



ユーザアカウントおよびRBACの設定

この章では、Cisco NX-OS デバイス上でユーザアカウントおよびロールベース アクセス コントロール (RBAC) を設定する手順について説明します。

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](#)
- [ユーザアカウントおよびRBACの注意事項と制約事項 \(4 ページ\)](#)
- [ユーザアカウントおよびRBACのデフォルト設定, on page 5](#)
- [パスワードの強度確認のイネーブル化, on page 6](#)
- [ユーザアカウントの設定, on page 7](#)
- [ロールの設定, on page 9](#)
- [No Service Password-Recovery について \(17 ページ\)](#)
- [No Service Password-Recovery のイネーブル化 \(18 ページ\)](#)
- [ユーザアカウントおよびRBAC設定の確認, on page 19](#)
- [ユーザアカウントおよびRBACの設定例, on page 20](#)
- [ユーザアカウントおよびRBACに関する追加情報, on page 21](#)

ユーザアカウントとRBACについて

ユーザアカウントを作成して管理し、Cisco NX-OS で行える操作を制限するロールを割り当てることができます。RBACは、ユーザが実行する必要がある管理操作の許可を制限するロールの割り当てのルールを定義することを可能にします。

ユーザアカウント

最大256のユーザアカウントを作成できます。デフォルトでは、明示的に期限を指定しないかぎり、ユーザアカウントは無期限に有効です。expire オプションを使用すると、ユーザアカウントをディセーブルにする日付を設定できます。

次の語は予約済みであり、ユーザ設定に使用できません。bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、root、rpc、rpcuser、xfs、gdm、mtuser、ftuser、man、および sys。



Note ユーザのパスワードは、設定ファイルでは表示されません。



Caution ユーザ名は、先頭が英数字で始まる必要があり、その他に使用できる特殊文字は(+ = . _ \ -)。#記号と!記号はサポートされていません。ユーザ名に許可されていない文字が含まれている場合、指定したユーザはログインできません。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。



Note 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。

- 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
- 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
- 2004AsdfLkj30
- Cb1955S21



Note クリアテキストのパスワードでは、パスワードの先頭に引用符 (" または ')、縦棒 (|)、大なり記号 (>) などの特殊文字を含めることはできません。パスワードの強度確認をイネーブルにすると、パスワードが単純である場合 (短く、簡単に解読されるパスワードなど) に、Cisco NX-OS ソフトウェアによってパスワード設定が拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは大文字と小文字が区別されます。



Note 出力可能なすべてのASCII文字は、引用符で囲めば、パスワード文字列でサポートされます。

Related Topics

[パスワードの強度確認のイネーブル化](#) (6 ページ)

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、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。また、特定の仮想ルーティング/転送 (VRF) インスタンス、VLAN、およびインターフェイスへのアクセスも制限できます。

Cisco NX-OS ソフトウェアには、次のユーザロールが用意されています。

- `network-admin` : Cisco NX-OS デバイス全体への完全な読み取り/書き込みアクセス権
- `network-operator` または `vdc-operator` : Cisco NX-OS デバイス全体への完全な読み取りアクセス権



Note

- Cisco Nexus 9000シリーズスイッチは複数のVDCをサポートしていません。ただし、`vdc-operator`ロールは使用可能で、`network-operator`ロールと同じ権限と制限があります。
- Cisco Nexus 9000 シリーズ スイッチは、VDC 管理者がネットワーク管理者と同じ権限と制限を持つような、単一の VDC をサポートします。



Note ユーザロールは変更できません。



Note 一部の `show` コマンドは、`network-operator` ユーザには表示されないようにすることができます。加えて、一部の `show` 以外のコマンド (`telnet` など) を、このユーザロールで使用できるようにすることができます。

デフォルトでは、管理者のロールがないユーザアカウントでは `show`、`exit`、`end`、および `configure terminal` コマンドにしかアクセスできません。ルールを追加して、ユーザが機能を設定できるようにすることが可能です。



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

ユーザ ロールのルール

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

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

OID

SNMP オブジェクト ID (OID)。

command、feature、および feature group の各パラメータにより、階層的な関係が作成されます。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。Cisco NX-OS ソフトウェアは、使用可能な事前定義済み機能グループもサポートしています。

