



TACACS+ の設定

この章は、次の項で構成されています。

- [TACACS+ の設定について \(1 ページ\)](#)

TACACS+ の設定について

TACACS+ の設定に関する情報

Terminal Access Controller Access Control System Plus (TACACS+) セキュリティプロトコルは、Cisco Nexus デバイスにアクセスしようとするユーザーの検証を集中的に行います。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デモンのデータベースで管理されます。設定済みの TACACS+ 機能を Cisco Nexus デバイス上で使用するには、TACACS+ サーバーへのアクセス権を持ち、このサーバーを設定する必要があります。

TACACS+ では、認証、許可、アカウントिंगの各ファシリティを個別に提供します。TACACS+ を使用すると、単一のアクセスコントロールサーバー (TACACS+ デモン) で、各サービス (認証、許可、アカウントING) を個別に提供できます。各サービスは固有のデータベースにアソシエートされており、デモンの機能に応じて、そのサーバーまたはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ クライアント/サーバー プロトコルでは、トランスポート要件を満たすため TCP (TCP ポート 49) を使用します。Cisco Nexus デバイスは、TACACS+ プロトコルを使用して集中型の認証を行います。

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Cisco Nexus デバイスは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポートプロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。

- スイッチと AAA サーバ間でプロトコルペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ を使用したユーザー ログイン

ユーザーが TACACS+ を使用して、Cisco Nexus デバイスに対しパスワード認証プロトコル (PAP) によるログインを試行すると、次のプロセスが実行されます。

1. Cisco Nexus デバイスが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザー名とパスワードを取得します。



Note TACACS+ では、デーモンがユーザーを認証するために十分な情報を得られるまで、デーモンとユーザーとの自由な対話を許可します。この動作では通常、ユーザー名とパスワードの入力が要求されますが、ユーザーの母親の旧姓など、その他の項目の入力が要求されることもあります。

2. Cisco Nexus デバイスが、TACACS+ デーモンから次のいずれかの応答を受信します。
 - **ACCEPT** : ユーザーの認証に成功したので、サービスを開始します。Cisco Nexus デバイスがユーザーの許可を要求している場合は、許可が開始されます。
 - **REJECT** : ユーザーの認証に失敗しました。TACACS+ デーモンは、ユーザーに対してそれ以上のアクセスを拒否するか、ログインシーケンスを再試行するよう要求します。
 - **ERROR** : 認証中に、デーモン内、またはデーモンと Cisco Nexus デバイス間のネットワーク接続でエラーが発生しました。Cisco Nexus デバイスが ERROR 応答を受信した場合、スイッチは代替りのユーザー認証方式の使用を試みます。

Cisco Nexus デバイスで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。ユーザーは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合、Cisco Nexus デバイスは、再度、TACACS+ デーモンにアクセスします。デーモンは **ACCEPT** または **REJECT** 許可応答を返します。**ACCEPT** 応答には、ユーザに対する **EXEC** または **NETWORK** セッションの送信に使用される属性が含まれます。また **ACCEPT** 応答により、ユーザがアクセス可能なサービスが決まります。

この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイントプロトコル (PPP)、シリアルラインインターネットプロトコル (SLIP)、EXEC サービス
- ホストまたはクライアントの IP アドレス (IPv4)、アクセスリスト、ユーザー タイムアウトなどの接続パラメータ

デフォルトの TACACS+ サーバー暗号化タイプと事前共有キー

TACACS+ サーバーに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバー ホスト間の共有秘密テキストストリングです。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）。Cisco Nexus デバイス上のすべての TACACS+ サーバー設定で使用されるグローバルな事前共有秘密キーを設定できます。

