



S コマンド

この章では、S 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。

server

RADIUS サーバ グループまたは TACACS+ サーバ グループにサーバを追加するには、**server** コマンドを使用します。サーバ グループからサーバを削除するには、このコマンドの **no** 形式を使用します。

server {*ipv4-address* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

構文の説明

<i>ipv4-address</i>	A.B.C.D 形式のサーバの IPv4 アドレス
<i>ipv6-address</i>	X:X:X::X 形式のサーバの IPv6 アドレス
<i>hostname</i>	サーバ名。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。

コマンドデフォルト

なし

コマンドモード

RADIUS サーバ グループ コンフィギュレーション モード
TACACS+ サーバ グループ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

サーバ グループには、最大 64 のサーバを設定できます。

RADIUS サーバ 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、**aaa group server radius** コマンドを使用します。TACACS+ サーバ 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、**aaa group server tacacs+** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。



(注)

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループにサーバを追加する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.1.1
```

次に、RADIUS サーバ グループからサーバを削除する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.1.1
```

次に、TACACS+ サーバ グループにサーバを追加する例を示します。

```
switch(config)# feature tacacs+
```

```
switch(config)# aaa group server tacacs+ TacServer  
switch(config-tacacs+)# server 192.168.2.2
```

次に、TACACS+ サーバ グループからサーバを削除する例を示します。

```
switch(config)# feature tacacs+  
switch(config)# aaa group server tacacs+ TacServer  
switch(config-tacacs+)# no server 192.168.2.2
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

ssh

IPv4 を使用してセキュア シェル (SSH) セッションを作成するには、**ssh** コマンドを使用します。

```
ssh [username@]{ipv4-address | hostname} [vrf {vrf-name | default | management}]
```

構文の説明

<i>username</i>	(任意) SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がなく、最大文字数は 64 です。
<i>ipv4-address</i>	リモート ホストの IPv4 アドレスです。
<i>hostname</i>	リモート ホストのホスト名です。ホスト名は、大文字と小文字が区別され、最大文字数は 64 です。
vrf <i>vrf-name</i>	(任意) SSH セッションで使用する Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) 名を指定します。この名前には最大 32 文字までの英数字を指定できます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

デフォルト VRF

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、IPv4 を使用して SSH セッションを開始する例を示します。

```
switch# ssh 192.168.1.1 vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh server enable	SSH サーバをイネーブルにします。
ssh6	IPv6 アドレスを使用して SSH セッションを開始します。

ssh6

IPv6 を使用してセキュア シェル (SSH) セッションを作成するには、**ssh6** コマンドを使用します。

```
ssh6 [username@]{ipv6-address | hostname} [vrf {vrf-name | default | management}]
```

構文の説明

<i>username</i>	(任意) SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がなく、最大文字数は 64 です。
<i>ipv6-address</i>	リモート ホストの IPv6 アドレスです。
<i>hostname</i>	リモート ホストのホスト名です。ホスト名は、大文字と小文字が区別され、最大文字数は 64 です。
vrf <i>vrf-name</i>	(任意) SSH IPv6 セッションで使用する Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) 名を指定します。この名前には最大 32 文字までの英数字を指定できます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

デフォルト VRF

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、IPv6 を使用して SSH セッションを開始する例を示します。

```
switch# ssh6 2001:0DB8::200C:417A vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh	IPv4 アドレスを使用して SSH セッションを開始します。
ssh server enable	SSH サーバをイネーブルにします。

ssh key

セキュア シェル (SSH) サーバ キーを作成するには、**ssh key** コマンドを使用します。SSH サーバ キーを削除するには、このコマンドの **no** 形式を使用します。