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 アカウントおよび RBAC の注意事項と制約事項

ユーザ アカウントおよび RBAC には、次の設定ガイドラインと制約事項があります。

- 1つのユーザ ロールには最大 256 のルールを追加できます。
- デフォルトの機能グループである L3に加えて、最大 64 のユーザ定義機能グループを追加できます。

- 最大 256 人のユーザを設定できます。
- ユーザアカウントには最大 64 個のユーザ ロールを割り当てることができます。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザアカウントが、AAA サーバ上のリモートユーザアカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカルユーザアカウントのユーザ ロールをリモートユーザに適用します。
- デフォルトの admin と SNMP ユーザアカウントは削除できません。
- デフォルトのユーザ ロールを、デフォルトの admin ユーザアカウントから削除することはできません。
- network-operator ロールでは、`ssh show running-config` および `show startup-config` コマンドを実行できません。
- Cisco Nexus 9000 シリーズスイッチは、VDC 管理者がネットワーク管理者と同じ権限と制限を持つ単一の VDC をサポートします。
- AAA ポリシーに従って、ロールがユーザに最後のロールとして関連付けられている場合、そのロールは、そのユーザから関連付けが解除されるまで削除できません。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

ユーザアカウントおよびRBACのデフォルト設定

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。

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
ユーザアカウントロール	作成ユーザが network-admin ロールを持つ場合は network-operator
デフォルトユーザロール	network-operator
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

パラメータ	デフォルト
VRF ポリシー	すべての VRF にアクセス可能
機能グループ	L3

パスワードの強度確認のイネーブル化

ユーザアカウントに対して弱いパスワードを設定しないように、パスワードの強度確認機能をイネーブルにすることができます。



Note パスワード強度確認をイネーブルにしても、Cisco NX-OS ソフトウェアでは、既存パスワードの強度確認は行われません。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	password strength-check Example: switch(config)# password strength-check	パスワードの強度確認をイネーブルにします。デフォルトではイネーブルになっています。 パスワードの強度確認をディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	exit Example: switch(config)# exit switch#	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) show password strength-check Example: switch# show password strength-check	パスワードの強度確認の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

Related Topics

[強力なパスワードの特性](#) (2 ページ)

ユーザアカウントの設定

1 つの Cisco NX-OS デバイスに最大 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。

- ユーザー名 (Username)
- パスワード (Password)
- 失効日
- ユーザ ロール

パスワードはクリアテキストか暗号化された形式で入力できます。Cisco NX-OS パスワードは、実行コンフィギュレーションに保存する前にクリアテキストのパスワードを暗号化します。暗号化された形式のパスワードは、これ以上の暗号化を行わずに実行コンフィギュレーションに保存されます。

SHA256 は、パスワードの暗号化に使用されるハッシュアルゴリズムです。暗号化の一環として、64 ビット SALT の 5000 回の反復がパスワードに追加されます。

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。コマンドラインインターフェイス (CLI) の状況依存ヘルプユーティリティを使用して、利用できるコマンドを確認できます。



Note 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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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) show role Example: 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。

	Command or Action	Purpose
ステップ 3	<p>username <i>user-id</i> [password [0 5] <i>password</i>] [expire date] [role <i>role-name</i>]</p> <p>Example:</p> <pre>switch(config)# username NewUser password 4Ty18Rnt</pre>	<p>ユーザアカウントを設定します。 <i>user-id</i> 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。指定できる文字は、A～Z の英大文字、a～z の英小文字、0～9 の数字、ハイフン (-)、ピリオド (.)、アンダースコア (_)、プラス符号 (+)、および等号 (=) です。アットマーク (@) はリモートユーザ名では使用できますが、ローカルユーザ名では使用できません。</p> <p>ユーザ名の先頭は英数字で始まる必要があります。</p> <p>デフォルトパスワードは定義されていません。オプションの 0 は、パスワードがクリアテキストであり、5 はパスワードが暗号化されていることを意味します。デフォルトは 0 (クリアテキスト) です。</p> <p>Note パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。</p> <p>Note 暗号化パスワードオプションを使用してユーザアカウントを作成する場合、対応する SNMP ユーザは作成されません。</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> <p>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。</p>
ステップ 4	<p>username <i>user-id</i> ssh-cert-dn <i>dn-name</i> {dsa rsa}</p> <p>Example:</p> <pre>switch(config)# username NewUser ssh-cert-dn "/CN = NewUser, OU = Cisco Demo, O = Cisco, C = US" rsa</pre> <p>Example:</p>	<p>既存のユーザアカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ emailAddress と ST に設定されていることを確認します。</p>

