



ユーザアカウントおよび RBAC の設定

この章の内容は、次のとおりです。

- [ユーザアカウントおよび RBAC の概要, 1 ページ](#)
- [ユーザアカウントの注意事項および制約事項, 5 ページ](#)
- [ユーザアカウントの設定, 5 ページ](#)
- [RBAC の設定, 6 ページ](#)
- [ユーザアカウントと RBAC の設定の確認, 10 ページ](#)
- [ユーザアカウントおよび RBAC のユーザアカウント デフォルト設定, 11 ページ](#)

ユーザアカウントおよび RBAC の概要

Cisco Nexus シリーズ スイッチは、ロールベース アクセス コントロール (RBAC) を使用して、ユーザがスイッチにログインするときに各ユーザが持つアクセス権の量を定義します。

RBAC では、1 つまたは複数のユーザ ロールを定義し、各ユーザ ロールがどの管理操作を実行できるかを指定します。スイッチのユーザアカウントを作成するとき、そのアカウントにユーザ ロールを関連付けます。これにより個々のユーザがスイッチで行うことができる操作が決まります。

ユーザ ロール

ユーザ ロールには、そのロールを割り当てられたユーザが実行できる操作を定義するルールが含まれています。各ユーザ ロールに複数のルールを含めることができ、各ユーザが複数のロールを持つことができます。たとえば、role1 では設定操作へのアクセスだけが許可されており、role2 ではデバッグ操作へのアクセスだけが許可されている場合、role1 と role2 の両方に属するユーザは、設定操作とデバッグ操作にアクセスできます。特定の、VLAN、およびインターフェイスへのアクセスを制限することもできます。

スイッチには、次のデフォルト ユーザ ロールが用意されています。

network-admin

スイッチ全体に対する完全な読み取りと書き込みのアクセス権。

network-operator

スイッチに対する完全な読み取りアクセス権。



(注) 複数のルールに属するユーザは、そのルールで許可されるすべてのコマンドの組み合わせを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、ユーザが、コンフィギュレーション コマンドへのアクセスが拒否されたルール A を持っていたとします。しかし、同じユーザが RoleB も持ち、このルールではコンフィギュレーション コマンドにアクセスできるとします。この場合、このユーザ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。



(注) network-admin ユーザのみ、チェックポイントやロールバックを RBAC ロールで実行できます。他のユーザは、そのロールの permit ルールにこれらのコマンドがあるにはありますが、それらのコマンドを実行しようとするとうユーザアクセスが拒否されます

ルール

ルールは、ロールの基本要素です。ルールは、そのロールがユーザにどの操作の実行を許可するかを定義します。ルールは次のパラメータで適用できます。

コマンド

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

Cisco Nexus デバイスにより提供される機能に適用されるコマンド。show role featureshow role feature コマンドを入力すると、このパラメータに指定できる機能名が表示されます。

機能グループ

機能のデフォルト グループまたはユーザ定義グループ show role feature-groupshow role feature-group コマンドを入力すると、このパラメータに指定できるデフォルトの機能グループが表示されます。

これらのパラメータは、階層状の関係を作成します。最も基本的な制御パラメータは command です。次の制御パラメータは feature です。これは、その機能にアソシエートされているすべてのコマンドを表します。最後の制御パラメータが、feature group 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す。機能グループによりルールを簡単に管理できます。

ロールごとに最大 256 のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。ルールは降順で適用されます。たとえば、1つのロールが3つのルールを持っている場合、ルール3がルール2よりも前に適用され、ルール2はルール1よりも前に適用されます。

ユーザロールポリシー

ユーザがアクセスできるスイッチリソースを制限するために、またはインターフェイスとVLANへのアクセスを制限するために、ユーザロールポリシーを定義できます。

ユーザロールポリシーは、ロールに定義されている規則で制約されます。たとえば、特定のインターフェイスへのアクセスを許可するインターフェイスポリシーを定義した場合、`interfaceinterface` コマンドを許可するコマンドルールをロールに設定しないと、ユーザはインターフェイスにアクセスできません。