グローバルな事前共有キーの設定は、個々の TACACS+ サーバーの設定時に **key** オプションを使用することによって無効にできます。

TACACS+ サーバのコマンド許可サポート

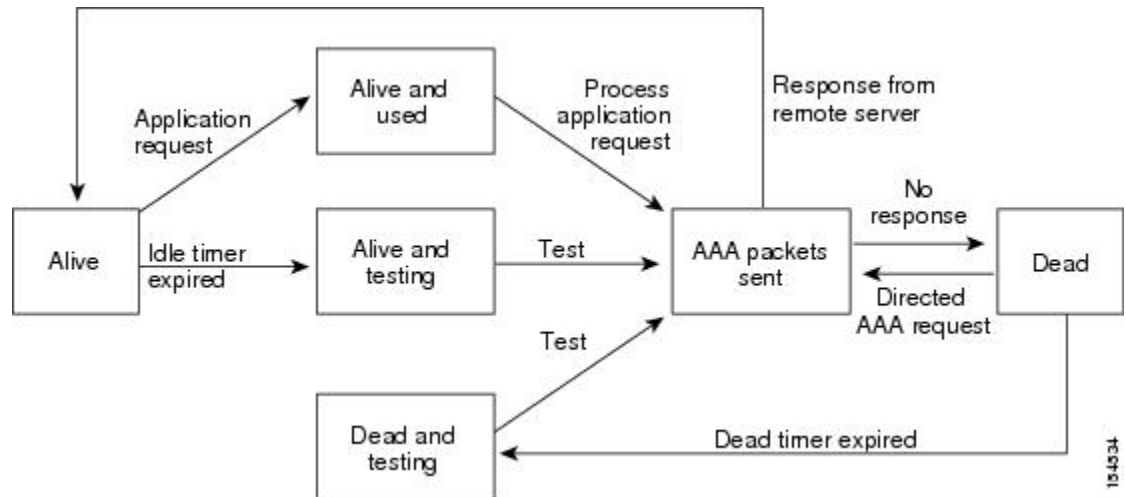
デフォルトでは、認証されたユーザーがコマンドラインインターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカルデータベースに対してコマンド許可が行われます。また、TACACS+ を使用して、認証されたユーザーに対して許可されたコマンドを確認することもできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバーがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、Cisco Nexus デバイスは定期的に TACACS+ サーバーをモニタリングし、TACACS+ サーバーが応答を返す（アライブ）かどうかを調べることができます。Cisco Nexus デバイスは、応答を返さない TACACS+ サーバーをデッド（dead）としてマークし、デッド TACACS+ サーバーには AAA 要求を送信しません。また、Cisco Nexus デバイスは定期的にデッド TACACS+ サーバーをモニタリングし、それらのサーバーが応答を返すようになった時点でアライブ状態に戻します。このプロセスでは、TACACS+ サーバーが稼働状態であることを確認してから、実際の AAA 要求がサーバーに送信されます。TACACS+ サーバーの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco Nexus デバイスによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラーメッセージが表示されます。

次の図に、さまざまな TACACS+ サーバーの状態を示します。

Figure 1: TACACS+ サーバーの状態



Note アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+サーバモニタリングを実行するには、テスト認証要求をTACACS+サーバに送信します。

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバーの IPv4 アドレスまたはホスト名を取得すること。
- TACACS+ サーバーから事前共有キーを取得していること。
- Cisco Nexus デバイスが、AAA サーバーの TACACS+ クライアントとして設定されていること。

TACACS+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco Nexus デバイスに設定できる TACACS+ サーバーの最大数は 64 です。
- TACACS+サーバホストを構成し、実際にホストを使用するように AAA 構成を行った後、次のエラーメッセージが散発的に表示されることがあります：

```
[%TACACS-3-TACACS_ERROR_MESSAGE: すべてのサーバーが応答に失敗しました
(%TACACS-3-TACACS_ERROR_MESSAGE: All servers failed to respond) ]
```

