R コマンド

この章では、R で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

radius-server deadtime

NX-OS デバイスにすべての RADIUS サーバのデッド タイム間隔を設定するには、**radius-server deadtime** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

シンタックスの説明

minutes	デッド タイム間隔の分数。有効範囲は 1 ～ 1440 分です。

デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デッド タイム間隔は、NX-OS デバイスが応答のなかった RADIUS サーバを確認するまでの分数です。

（注） デフォルトのアイドル タイマー値は、0 分です。アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての RADIUS サーバの定期的なモニタリングを実行するグローバル デッド タイム間隔を設定する例を示します。

```
switch# config t
switch(config)# radius-server deadtime 5
```

次に、すべての RADIUS サーバのグローバル デッド タイム間隔をデフォルトに戻して、サーバの定期的なモニタリングをディセーブルにする例を示します。

```
switch# config t
switch(config)# no radius-server deadtime 5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server directed-request

ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにするには、**radius-server directed-request** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server directed-request

no radius-server directed-request

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト 設定した RADIUS サーバ グループに認証要求を送信します。

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン ログイン時、*username@vrfname*:*hostname* を指定できます。*vrfname* は、使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスで、*hostname* は、設定した RADIUS サーバ名です。ユーザ名が認証用に RADIUS サーバに送信されます。

このコマンドには、ライセンスは必要ありません。

例 次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにする例を示します。

```
switch# config t
switch(config)# radius-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できないようにする例を示します。

```
switch# config t
switch(config)# no radius-server directed-request
```

関連コマンド

コマンド	説明
show radius-server directed-request	指定要求 RADIUS サーバ設定を表示します。

radius-server host

RADIUS サーバ パラメータを設定するには、**radius-server host** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

シンタックスの説明

hostname	RADIUS サーバの Domain Name Server（DNS）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	*A.B.C.D* フォーマットの RADIUS サーバの IPv4 アドレス
ipv6-address	*X:X:X::X* フォーマットの RADIUS サーバの IPv6 アドレス
key	（任意）RADIUS サーバ事前共有秘密鍵を設定します。
0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有鍵を設定します。これがデフォルトです。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有鍵（7 で表示）を設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証する事前共有鍵。事前共有鍵には、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、長さは 63 文字に制限されています。
pac	（任意）Cisco TrustSec と連動させるために、RADIUS Cisco Access Control Server（ACS）で Protected Access Credentials（PAC）の生成をイネーブルにします。
accounting	（任意）アカウンティングを設定します。
acct-port *port-number*	（任意）アカウンティング用の RADIUS サーバのポートを設定します。範囲は 0 ～ 65535 です。
auth-port *port-number*	（任意）認証用の RADIUS サーバのポートを設定します。範囲は 0 ～ 65535 です。
authentication	（任意）認証を設定します。
retransmit *count*	（任意）デバイスがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数を設定します。有効範囲は 1 ～ 5 回で、デフォルトは 1 回です。
test	（任意）テスト パケットを RADIUS サーバに送信するようにパラメータを設定します。
idle-time *time*	サーバをモニタリングするための時間間隔を分で指定します。範囲は 1 ～ 1440 分です。
password *password*	テスト パケット内のユーザ パスワードを指定します。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。
username *name*	テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字の区別がなく、最大文字数は 32 です。
timeout *seconds*	RADIUS サーバへの再送信タイムアウト（秒単位）を設定します。デフォルトは 5 秒で、有効な範囲は 1 ～ 60 秒です。

デフォルト

アカウンティング ポート：1813

認証ポート：1812

アカウンティング：イネーブル

認証：イネーブル

再送信数：1

アイドル時間：なし

サーバのモニタリング：ディセーブル

タイムアウト：5 秒

テスト ユーザ名：test

テスト パスワード：test

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバの認証とアカウンティングのパラメータを設定する例を示します。

```
switch# config terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server key

RADIUS 共有秘密鍵を設定するには、**radius-server key** コマンドを使用します。設定した共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

シンタックスの説明

0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有鍵を設定します。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有鍵を設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証するのに使用される事前共有鍵。事前共有鍵には、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、長さは 63 文字に制限されています。

デフォルト

クリア テキスト

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS 事前共有鍵を設定して、RADIUS サーバに対してスイッチを認証する必要があります。鍵の長さは 63 文字に制限されており、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。グローバル鍵は、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。**radius-server host** コマンドで **key** キーワードを使用することでこのグローバル鍵の割り当てを上書きできます。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS 認証を設定する各種のシナリオを提供する例を示します。

```
switch# config terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server retransmit

デバイスが RADIUS サーバで要求を試行する回数を指定するには、**radius-server retransmit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server retransmit *count*

no radius-server retransmit *count*

シンタックスの説明

count	デバイスがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数。有効範囲は 1 ～ 5 回です。

