



CHAPTER 6

TACACS+ の設定

この章では、Terminal Access Controller Access Control System Plus (TACACS+) プロトコルを設定する手順について説明します。

ここでは、次の内容について説明します。

- 「TACACS+ の概要」 (P.6-1)
- 「TACACS+ の前提条件」 (P.6-4)
- 「注意事項および制約事項」 (P.6-4)
- 「デフォルト設定」 (P.6-4)
- 「TACACS+ の設定」 (P.6-5)
- 「TACACS+ ホストの統計情報の表示」 (P.6-23)
- 「TACACS+ 設定例」 (P.6-24)
- 「その他の関連資料」 (P.6-25)
- 「TACACS+ 機能の履歴」 (P.6-24)

TACACS+ の概要

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場合に使用できます。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動する 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、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稼動する 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、およびアカウントिंग 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。各サービスをそれぞれ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上で使用できる他のサービスを利用できます。

TACACS+ クライアント/サーバプロトコルは、TCP (TCP ポート 49) を使用して転送を行います。TACACS+ プロトコルを使用して集中型の認証が提供されます。

ここでは、次の内容について説明します。

- 「ユーザ ログインにおける TACACS+ の動作」 (P.6-2)
- 「デフォルトの TACACS+ サーバ暗号化タイプおよび事前共有鍵」 (P.6-2)

- 「TACACS+ サーバ モニタリング」 (P.6-3)
- 「ベンダー固有属性」 (P.6-3)

ユーザ ログインにおける TACACS+ の動作

Password Authentication Protocol (PAP; パスワード認証プロトコル) 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+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザの認証に必要な情報を取得できるようになります。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 : ユーザが認証され、サービスが始まります。ユーザ許可が必要な場合は、許可が始まります。
 - b. REJECT : ユーザは認証されませんでした。TACACS+ デーモンは、ユーザ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にユーザに求めます。
 - 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。TACACS+ 許可に進むには、まず TACACS+ 認証を正常に終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、そのユーザに対する EXEC または NETWORK セッションに使用されるアトリビュートが含まれ、ユーザがアクセスできるサービスが確定します。

サービスには次のものが含まれます。

- Telnet、rlogin、Point-to-Point Protocol (PPP; ポイントツーポイント プロトコル)、Serial Line Internet Protocol (SLIP; シリアル ライン インターネット プロトコル) または、EXEC サービス
- 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、ユーザタイムアウトなどの接続パラメータ

デフォルトの TACACS+ サーバ暗号化タイプおよび事前共有鍵

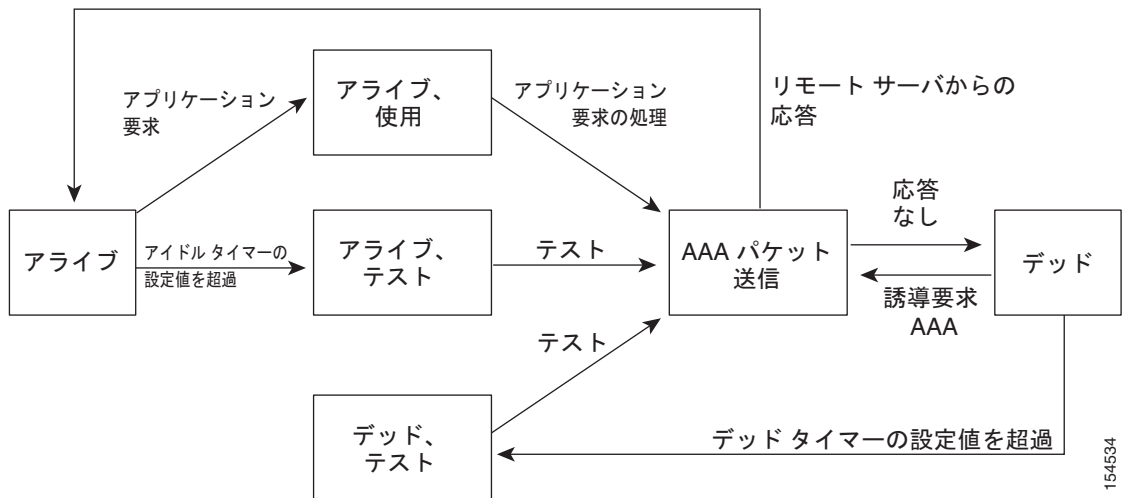
TACACS+ サーバに認証するには、TACACS+ 事前共有鍵を設定する必要があります。事前共有鍵は、デバイスと TACACS+ サーバ ホストの間で共有される秘密テキストストリングです。鍵の長さは 63 文字に制限され、任意の印字可能な ASCII 文字を含めることができます (スペースは使用できません)。すべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密鍵を設定できます。

このグローバル事前共有鍵の割り当ては、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 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+ サーバが稼動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 Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) 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 6-1 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 モニタリングは、テスト認証要求を TACACS+ サーバに送信して行われます。

ベンダー固有属性

Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) 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 Vendor-Specific Attribute (VSA; ベンダー固有属性) を伝達する方法が規定されています。IETF はアトリビュート 26 を使用しています。VSA を使用すると、ベンダーは一般的な用途に適さない独自の拡張アトリビュート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 で、サポートするオプションはベンダータイプ 1、名前は 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アトリビュートです。separator は、必須アトリビュートの場合は = (等号)、任意のアトリビュートの場合は * (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 アトリビュートを返すように指示します。この権限付与情報は、VSA を通じて指定されます。