	Command or Action	Purpose
	<pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre>	
ステップ 5	<p>exit</p> <p>Example:</p> <pre>switch(config)# exit switch#</pre>	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 6	<p>(Optional) show user-account</p> <p>Example:</p> <pre>switch# show user-account</pre>	ロール設定を表示します。
ステップ 7	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

Related Topics

[ロールの設定 \(9 ページ\)](#)

[ユーザ ロールおよびルールの作成 \(9 ページ\)](#)

ロールの設定

ここでは、ユーザ ロールの設定方法について説明します。

ユーザ ロールおよびルールの作成

最大 64 個のユーザ ロールを設定できます。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。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。



Note

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。

Before you begin

ユーザロール設定を配布する場合は、設定を配布する対象のすべてのCisco NX-OSデバイスでユーザロール設定の配布を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	role name role-name Example: switch(config)# role name UserA switch(config-role)#	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	rule number {deny permit} command command-string Example: switch(config-role)# rule 1 deny command clear users	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 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。 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	rule number {deny permit} {read read-write} Example: switch(config-role)# rule 2 deny 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	rule number {deny permit} {read read-write} feature feature-name Example: switch(config-role)# rule 3 permit read feature router-bgp	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	rule number {deny permit} {read read-write} feature-group group-name Example:	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。

	Command or Action	Purpose
	<pre>switch(config-role)# rule 4 deny read-write feature-group L3</pre>	<p>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。</p> <p>必要な規則の数だけこのコマンドを繰り返します。</p>
ステップ 7	<p>rule number {deny permit} {read read-write} oid snmp_oid_name</p> <p>Example:</p> <pre>switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9</pre>	<p>SNMP オブジェクト ID (OID) の読み取り専用または読み書きルールを設定します。OIDには最大32の要素を入力することができます。このコマンドは、SNMP ベースのパフォーマンスモニタリングツールがデバイスをポーリングするために使用できますが、IP ルーティングテーブル、MAC アドレステーブル、特定の MIB などのシステムの集中的な拠点へのアクセスは制限されます。</p> <p>Note 一番深層の OID はスカラレベルまたはテーブルルートレベルにすることができます。</p> <p>必要な規則の数だけこのコマンドを繰り返します。</p>
ステップ 8	<p>(Optional) description text</p> <p>Example:</p> <pre>switch(config-role)# description This role does not allow users to use clear commands</pre>	<p>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。</p>
ステップ 9	<p>exit</p> <p>Example:</p> <pre>switch(config-role)# exit switch(config)#</pre>	<p>ロールコンフィギュレーションモードを終了します。</p>
ステップ 10	<p>(Optional) show role</p> <p>Example:</p> <pre>switch(config)# show role</pre>	<p>ユーザロールの設定を表示します。</p>
ステップ 11	<p>(Optional) show role {pending pending-diff}</p> <p>Example:</p> <pre>switch(config)# show role pending</pre>	<p>配布するために保留状態になっているユーザロール設定を表示します。</p>

	Command or Action	Purpose
ステップ 12	(Optional) role commit Example: switch(config)# role commit	一時データベース内にあるユーザロールの設定変更を実行コンフィギュレーションに適用します。
ステップ 13	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

機能グループの作成

カスタム機能グループを作成して、Cisco NX-OS ソフトウェアが提供するデフォルトの機能リストに追加できます。これらの機能グループは1つまたは複数の機能を含んでいます。最大 64 個の機能グループを作成できます。



Note デフォルト機能グループ L3 を変更することはできません。

Before you begin

ユーザロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザロール設定の配布を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	role feature-group name group-name Example: switch(config)# role feature-group name GroupA switch(config-role-featuregrp)#	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> 引数は、最大 32 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	feature feature-name Example: switch(config-role-featuregrp)# feature radius	機能グループの機能を指定します。 必要な機能の数だけこのコマンドを繰り返します。

