TACACS+ の設定

この章の内容は、次のとおりです。

TACACS+ について

TACACS+ は、デバイスにアクセスしようとするユーザの検証を集中的に行うセキュリティ プロトコルです。 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動作する TACACS+ デーモンのデータベースで管理されます。 デバイスに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ は、独立した認証、許可、アカウンティング サービスを提供します。 TACACS+ デーモンは各サービスを個別に提供します。 各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ クライアント/サーバ 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。 TACACS+ プロトコルを使用して集中型の認証が提供されます。

ユーザ ログインにおける TACACS+ の動作

パスワード認証プロトコル（PAP）を使用して TACACS+ サーバへのログインを試みると、次の一連のイベントが発生します。

1 接続が確立すると、ユーザ名とパスワードを取得するために TACACS+ デーモンが接続されます。

（注） 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。 通常、デーモンはユーザ名とパスワードを入力するよう求めますが、ユーザの母親の旧姓などの追加情報を求めることもできます。

2 TACACS+ デーモンは、次のいずれかの応答を提供します。

   a ACCEPT：ユーザの認証に成功したので、サービスを開始します。 ユーザ許可が必要な場合は、許可が始まります。

   b REJECT：ユーザの認証に失敗しました。 TACACS+ デーモンは、ユーザ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。

   c ERROR：デーモンによる認証の途中でエラーが発生したか、またはネットワーク接続でエラーが発生しました。 ERROR 応答を受信した場合、デバイスは別の方法でユーザの認証を試行します。

   認証後、さらに許可が必要な場合は、続いてユーザの許可フェーズに入ります。 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+ 許可が必要な場合は、TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の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、アクセス リスト、およびユーザ タイムアウトを含む）

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

TACACS+ サーバに認証するには、TACACS+ 事前共有キーを設定する必要があります。 事前共有キーは、デバイスと TACACS+ サーバ ホストの間で共有される秘密テキスト 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

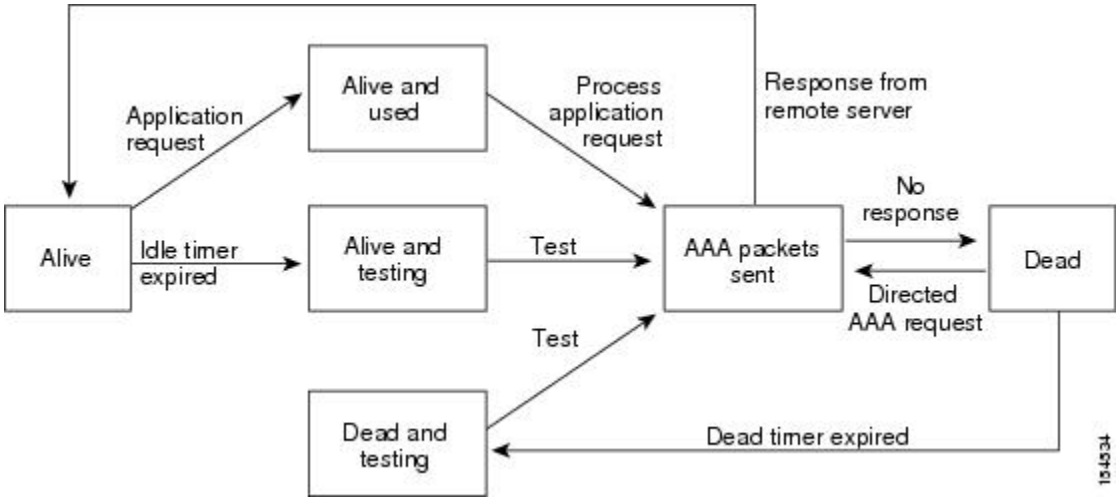
できません）。 すべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