この問題の既知されていて、回避策はありません。リモート認証が TACACS サーバ接続の問題なしに正しく機能する場合は、メッセージを無視して構成を続行できます。

TACACS+ の設定

TACACS+ サーバの設定プロセス

ここでは、TACACS+ サーバーを設定する方法について説明します。

Procedure

-
- ステップ 1** TACACS+ をイネーブルにします。
- ステップ 2** TACACS+ サーバーと Cisco Nexus デバイスとの接続を確立します。
- ステップ 3** TACACS+ サーバーの事前共有秘密キーを設定します。
- ステップ 4** 必要に応じて、AAA 認証方式用に、TACACS+ サーバーのサブセットを使用して TACACS+ サーバー グループを設定します。
- ステップ 5** 必要に応じて、次のオプションのパラメータを設定します。
- デッドタイム間隔
 - ログイン時に TACACS+ サーバーの指定を許可
 - タイムアウト間隔
 - TCP ポート
- ステップ 6** 必要に応じて、定期的に TACACS+ サーバーをモニタリングするよう設定します。
-

TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus デバイスで TACACS+ 機能はディセーブルに設定されています。TACACS+ 機能をイネーブルに設定すると、認証に関するコンフィギュレーションコマンドと検証コマンドを使用できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# feature tacacs+	TACACS+ をイネーブルにします。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) 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。

TACACS+ サーバホストの設定

リモートの TACACS+ サーバーにアクセスするには、Cisco Nexus デバイス上に、TACACS+ サーバーの IPv4 アドレスまたはホスト名を設定する必要があります。すべての TACACS+ サーバーホストは、デフォルトの TACACS+ サーバーグループに追加されます。最大 64 の TACACS+ サーバーを設定できます。

設定済みの TACACS+ サーバーに事前共有キーが設定されておらず、グローバルキーも設定されていない場合は、警告メッセージが表示されます。TACACS+ サーバーキーが設定されていない場合は、グローバルキー（設定されている場合）が該当サーバーで使用されます。

TACACS+ サーバーホストを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。
- リモートの TACACS+ サーバーの IPv4 アドレスまたはホスト名を取得します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> }	TACACS+ サーバーの IPv4 アドレスまたはホスト名を指定します。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) 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。

Example

サーバーグループから TACACS+ サーバーホストを削除できます。

TACACS+ のグローバルな事前共有キーの設定

Cisco Nexus デバイスで使用するすべてのサーバーについて、グローバルレベルで事前共有キーを設定できます。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバーホスト間の共有秘密テキストストリングです。

事前共有キーを設定する前に、次の点を確認してください。

- TACACS+ をイネーブルにします。
- リモートの TACACS+ サーバーの事前共有キー値を取得していること。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	tacacs-server key [0 6 7] key-value	すべての TACACS+ サーバ用の TACACS+ キーを指定します。 <i>key-value</i> がクリアテキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) かを指定できます。デフォルトの形式はクリアテキストです。最大で 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。 Note 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、 show running-config コマンドを使用します。
ステップ 5	(Optional) 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。

Example

次に、グローバルな事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUkO
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバーの事前共有キーの設定

TACACS+ サーバーの事前共有キーを設定できます。事前共有キーとは、Cisco Nexus デバイスと TACACS+ サーバー ホスト間の共有秘密テキストストリングです。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> } key [0 7] <i>key-value</i>	特定の TACACS+ サーバーの事前共有キーを指定します。クリア テキスト形式 (0) または暗号化形式 (7) 事前共有キーを指定できます。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。 Note 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、 show running-config コマンドを使用します。
ステップ 5	(Optional) 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。

Example

次に、TACACS+ 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバグループの設定

サーバグループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて、TACACS+ プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバグループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

