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

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の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。

ユーザーアカウント

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、mtsuser、ftpuser、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 (+ = . _ \ -)。#, @ および ! 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 （7 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。

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 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限事項があります。

- 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、s**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。

- Cisco NX-OS Release 10.2(2)F 以降、新しい非同期化 CLI が導入され、SNMP とセキュリティ コンポーネントの間のユーザー同期を無効にするオプションを提供します。詳細については、システム管理構成ガイドの *SNMP* の構成の章を参照してください。

  リリース 7.0(3)I7(1) から現在のリリースまでのさまざまな機能をサポートする Cisco Nexus 9000 スイッチの詳細については、Nexus スイッチ プラットフォーム サポート マトリックスを参照してください。
- 非同期 CLI が有効になっている場合、リモート ユーザーは SNMP データベースに同期されません。
- DCNM（リリース 12.0.1.a 以降 Nexus Dashboard Fabric Controller とも呼ばれる）を使用したセキュリティ ユーザーには、非同期 CLI が有効でないとき、対応する SNMPv3 プロファ

イルが存在しません。同期が無効になっている場合、セキュリティ コンポーネントで作成されたユーザーはスイッチにログインできますが、コントローラはスイッチを検出しません。コントローラは、セキュリティ ユーザー用に作成された SNMP 構成を使用してスイッチを検出するためです。さらに、SNMP は、userDB の非同期状態のため、作成されたセキュリティ ユーザーを認識しないので、スイッチを検出できません。したがって、コントローラによってスイッチが検出されるようにするには、SNMP ユーザーを明示的に作成する必要があります。DCNM 機能とともに非同期 CLI を使用することはお勧めしません。詳細については、*Cisco Nexus 9000 NX-OS* セキュリティ構成ガイドを参照してください。

- Cisco NX-OS Release 10.3(1)F 以降、タイプ 8 とタイプ 9 パスワード ハッシュが Cisco Nexus 9000 シリーズ スイッチでサポートされます。

（注） タイプ 5 は下位互換性をサポートしていますが、タイプ 8 とタイプ 9 をダウングレードすることはできません。

- Cisco NX-OS リリース 10.3(1)F 以降、パスワードの連続文字チェックは Cisco Nexus 9000 シリーズ スイッチでサポートされています。

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
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。

Related Topics

強力なパスワードの特性 （2 ページ）

パスワードの連続文字チェックの有効化

パスワードシーケンスで、キーボード上の並び文字やアルファベットの並び文字は、攻撃に対して脆弱なため、制限が課されます。

パスワードには、次のパスワード文字列シーケンスの長さ制限が課されます。

- 設定可能な値の繰り返しの文字数（aaaa、bbbb など）
- 連続するアルファベット/数字の文字数（abcd...、1234...、）
- キーボード上で連続している文字の数 (qwer...、asdf...)

この手順では、パスワードのシーケンスに対する制限の構成方法について説明します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードを入力します。

ステップ 2	**[no] userpassphrase sequence alphabet length** *Value* 例： `switch(config)#userpassphrase sequence alphabet length 4`	連続したアルファベットの長さの制限を設定します。キーボード上で並んだ文字の長さの範囲は 2 ～ 10 です。 例：**userpassphrase sequence alphabet length** *4* **username user password** *AbcDe19jd* このパスワードの文字は指定数を超えて連続しているため、受け入れられません。 **no** オプションは、アルファベット順のチェックを無効にします。
ステップ 3	**[no] userpassphrase sequence keyboard length** *Value* 例： `switch(config)# userpassphrase sequence keyboard length 4`	キーボード上で並んだ文字の長さの制限を設定します。キーボード上で並んだ文字の長さの範囲は 2 ～ 10 です。 例：**userpassphrase sequence keyboard length** *4* **username user password** *CvBnmwu204*

	コマンドまたはアクション	目的
		このパスワードの文字はキーボード上で指定数を超えて連続しているため、受け入れられません **no** オプションは、キーボード上で並んだ文字のチェックを無効にします。

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
- パスワード
- 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。

SHA256は、パスワードの暗号化に使用されるデフォルトのハッシュ アルゴリズムです。タイプ 8 およびタイプ 9 のパスワードのハッシュを生成するには、クリア テキスト パスワードとともに PBKDF2/SCRYPT オプションを指定する必要があります。