```
ssh key {dsa [force] | rsa [length [force]]}
```

```
no ssh key [dsa | rsa]
```

構文の説明

dsa	Digital System Algorithm (DSA) SSH サーバ キーを指定します。
force	(任意) 以前のイベントが存在する場合に、DSA SSH キー イベントを強制的に生成します。
rsa	Rivest, Shamir, and Adelman (RSA) 公開キー暗号法の SSH サーバ キーを指定します。
length	(任意) SSH サーバ キーを作成するときに使用するビット数。有効な範囲は 768 ~ 2048 です。

コマンドデフォルト

1024 ビットの長さ

コマンドモード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS ソフトウェアは SSH バージョン 2 をサポートしています。

SSH サーバ キーを削除または交換する場合、**no ssh server enable** コマンドを使用してまず SSH サーバをディセーブルにする必要があります。

例

次に、デフォルトのキーの長さで RSA を使用して SSH サーバ キーを作成する例を示します。

```
switch(config)# ssh key rsa
```

次に、指定したキーの長さで RSA を使用して SSH サーバ キーを作成する例を示します。

```
switch(config)# ssh key rsa 768
```

次に、**force** オプションで DSA を使用して SSH サーバ キーを交換する例を示します。

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

次に、DSA SSH サーバ キーを削除する例を示します。

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
```

```
switch(config)# ssh server enable
```

次に、すべての SSH サーバ キーを削除する例を示します。

```
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
```

関連コマンド

コマンド	説明
<code>show ssh key</code>	SSH サーバ キーの情報を表示します。
<code>ssh server enable</code>	SSH サーバをイネーブルにします。

ssh server enable

セキュア シェル (SSH) サーバをイネーブルにするには、**ssh server enable** コマンドを使用します。SSH サーバ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。

ssh server enable

no ssh server enable

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch(config)# ssh server enable
```

次に、SSH サーバをディセーブルにする例を示します。

```
switch(config)# no ssh server enable
```

関連コマンド

コマンド	説明
show ssh server	SSH サーバ キーの情報を表示します。

storm-control level

トラフィック ストーム制御の抑制レベルを設定するには、**storm-control level** コマンドを使用します。抑制モードをオフにしたり、デフォルトの設定に戻したりするには、このコマンドの **no** 形式を使用します。

```
storm-control {broadcast | multicast | unicast} level percentage[.fraction]
```

```
no storm-control {broadcast | multicast | unicast} level
```

構文の説明

broadcast	ブロードキャストトラフィックを指定します。
multicast	マルチキャストトラフィックを指定します。
unicast	ユニキャストトラフィックを指定します。
level percentage	抑制レベルの割合を指定します。有効な範囲は 0 ~ 100% です。
fraction	(任意) 抑制レベルの端数。有効な範囲は 0 ~ 99 です。

コマンドデフォルト

すべてのパケットが渡されます。

コマンドモード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

storm-control level コマンドを入力して、インターフェイス上のトラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、インターフェイスでイネーブルにされているすべてのトラフィック ストーム制御モードにトラフィック ストーム制御レベルを適用します。

端数の抑制レベルを入力する場合、ピリオド (.) が必要になります。

抑制レベルは、合計帯域幅の割合です。100% のしきい値は、トラフィックに制限がないことを意味します。0 または 0.0 (端数) % のしきい値は、指定されたすべてのトラフィックがポートでブロックされることを意味します。

廃棄カウントを表示するには、**show interfaces counters storm-control** コマンドを使用します。

指定したトラフィック タイプの抑制をオフにするには、次のいずれかの方式を使用します。

- 指定したトラフィック タイプのレベルを 100% に設定する。
- このコマンドの **no** 形式を使用する。

例

次に、ブロードキャストトラフィックの抑制をイネーブルにし、抑制しきい値レベルを設定する例を示します。

```
switch(config-if)# storm-control broadcast level 30
```

次に、マルチキャスト トラフィックの抑制モードをディセーブルにする例を示します。

```
switch(config-if)# no storm-control multicast level
```

関連コマンド

コマンド	説明
show interface	インターフェイスのストーム制御抑制カウンタを表示します。
show running-config	インターフェイスの設定を表示します。