	Command or Action	Purpose
		Note 機能の一覧を表示する場合は、 show role component コマンドを使用します。
ステップ 4	exit Example: switch(config-role-featuregrp)# exit switch(config)#	ロール機能グループ 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) show role feature-group Example: switch(config)# 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 6	(Optional) show role {pending pending-diff} Example: switch(config)# show role pending	配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 7	(Optional) role commit Example: switch(config)# role commit	一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用します。
ステップ 8	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

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。デフォルトでは、ユーザ ロールによってすべてのインターフェイスへのアクセスが許可されます。

Before you begin

1 つまたは複数のユーザ ロールを作成します。

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	role name role-name Example: switch(config)# role name UserA switch(config-role)#	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	interface policy deny Example: switch(config-role)# interface policy deny switch(config-role-interface)#	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	permit interface interface-list Example: switch(config-role-interface)# permit interface ethernet 2/1-4	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。
ステップ 5	exit Example: switch(config-role-interface)# exit switch(config-role)#	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) show role Example: switch(config-role)# show role	ロール設定を表示します。
ステップ 7	(Optional) show role {pending pending-diff} Example: switch(config-role)# show role pending	配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 8	(Optional) role commit Example: switch(config-role)# role commit	一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用します。
ステップ 9	(Optional) copy running-config startup-config Example: switch(config-role)# copy running-config startup-config	実行設定を、スタートアップ設定にコピーします。

Related Topics

[ユーザロールおよびルールの作成](#) (9 ページ)

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。デフォルトでは、ユーザロールによってすべてのVLANへのアクセスが許可されます。

Before you begin

1つまたは複数のユーザロールを作成します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: switch# configure terminal switch(config)#	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	role name role-name Example: switch(config)# role name UserA switch(config-role)#	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	vlan policy deny Example: switch(config-role)# vlan policy deny switch(config-role-vlan)#	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	permit vlan vlan-list Example: switch(config-role-vlan)# permit vlan 1-4	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	exit Example: switch(config-role-vlan)# exit switch(config-role)#	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) show role Example: switch(config)# show role	ロール設定を表示します。
ステップ 7	(Optional) show role {pending pending-diff} Example:	配布するために保留状態になっているユーザロール設定を表示します。

	Command or Action	Purpose
	<code>switch(config-role)# show role pending</code>	
ステップ 8	(Optional) role commit Example: <code>switch(config-role)# role commit</code>	一時データベース内にあるユーザロールの設定変更を実行コンフィギュレーションに適用します。
ステップ 9	(Optional) copy running-config startup-config Example: <code>switch(config-role)# copy running-config startup-config</code>	実行設定を、スタートアップ設定にコピーします。

Related Topics

[ユーザロールおよびルールの作成 \(9 ページ\)](#)

ユーザロールのVRFポリシーの変更

ユーザロールのVRFポリシーを変更して、ユーザがアクセスできるVRFを制限できます。デフォルトでは、ユーザロールによってすべてのVRFへのアクセスが許可されます。

Before you begin

1 つまたは複数のユーザロールを作成します。

ユーザロール設定を配布する場合は、設定を配布する対象のすべてのCisco NX-OSデバイスでユーザロール設定の配布をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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	role name role-name Example: <code>switch(config)# role name UserA</code> <code>switch(config-role)#</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	vrf policy deny Example: <code>switch(config-role)# vrf policy deny</code> <code>switch(config-role-vrf)#</code>	ロールVRFポリシーコンフィギュレーションモードを開始します。

	Command or Action	Purpose
ステップ 4	permit vrf vrf-name Example: <pre>switch(config-role-vrf)# permit vrf vrf1</pre>	ロールがアクセスできる VRF を指定します。 必要な VRF の数だけこのコマンドを繰り返します。
ステップ 5	exit Example: <pre>switch(config-role-vrf)# exit switch(config-role)#</pre>	ロール VRF 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) show role Example: <pre>switch(config-role)# show role</pre>	ロール設定を表示します。
ステップ 7	(Optional) show role {pending pending-diff} Example: <pre>switch(config-role)# show role pending</pre>	配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 8	(Optional) role commit Example: <pre>switch(config-role)# role commit</pre>	一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用します。
ステップ 9	(Optional) copy running-config startup-config Example: <pre>switch(config-role)# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

Related Topics

[ユーザ ロールおよびルールの作成 \(9 ページ\)](#)