Before you begin

TACACS+ を設定する前に、`feature tacacs+` コマンドを使用して、TACACS+ をイネーブルにする必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	<code>switch# configure terminal</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	<code>switch(config)# aaa group server tacacs+ group-name</code>	TACACS+ サーバグループを作成し、そのグループの TACACS+ サーバグループ コンフィギュレーション モードを開始します。
ステップ 3	<code>switch(config)# tacacs-server host {ipv4-address host-name} key [0 7] key-value</code>	特定の TACACS+ サーバの事前共有キーを指定します。クリアテキスト形式 (0) または暗号化形式 (7) 事前共有キーを指定できます。デフォルトの形式はクリアテキストです。最大で 63 文字です。 この事前共有キーがグローバル事前共有キーの代わりに使用されます。
ステップ 4	(Optional) <code>switch(config-tacacs)# deadtime minutes</code>	モニタリング デッドタイムを設定します。デフォルト値は 0 分です。指定できる範囲は 0 ~ 1440 です。 Note TACACS+ サーバグループのデッドタイム間隔が 0 より大きい場合は、その値がグローバルなデッドタイム値より優先されます。
ステップ 5	(Optional) <code>switch(config-tacacs)# source-interface interface</code>	特定の TACACS+ サーバグループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。

	Command or Action	Purpose
		Note source-interface コマンドを使用して、ip tacacs source-interface コマンドによって割り当てられたグローバル ソース インターフェイスをオーバーライドします。
ステップ 6	switch(config-tacacs+)# exit	コンフィギュレーション モードを終了します。
ステップ 7	(Optional) switch(config)# show tacacs-server groups	TACACS+ サーバグループの設定を表示します。
ステップ 8	(Optional) 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。

Example

次に、TACACS+ サーバグループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

TACACS+ サーバグループのためのグローバル発信元インターフェイスの設定

TACACS+ サーバグループにアクセスする際に使用する、TACACS+ サーバグループ用のグローバル発信元インターフェイスを設定できます。また、特定のTACACS+サーバグループ用に異なる発信元インターフェイスを設定することもできます。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal	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	ip tacacs source-interface interface Example:	このデバイスで設定されているすべてのTACACS+サーバグループ用のグローバル発信元インターフェイスを設定しま

	Command or Action	Purpose
	<code>switch(config)# ip tacacs source-interface mgmt 0</code>	す。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。
ステップ 3	exit Example: <code>switch(config)# exit switch#</code>	設定モードを終了します。
ステップ 4	(Optional) show tacacs-server Example: <code>switch# show tacacs-server</code>	TACACS+ サーバの設定情報を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <code>switch# 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。

ログイン時の TACACS+ サーバーの指定

認証要求の送信先 TACACS+ サーバーをユーザーが指定できるようにスイッチを設定するには、`directed-request` オプションをイネーブルにします。デフォルトでは、Cisco Nexus デバイスは、デフォルトの AAA 認証方式に基づいて認証要求を転送します。このオプションをイネーブルにすると、ユーザーは `username@hostname` としてログインできます。ここで、`hostname` は設定済みの RADIUS サーバーの名前です。



Note ユーザー指定のログインは、Telnet セッションでのみサポートされます。

Procedure

	Command or Action	Purpose
ステップ 1	<code>switch# configure terminal</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	<code>switch(config)# tacacs-server directed-request</code>	ログイン時にユーザーが認証要求の送信先となる TACACS+ サーバーを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	<code>switch(config)# exit</code>	設定モードを終了します。
ステップ 4	(Optional) <code>switch# show tacacs-server directed-request</code>	TACACS+ の <code>directed request</code> の設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) 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。

TACACS+ サーバでの AAA 許可の設定

TACACS+ サーバのデフォルトの AAA 許可方式を設定できます。

Before you begin

TACACS+ 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	aaa authorization ssh-certificate default { group group-list [none] local none} Example: switch(config)# aaa authorization ssh-certificate default group TACACSServer1 TACACSServer2	TACACS+ サーバのデフォルトの AAA 許可方式を設定します。 ssh-certificate キーワードは、証明書認証を使用した TACACS+ 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。 <i>group-list</i> 引数には、TACACS+ サーバグループの名前をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。 local 方式では、ローカル データベースを認証に使用します。 none 方式では、AAA 認証が使用されないように指定します。
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 aaa authorization [all] Example: switch# show aaa authorization	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。

