



T コマンド

この章では、T 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。

tacacs+ abort

処理中の TACACS+ Cisco Fabric Services (CFS) 配信セッションを廃棄するには、**tacacs+ abort** コマンドを使用します。

tacacs+ abort

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。

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	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、処理中の TACACS+ CFS 配信セッションを廃棄する例を示します。

```
switch# config terminal
switch(config)# tacacs+ abort
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs+	TACACS+ CFS の配信ステータスおよびその他の詳細を表示します。
tacacs+ distribute	TACACS+ の CFS 配信をイネーブルにします。

tacacs+ commit

ファブリック内で処理中の TACACS+ Cisco Fabric Service (CFS) 配信セッションに関連した保留中のコンフィギュレーションを適用するには、**tacacs+ commit** コマンドを使用します。

tacacs+ commit

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。

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
VDC ユーザ

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

TACACS+ の設定をファブリックにコミットする前に、**tacacs+ distribute** コマンドを使用して、ファブリックのすべてのスイッチで、配信をイネーブルにする必要があります。

CFS は、TACACS+ サーバグループ設定、定期的な TACACS+ サーバテスト設定、またはサーバおよびグローバル キーを配信しません。キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

このコマンドには、ライセンスは必要ありません。

例

次に、ファブリックのスイッチに TACACS+ の設定を適用する例を示します。

```
switch# config terminal  
switch(config)# tacacs+ commit
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs+	TACACS+ CFS の配信ステータスおよびその他の詳細を表示します。
tacacs+ distribute	TACACS+ の CFS 配信をイネーブルにします。

tacacs+ distribute

TACACS+ の Cisco Fabric Services (CFS) 配信をイネーブルにするには、**tacacs+ distribute** コマンドを使用します。この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。

tacacs+ distribute

no tacacs+ distribute

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。

デフォルト

ディセーブル

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

CFS は、TACACS+ サーバグループ設定、定期的な TACACS+ サーバテスト設定、またはサーバおよびグローバル キーを配信しません。キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

このコマンドには、ライセンスは必要ありません。

例

次の例では、TACACS+ のファブリック配信をイネーブルにする方法を示します。

```
switch# config terminal  
switch(config)# tacacs+ distribute
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs+	TACACS+ CFS の配信ステータスおよびその他の詳細を表示します。

tacacs-server deadline

応答性について到達不能（非応答）TACACS+ サーバをモニタする定期的な時間間隔を設定するには、**tacacs-server deadline** コマンドを使用します。非応答 TACACS+ サーバのモニタリング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。

tacacs-server deadline *minutes*

no tacacs-server deadline *minutes*

構文の説明

time 分単位の時間間隔です。有効な範囲は 1 ～ 1440 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	変更箇所
4.0(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

時間間隔の設定をゼロにすると、タイマーがディセーブルになります。個別の TACACS+ サーバのデッドタイム間隔がゼロ（0）よりも大きい場合は、サーバグループに設定された値よりもその値が優先されます。

デッドタイム間隔が 0 分の場合、TACACS+ サーバがサーバグループの一部でグループのデッドタイム間隔が 0 分を超えていない限り、TACACS+ サーバモニタリングは実行されません。

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。

このコマンドには、ライセンスは必要ありません。

例

次に、デッドタイム間隔を設定して、定期的なモニタリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# tacacs-server deadline 10
```

次に、デッドタイム間隔をデフォルトに戻して、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# configure terminal
switch(config)# no tacacs-server deadline 10
```

関連コマンド

コマンド	説明
deadtime	非応答 TACACS+ サーバをモニタリングするデッドタイム間隔を設定します。
show tacacs-server	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server directed-request

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

tacacs-server directed-request

no tacacs-server directed-request

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。

デフォルト

設定した TACACS+ 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	変更箇所
4.0(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

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。

ユーザは、ログイン中に `username@vrfname:hostname` を指定することができます。 `vrfname` は使用する Virtual Routing and Forwarding (VRF; VPN ルーティングおよび転送) 名で、 `hostname` は設定した TACACS+ サーバ名です。ユーザ名が認証用にサーバ名に送信されます。



(注)

`directed-request` オプションをイネーブルにすると、Cisco NX-OS デバイスでは認証に RADIUS 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。

このコマンドには、ライセンスは必要ありません。

例

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

```
switch# configure terminal
switch(config)# tacacs-server directed-request
```


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

```
switch# configure terminal  
switch(config)# no tacacs-server directed-request
```

関連コマンド

コマンド	説明
show tacacs-server directed request	指定要求 TACACS+ サーバ コンフィギュレーションを表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server host

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