コマンドルールが特定のリソース（インターフェイス、VLAN）へのアクセスを許可した場合、ユーザがそのユーザに関連付けられたユーザロールポリシーに表示されていない場合でも、ユーザはこれらのリソースへのアクセスを許可されます。

ユーザアカウントの設定の制限事項

次の語は予約済みであり、ユーザ設定に使用できません。

- adm
- bin
- daemon
- ftp
- ftpuser
- games
- gdm
- gopher
- halt
- lp
- mail
- mailnull
- man
- mtsuser
- news
- nobody
- san-admin

- shutdown
- sync
- sys
- uucp
- xfs



注意

ユーザパスワードの要件

Cisco Nexus デバイスパスワードには大文字小文字の区別があり、英数字だけを含むことができません。ドル記号 (\$) やパーセント記号 (%) などの特殊文字は使用できません。

パスワードが脆弱な場合（短い、解読されやすいなど）、Cisco Nexus デバイスはパスワードを拒否します。各ユーザアカウントには強力なパスワードを設定するようにしてください。強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰り返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2009AsdfLkj30
- Cb1955S21



(注) セキュリティ上の理由から、ユーザパスワードはコンフィギュレーションファイルに表示されません。

ユーザアカウントの注意事項および制約事項

ユーザアカウントおよびRBACを設定する場合、ユーザアカウントには次の注意事項および制約事項があります。

- 最大 256 個のルールをユーザ ロールに追加できます。
- 最大 64 個のユーザ ロールをユーザ アカウントに割り当てることができます。
- 1 つのユーザ ロールを複数のユーザ アカウントに割り当てることができます。
- network-admin、network-operator、san-admin などの事前定義されたロールは編集不可です。
- ルールの追加、削除、編集は、SAN 管理者ユーザ ロールではサポートされません。
- インターフェイス、VLAN、または VSAN 範囲は SAN 管理者ユーザ ロールでは変更できません。



(注) ユーザアカウントは、少なくとも 1 つのユーザ ロールを持たなければなりません。

ユーザアカウントの設定



(注) ユーザアカウントの属性に加えられた変更は、そのユーザがログインして新しいセッションを作成するまで有効になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	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	switch(config)# show role	(任意) 使用可能なユーザ ロールを表示します。必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	switch(config) # username user-id [password password] [expire date] [role role-name]	ユーザ アカウントを設定します。 user-id は、最大 28 文字の英数字の文字列で、大文字と小文字が区別されます。 デフォルトの password は定義されていません。

	コマンドまたはアクション	目的
		(注) パスワードを指定しなかった場合、ユーザはスイッチにログインできない場合があります。 expire date オプションの形式は、YYYY-MM-DD です。デフォルトでは、失効日はありません。
ステップ 4	switch(config) # exit	グローバル コンフィギュレーション モードを終了します。
ステップ 5	switch# show user-account	(任意) ロール設定を表示します。
ステップ 6	switch# copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、ユーザアカウントを設定する例を示します。

```
switch# configure terminal
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# exit
switch# show user-account
```

RBAC の設定

ユーザ ロールおよびルールの作成

指定したルール番号は、ルールが適用される順番を決定します。ルールは降順で適用されます。たとえば、1つのロールが3つのルールを持っている場合、ルール3がルール2よりも前に適用され、ルール2はルール1よりも前に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	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	switch(config) # role name role-name	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。 role-name 引数は、最大 16 文字の英数字の文字列で、大文字と小文字が区別されます。

	コマンドまたはアクション	目的
ステップ 3	<code>switch(config-role) #rule number {deny permit} command command-string</code>	コマンド規則を設定します。 <i>command-string</i> には、スペースおよび正規表現を含めることができます。たとえば、「 <code>interface ethernet *</code> 」は、すべてのイーサネットインターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	<code>switch(config-role)# rule number {deny permit} {read read-write}</code>	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。
ステップ 5	<code>switch(config-role)# rule number {deny permit} {read read-write} feature feature-name</code>	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 機能の一覧を表示するには、 <code>show role featureshow role feature</code> コマンドを使用します。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 6	<code>switch(config-role)# rule number {deny permit} {read read-write} feature-group group-name</code>	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 機能グループの一覧を表示するには、 <code>show role feature-groupshow role feature-group</code> コマンドを使用します。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 7	<code>switch(config-role)# description text</code>	(任意) ロールの説明を設定します。説明にはスペースも含めることができます。
ステップ 8	<code>switch(config-role)# end</code>	ロール コンフィギュレーション モードを終了します。
ステップ 9	<code>switch# show role</code>	(任意) ユーザロールの設定を表示します。
ステップ 10	<code>switch# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、ユーザロールを作成してルールを指定する例を示します。