デフォルト

再送信 1 回

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバに再送信回数を設定する例を示します。

```
switch# config t
switch(config)# radius-server retransmit 3
```

次に、RADIUS サーバに再送信のデフォルト数を設定する例を示します。

```
switch# config t
switch(config)# no radius-server retransmit 3
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server timeout

RADIUS サーバへの再送信間隔を指定するには、**radius-server timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout *seconds*

シンタックスの説明

seconds	RADIUS サーバへの再送信間隔の秒数。有効範囲は 1 ～ 60 秒です。

デフォルト

1 秒

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# radius-server timeout 30
```

次に、デフォルトの間隔に戻す例を示します。

```
switch# config t
switch(config)# no radius-server timeout 30
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

range

IP ポート オブジェクト グループにグループ メンバーとしてポートの範囲を指定するには、**range** コマンドを使用します。ポート オブジェクト グループからポート範囲のグループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **range** *starting-port-number ending-port-number*

no {*sequence-number* | **range** *starting-port-number ending-port-number*}

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号は、オブジェクト グループ内でグループ メンバーの順序を保ちます。有効なシーケンス番号は 1 ～ 4294967295 です。シーケンス番号を指定しない場合、デバイスは最大シーケンス番号より 10 大きい番号を現在のオブジェクト グループに割り当てます。
starting-port-number	このグループ メンバーに一致する最小ポート番号。有効値は、0 ～ 65535 です。
ending-port-number	このグループ メンバーに一致する最大ポート番号。有効値は、0 ～ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループには方向性がありません。**range** コマンドが送信元ポートまたは宛先ポートに一致するかどうか、または着信または発信トラフィックに適用するかどうかは、ACL 内のオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは必要ありません。

例

次に、ポート 137 ～ 139 間で送信されるトラフィックに一致するグループ メンバーで port-group-05 という名前の IP ポート オブジェクト グループを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# range 137 139
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに eq（等しい）グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに gt（より大きい）グループ メンバーを指定します。
lt	IP ポート オブジェクト グループに lt（より小さい）グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに neq（等しくない）グループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
show object-group	オブジェクト グループを表示します。

remark

IPv4 または MAC Access Control List（ACL; アクセス コントロール リスト）にコメントを入力するには、**remark** コマンドを使用します。**remark** コマンドを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

シンタックスの説明

sequence-number	（任意）**remark** コマンドのシーケンス番号。これにより、デバイスはアクセス リストの番号が指定された位置にコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、デバイスは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 **resequence** コマンドを使用して、シーケンス番号をリマークとルールに再度割り当てます。
remark	リマークのテキスト。この引数は、最大で 100 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

デフォルトでは、ACL にリマークが含まれません。

コマンド モード

IP アクセスリスト コンフィギュレーション
MAC アクセスリスト コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

remark 引数には、最大 100 文字を指定できます。*remark* 引数に 100 より多い文字を入力すると、デバイスは最初の 100 文字を受け入れ、それ以上の文字を廃棄します。

例

次に、IPv4 ACL にリマークを作成して、結果を表示する例を示します。

```
switch# config t
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the
lab
switch(config-acl)# show access-list acl-ipv4-01

IP access list acl-ipv4-01
        100 remark this ACL denies the marketing department access to the lab
ciscobox(config-acl)#
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-list	すべての ACL または 1 つの ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

replay-protection

インターフェイス上の Cisco TrustSec 認証のデータパス リプレイ保護機能をイネーブルにするには、**replay-protection** コマンドを使用します。データパス レプレイ保護機能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。

replay-protection

no replay-protection

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト イネーブル

コマンド モード Cisco TrustSec 802.1X コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、**shutdown**/**no shutdown** コマンド シーケンスを使用してインターフェイスをイネーブルおよびディセーブルにして、設定を有効にする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例 次に、インターフェイス上の Cisco TrustSec 認証のデータパス保護をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイス上の Cisco TrustSec 認証のデータパス保護をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts dot1x	インターフェイスの Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

resequence

Access Control List（ACL; アクセス コントロール リスト）のすべてのルールまたは時間の範囲にシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。

resequence *access-list-type* **access-list** *access-list-name starting-sequence-number increment*

resequence time-range *time-range-name starting-sequence-number increment*

シンタックスの説明

access-list-type	ACL のタイプ。この引数の有効値は、次のキーワードです。 • ***arp*** • ***ip*** • ***mac***
access-list *access-list-name*	ACL の名前を指定します。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
time-range *time-range-name*	時間の範囲の名前を指定します。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
starting-sequence-number	ACL の最初のルールまたは時間の範囲のシーケンス番号
increment	デバイスが後続の各シーケンス番号に追加する数

