



ユーザアカウントおよびRBACの設定

この章は、次の項で構成されています。

- [ユーザーアカウントおよびRBACの概要, on page 1](#)
- [ユーザー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, on page 5](#)
- [RBACの設定 \(8 ページ\)](#)
- [ユーザーアカウントとRBACの設定の確認, on page 13](#)
- [ユーザーアカウントおよびRBACのユーザーアカウントデフォルト設定, on page 13](#)

ユーザーアカウントおよび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、ユーザーがスイッチにログインするときに各ユーザー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ーロールを定義し、各ユーザーロールがどの管理操作を実行できるかを指定します。スイッチのユーザーアカウントを作成するとき、そのアカウントにユーザーロールを関連付けます。これにより個々のユーザー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

ユーザーロールには、そのロールを割り当てられたユーザーが実行できる操作を定義するルールが含まれています。各ユーザーロールに複数のルールを含めることができ、各ユーザー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ーは、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 ユーザー ロールが用意されています。

network-admin (スーパーユーザー)

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。



Note 複数のロールに属するユーザは、そのロ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ロール A を持っていたとします。しかし、同じユーザが ロール B も持ち、このロ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。

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 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-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。

OID

SNMP オブジェクト ID (OID)。

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コマンドです。次の制御パラメータは機能です。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、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す。機能グループによりルールを簡単に管理できます。

SNMP OID は RBAC でサポートされています。SNMP OID に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つのルールが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。

ユーザーロールポリシー

ユーザー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、ユーザーロールポリシーを定義できます。

ユーザーロールポリシーは、ロールに定義されているルールで制約されます。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、**interface** 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、ユーザーがそのユーザーに関連付けられたユーザーロールポリシーに表示されていなくても、ユーザーはこれらのリソースへのアクセスを許可されます。

ユーザーアカウントの設定の制限事項

次の語は予約済みであり、ユーザー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 Cisco Nexus シリーズ スイッチでは、すべて数字のユーザー名が TACACS+ または RADIUS で作成されている場合でも、すべて数字のユーザー名はサポートされません。AAA サーバに数字だけのユーザ名が登録されていて、ログイン時に入力しても、スイッチはログイン要求を拒否します。

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、英数字を含むことができます。



(注) Cisco Nexus デバイスのパスワードには、ドル記号 (\$) やパーセント記号 (%) などの特殊文字を使用できません。

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。各ユーザー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。

ユーザーアカウントの注意事項および制約事項

ユーザーアカウントおよびRBACを設定する場合、ユーザー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。

- ユーザロールに設定された読み取り/書き込みルールに関係なく、一部のコマンドは、あらかじめ定義された `network-admin` ロールでのみ実行できます。
- 最大 256 個のルールをユーザーロールに追加できます。
- 最大 64 個のユーザーロールをユーザーアカウントに割り当てることができます。
- 1 つのユーザーロールを複数のユーザー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 管理者ユーザー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 管理者ユーザーロールでは変更できません。



(注) ユーザーアカウントは、少なくとも 1 つのユーザー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



Note ユーザーアカウントの属性に加えられた変更は、そのユーザー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。

ユーザー名の最初の文字として、任意の英数字または `_` (アンダースコア) を使用できます。最初の文字にその他の特殊文字を使用することはできません。ユーザー名に許可されていない文字が含まれている場合、指定したユーザーはログインできません。

Procedure

	Command or Action	Purpose
ステップ 1	<code>switch# configure terminal</code>	グローバル設定モードを開始します。
ステップ 2	(Optional) <code>switch(config)# show role</code>	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。

	Command or Action	Purpose
ステップ 3	<code>switch(config) # username user-id [password password] [expire date] [role role-name]</code>	<p>ユーザーアカウントを設定します。</p> <p><i>user-id</i> 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。</p> <p>デフォルトの <i>password</i> は定義されていません。</p> <p>Note パスワードを指定しなかった場合、ユーザーはスイッチにログインできない場合があります。</p> <p>Note リリース 7.0(3)I2(1)以降では、パスワード強度をチェックするための新しい内部関数が実装されています。リリース 7.0(3)I2(1)の Cisco Nexus 3000 シリーズプラットフォームでパスワード強度チェックを有効にすると、以前のリリースとは異なる基準が適用されます。</p> <p>expire date オプションのフォーマットは YYYY-MM-DD です。デフォルトでは、失効日はありません。</p>
ステップ 4	<code>switch(config) # exit</code>	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	(Optional) <code>switch# show user-account</code>	ロール設定を表示します。
ステップ 6	(Optional) <code>switch# copy running-config startup-config</code>	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。