このグローバル事前共有キーの割り当ては、個別の TACACS+ サーバの設定時に明示的に key オプションを使用することによって上書きできます。

TACACS+ サーバのモニタリング

応答しない TACACS+ サーバはデッド（dead）としてマークされ、AAA 要求が送信されません。デッド TACACS+ サーバは定期的にモニタされ、応答があればアライブに戻されます。 このプロセスにより、TACACS+ サーバが稼働状態であることを確認してから、実際の AAA 要求が送信されます。 次の図に、TACACS+ サーバの状態変化によって、どのように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、パフォーマンスに影響が出る前に障害を示すエラーメッセージが生成されるかを示します。

図 *1*：*TACACS+* サーバの状態



（注） 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。

ベンダー固有属性

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと TACACS+ サーバの間でベンダー固有属性（VSA）を伝達する方法が規定されています。 IETF は、属性 26 を使用します。 VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。

シスコの VSA 形式

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用したベンダー固有のオプションを 1 つサポートしています。 シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1（名前付き cisco-av-pair）です。 値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

認証に TACACS+ サーバを使用した場合、TACACS+ プロトコルでは TACACS+ サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。 この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションがサポートされています。

- shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。
- Accounting：accounting-request パケットで使用されるプロトコル。 値にスペースが含まれている場合は、二重引用符で囲む必要があります。

次の属性もサポートされています。

- roles：ユーザが属するすべてのロールの一覧です。 値は、ロール名をスペースで区切ったストリングです。 このサブ属性は Access-Accept フレームの VSA 部分に格納され、TACACS+ サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。
- accountinginfo：標準の TACACS+ アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。 この属性は、スイッチ上の TACACS+ クライアントから、Account-Request フレームの VSA 部分にだけ格納されて送信されます。 この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット（PDU）だけです。

TACACS+ の前提条件

- TACACS+ サーバの IP アドレスまたはホスト名を取得すること。
- TACACS+ サーバから事前共有キーを取得していること。
- Cisco Nexus 1000V が AAA サーバの TACACS+ クライアントとして設定されていること。
- すでに、リモート TACACS+ 認証を含む AAA が設定されていること。

TACACS+ の注意事項と制約事項

- 最大 64 の TACACS+ サーバを設定できます。
- TACACS+ のログレベルは 5 に設定する必要があります。

TACACS+ のデフォルト設定

パラメータ	デフォルト
TACACS+	Disabled
デッド タイマー間隔	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	test