```
tacacs-server host {hostname | ipv4-address | ipv6-address}
  [key [0 | 7] shared-secret] [port port-number]
  [test {idle-time time | password password | username name}]
  [timeout seconds]
```

```
no tacacs-server host {hostname | ipv4-address | ipv6-address}
  [key [0 | 7] shared-secret] [port port-number]
  [test {idle-time time | password password | username name}]
  [timeout seconds]
```

構文の説明

<i>hostname</i>	TACACS+ サーバの Domain Name Server (DNS; ドメイン ネーム 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。
<i>ipv4-address</i>	A.B.C.D 形式の TACACS+ サーバの IPv4 アドレス。
<i>ipv6-address</i>	X:X:X:X 形式の TACACS+ サーバの IPv6 アドレス。
key	(任意) TACACS+ サーバ用の共有秘密キーを設定します。
0	(任意) TACACS+ 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キー (0 で表示) を設定します。これはデフォルトです。
7	(任意) TACACS+ 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キー (7 で表示) を設定します。
<i>shared-secret</i>	TACACS+ クライアントとサーバ間の通信を認証する事前共有キー。事前共有キーは、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 63 です。
port port-number	(任意) 認証用の TACACS+ サーバのポートを設定します。有効な範囲は 1 ~ 65535 です。
test	(任意) テスト パケットを TACACS+ 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	(任意) サーバをモニタリングするための時間間隔を分数で指定します。時間の範囲は 1 ~ 1440 分です。
password password	(任意) 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	(任意) 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。大文字と小文字が区別され、最大文字数は 32 です。
timeout seconds	(任意) TACACS+ サーバへの再送信 TACACS+ サーバタイムアウト期間 (秒単位) を設定します。有効な範囲は 1 ~ 60 秒です。

デフォルト

アイドル時間 : ディセーブル
 サーバ モニタリング : ディセーブル
 タイムアウト : 1 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	変更箇所
	4.0(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 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。
 アイドル時間間隔が 0 分の場合、TACACS+ サーバの定期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、TACACS+ サーバ ホスト パラメータを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド	コマンド	説明
	show tacacs-server	TACACS+ サーバ情報を表示します。
	feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server key

グローバル TACACS+ 共有秘密キーを設定するには、**tacacs-server key** コマンドを使用します。設定した共有秘密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。

```
tacacs-server key [0 | 6 | 7] shared-secret
```

```
no tacacs-server key [0 | 6 | 7] shared-secret
```

構文の説明

0	(任意) TACACS+ 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キーを設定します。これはデフォルトです。
6	(任意) TACACS+ 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キーを設定します。
7	(任意) TACACS+ 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キーを設定します。
<i>shared-secret</i>	TACACS+ クライアントとサーバ間の通信を認証する事前共有キー。事前共有キーは、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 63 です。

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	変更箇所
4.0(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

TACACS+ 事前共有キーを設定して TACACS+ サーバに対してデバイスを認証する必要があります。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます (スペースは使用できません)。グローバル キーを設定して、デバイスにあるすべての TACACS+ サーバ コンフィギュレーションで使用するようにできます。**tacacs-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 キーの割り当てを上書きできます。

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。

このコマンドには、ライセンスは必要ありません。

例

次に、TACACS+ サーバ共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

関連コマンド

コマンド	説明
show tacacs-server	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server test

TACACS+ サーバごとに個別にテスト パラメータを設定する必要なく、すべてのサーバの可用性をモニタするには、**tacacs-server test** コマンドを使用します。この設定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。

```
tacacs-server test {idle-time time | password password | username name}
```

```
no tacacs-server test {idle-time time | password password | username name}
```

構文の説明

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。有効な範囲は 1 ～ 1440 分です。 (注) アイドル時間間隔が 0 分の場合、TACACS+ サーバの定期モニタリングは実行されません。
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。名前は、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。 (注) ネットワークのセキュリティを保護するため、TACACS+ データベースの既存のユーザ名と異なるユーザ名を使用することを推奨します。

デフォルト

サーバ モニタリング : ディセーブル
 アイドル時間 : 0 分
 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	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、TACACS+ 認証をイネーブルにする必要があります。

テスト パラメータが設定されていないサーバは、グローバル レベルのパラメータを使用してモニタリングされます。

各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

アイドル時間間隔が 0 分の場合、TACACS+ サーバの定期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、TACACS+ サーバ グローバル モニタリング用のパラメータを設定する例を示します。