	Command or Action	Purpose
ステップ 5	(Optional) copy running-config startup-config Example: <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。

TACACS+ サーバでのコマンド許可の設定

TACACS+ サーバでコマンド許可を設定できます。コマンド許可では、デフォルト ロールを含むユーザのロールベース許可コントロール (RBAC) がディセーブルになります。

Before you begin

TACACS+ を有効にします。

AAA コマンドの許可を設定する前に TACACS ホストおよびサーバー グループを設定してください。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	aaa authorization {commands config-commands} default [group group-list [local] local] Example: <pre>switch(config)# aaa authorization commands default group TacGroup</pre>	<p>すべてのロールに関するデフォルトのコマンド許可方式を設定します。</p> <p>commands キーワードを使用するとすべての EXEC コマンドの許可ソースを設定でき、config-commands キーワードを使用するとすべてのコンフィギュレーション コマンドの許可ソースを設定できます。すべてのコマンドのデフォルト許可は、ユーザーに割り当てたロールに関する許可されたコマンドのリストであるローカル許可です。</p> <p>group-list 引数には、TACACS+ サーバーグループの名前をスペースで区切ったリストを指定します。このグループに属するサーバーに対して、コマンドの許可のためのアクセスが行われます。local 方式では、許可にローカル ロールベースデータベースが使用されます。</p>

	Command or Action	Purpose
		<p>local 方式は、設定されたすべてのサーバグループから応答が得られなかった場合に、local をフォールバック方式として設定しているときにだけ使用されます。</p> <p>デフォルトの方式は local です。</p> <p>TACACS+サーバグループの方式のあとにフォールバック方式を設定していないと、すべてのサーバグループから応答が得られなかった場合は許可に失敗します。</p>
ステップ 3	exit Example: <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 4	(Optional) show aaa authorization [all] Example: <pre>switch(config)# show aaa authorization</pre>	AAA 許可設定を表示します。 all キーワードを指定すると、デフォルト値が表示されます。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# 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。

TACACS+ サーバでのコマンド許可のテスト

TACACS+ サーバで、ユーザに対するコマンド許可をテストできます。



Note 許可用の正しいコマンドを送信しないと、結果の信頼性が低くなります。

Before you begin

TACACS+ をイネーブルにします。

TACACS+ サーバにコマンド許可が設定されていることを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	test aaa authorization command-type {commands config-commands} user username command command-string Example: <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	<p>TACACS+サーバで、コマンドに対するユーザの許可をテストします。</p> <p>commands キーワードはEXEC コマンドだけを指定し、config-commands キーワードはコンフィギュレーション コマンドだけを指定します。</p> <p>Note <i>command-string</i> 引数にスペースが含まれる場合は、二重引用符 (") で囲みます。</p>

コマンド許可検証のイネーブル化とディセーブル化

デフォルトのユーザセッションまたは別のユーザ名に対して、コマンドライン インターフェイス (CLI) でコマンド許可検証をイネーブルにしたり、ディセーブルにしたりできます。



(注) 許可検証をイネーブルにした場合は、コマンドは実行されません。

手順

	コマンドまたはアクション	目的
ステップ 1	terminal verify-only [username username] 例 : <pre>switch# terminal verify-only</pre>	<p>コマンド許可検証をイネーブルにします。このコマンドを入力すると、入力したコマンドが許可されているかどうか Cisco NX-OS ソフトウェアによって示されます。</p>
ステップ 2	terminal no verify-only [username username] 例 : <pre>switch# terminal no verify-only</pre>	<p>コマンド許可検証をディセーブルにします。</p>