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

resequence コマンドを使用すると、ACL のルールまたは時間の範囲にシーケンス番号を再度割り当てることができます。最初のルールの新しいシーケンス番号は、*starting-sequence-number* 引数によって決まります。その他の各ルールは、*increment* 引数によって決まる新しいシーケンス番号を受け取ります。最大シーケンス番号がシーケンス番号の許容最大値を超えると、シーケンスが実行されず、次のメッセージが表示されます。

```
ERROR: Exceeded maximum sequence number.
```

最大シーケンス番号は、4294967295 です。

このコマンドには、ライセンスは必要ありません。

例

次に、**show ip access-lists** コマンドを使用して、100 のシーケンス番号で開始し、10 ずつ増える ip-acl-01 という名前の IPv4 ACL のシーケンスを再度実行し、**resequence** コマンドの使用の前後のシーケンス番号を確認する例を示します。

```
switch# config t
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        7 permit tcp addrgroup lab-machines any
        10 permit udp addrgroup lab-machines any
        13 permit icmp addrgroup lab-machines any
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp addrgroup lab-machines any
        110 permit udp addrgroup lab-machines any
        120 permit icmp addrgroup lab-machines any
        130 deny igmp any any
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。

role feature-group name

ユーザ ロール機能グループを作成または指定し、ユーザ ロール機能グループ コンフィギュレーション モードを開始するには、**role feature-group name** コマンドを使用します。ユーザ ロール機能グループを削除するには、このコマンドの **no** 形式を使用します。

role feature-group name *group-name*

no role feature-group name *group-name*

シンタックスの説明

group-name	ユーザ ロール機能グループ名。*group-name* の最大文字数は 32 で、大文字と小文字が区別され、英数字文字列で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、レイヤ 3 機能のデフォルト ユーザ ロール機能グループを備えています。L3 ユーザ ロール機能グループを変更または削除できません。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロール機能グループを作成して、ユーザ ロール機能グループ コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

次に、ユーザ ロール機能グループを削除する例を示します。

```
switch# config t
switch(config)# no role feature-group name MyGroup
```

関連コマンド

コマンド	説明
feature-group name	ユーザ ロール機能グループを指定または作成して、ユーザ 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。
show role feature-group	ユーザ ロール機能グループを表示します。

role name

ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始するには、**role name** コマンドを使用します。ユーザ ロールを削除するには、このコマンドの **no** 形式を使用します。

role name *role-name*

no role name *role-name*

シンタックスの説明

role-name	ユーザ ロール名。*role-name* の最大文字数は 16 で、大文字と小文字が区別され、英数字文字列で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、4 つのデフォルト ユーザ ロールを備えています。

- network-admin — NX-OS デバイス全体に対する読み取り / 書き込みアクセスを実行できます（デフォルト DVC でのみ使用可能）
- network-operator — NX-OS デバイス全体に対する読み取りアクセスを実行できます（デフォルト DVC でのみ使用可能）
- vdc-admin — VDC に限定した読み取り / 書き込みアクセス
- vdc-operator — VDC に限定した読み取りアクセス

デフォルトのユーザ ロールは変更または削除できません。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロールを作成して、ユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role MyRole
switch(config-role)#
```

次に、ユーザ ロールを削除する例を示します。

```
switch# config t
switch(config)# no role name MyRole
```

関連コマンド

コマンド	説明
show role	ユーザ ロールを表示します。

rule

ユーザ ロールのルールを設定するには、**rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

シンタックスの説明

number	ルールのシーケンス番号。NX-OS ソフトウェアは、最初に最大値を使用してルールを適用し、それ以降は降順で適用されます。有効範囲は 1 ～ 256 です。
deny	コマンドまたは機能へのアクセスを拒否します。
permit	コマンドまたは機能へのアクセスを許可します。
command *command-string*	コマンド ストリングを指定します。
read	読み取りアクセスを指定します。
read-write	読み取り / 書き込みアクセスを指定します。
feature *feature-name*	（任意）機能名を指定します。NX-OS 機能名を表示するには、**show role feature** コマンドを使用します。
feature-group *group-name*	（任意）機能グループを指定します。

デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

各ロールに最大 256 のルールを設定できます。

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 つのロールに 3 つのルールがある場合は、ルール 3、ルール 2、ルール 1 の順に適用されます。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロールにルールを追加する例を示します。

```
switch# config t
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

次に、ユーザ ロールからルールを削除する例を示します。

```
switch# config t
switch(config)# role MyRole
switch(config-role)# no rule 10
```

関連コマンド

コマンド	説明
role name	ユーザ ロール名を作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールを表示します。