# 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+ デーモンのデータベースで管理されます。Cisco Nexus デバイスに構成した TACACS+ 機能を使用できるようにするには、TACACS+ サーバーにアクセスして構成しておく必要があります。

TACACS+ では、認証、許可、アカウンティング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+ デーモン）で、各サービス（認証、許可、アカウンティング）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、デー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。

Cisco NX-OS リリース 10.4(3)F 以降、TACACS+ サーバーを使用した X.509 証明書の SSH ベースの認証は、Cisco Nexus 3600 シリーズ プラットフォーム スイッチで **aaa authorization ssh-certificate default group** コマンドを使用して実行できます。し設定の詳細については、TACACS サーバーを使用した X.509 証明書ベースの SSH 認証の設定, on page 16を参照してください。

# 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

ユーザが TACACS+ を使用して、パスワード認証プロトコル（PAP）によるログインを Cisco Nexus デバイスに対して試行すると、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、デーモンとユーザとの自由な対話を許可します。この動作では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許可を必要とする場合は、許可処理が始まります。
   - 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：デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco Nexus デバイスの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、スイッチは代わりのユーザー認証方式の使用を試します。

   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
- 接続パラメータ（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 タイムアウトなどを含みます）

# 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文字列です。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）。使用する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。

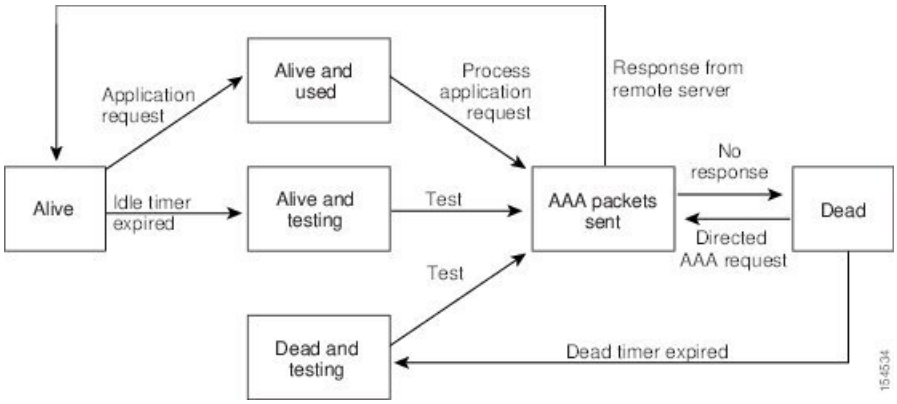
グローバルな事前共有キーの設定は、個々の TACACS+ サーバーの設定時に **key** オプションを使用することによって無効にできます。

# 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、それらが応答を返したら、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 または IPv6 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構成されていること。

# 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+ 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。

### SUMMARY STEPS

1. TACACS+ をイネーブルにします。
2. TACACS+ サーバーと Cisco Nexus デバイスとの接続を確立します。
3. TACACS+ サーバーの事前共有秘密キーを設定します。
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。
5. 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。

### DETAILED STEPS

#### Procedure

**ステップ 1** TACACS+ をイネーブルにします。

「TACACS+ のイネーブル化 , on page 5」を参照してください。

**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。

TACACS+ サーバ ホストの設定, on page 6

**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。

TACACS+ のグローバルな事前共有キーの設定, on page 7

**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。

TACACS+ サーバ グループの設定, on page 9

**ステップ 5** 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+ サーバーの定期的モニタリングの設定, on page 13

## TACACS+ のイネーブル化

デフォルトでは、Cisco Nexus デバイスで TACACS+ 機能は無効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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **feature tacacs+**
3. switch(config)# **exit**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

### 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** | コンフィグレーション モードを終了します。 |
| ステップ 4 | (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。 |

## TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバにアクセスするには、Cisco Nexus デバイス上でその TACACS+ サーバの IPv4 または IPv6 アドレスかホスト名を構成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。