```
switch# configure terminal  
switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3
```

関連コマンド

コマンド	説明
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server timeout

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

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

構文の説明	<i>seconds</i>	TACACS+ サーバへの再送信間隔を秒単位で設定します。有効な範囲は 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	変更箇所
	4.0(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	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。このコマンドには、ライセンスは必要ありません。	
例	次に、TACACS+ サーバのタイムアウト値を設定する例を示します。 <pre>switch# configure terminal switch(config)# tacacs-server timeout 3</pre> 次に、デフォルトの TACACS+ サーバのタイムアウト値に戻す例を示します。 <pre>switch# configure terminal switch(config)# no tacacs-server timeout 3</pre>	
関連コマンド	コマンド	説明
	show tacacs-server	TACACS+ サーバ情報を表示します。
	feature tacacs+	TACACS+ をイネーブルにします。

telnet

Cisco NX-OS デバイス上に IPv4 による Telnet セッションを作成するには、**telnet** コマンドを使用します。

```
telnet {ipv4-address | hostname} [port-number] [vrf vrf-name]
```

構文の説明

<i>ipv4-address</i>	リモート デバイスの IPv4 アドレス。
<i>hostname</i>	リモート デバイスのホスト名。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 64 です。
<i>port-number</i>	(任意) Telnet セッションのポート番号。有効な範囲は 1 ~ 65535 です。
vrf <i>vrf-name</i>	(任意) Telnet 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。名前では、大文字と小文字が区別されます。

デフォルト

ポート 23
デフォルト VRF

コマンド モード

任意のコマンド モード

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	変更箇所
4.0(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

このコマンドを使用するには、**feature telnet** コマンドを使用して Telnet サーバをイネーブルにする必要があります。

IPv6 アドレスで Telnet セッションを作成するには、**telnet6** コマンドを使用します。

Cisco NX-OS ソフトウェアは、最大で 60 の並列の SSH セッションおよび Telnet セッションをサポートしています。

このコマンドには、ライセンスは必要ありません。

例

次に、IPv4 アドレスで Telnet セッションを開始する例を示します。

```
switch# telnet 10.10.1.1 vrf management
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet6	IPv6 アドレスで Telnet セッションを作成します。
feature telnet	Telnet サーバをイネーブルにします。

telnet server enable

仮想デバイス コンテキスト (VDC) の Telnet サーバをイネーブルにするには、**telnet server enable** コマンドを使用します。Telnet 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。

telnet server enable

no telnet 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。

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

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	変更箇所
4.1(2)	このコマンドは廃止予定で、 feature telnet コマンドに置き換えられます。
4.0(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

このコマンドには、ライセンスは必要ありません。

例

次に、Telnet サーバをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# telnet server enable
```

次に、Telnet サーバをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no telnet server enable
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

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

telnet6

Cisco NX-OS デバイス上に IPv6 による Telnet セッションを作成するには、**telnet6** コマンドを使用します。

```
telnet6 {ipv6-address | hostname} [port-number] [vrf vrf-name]
```

構文の説明

<i>ipv6-address</i>	リモートデバイスの IPv6 アドレス。
<i>hostname</i>	リモートデバイスのホスト名。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 64 です。
<i>port-number</i>	(任意) Telnet セッションのポート番号。有効な範囲は 1 ~ 65535 です。
vrf <i>vrf-name</i>	(任意) Telnet 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。名前では、大文字と小文字が区別されます。

デフォルト

ポート 23
デフォルト VRF

コマンドモード

任意のコマンドモード

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	変更箇所
4.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature telnet** コマンドを使用して Telnet サーバをイネーブルにする必要があります。

IPv4 アドレスで Telnet セッションを作成するには、**telnet** コマンドを使用します。

Cisco NX-OS ソフトウェアは、最大で 60 の並列の SSH セッションおよび Telnet セッションをサポートしています。

このコマンドには、ライセンスは必要ありません。

例

次に、IPv6 アドレスで Telnet セッションを開始する例を示します。

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
```

関連コマンド

コマンド	説明
<code>clear line</code>	Telnet セッションを消去します。
<code>telnet</code>	IPv4 アドレスで Telnet セッションを作成します。
<code>feature telnet</code>	Telnet サーバをイネーブルにします。

terminal verify-only

コマンドライン インターフェイス (CLI) でコマンドの認可を確認するには、**terminal verify-only** コマンドを使用します。この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。

terminal verify-only [**username** *username*]

terminal no verify-only [**username** *username*]

