



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, 1 ページ](#)
- [ユーザアカウントの注意事項および制約事項, 7 ページ](#)
- [ユーザアカウントの設定, 8 ページ](#)
- [RBAC の設定, 10 ページ](#)
- [ユーザアカウントと RBAC の設定の確認, 15 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, 16 ページ](#)

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 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。

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。

san-admin

SNMP または CLI を使用した FCoE 管理タスクへの完全な読み取りと書き込みのアクセス権。



(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。

事前定義された SAN 管理者ユーザ ロール

SAN 管理者ユーザ ロールは、LAN および SAN の管理タスクを分離するように設計された、編集不可能な事前定義されたユーザ ロールです。SAN 管理者ユーザ ロールを割り当てられたユーザは、すべてのイーサネット コンフィギュレーション タスクへの読み取り専用アクセスがあります。別のユーザ ロールによって割り当てられていない場合、SAN の管理者ユーザには、イーサネット機能に対する書き込みアクセスが許可されません。

SAN 管理者ユーザには、次の機能が許可されます。

- インターフェイス コンフィギュレーション
- VSAN の設定 (データベースやメンバーシップなど)。
- FCoE 用に事前設定された VLAN の VSAN へのマッピング
- ゾーン分割設定
- SNMP コミュニティと SNMP ユーザを除く SNMP 関連パラメータの設定
- 他のすべての設定に対する読み取り専用アクセス
- 次のような SAN 機能の設定および管理：
 - FC-SP
 - FC-PORT-SECURITY
 - FCoE
 - FCoE-NPV

- FPORT-CHANNEL-TRUNK
 - PORT-TRACK
 - FABRIC-BINDING
- 次の EXEC モード コマンドの設定および管理：
- DEBUG
 - FCDOMAIN
 - FCPING
 - SAN-PORT-CHANNEL
 - SHOW
 - ZONE
 - ZONESET



(注) SAN 管理者ロールは、すべてのインターフェイスタイプでの設定を許可します。事前定義された SAN 管理者ユーザロールは、イーサネットインターフェイスを含むすべてのインターフェイスへのアクセスを許可するように設計されています。そのため、SNMPの動作は妨げられません。

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。

SAN 管理者ロール機能のルール マッピング

SAN 管理者ロールは編集不可です。次のロール機能は、設定済みのロールの一部です。事前設定されたロールには、完全な読み取りアクセス権があり、次のルールが適用されます。

表 1: SAN 管理者ユーザロールのロール機能のルール

| 機能 | 権限 |
|----------------|---|
| copy | コピー関連コマンドに対する読み取りおよび書き込み権限 |
| fabric-binding | ファブリックバインディング関連コマンドに対する読み取りおよび書き込み権限 |
| fcoe | Fibre Channel over Ethernet 関連コマンドに対する読み取りおよび書き込み権限 |
| fdmi | Fabric Device Management Interface (FDMI) 関連コマンドに対する読み取りおよび書き込み権限 |
| fspf | Fabric Shortest Path First (FSPF) 関連コマンドに対する読み取りおよび書き込み権限 |
| interface | インターフェイス関連コマンドに対する読み取りおよび書き込み権限。 |
| port-track | ポートトラック関連コマンドに対する読み取りおよび書き込み権限 |
| port-security | ポートセキュリティ関連コマンドに対する読み取りおよび書き込み権限 |
| rdl | Remote Domain Loopback (RDL) 関連コマンドに対する読み取りおよび書き込み権限 |
| rmon | RMON 関連コマンドに対する読み取りおよび書き込み権限 |

| 機能 | 権限 |
|-----------------------|---|
| rscn | Registered State Change Notification (RSCN) 関連コマンドに対する読み取りおよび書き込み権限 |
| snmp | SNMP 関連コマンドに対する読み取りおよび書き込み権限 |
| snmpTargetAddrEntry | SNMP トラップターゲット関連コマンドに対する読み取りおよび書き込み権限 |
| snmpTargetParamsEntry | SNMP トラップターゲットパラメータ関連コマンドに対する読み取りおよび書き込み権限 |
| span | SPAN 関連コマンドに対する読み取りおよび書き込み権限 |
| trapRegEntry | SNMP トラップレジストリ関連コマンドに対する読み取りおよび書き込み権限 |
| vsan | VSAN 関連コマンドに対する読み取りおよび書き込み権限 |
| vsanIfvsan | FCoE VLAN と VSAN 間マッピング コマンド関連コマンドに対する読み取りおよび書き込み権限 |
| wwnm | World Wide Name (WWN) 関連コマンドに対する読み取りおよび書き込み権限 |
| zone | ゾーン分割コマンドに対する読み取りおよび書き込み権限 |

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、VLAN、VSAN 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 デバイスでは、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、デバイス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 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

ユーザアカウントおよびRBACを設定する場合、次の注意事項および制約事項を考慮してください。

- 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 <i>user-id</i> [password <i>password</i>] [expire date] [role <i>role-name</i>] | ユーザ アカウントを設定します。 <i>user-id</i> 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。 デフォルトの <i>password</i> 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。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| 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
```

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 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) # 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 | switch(config) # show user-account | (任意) ロール設定を表示します。 |
| ステップ 4 | switch(config) # show snmp-user | (任意) SNMP ユーザの設定を表示します。 |
| ステップ 5 | switch(config)# 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、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

| | 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。 <i>role-name</i> 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 <i>number {deny permit}</i> command <i>command-string</i> | 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。 必要なルールの数だけこのコマンドを繰り返します。 |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| 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 | <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 | <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。 <i>group-name</i> 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(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 <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。 このコマンドには、イーサネットまたは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 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、変更を永続的に保存します。 |

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

| | 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) # 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。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| 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(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 | 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 2: 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。 |