（詳細については、「TACACS+ グローバル事前共有キーの構成」および「TACACS+ サーバー事前共有キーの構成」の項を参照してください）。

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。詳細については、「TACACS+ のイネーブル化 , on page 5」を参照してください。
- リモート TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}
4. switch(config)# **exit**
5. (Optional) switch# **show tacacs-server**
6. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

**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* \| *ipv6-address* \| *host-name*} | TACACS+ サーバの IPv4 または IPv6 アドレスまたはホスト名を指定します。 |
| ステップ 3 | switch(config)# **tacacs-server host** {*ipv4-address* \| *host-name*} | 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 4 | switch(config)# **exit** | コンフィグレーション モードを終了します。 |
| 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**

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構成できます。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文字列です。

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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. **tacacs-server key** [**0** | **6** | **7**] *key-value*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

## DETAILED STEPS

### 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*<br>**Example:**<br>`switch(config)# tacacs-server key 0 QsEfThUkO`<br>**Example:**<br>`switch(config)# tacacs-server key 7 "fewhg"` | すべての TACACS+ サーバ用の TACACS+ キーを指定します。*key-value* 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。Cisco NX-OS ソフトウェアでは、実行構成に保存する前にクリア テキストのキーを暗号化します。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。<br>デフォルトでは、秘密キーは設定されていません。<br>**Note**<br>**generate type7_encrypted_secret** を使用してすでに共有秘密を設定している場合コマンドを使用して、二番目の例に示すように引用符に入力します。 |
| ステップ 3 | switch(config)# **exit** | コンフィグレーション 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。<br>**Note**<br>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 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **aaa group server tacacs+** *group-name*
3. (Optional) switch(config-tacacs+)# **deadtime** *minutes*
4. (Optional) switch(config-tacacs+)# **source-interface** *interface*
5. switch(config-tacacs+)# **exit**
6. (Optional) switch(config)# **show tacacs-server groups**
7. (Optional) switch(config)# **copy running-config startup-config**

### DETAILED STEPS

### 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)# **aaa group server tacacs+** *group-name* | TACACS+ サーバー グループを作成し、そのグループのTACACS+ サーバー 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 | (Optional) switch(config-tacacs+)# **deadtime** *minutes* | 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。<br>**Note**<br>TACACS+ サーバー 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 4 | (Optional) switch(config-tacacs+)# **source-interface** *interface* | 特定の TACACS+ サーバー グループに発信元インターフェイスを割り当てます。 |

| | Command or Action | Purpose |
|---|---|---|
| | | 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。<br>**Note**<br>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 5 | switch(config-tacacs+)# **exit** | コンフィグレーション モードを終了します。 |
| ステップ 6 | (Optional) switch(config)# **show tacacs-server groups** | TACACS+ サーバー グループの設定を表示します。 |
| ステップ 7 | (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+ サーバー 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。

### SUMMARY STEPS

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. (Optional) **show tacacs-server**
5. (Optional) **copy running-config startup config**

**DETAILED STEPS**

**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*<br>**Example:**<br>`switch(config)# ip tacacs source-interface mgmt 0` | このデバイスで設定されているすべての TACACS+ サーバー 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**<br>**Example:**<br>`switch(config)# exit`<br>`switch#` | 設定モードを終了します。 |
| ステップ 4 | (Optional) **show tacacs-server**<br>**Example:**<br>`switch# show tacacs-server` | 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**<br>**Example:**<br>`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。 |

## グローバルな TACACS+ タイムアウト間隔の設定

Cisco Nexus デバイスの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 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時間です。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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **tacacs-server timeout** *seconds*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

**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** *seconds* | 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** | コンフィグレーション 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。 |

## 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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **exit**
3. (Optional) switch# **show tacacs-server**
4. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

