Nexus N5500、5600、およびN6000ロールベースアクセスコントロール(RBAC)

内容

概要

このドキュメントでは、ロールベースアクセスコントロール(RBAC)を使用して、Nexus 5500、Nexus 5600、およびNexus 6000スイッチへのアクセスをユーザに制限する方法について説明します。

RBACを使用すると、割り当てられたユーザロールのルールを定義して、スイッチ管理操作にアクセスできるユーザの許可を制限できます。

ユーザアカウントを作成して管理し、Nexus 5500、Nexus 5600、およびNexus 6000スイッチへの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スイッチのCLIコンフィギュレーションコマンド
- シスコファブリックサービス(CFS)

使用するコンポーネント

このドキュメントの情報は、NXOS 5.2(1)N1(9) 7.3(1)N1(1)を実行する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ました。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。

ユーザ要件

満たす必要があるユーザ要件は次のとおりです。

- ロールを作成できるのは、ネットワーク管理者ロールを持つユーザだけです。
- network-adminロールを持つユーザだけがshow roleの出力を表示できます。
- ユーザがすべてのshowコマンドの実行を許可されている場合でも、これらのユーザにnetwork-adminロールが割り当てられていない限り、show roleの出力は表示できません。
- ユーザーアカウントには、少なくとも1つのユーザーロールが必要です。

ユーザ ロール

各ロールは複数のユーザに割り当てることができ、各ユーザは複数のロールに属することができます。

たとえば、ロールAのユーザはshowコマンドを発行でき、ロールBのユーザは設定を変更できます。

ユーザがロールAとロールBの両方に割り当てられている場合は、showコマンドを発行して設定を変更できます。

permit accessコマンドは、deny accessコマンドよりも優先されます。

たとえば、設定コマンドへのアクセスを拒否するロールに属している場合です。

ただし、コンフィギュレーションコマンドにアクセスできるロールにも属している場合は、コンフィギュレーションコマンドにアクセスできます。

デフォルトのユーザロールは5つあります。

- network-admin：スイッチ全体への読み取りと書き込みの完全なアクセス。
- network-operator：スイッチ全体への完全な読み取りアクセス。
- vdc-admin:VDCに限定された読み取りと書き込みのアクセス
- vdc-operator:VDCに限定された読み取りアクセス
- san-admin:SAN管理者への読み取りと書き込みの完全なアクセス。

注：デフォルトのユーザロールは変更/削除できません。

注：show roleコマンドを実行すると、スイッチで使用可能なロールが表示されます

ユーザロールルール

ルールは、ロールの基本要素です。

ルールは、ユーザが実行できるロールの操作を定義します。

次のパラメータにルールを適用できます。

- Command：正規表現で定義されたコマンドまたはコマンドグループ。
- 機能：NX-OSソフトウェアによって提供される機能に適用されるコマンド。
- フィーチャグループ：デフォルトまたはユーザ定義のフィーチャグループ。

これらのパラメータは、階層関係を作成します。最も基本的な制御パラメータはコマンドです。

次の制御パラメータは機能で、この機能に関連するすべてのコマンドを表します。

最後の制御パラメータは機能グループです。機能グループは、関連する機能を組み合わせたもので、ルールを簡単に管理できます。

ユーザ指定のルール番号によって、ルールが適用される順序が決まります。

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2の前に適用され、ルール3の前に適用されます。

ruleコマンドは、特定のロールで実行できる操作を指定します。各ルールは、ルール番号、ルールタイプ（許可または拒否）、

コマンドタイプ（設定、show、exec、debugなど）、およびオプションの機能名（FCOE、HSRP、VTP、インターフェイスなど）。

ユーザロールの配布

ロールベースの設定では、Cisco Fabric Services(CFS)インフラストラクチャを使用して、効率的なデータベース管理を可能にし、ネットワークのシングルポイント構成を実現します。

デバイス上の機能に対してCFS配布を有効にすると、そのデバイスは、ネットワーク内の他のデバイスを含むCFS領域に属し、その機能に対するCFS配布も有効になります。ユーザロール機能のCFS配布は、デフォルトでは無効になっています。