TACACS+ の設定

次のフロー チャートで、TACACS+ を設定する手順を示します。

（注） Cisco Nexus 1000V のコマンドは Cisco IOS のコマンドと異なる場合があることに注意してください。

図 *2* : ***TACACS+*** 設定のフロー チャート

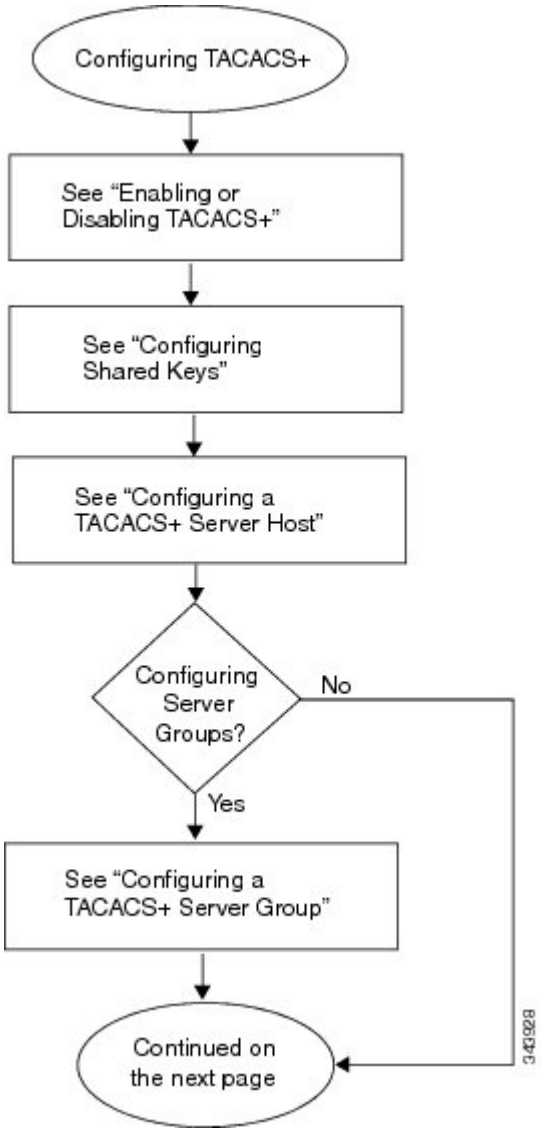


図 *3* : ***TACACS+*** 設定のフロー チャート（続き）

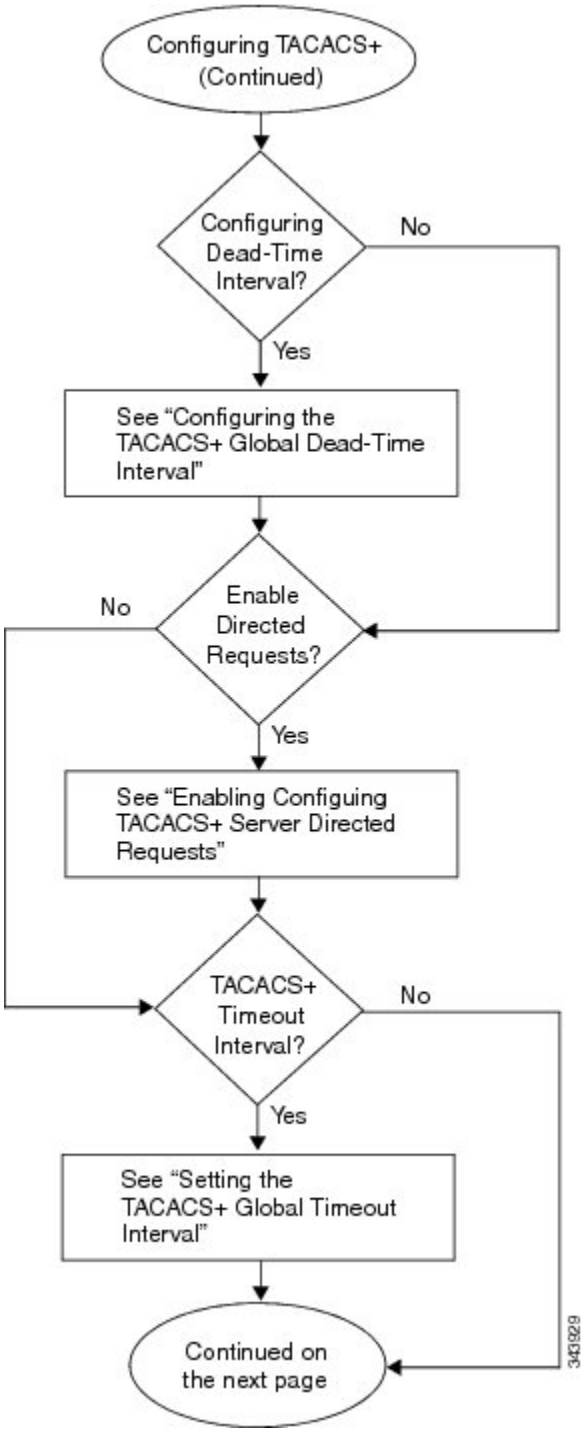
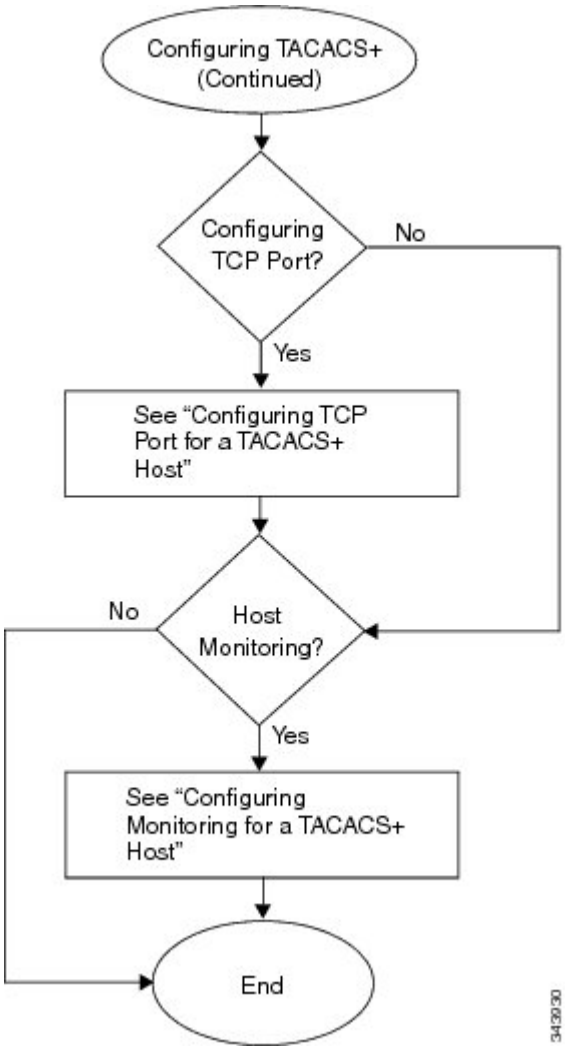


