ユーザ アカウントと RBAC の設定

この章は、次の内容で構成されています。

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、各ユーザがスイッチにログインしたときに取得するアクセスの量を定義します。

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規則が含まれています。各ユーザ ロールに複数の規則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、ロール 1 では設定操作の実行だけが許可されており、ロール 2 ではデバッグ操作の実行だけが許可されている場合、ロール 1 とロール 2 の両方に属するユーザは、設定操作とデバッグ操作を実行できます。 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（スーパーユーザ）

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。

ネットワーク オペレータ

スイッチに対する完全な読み取りアクセス権。

（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 RoleB 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

規則は、ロールの基本要素です。 規則は、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。 規則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 3000 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。

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、その機能に関連付けら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。 規則が適用される順序は、ユーザ指定の規則番号で決まります。 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 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 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か、またはインターフェイスおよび VLAN 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は、ロールで **インターフェイス** コマンドを許可するためのコマンドルールを設定しない限り、ユーザはそのインターフェイスにアクセスできません。

コマンド ルールで特定のリソース（インターフェイス、VLAN）へのアクセスが許可されている場合は、ユーザがそのユーザに関連付けられたユーザ ロール ポリシーにリストされていなくても、ユーザはこれらのリソースへのアクセスが許可されます。

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
- shutdown
- sync
- sys
- uucp

- xfs

注意 Cisco Nexus 3000 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 3000 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 3000 シリーズ スイッチはその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 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 を設定する場合は、次の注意事項および制約事項を考慮してください。

- ユーザ ロールには最大 256 のルールを追加できます。
- ユーザ アカウントには最大 64 のユーザ ロールを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 などの定義済みのロールは編集できません。
- SAN admin ユーザ ロールの場合、ルールの追加、削除、および編集はサポートされません。
- SAN admin ユーザ ロールの場合、インターフェイス、VLAN、または VSAN の範囲は変更できません。

（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。 （注） パスワードを指定しない場合は、ユーザがスイッチにログインできない可能性があります。 **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。

	コマンドまたはアクション	目的
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

指定するルール番号は、適用した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 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 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*	コマンド規則を設定します。 *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 * には、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** コマンドを使用すれば、機能のリストが表示されます。 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 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** コマンドを使用すれば、機能グループのリストが表示されます。 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 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(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	switch# **show role**	（任意） ユーザ ロールの設定を表示します。
ステップ 10	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、変更を永続的に保存します。

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。 *group-name* は、最大 32 文字の英数字で、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、変更を永続的に保存します。

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** *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、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** *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(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、変更を永続的に保存します。

ユーザ アカウントおよび RBAC 設定の確認

設定を確認するには、次のいずれかのコマンドを使用します。

コマンド	目的
show role [*role-name*]	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
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。