Example

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
```

次に、リリース 7.0(3)I2(1)以降でパスワード強度チェックを有効にする基準の例を示します。

```
switch(config)# username xyz password nbv12345
password is weak
Password should contain characters from at least three of the following classes: lower
case letters, upper case letters, digits and special characters.
switch(config)# username xyz password Nbv12345
password is weak
it is too simplistic/systematic
switch(config)#
```

SAN 管理者ユーザの設定

手順

	コマンドまたはアクション	目的
ステップ 1	switch# configure terminal	グローバル設定モードを開始します。
ステップ 2	switch(config) # username user-id role san-admin password password	指定したユーザに対する SAN 管理者ユーザ ロールのアクセス権を設定します。
ステップ 3	(任意) switch(config) # show user-account	ロール設定を表示します。
ステップ 4	(任意) switch(config) # show snmp-user	SNMP ユーザの設定を表示します。
ステップ 5	(任意) switch(config)# copy running-config startup-config	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。

例

次に、SAN 管理者ユーザを設定し、ユーザアカウントおよび SNMP ユーザ設定を表示する例を示します。

```
switch# configure terminal
switch(config)# username user1 role san-admin password xyz123
switch(config)# show user-account
user:admin
    this user account has no expiry date
    roles:network-admin
user:user1
    this user account has no expiry date
    roles:san-admin
switch(config) # show snmp user
```

SNMP USERS

User	Auth	Priv(enforce)	Groups
admin	md5	des(no)	network-admin

```
user1    md5    des(no)    san-admin
```

```
NOTIFICATION TARGET USES (configured for sending V3 Inform)
```

```
User      Auth      Priv
```

```
switch(config) #
```

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル設定モードを開始します。
ステップ 2	switch(config) # role name role-name	ユーザーロールを指定し、ロールコンフィギュレーションモードを開始します。 <i>role-name</i> 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。
ステップ 3	switch(config-role) # rule number {deny permit} command command-string	コマンドルールを設定します。 <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、「interface ethernet *」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	switch(config-role)# rule number {deny permit} {read read-write}	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。

	Command or Action	Purpose
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。 機能リストを表示するには、 show role feature 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。 機能グループのリストを表示するには、 show role feature-group 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	(Optional) <code>switch(config-role)# description text</code>	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	(Optional) <code>switch# show role</code>	ユーザロールの設定を表示します。
ステップ 10	(Optional) <code>switch# copy running-config startup-config</code>	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。

Example

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

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル設定モードを開始します。
ステップ 2	switch(config) # role feature-group <i>group-name</i>	ユーザー 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せん。
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	(Optional) switch# show role feature-group	ロール機能グループ設定を表示します。
ステップ 5	(Optional) switch# copy running-config startup-config	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。

Example

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

ユーザー ロール インターフェイス ポリシーを変更することで、ユーザー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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル設定モードを開始します。

	Command or Action	Purpose
ステップ 2	<code>switch(config) # role name role-name</code>	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	<code>switch(config-role) # interface policy deny</code>	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	<code>switch(config-role-interface) # permit interface interface-list</code>	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	<code>switch(config-role-interface) # exit</code>	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	(Optional) <code>switch(config-role) # show role</code>	ロール設定を表示します。
ステップ 7	(Optional) <code>switch(config-role) # copy running-config startup-config</code>	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。

Example

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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル設定モードを開始します。
ステップ 2	switch(config) # role name <i>role-name</i>	ユーザーロールを指定し、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	(Optional) switch# show role	ロール設定を表示します。
ステップ 7	(Optional) switch# copy running-config startup-config	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。

ユーザロールVSANポリシーの変更

ユーザーロールVSANポリシーを変更して、ユーザーがアクセスできるVSANを制限できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	グローバル設定モードを開始します。
ステップ 2	switch(config-role) # role name <i>role-name</i>	ユーザーロールを指定し、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) # vsan policy deny	ロールVSAN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-vsan) # permit vsan <i>vsan-list</i>	ロールがアクセスできるVSAN範囲を指定します。

	Command or Action	Purpose
		必要な VSAN 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-vsan) # exit	ロール VSAN 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	(Optional) switch# show role	ロール設定を表示します。
ステップ 7	(Optional) switch# copy running-config startup-config	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。

ユーザーアカウントと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 [role-name]	ユーザー 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。
show running-config security [all]	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。
show user-account	ユーザアカウント情報を表示します。

ユーザーアカウントおよびRBACのユーザーアカウントデフォルト設定

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

Table 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にアクセス可能。
VLANポリシー	すべてのVLANにアクセス可能。
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。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。