ユーザ アカウントと RBAC の設定

この章の内容は、次のとおりです。

ユーザ アカウントと 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 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	nscd	operator	rpc	rpcuser
shutdown	sync	sys	uucp	xfs

注意 Cisco Nexus 5000 シリーズ スイッチでは、すべて数字のユーザ名が 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 5000 シリーズ 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。

パスワードが脆弱な場合（短い、解読されやすいなど）、Cisco Nexus 5000 シリーズ スイッチ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。 強固なパスワードは、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
- 固有名詞を含んでいない
- 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

強固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 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 VSAN、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。

Cisco Nexus 3000 シリーズ スイッチは、次のデフォルトのユーザ ロールを提供します。

- network-admin（スーパーユーザ）：スイッチ全体に対して完全な読み取りと書き込みのアクセス権を持ちます。
- network-operator：スイッチに対して完全な読み取りアクセス権を持ちます。

（注） 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。

- Command：コマンドまたは正規表現で定義された一連のコマンド。
- Feature：Cisco Nexus 5000 シリーズ スイッチにより提供される機能に適用されるコマンド。
  - **show role feature** コマンドを入力すれば、このパラメータに指定できる機能名が表示されます。
- Feature group：デフォルトまたはユーザ定義の機能グループ。
  - **show role feature-group** コマンドを入力すれば、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 ロール ポリシーを定義することにより、ユーザがアクセスできるスイッチ リソースを制限できます。 インターフェイス、VLAN、および VSAN へのアクセスを制限するユーザ 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、または VSAN）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くても、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 アカウントの注意事項および制約事項

ユーザ アカウントと RBAC には、次の設定ガイドラインと制限事項があります。

- ユーザ ロールには最大 256 個の規則を追加できます。
- 1 つのユーザ アカウントに最大 64 個のユーザ ロールを割り当てられます。

（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

1 台の Cisco Nexus シリーズ スイッチ上に最大 256 個のユーザ アカウントを作成できます。 ユーザ アカウントは、次の属性を持ちます。

- ユーザ名
- パスワード
- 失効日
- ユーザ ロール

ユーザ アカウントは、最大 64 個のユーザ ロールを持つことができます。

（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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	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 2	switch# **configure terminal**	コンフィギュレーション モードに入ります。
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 文字の英数字のストリングで、大文字と小文字が区別されます。 デフォルト パスワードは定義されていません。 （注） パスワードを指定しなかった場合、ユーザは Cisco Nexus 5000 シリーズ 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# **show user-account**	（任意） ロール設定を表示します。
ステップ 5	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

各ユーザ ロールが、最大 256 個のルールを持つことができます。 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。

指定するルール番号は、適用するルールの順序を決めます。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。

手順の概要

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. （任意） switch(config-role)# **description** *text*
8. （任意） switch# **show role**
9. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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 文字の長さの英数字のストリングで、大文字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。 *command-string* 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。

	コマンドまたはアクション	目的
		必要なルール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、読み取り専用ルールか読み取りと書き込みのルールかを設定します。 **show role feature** コマンドを使用すれば、機能のリストが表示されます。 必要なルール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、読み取り専用ルールか読み取りと書き込みのルールかを設定します。 **show role feature-group** コマンドを使用すれば、機能グループのリストが表示されます。 必要なルールの数だけこのコマンドを繰り返します。
ステップ 7	switch(config-role)# **description** *text*	（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	switch# **show role**	（任意） ユーザ ロールの設定を表示します。
ステップ 9	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 ロールを作成して規則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

機能グループを作成できます。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。 *group-name* は、最大 32 文字の英数字のストリングで、大文字と小文字が区別されます。
ステップ 3	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 4	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。

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。

手順の概要

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. （任意） switch(config-role)# **show role**
7. （任意） switch(config-role)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。
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。 このコマンドの場合、イーサネット インターフェイス、ファイバ チャネル インターフェイス、および仮想ファイバ チャネル 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
```

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できます。 これを必要なインターフェイスの数だけ指定できます。

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。

手順の概要

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. （任意） switch# **show role**
6. （任意） switch# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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。
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。
ステップ 5	switch# **show role**	（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。

ユーザ ロール VSAN ポリシーの変更

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **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。
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** *vsan-list*	ロールがアクセスできる VSAN 範囲を指定します。 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# **show role**	（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。

ユーザ アカウントと RBAC の設定の確認

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行います。

コマンド	目的
show role	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。

コマンド	目的
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 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 アカウントと *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。