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。
ステップ 3	**username** *user-id* [**password** [**0** | **5** | **8** | **9**] *password* **[pbkdf2 | scrypt]**] [**expire** *date*] [**role** *role-name*] **Example:** `switch(config)# username NewUser password 4Ty18Rnt`	ユーザ アカウントを設定します。*user-id* 引数は、大文字と小文字が区別される英数字で、最大 28 文字です。これはローカルおよびリモート ユーザーの両方に当てはまります。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。 ユーザ名の先頭は英数字で始まる必要があります。 デフォルト パスワードは定義されていません。 • **0** オプションは、パスワードがクリア テキストであることを示しています。 • **5** オプションは、パスワードが SHA-256 ハッシュされていることを示します。 • **8** オプションは、パスワードが PBKDF2 ハッシュされていることを示します。 • **9** オプションは、パスワードが Scrypt ハッシュされていることを示します。

	Command or Action	Purpose
		デフォルト オプションは **0**（クリア テキスト）です。 **Note** pbkdf2/scrypt キーワードはオプションであり、実行構成に保存されます。 **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。 **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。 **Note** 非同期 CLI が有効になっている場合、ユーザー アカウントを作成しても、対応する SNMP ユーザーは作成されません。 **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。 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。

ステップ 4	**username** *user-id* **ssh-cert-dn** *dn-name* {**dsa** | **rsa**}
	Example:
	`switch(config)# username NewUser ssh-cert-dn "/CN = NewUser, OU = Cisco Demo, O = Cisco, C = US" rsa`
	Example:
	`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`
		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。

ステップ 5	**exit** **Example:**	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。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 6	(Optional) **show user-account** **Example:** `switch# show user-account`	ロール設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

ロールの設定 （12 ページ）
ユーザ ロールおよびルールの作成 （12 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。

一致に対して RBACL 処理を実行する場合、部分一致では評価プロセスは停止しません。完全一致が見つかるまで、各ルールの評価が続行されます。完全一致が見つからない場合、リスト内で最も正確なルールが結果として選択されます。また、同じ一致ロジックに対して許可ルールと拒否ルールが存在する場合、（先に評価された）番号の大きいルールが結果として選択されます。

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。*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	**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。 *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。 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:** `switch(config-role)# rule 4 deny read-write feature-group L3`	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。

	Command or Action	Purpose
		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	**rule** *number* {**deny** | **permit**} {**read** | **read-write**} **oid** *snmp_oid_name* **Example:** `switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9`	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。 **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。 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 8	(Optional) **description** *text* **Example:** `switch(config-role)# description This role does not allow users to use clear commands`	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 9	**exit** **Example:** `switch(config-role)# exit switch(config)#`	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 10	(Optional) **show role** **Example:** `switch(config)# show role`	ユーザ ロールの設定を表示します。
ステップ 11	(Optional) **copy running-config startup-config** **Example:** `switch(config)# 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。

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 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。
		group-name 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。 **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。

	Command or Action	Purpose
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# 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。

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。

	Command or Action	Purpose

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) **copy running-config startup-config** **Example:** `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。

Related Topics

ユーザ ロールおよびルールの作成 （12 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。

	Command or Action	Purpose
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) **copy running-config startup-config** **Example:** `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。

Related Topics

ユーザ ロールおよびルールの作成 （12 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:
	`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

	Command or Action	Purpose

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	**vrf policy deny**
	Example:
	`switch(config-role)# vrf policy deny`
	`switch(config-role-vrf)#`
		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。

ステップ 4	**permit vrf** *vrf-name* **Example:** `switch(config-role-vrf)# permit vrf vrf1`	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:
	`switch(config-role-vrf)# exit`
	`switch(config-role)#`
		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:** `switch(config-role)# show role`	ロール設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

ユーザ ロールおよびルールの作成 （12 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になります。No Service Password-Recovery 機能を使用すると、Cisco Nexus 9000 シリーズ NX-OS トラブルシューティング ガイド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：
	`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	**no service password-recovery**
	例：
	`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.`
		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： `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。

ステップ 4	**Reload**
	例：
	`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`	

	コマンドまたはアクション	目的
	Interface 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)#	
ステップ 5	**exit** 例： 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 6	（任意） **show user-account** 例： switch# show user-account	ロール設定を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： 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。

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* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイド』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

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。 https://cisco.github.io/cisco-mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

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。