisco123 role Cisco

C5548P-1(config)# show user-account TAC
user:TAC
        this user account has no expiry date
        roles:Cisco
```

ライセンス の 必要条件

製品	ライセンス要件
NX-OS	ユーザアカウントおよび RBAC はライセンスを必要としません。

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

現在のところ、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。