構文の説明

username *username* (任意) コマンド認可を確認するユーザ名を指定します。

デフォルト

ディセーブル

username キーワードのデフォルトは、現在のユーザセッションです。

コマンドモード

任意のコマンドモード

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	変更箇所
4.2(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

コマンド認可の確認をイネーブルにすると、CLI は、そのユーザに対してコマンドが正常に認可されたかについて示しますが、コマンドは実行しません。

コマンド認可の確認では、**aaa authorization commands default** コマンドおよび **aaa authorization config-commands default** コマンドで設定された方式が使用されます。

このコマンドには、ライセンスは必要ありません。

例

次に、コマンド認可の確認をイネーブルにする例を示します。

```
switch# terminal verify-only
```

次に、コマンド認可の確認をディセーブルにする例を示します。

```
switch# terminal no verify-only
```

関連コマンド

コマンド	説明
aaa authorization commands default	EXEC コマンドで認可を設定します。
aaa authorization config-commands default	コンフィギュレーション コマンドで認可を設定します。

test aaa authorization command-type

あるユーザ名に対して TACACS+ コマンド認可をテストするには、**test aaa authorization command-type** コマンドを使用します。

```
test aaa authorization command-type {commands | config-commands} user username
command command-string
```

構文の説明

commands	EXEC コマンドをテストします。
config-commands	コンフィギュレーション コマンドをテストします。
user username	TACACS+ コマンド認可をテストするユーザ名を指定します。
command command-string	認可テストに使用するユーザ名を指定します。コマンドにスペースが含まれている場合は、 <i>command-string</i> 引数を二重引用符で囲みます。

デフォルト

なし

コマンドモード

任意のコマンドモード

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	変更箇所
4.2(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

test aaa authorization command-type コマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

コマンド認可をテストする前に、**aaa server group** コマンドを使用して Cisco NX-OS デバイス上で TACACS+ グループを設定する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、あるユーザ名で TACACS+ コマンド認可をテストする例を示します。

```
switch# test aaa authorization command-type commands user testuser command "configure terminal"
```


関連コマンド

コマンド	説明
aaa authorization commands default	EXEC コマンドで認可を設定します。
aaa authorization config-commands default	コンフィギュレーション コマンドで認可を設定します。
aaa group server	AAA サーバ グループを設定します。

time-range

時間の範囲を設定するには、**time-range** コマンドを使用します。時間の範囲を削除するには、このコマンドの **no** 形式を使用します。

time-range *time-range-name*

no time-range *time-range-name*

構文の説明

time-range-name 時間の範囲名。範囲名では最大で 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。

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	変更箇所
4.0(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

このコマンドには、ライセンスは必要ありません。

IPv4 ACL および IPv6 ACL では、**permit** コマンドおよび **deny** コマンドで時間の範囲を使用できません。

例

次に、**time-range** コマンドを使用して、時間範囲の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# configure terminal
switch(config)# time-range workweek-vpn-access
switch(config-time-range)#
```

関連コマンド

コマンド	説明
absolute	特定の開始日時を持つ時間範囲を指定します。
deny (IPv4)	IPv4 拒否規則を設定します。
periodic	1 週間に 1 回または複数回アクティブである時間の範囲を指定します。
permit (IPv4)	IPv4 許可規則を設定します。

trustedCert

検索クエリーを Lightweight Directory Access Protocol (LDAP) サーバに送信するために、信頼される証明書検索操作の属性名、検索フィルタ、ベース DN を設定するには、**trustedCert** コマンドを使用します。この設定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。

```
trustedCert attribute-name attribute-name search-filter filter base-DN base-DN-name
no trustedCert
```

構文の説明

attribute-name <i>attribute-name</i>	LDAP 検索マップの属性名を指定します。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 128 です。
search-filter <i>filter</i>	LDAP 検索マップ用のフィルタを指定します。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 128 です。
base-DN <i>base-DN-name</i>	LDAP 検索マップのベース指定名を指定します。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 128 です。

デフォルト

なし

コマンドモード

LDAP 検索マップ 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	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。
このコマンドには、ライセンスは必要ありません。

例

次に、検索クエリーを LDAP サーバに送信するために、信頼される証明書検索操作の属性名、検索フィルタ、ベース DN を設定する例を示します。

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# trustedCert attribute-name cACertificate search-filter
(&(objectClass=certificationAuthority)) base-DN CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=mdslldaptestlab,DC=com
switch(config-ldap-search-map)#
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap search-map	LDAP 検索マップを設定します。
show ldap-search-map	設定された LDAP 検索マップを表示します。