TACACS+ サーバでの許可に使用する特権レベルのサポートの設定

TACACS+ サーバでの許可に使用する特権レベルのサポートを設定できます。

許可の決定に特権レベルを使用する Cisco IOS デバイスとは異なり、Cisco NX-OS デバイスでは、ロールベースアクセスコントロール (RBAC) を使用します。両方のタイプのデバイスと同じ TACACS+ サーバで管理できるようにするには、TACACS+ サーバで設定した特権レベルを、Cisco NX-OS デバイスで設定したユーザー ロールにマッピングします。

TACACS+サーバでのユーザの認証時には、特権レベルが取得され、それを使用して「priv-*n*」という形式（*n*が特権レベル）のローカルユーザロール名が生成されます。このローカルロールの権限がユーザに割り当てられます。特権レベルは16あり、対応するユーザロールに直接マッピングされます。次の表に、各特権レベルに対応するユーザロール権限を示します。

特権レベル	ユーザロール権限
15	network-admin 権限
13 ~ 1	<ul style="list-style-type: none"> • スタンドアロン ロール権限 (feature privilege コマンドがディセーブルの場合) • ロールの累積権限からなる特権レベル 0 と同じ権限 (feature privilege コマンドが有効の場合)
0	show コマンドや exec コマンド (ping 、 trace 、 ssh など) を実行するための権限

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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] feature privilege Example: <pre>switch(config)# feature privilege</pre>	ロールの累積権限を有効または無効にします。 enable コマンドは、この機能を有効にした場合しか表示されません。デフォルトは無効です。
ステップ 3	[no] enable secret [0 5] password [priv-lvl priv-lvl all] Example: <pre>switch(config)# enable secret 5 def456 priv-lvl 15</pre>	<p>特定の特権レベルのシークレットパスワードを有効または無効にします。特権レベルが上がるたびに、正しいパスワードを入力するようにユーザに要求します。デフォルトは無効です。</p> <p>パスワードの形式としてクリアテキストを指定する場合は0を入力し、暗号化された形式を指定する場合は5を入力します。 <i>password</i> 引数に指定できる文字数は、最大 64 文字です。 <i>priv-lvl</i> 引数は、1 ~ 15 です。</p>

	Command or Action	Purpose
		Note シークレットパスワードを有効にするには、 feature privilege コマンドを入力してロールの累積権限を有効にする必要があります。
ステップ 4	[no] username username priv-lvl n Example: switch(config)# username user2 priv-lvl 15	ユーザの許可に対する特権レベルの使用を有効または無効にします。デフォルトは無効です。 priv-lvl キーワードはユーザに割り当てる特権レベルを指定します。デフォルトの特権レベルはありません。特権レベル 0 ~ 15 (priv-lvl 0 ~ priv-lvl 15) は、ユーザ ロール priv-0 ~ priv-15 にマッピングされます。
ステップ 5	(Optional) show privilege Example: switch(config)# show privilege	ユーザ名、現在の特権レベル、および累積権限のサポートのステータスを表示します。
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。
ステップ 7	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 8	enable level Example: switch# enable 15	上位の特権レベルへのユーザの昇格を有効にします。このコマンドの実行時にはシークレットパスワードが要求されます。 level 引数はユーザのアクセスを許可する特権レベルを指定します。指定できるレベルは 15 だけです。