設定変更を配布する各デバイスで、ユーザロールに対してCFSを有効にする必要があります。

スイッチでユーザロールのCFSディストリビューションを有効にした後、最初にユーザロール設定コマンドを入力すると、スイッチNX-OSソフトウェアで次のアクションが実行されます。

1. スイッチにCFSセッションを作成します。
2. ユーザロール機能に対してCFSが有効になっている状態で、CFS領域内のすべてのスイッチのユーザロール設定をロックします。
3. ユーザロールの設定変更をスイッチの一時バッファに保存します。

変更は、CFS領域内のデバイスに配布されるように明示的にコミットするまで、スイッチの一時バッファに保持されます。

変更をコミットすると、NX-OSソフトウェアは次のアクションを実行します。

1. スイッチの実行コンフィギュレーションに変更を適用します。
2. 更新されたユーザロール設定をCFSリージョン内の他のスイッチに配布します。
3. CFSリージョンのデバイスのユーザロール設定をロック解除します。
4. CFSセッションを終了します。

次の設定が分散されています。

- ロール名と説明
- ロールのルールのリスト

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
ステップ2.	**role name** *role-name* 例： switch(config)# **role name UserA** switch(config-role)#	ユーザロールを指定し、ロールコンフィギュレーションモードを開
手順 3：	**vlan policy deny** 例： switch(config-role)# **vlan policy deny** switch(config-role-vlan)#	ロールVLANポリシーコンフィギュレーションモードを開始します。
ステップ4.	**permit vlan** vlan-*id* 例： switch(config-role-vlan)# **permit vlan 1**	ロールがアクセスできるVLANを指定します。 必要な数のVLANでこのコマンドを繰り返します。
ステップ5:	**exit** 例： switch(config-role-vlan)# **exit** switch(config-role)#	ロールVLANポリシーコンフィギュレーションモードを終了します。
ステップ6。	**show role** 例： switch(config-role)# **show role**	（オプション）ロール設定を表示します。
ステップ7：	**show role {pending| pending-diff}** 例： switch(config-role)# **show role pending**	（オプション）配布のために保留中のユーザロールの設定を表示し
ステップ8：	**ロールコミット** 例： switch(config-role)# **role commit**	（オプション）ユーザロール機能のCFS設定配布を有効にしている
ステップ	**copy running-config**	（オプション）実行コンフィギュレーションをスタートアップコン

9：	**startup-config** 例： switch# **copy running-config startup-config**	

次の手順により、ロール設定の配布が有効になります。

	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。
ステップ 2：	switch(config)# **role distribute**	ロール設定の配布を有効にします。
	switch(config)# **no role distribute**	ロール構成の配布を無効にします（デフォルト）。

次の手順で、ロール設定の変更を確定します。

	コマンド	目的
手順 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。
手順 2	Nexus(config)# **role commit**	ロール設定の変更を確定します。

次の手順では、ロール設定の変更を破棄します。

	コマンド	目的
手順 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。
手順 2	Nexus(config)# **role abort**	ロール設定の変更を破棄し、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設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show role	ユーザロールの設定が表示されます。
show role機能	機能リストが表示されます。
show role feature-group	機能グループの設定を表示します。

ユーザロール配布セッションのクリア

進行中のシスコファブリックサービスのディストリビューションセッションをクリアし（存在する場合）、ユーザロール機能のファブリックのロックを解除できます。

注意：このコマンドを発行すると、保留中のデータベースの変更はすべて失われます。

	コマンド	目的
ステップ 1	switch# **clear role session** **例：** switch# clear role session	セッションをクリアし、ファブリックをロック解除します。
ステップ 2	**show role session status** **例：** switch# show role session status	（オプション）ユーザロールCFSセッションステータスを表示しま

設定例

この例では、次のアクセス許可を持つユーザアカウントTACを作成します。

- 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
- show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
```

ライセンス要件

Product ライセンス要件

NX-OS ユーザアカウントとRBACにはライセンスは必要ありません。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

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。