図 *4* : ***TACACS+*** 設定のフロー チャート（続き）



TACACS+ のイネーブル化またはディセーブル化

デフォルトでは、TACACS+ がディセーブルです。 TACACS+ 認証をサポート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するには、TACACS+ 機能を明示的にイネーブルにする必要があります。

注意 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。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
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**] **tacacs+ enable**	TACACS+ をイネーブルまたはディセーブルにします。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	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。

```
switch# configure terminal
switch(config)# tacacs+ enable
switch(config)# exit
switch# copy running-config startup-config
```

共有キーの設定

デフォルトでは、グローバル キーは設定されません。

次のものを設定するには、次の手順を実行します。

- グローバル キー（Cisco Nexus 1000V とすべての TACACS+ サーバ ホストの間で共有される秘密テキスト ストリング）
- キー（Cisco Nexus 1000V と単一の TACACS+ サーバ ホストの間で共有される秘密テキスト ストリング）

はじめる前に

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバ ホストのキーがわかっていること。

手順

	コマンドまたはアクション	目的
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。 次のいずれかを実行します。

	コマンドまたはアクション	目的
		• すべての TACACS+ サーバ ホストのグローバル キーを設定する場合は、次のステップに進みます。 • 単一の TACACS+ サーバ ホストのキーを設定する場合は、ステップ 3 に進みます。
ステップ 2	switch(config)# **tacacs-server key** [**0** | **7**] *global_key*	Cisco Nexus 1000V と TACACS+ サーバ ホストの間で共有されるグローバル キーを指定します。 • 0：使用するクリアテキスト ストリング（キー）を指定します。これがデフォルトです。 • 7：使用する暗号化された文字列（キー）を指定します。 • *global_key*：最大 63 文字のストリングです。 デフォルトでは、グローバル キーは設定されません。 ステップ 4 に進みます。
ステップ 3	switch(config)# **tacacs-server host** { *ipv4-address* | *host-name*} **key** [**0** | **7**] *shared_key*	Cisco Nexus 1000V とこの特定の TACACS+ サーバ ホストの間で共有されるキーを指定します。 0：使用するクリアテキスト ストリング（キー）を指定します。これがデフォルトです。 7：使用する暗号化された文字列（キー）を指定します。 *global key*：最大 63 文字の文字列です。 グローバル共有キーではなく、この共有キーが使用されます。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。 （注） グローバル共有キーは実行コンフィギュレーションに暗号化形式で保存されます。 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 6	switch(config)# **copy running-config startup-config**	（任意） 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。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEFtkI#
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
switch# copy running-config startup-config
```

TACACS+ サーバ ホストの設定

すべての TACACS+ サーバ ホストはデフォルトの TACACS+ サーバ グループに追加されます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- 共有キーが設定されていること。
- リモート TACACS+ サーバ ホストの IP アドレスまたはホスト名がわかっていること。

手順

	コマンドまたはアクション	目的
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*}	サーバの IP アドレスまたはホスト名を TACACS+ サーバ ホストとして設定します。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(confgi)# **copy running-config startup-config**	（任意） 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。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.2
switch(config)# exit
switch# show tacacs-server
timeout value:5
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
switch# copy running-config startup-config
```

