



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 アカウントと RBAC について, on page 1
- ユーザー アカウントの注意事項および制約事項, on page 5
- ユーザ アカウントの設定, on page 5
- RBAC の設定 (7 ページ)
- ユーザー アカウントと RBAC の設定の確認, on page 12
- ユーザー アカウントおよび RBAC のデフォルト設定, on page 12

ユーザ アカウントと RBAC について

Cisco Nexus 3600 プラットフォームスイッチは、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ます。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 やインターフェイスだけに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。

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。

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 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構成しないと、ユーザー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 ポリシーに含まれていなくても、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

■ ユーザ パスワードの要件



注意

Cisco Nexus 3600 プラットフォーム 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ー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。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。



(注)

Cisco NX-OS Release 7.2(0)N1(1) 以降、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す。

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 および network-operator などの事前定義されたロールは編集不可です。



Note 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。

SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# **show role**
3. switch(config) # **username user-id [password password] [expire date] [role role-name]**
4. switch(config) # **exit**
5. (Optional) switch# **show user-account**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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	(Optional) switch(config)# show role	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]	<p>ユーザ アカウントを設定します。</p> <p>値は、<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 パスワード は、未定義です。</p> <p>Note</p> <p>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</p> <p>リリース 7.0 (3) F3 (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。</p> <p>値は、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	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	(Optional) switch# show user-account	ロール設定を表示します。
ステップ 6	(Optional) switch# copy running-config startup-config	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
```

次の例は、リリース 7.0 (3) F3 (1) 以降のパスワード強度チェックを有効にする基準を示しています。

```

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 Nbvl2345
password is weak
it is too simplistic/systematic
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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role name role-name**
3. switch(config-role) # **rule number {deny | permit} command command-string**
4. switch(config-role) # **rule number {deny | permit} {read | read-write}**
5. switch(config-role) # **rule number {deny | permit} {read | read-write} feature feature-name**
6. switch(config-role) # **rule number {deny | permit} {read | read-write} feature-group group-name**
7. (Optional) switch(config-role) # **description text**
8. switch(config-role) # **end**
9. (Optional) switch# **show role**
10. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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。 値は、 <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。

ユーザ ロールおよびルールの作成

	Command or Action	Purpose
		値は、 <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。
ステップ 5	switch(config-role)# rule number {deny permit} {read read-write} feature feature-name	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。 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	switch(config-role)# rule number {deny permit} {read read-write} feature-group group-name	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。 show role feature-group コマンドを使用して、機能グループのリストを表示します。 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) switch(config-role)# description text	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	switch(config-role)# end	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) switch# show role	ユーザ ロールの設定を表示します。
ステップ 10	(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、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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role feature-group group-name**
3. switch(config) # **exit**
4. (Optional) switch# **show role feature-group**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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。 [group-name] 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	(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ト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 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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role name role-name**
3. switch(config-role) # **interface policy deny**
4. switch(config-role-interface) # **permit interface interface-list**
5. switch(config-role-interface) # **exit**
6. (Optional) switch(config-role) # **show role**
7. (Optional) switch(config-role) # **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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) # 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 interface-list	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。 このコマンドでは、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	(Optional) switch(config-role) # show role	ロール 設定を表示します。
ステップ 7	(Optional) switch(config-role) # copy running-config startup-config	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、ユーザーがアクセスできるインターフェイスを制限するために、ユーザー 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

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

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config) # **role name role-name**
3. switch(config-role) # **vlan policy deny**
4. switch(config-role-vlan) # **permit vlan vlan-list**
5. switch(config-role-vlan) # **exit**
6. (Optional) switch# **show role**
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
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 vlan-list	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。

■ ユーザー アカウントと RBAC の設定の確認

	Command or Action	Purpose
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ー 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。
ユーザー 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。

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。