**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)# **exit** | コンフィグレーション モードを終了します。 |
| ステップ 3 | (Optional) switch# **show tacacs-server** | TACACS+ サーバーの設定を表示します。 |
| ステップ 4 | (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。 |

## 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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **exit**
3. (Optional) switch# **show tacacs-server**
4. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### 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)# **exit** | コンフィグレーション モードを終了します。 |
| ステップ 3 | (Optional) switch# **show tacacs-server** | TACACS+ サーバーの設定を表示します。 |
| ステップ 4 | (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したりすることができます。

**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名と同じユーザ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。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server dead-time** *minutes*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### 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 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 3 | switch(config)# **exit** | コンフィグレーション 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、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+ サーバをデッド状態であると宣言した後、そのサーバ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、デット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。「TACACS+ サーバ グループの設定, on page 9」を参照してください。

### SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **tacacs-server deadtime** *minutes*
3. switch(config)# **exit**
4. (Optional) switch# **show tacacs-server**
5. (Optional) switch# **copy running-config startup-config**

### DETAILED STEPS

#### 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** | コンフィグレーション 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。 |

# TACACS サーバーを使用した X.509 証明書ベースの SSH 認証の設定

Cisco NX-OS リリース 10.4(3)F 以降では、Cisco Nexus スイッチの TACAC+ サーバーを使用して、x509v3 証明書の SSH ベースの認証を設定できます。

TACAC+ サーバーを使用して X.509 証明書ベースの SSH 認証を設定するには、次の手順に従います。

## 手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default group** *tacacs-group-name*
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

## 手順の詳細

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **configure terminal**<br>例：<br>`switch# configure terminal`<br>`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** *tacacs-group-name*<br>例：<br>`switch(config)# aaa authorization ssh-certificate default group tac` | TACAC+ サーバーのデフォルトの AAA 許可方式を設定します。<br>**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構成します。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。<br>（注）<br>• **aaa group server tacacs+** *tacacs-group-name* コマンドを使用して、TACACS サーバー構成で *tacacs-group-name* が構成されていることを確認します。<br>• SSH 証明書ベースの認証をサポートするには、暗号トラストポイントを設定し、ルート CA をインストールします。詳細については、PKI の設定のセクションを参照してください。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **exit**<br>例：<br>`switch(config)# exit`<br>`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 | （任意） **show aaa authorization** [**all**]<br>例：<br>`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。 |
| ステップ 5 | （任意） **copy running-config startup-config**<br>例：<br>`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。 |

## TACACS+ サーバまたはサーバ グループの手動モニタリング

### SUMMARY STEPS

1. switch# **test aaa server tacacs+** {*ipv4-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. switch# **test aaa group** *group-name username password*

### DETAILED STEPS

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| ステップ 1 | switch# **test aaa server tacacs+** {*ipv4-address* \| *host-name*} [**vrf** *vrf-name*] *username password* | 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** *group-name username password* | 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。

**SUMMARY STEPS**

1. switch# **configure terminal**
2. switch(config)# **no feature tacacs+**
3. switch(config)# **exit**
4. (Optional) switch# **copy running-config startup-config**

**DETAILED STEPS**

**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** | コンフィグレーション モードを終了します。 |
| ステップ 4 | (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。 |

# 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。

**SUMMARY STEPS**

1. switch# **show tacacs-server statistics** [*hostname* | *ipv4-address* | *ipv6-address*]

**DETAILED STEPS**

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| ステップ 1 | switch# **show tacacs-server statistics** [*hostname* \| *ipv4-address* \| *ipv6-address*] | TACACS+ 統計情報を表示します。<br>**Note** *ipv6-address* パラメータは Nexus 3548 ではサポートされていません。 |

**Example**

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

# TACACS+ の設定の確認

TACACS+ の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 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。 |
| **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。 |
| **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。 |
| **show tacacs-serve** [*host-name* \| *ipv4-address* \| *ipv6-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 "ShMoMhTl"
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。