TACACS+ サーバ グループの設定

メンバー サーバが認証機能を共有する TACACS+ サーバ グループを設定するには、次の手順を実行します。

TACACS+ サーバ グループが設定されると、メンバーのサーバへのアクセスは、サーバを設定した順番で行われます。

TACACS+ サーバ グループでは、1 台のサーバが応答できない場合に備えて、フェールオーバーを提供できます。 グループ内の最初のサーバが応答しない場合は、同じグループ内の次のサーバが試行され、サーバが応答するまでこの処理が行われます。複数のサーバ グループがある場合、同じ方法で、相互にフェールオーバーを提供できます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- EXEC モードで CLI にログインしていること。
- TACACS+ サーバ グループに追加されたすべてのサーバが、TACACS+ プロトコルを使用していること。
- すでに事前共有キーが設定されていること。
- 認証用に TACACS+ がイネーブルになっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminalt**	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*	指定した名前で TACACS+ サーバ グループを作成し、そのグループの TACACS+ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-tacacs+)# **server** { *ipv4-address* | *host-name*}	TACACS+ サーバのホスト名または IP アドレスを TACACS+ サーバ グループのメンバーとして設定します。 指定した TACACS+ サーバが見つからない場合は、tacacs-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。 （注） 指定した TACACS+ サーバが見つからない場合は、tacacs-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	switch(config-tacacs+)# **deadtime** *minutes*	（任意） この TACACS+ グループのモニタリングのデッド 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。 （注） 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	switch(config-tacacs+)# **use-vrf** *vrf-name*	（任意） このサーバ グループとの接続に使用する仮想ルーティングおよび転送（VRF）インスタンスを指定します。
ステップ 6	switch(config-tacacs+)# **source-interface** {*interface-type*} {*interface-number*}	（任意） TACACS+ サーバに到達するために使用される送信元インターフェイスを指定します。 • loopback = 0 ～ 1023 の仮想インターフェイス番号 • mgmt = 管理インターフェイス 0 • null = ヌル インターフェイス 0 • port-channel = 1 ～ 4096 のポート チャネル番号
ステップ 7	switch(config-tacacs+)# **show tacacs-server groups**	（任意） TACACS+ サーバ グループの設定を表示します。
ステップ 8	switch(config-tacacs+)# **copy running-config startup-config**	（任意） 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。

```
switch# config terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

```
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# use-vrf management
switch(config-tacacs+)# source-interface mgmt0
switch(config-tacacs+)# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 30
                vrf is management
switch# copy running-config startup-config
```

TACACS+ サーバの誘導要求のイネーブル化

この手順では、認証要求の送信先となる TACACS+ サーバを指定することができます。 これは directed-request（誘導要求）と呼ばれます。

誘導要求をイネーブルにした場合、ユーザは username@vrfname:hostname としてログインできます（*vrfname* は使用する VRF、hostname は設定された TACACS+ サーバの名前）。

（注） ユーザ指定のログインは Telnet セッションに限りサポートされます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。

手順

	コマンドまたはアクション	目的
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 directed-request**	ログイン時に認証要求を送信する TACACS+ サーバを指定するために、誘導要求の使用をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server directed-request**	（任意） TACACS+ の directed request の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	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。