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule deny command clear users
```

```
switch(config-role)# rule deny read-write
switch(config-role)# description This role does not allow users to use clear commands
switch(config-role)# end
switch(config)# show role
```

機能グループの作成

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	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	switch(config) # role feature-group group-name	ユーザ ロール機能グループを指定して、ロール機能グループコンフィギュレーションモードを開始します。 <i>group-name</i> は、最大 32 文字の英数字の文字列で、大文字と小文字が区別されます。
ステップ 3	switch(config) # exit	グローバルコンフィギュレーションモードを終了します。
ステップ 4	switch# show role feature-group	(任意) ロール機能グループ設定を表示します。
ステップ 5	switch# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

次に、機能グループを作成する例を示します。

```
switch# configure terminal
switch(config) # role feature-group group1
switch(config) # exit
switch# show role feature-group
switch# copy running-config startup-config
switch#
```

ユーザ ロール インターフェイス ポリシーの変更

ユーザ ロール インターフェイス ポリシーを変更することで、ユーザがアクセスできるインターフェイスを制限できます。ロールがアクセスできるインターフェイスのリストを指定します。これを必要なインターフェイスの数だけ指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	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	switch(config) # role name <i>role-name</i>	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始します。
ステップ 3	switch(config-role) # interface policy deny	ロールインターフェイス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	switch(config-role-interface) # permit interface <i>interface-list</i>	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。 このコマンドの場合、イーサネットインターフェイスを指定できます。
ステップ 5	switch(config-role-interface) # exit	ロールインターフェイス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	switch(config-role) # show role	(任意) ロール設定を表示します。
ステップ 7	switch(config-role) # copy running-config startup-config	(任意) 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

次に、ユーザがアクセスできるインターフェイスを制限するために、ユーザロールインターフェイスポリシーを変更する例を示します。

```
switch# configure terminal
switch(config)# role name UserB
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1
switch(config-role-interface)# permit interface fc 3/1
switch(config-role-interface)# permit interface vfc 30/1
```

ユーザロールVLANポリシーの変更

ユーザロールVLANポリシーを変更することで、ユーザがアクセスできるVLANを制限できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	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	switch(config) # role name <i>role-name</i>	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始します。
ステップ 3	switch(config-role) # vlan policy deny	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	switch(config-role-vlan) # permit vlan <i>vlan-list</i>	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。
ステップ 5	switch(config-role-vlan) # exit	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	switch# show role	(任意) ロール設定を表示します。
ステップ 7	switch# copy running-config startup-config	(任意) リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。

ユーザアカウントとRBACの設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show role [<i>role-name</i>]	ユーザ ロールの設定を表示します。
show role feature	機能リストを表示します。
show role feature-group	機能グループの設定を表示します。
show startup-config security	スタートアップコンフィギュレーションのユーザアカウント設定を表示します。

コマンド	目的
<code>show running-config security [all]</code>	実行コンフィギュレーションのユーザアカウント設定を表示します。 all キーワードを指定すると、ユーザアカウントのデフォルト値が表示されます。
<code>show user-account</code>	ユーザアカウント情報を表示します。

ユーザアカウントおよびRBACのユーザアカウントデフォルト設定

次の表に、ユーザアカウントおよびRBACパラメータのデフォルト設定を示します。

表 1: デフォルトのユーザアカウントおよびRBACパラメータ

パラメータ	デフォルト
ユーザアカウントパスワード	未定義
ユーザアカウントの有効期限	なし。
インターフェイスポリシー	すべてのインターフェイスがアクセス可能
VLANポリシー	すべてのVLANがアクセス可能
VFCポリシー	すべてのVFCにアクセス可能。
VETHポリシー	すべてのVETHにアクセス可能。