No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることとなります。No Service Password-Recovery 機能を使用すると、『[Cisco Nexus 9000 Series NX-OS Troubleshooting Guide](#)』に記載されている標準的な手順でパスワードを回復できなくなります。

No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： <pre>switch# configure terminal switch(config)#</pre>	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	no service password-recovery 例： <pre>switch(config)# no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [#####] 100% Copy complete, now saving to disk (please wait)... Copy complete.</pre>	パスワード回復メカニズムを無効にします。
ステップ 3	(任意) copy running-config startup-config 例： <pre>switch# copy running-config startup-config</pre>	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。
ステップ 4	Reload 例： <pre>switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %\$ VDC-1 %\$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface</pre>	

	コマンドまたはアクション	目的
	<pre>CISCO SWITCH Ver 8.34 CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, switch(boot)# config t Enter configuration commands, one per line. End with CNTL/Z. switch(boot) (config)# admin-password Abcd!123\$ ERROR: service password-recovery disabled. Cannot change password! switch(boot) (config)#</pre>	
ステップ5	<p>exit</p> <p>例:</p> <pre>switch(config)# exit switch#</pre>	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6	<p>(任意) show user-account</p> <p>例:</p> <pre>switch# show user-account</pre>	ロール設定を表示します。
ステップ7	<p>(任意) copy running-config startup-config</p> <p>例:</p> <pre>switch# copy running-config startup-config</pre>	実行設定を、スタートアップ設定にコピーします。

ユーザアカウントおよびRBAC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 cli syntax roles network-admin	network-admin ロールが使用できるが、コマンドの構文を表示します。
show cli syntax roles network-operator	network-operator ロールで。
show role	ユーザ ロールの設定を表示します。

コマンド	目的
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 の設定例

次に、ユーザ ロールを設定する例を示します。

```
role name User-role-A
  rule 2 permit read-write feature bgp
  rule 1 deny command clear *
```

次に、BGP を有効にして表示し、EIGRP を表示するようにインターフェイスを設定できるユーザ ロールを作成する例を示します。

```
role name iftest
  rule 1 permit command config t; interface *; bgp *
  rule 2 permit read-write feature bgp
  rule 3 permit read feature eigrp
```

上の例で、ルール 1 はインターフェイス上で BGP を設定することを可能にし、ルール 2 は **config bgp** コマンドを設定して実行レベルの **show** コマンドと **debug** コマンドを BGP に対して有効にすることを有効にし、ルール 3 は実行レベルの **show** コマンドと **debug eigrp** コマンドを有効にすることを可能にしています。

次に、特定のインターフェイスだけを設定できるユーザ ロールを設定する例を示します。

```
role name Int_Eth2-3_only
  rule 1 permit command configure terminal; interface *
  interface policy deny
  permit interface Ethernet2/3
```

次に、ユーザ ロール機能グループを設定する例を示します。

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature aaa
  feature acl
  feature access-list
```

次に、ユーザ アカウントを設定する例を示します。

```
username user1 password A1s2D4f5 role User-role-A
```

次に、アクセスを OID サブツリーの一部に制限するための OID ルールを追加する例を示します。

```
role name User1
  rule 1 permit read feature snmp
  rule 2 deny read oid 1.3.6.1.2.1.1.9
show role name User1
```

```
Role: User1
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Rule	Perm	Type	Scope	Entity
2	deny	read	oid	1.3.6.1.2.1.1.9
1	permit	read	feature	snmp

次に、指定された OID サブツリーへの書き込み権限を許可する例を示します。

```
role name User1
  rule 3 permit read-write oid 1.3.6.1.2.1.1.5
show role name User1
```

```
Role: User1
Description: new role
Vlan policy: permit (default)
Interface policy: permit (default)
Vrf policy: permit (default)
```

Rule	Perm	Type	Scope	Entity
3	permit	read-write	oid	1.3.6.1.2.1.1.5
2	deny	read	oid	1.3.6.1.2.1.1.9
1	permit	read	feature	snmp

ユーザアカウントおよびRBACに関する追加情報

ここでは、ユーザアカウントおよびRBACの実装に関する追加情報について説明します。

関連資料

関連項目	マニュアルタイトル
Cisco NX-OS のライセンス	Cisco NX-OS ライセンス ガイド
VRF コンフィギュレーション	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB のリンク
ユーザアカウントおよびRBACに関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html