```
switch# config terminal
switch(config)# tacacs-server directed-request
switch(config)# exit
switch# show tacacs-server directed-request
enabled
switch# copy running-config startup-config
```

TACACS+ のグローバル タイムアウト間隔の設定

Cisco Nexus 1000V が任意の TACACS+ サーバからの応答を待つ時間を秒単位で設定するには、次の手順を実行します。これを過ぎるとタイムアウトが宣言されます。

個別の TACACS+ サーバに指定したタイムアウトは、グローバル タイムアウト間隔に優先します。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。

手順

	コマンドまたはアクション	目的
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*	Cisco Nexus 1000V がサーバからの応答を待つ時間を秒単位で指定します。 デフォルトのタイムアウト間隔は 5 秒です。 有効な範囲は 1 ～ 60 秒です。
ステップ 3	switch(confi)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch(confi)# **copy running-config startup-config**	（任意） 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。

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

switch# n1000v# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
switch# copy running-config startup-config
```

個別 TACACS+ ホストのタイムアウト間隔の設定

Cisco Nexus 1000V が特定の TACACS+ サーバからの応答を待つ時間を秒単位で設定するには、次の手順を実行します。これを過ぎるとタイムアウトが宣言されます。 この設定は TACACS+ ホスト単位で設定します。

個別の TACACS+ サーバのタイムアウト設定は、グローバル タイムアウト間隔に優先します。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
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*} **timeout** *seconds*	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 タイムアウト間隔です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 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。

```
switch# config terminal
switch(config)#  tacacs-server host 10.10.2.2 timeout 10
switch(config)# exit
switch# n1000v# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
                timeout:10
switch# copy running-config startup-config
```

TACACS+ ホストの TCP ポートの設定

ポート 49（TACACS+ 要求のデフォルト）以外の TCP ポートを設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
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。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*	使用する TCP ポートを指定します。 指定できるポート範囲：1 ～ 65535 デフォルトは 49 です。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 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。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.2 port 2
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:2
                timeout:10
switch# copy running-config startup-config
```

TACACS+ ホストのモニタリングの設定

次の情報を知っている必要があります。

- アイドル タイマーには、TACACS+ サーバがアイドル（要求を受信しない）状態を続ける時間を指定します。これを過ぎると TACACS+ サーバにテスト パケットが送信されます。
- デフォルトのアイドル タイマー値は 0 分です。 アイドル時間の間隔が 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。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
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 モニタリングを設定します。 次のキーワードと引数があります。 • **username**：デフォルトは test です。 （注） ネットワークのセキュリティを保護するために、TACACS+ データベースに存在しないユーザ名を割り当てることを推奨します。 • **password**：デフォルトは test です。 • **idle-time**：デフォルトは 0 分です。 有効な範囲は 0 ～ 1440 分です。 （注） TACACS+ サーバ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*	以前に応答しなかった TACACS+ サーバのチェックを始めるまでの時間を分単位で指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） 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。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.2 test username pvk2 password a3z9yjqz7 idle-time
 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:5
total number of servers:1
```

```
following TACACS+ servers are configured:
        10.10.2.2:
                available on port:2
                timeout:10
switch# copy running-config startup-config
```

TACACS+ グローバル デッド タイム間隔の設定

以前に応答しなかったサーバにテスト パケットを送信するまで待機する時間を設定するには、次の手順を実行します。

デッド タイム間隔が 0 分の場合、TACACS+ サーバは、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 タイムはグループ単位で設定できます。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
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**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 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。

```
switch# configure terminal
switch(config)#  tacacs-server deadtime 5
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:5
```

```
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:2
                timeout:10
switch# copy running-config startup-config
```

TACACS+ ホストの統計情報の表示

TACACS+ ホストの統計情報を表示するには、次のコマンドを使用します。

show tacacs-server statistics {*hostname* | *ipv4-address*}

TACACS+ の設定例

次に、TACACS+ 設定の例を示します。

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

TACACS+ 機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
TACACS+	4.0(4)SV1(1)	この機能が導入されました。