権限ロールのユーザ コマンドの許可または拒否

ネットワーク管理者は、権限ロールを変更して、ユーザが特定のコマンドを実行できるようにしたり実行できなくしたりすることができます。

権限ロールのルールを変更する場合は、次の注意事項に従う必要があります。

- **priv-14** ロールと **priv-15** ロールは変更できません。

- 拒否ルールは `priv-0` ロールにだけ追加できます。
- `priv-0` ロールでは以下のコマンドは常に許可されます。 `configure`、`copy`、`dir`、`enable`、`ping`、`show`、`ssh`、`telnet`、`terminal`、`traceroute`、`end`、`exit`。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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] role name priv-n Example: <pre>switch(config)# role name priv-5 switch(config-role)#</pre>	権限ロールをイネーブルまたはディセーブルにして、ロール コンフィギュレーション モードを開始します。 <i>n</i> 引数には、特権レベルを 0 ~ 13 の数値で指定します。
ステップ 3	rule number {deny permit} command command-string Example: <pre>switch(config-role)# rule 2 permit command pwd</pre>	<p>権限ロールのユーザ コマンド ルールを設定します。これらのルールで、ユーザによる特定のコマンドの実行を許可または拒否します。ルールごとに最大 256 のルールを設定できます。ルール番号によって、ルールが適用される順序が決まります。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。</p> <p><i>command-string</i> 引数には、空白スペースを含めることができます。</p> <p>Note 256個の規則に対してこのコマンドを繰り返します。</p>
ステップ 4	exit Example: <pre>switch(config-role)# exit switch(config)#</pre>	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 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# 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。

グローバルな TACACS+ タイムアウト間隔の設定

Cisco Nexus デバイスが、タイムアウトエラーを宣言する前に、すべての TACACS+ サーバーからの応答を待機するグローバルなタイムアウト間隔も設定できます。タイムアウト間隔には、スイッチが TACACS+ サーバーからの応答を待つ時間を指定します。これを過ぎるとタイムアウトエラーになります。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# tacacs-server timeout <i>seconds</i>	TACACS+ サーバーのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ~ 60 秒です。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) 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。

サーバーのタイムアウト間隔の設定

Cisco Nexus デバイスが、タイムアウトエラーを宣言する前に、TACACS+ サーバーからの応答を待機するタイムアウト間隔を設定できます。タイムアウト間隔は、スイッチがタイムアウトエラーを宣言する前に、TACACS+ サーバーからの応答を待機する時間を決定します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# switch(config)# tacacs-server host { <i>ipv4-address</i> <i>host-name</i> } timeout <i>seconds</i>	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 Note 特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。

	Command or Action	Purpose
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) 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。

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバー用に別の TCP ポートを設定できます。デフォルトでは、Cisco Nexus デバイスは、すべての TACACS+ 要求にポート 49 を使用します。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# tacacs-server host <i>{ipv4-address host-name}</i> port tcp-port	TACACS+ アカウンティングメッセージ用の UDP ポートを指定します。デフォルトの TCP ポートは 49 です。有効な範囲は 1 ~ 65535 です。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。
ステップ 5	(Optional) 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。

Example

次に、TCP ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバーの定期的モニタリングの設定

TACACS+ サーバーの可用性をモニタリングできます。パラメータとして、サーバーに使用するユーザー名とパスワード、およびアイドルタイマーがあります。アイドルタイマーには、TACACS+サーバーがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus デバイスがテストパケットを送信するかを指定します。このオプションを設定して、サーバーを定期的にテストしたり、1 回だけテストを実行できます。



Note ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザー名と同じユーザー名を使用しないことを推奨します。

テストアイドルタイマーには、TACACS+サーバーがどのくらいの期間要求を受信しなかった場合に、Cisco Nexus デバイスがテストパケットを送信するかを指定します。



Note デフォルトのアイドルタイマー値は 0 分です。アイドルタイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# tacacs-server host {ipv4-address host-name} test { idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]}	サーバー モニタリング用のパラメータを指定します。デフォルトのユーザー名は test、デフォルトのパスワードは test です。アイドルタイマーのデフォルト値は 0 分です。有効な範囲は 0 ~ 1440 分です。 Note TACACS+ サーバーの定期的なモニタリングを行うには、アイドルタイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# tacacs-server dead-time minutes	Cisco Nexus デバイスが、前回応答しなかった TACACS+サーバーをチェックするまでの時間 (分) を指定します。デフォルト値は 0 分、指定できる範囲は 0 ~ 1440 分です。
ステップ 4	switch(config)# exit	設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。
ステップ 6	(Optional) 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。

Example

次に、TACACS+ サーバーの定期的モニタリングを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

デッドタイム間隔の設定

すべての TACACS+ サーバーのデッドタイム間隔を設定できます。デッドタイム間隔には、Cisco Nexus デバイスが TACACS+ サーバーをデッド状態であると宣言した後、そのサーバーがアライブ状態に戻ったかどうかを判断するためにテストパケットを送信するまでの間隔を指定します。



Note デッドタイム間隔が0分の場合、TACACS+サーバーは、応答を返さない場合でも、デッドとしてマークされません。デッドタイム間隔はグループ単位で設定できます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# tacacs-server deadtime minutes	グローバルなデッドタイム間隔を設定します。デフォルト値は0分です。有効な範囲は1～1440分です。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) switch# show tacacs-server	TACACS+ サーバーの設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) 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。

TACACS+ サーバまたはサーバグループの手動モニタリング

Procedure

	Command or Action	Purpose
ステップ 1	switch# test aaa server tacacs+ { <i>ipv4-address</i> <i>host-name</i> } [vrf <i>vrf-name</i>] <i>username password</i>	TACACS+ サーバーにテストメッセージを送信して可用性を確認します。
ステップ 2	switch# test aaa group <i>group-name</i> <i>username password</i>	TACACS+ サーバー グループにテストメッセージを送信して可用性を確認します。

Example

次に、手動でテストメッセージを送信する例を示します。

```
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。



Caution TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

Procedure

	Command or Action	Purpose
ステップ 1	switch# configure terminal	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	switch(config)# no feature tacacs+	TACACS+ をディセーブルにします。
ステップ 3	switch(config)# exit	設定モードを終了します。
ステップ 4	(Optional) 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。

TACACS+ 統計情報の表示

スイッチが TACACS+ のアクティビティについて保持している統計情報を表示するには、次の作業を行います。

Procedure

	Command or Action	Purpose
ステップ 1	switch# show tacacs-server statistics {hostname ipv4-address}	TACACS+ 統計情報を表示します。

Example

このコマンドの出力フィールドの詳細については、Nexus スwitch の『*Command Reference*』を参照してください。

TACACS+ の設定の確認

TACACS+ の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。

Procedure

	Command or Action	Purpose
ステップ 1	switch# show tacacs+ {status pending pending-diff}	Cisco Fabric Services の TACACS+ 設定の配布状況と他の詳細事項を表示します。
ステップ 2	switch# show running-config tacacs [all]	実行コンフィギュレーションの TACACS+ 設定を表示します。
ステップ 3	switch# show startup-config tacacs	スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
ステップ 4	switch# show tacacs-serve [host-name ipv4-address] [directed-request groups sorted statistics]	設定済みのすべての TACACS+ サーバーのパラメータを表示します。

TACACS+ の設定例

次に、TACACS+ を設定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ToIkLhPpG"
switch(config)# tacacs-server host 10.10.2.2 key 7 "ShMoMhT1"
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```



```
switch(config-tacacs+)# use-vrf management
```

次に、TACACS+をイネーブルにし、TACACS+サーバーの事前共有キーを設定して、サーバーグループ TacServer1 を認証するためにリモート AAA サーバーを指定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ikvhw10"
switch(config)# tacacs-server host 1.1.1.1
switch(config)# tacacs-server host 1.1.1.2

switch(config)# aaa group server tacacs+ TacServer1
switch(config-tacacs+)# server 1.1.1.1
switch(config-tacacs+)# server 1.1.1.2
```

TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定を示します。

Table 1: TACACS+ のデフォルトパラメータ

パラメータ	デフォルト
TACACS+	ディセーブル
デッドタイム間隔	0 分
タイムアウト間隔	5 秒
アイドルタイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	テスト

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。