次に、サポートされる VSA プロトコル オプションを示します。

- **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る場合は、二重引用符で囲む必要があります。

次に、サポートされるその他のアトリビュートを示します。

- **roles** : ユーザが属しているすべてのロールをリストします。値は、ロール名をスペースで区切ったストリングです。このサブアトリビュートは **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。このアトリビュートはシェル 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アトリビュートとともにアカウンティング情報を格納します。このアトリビュートは、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。このアトリビュートはアカウンティングの Protocol Data Unit (PDU; プロトコル データ ユニット) とだけ併用できます。

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鍵を取得すること (ある場合)。
- 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。
- 次の手順に従って、リモート TACACS+ 認証を含む AAA がすでに設定されていること。
 - 「ログイン認証方式の設定」(P.4-6)
 - 「AAA の設定」(P.4-4)

注意事項および制約事項

TACACS+ には、次の注意事項と制限事項があります。

- 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。

デフォルト設定

次の表に、TACACS+ のデフォルトを示します。

パラメータ	デフォルト
TACACS+	ディセーブル
デッドタイマー間隔	0 分

パラメータ	デフォルト
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
定期サーバ モニタリングのユーザ名	test
定期サーバ モニタリングのパスワード	test

TACACS+ の設定

ここでは、次の内容について説明します。

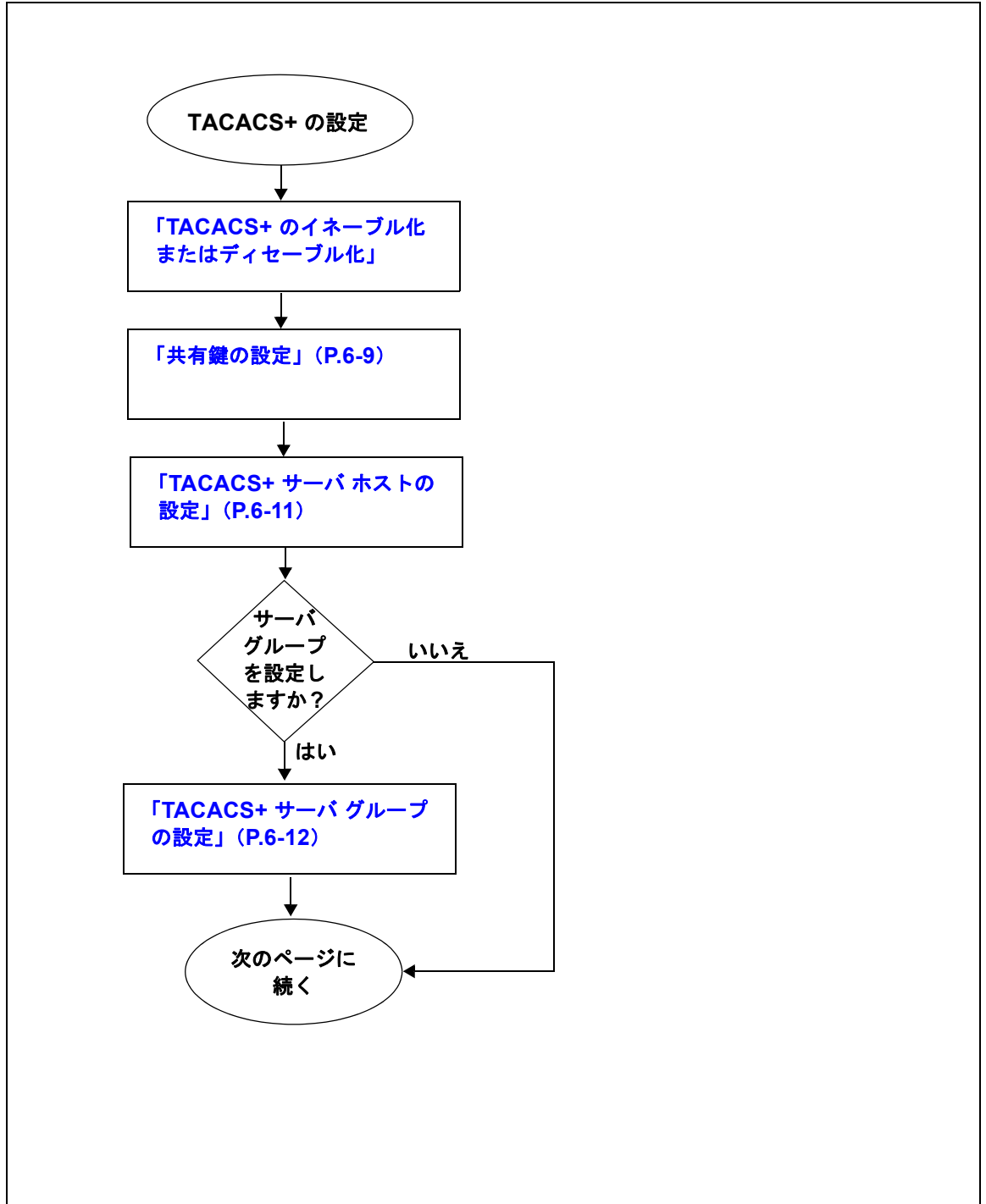
- 「フロー チャート： TACACS+ の設定」 (P.6-6)
- 「TACACS+ サーバ ホストの設定」 (P.6-11)
- 「TACACS+ サーバ ホストの設定」 (P.6-11)
- 「共有鍵の設定」 (P.6-9)
- 「TACACS+ サーバ グループの設定」 (P.6-12)
- 「TACACS+ サーバの誘導要求のイネーブル化」 (P.6-14)
- 「TACACS+ のグローバル タイムアウト間隔の設定」 (P.6-16)
- 「個別 TACACS+ ホストのタイムアウト間隔の設定」 (P.6-17)
- 「TACACS+ ホストの TCP ポートの設定」 (P.6-18)
- 「TACACS+ ホストのモニタリングの設定」 (P.6-20)
- 「TACACS+ グローバル デッド タイム間隔の設定」 (P.6-22)



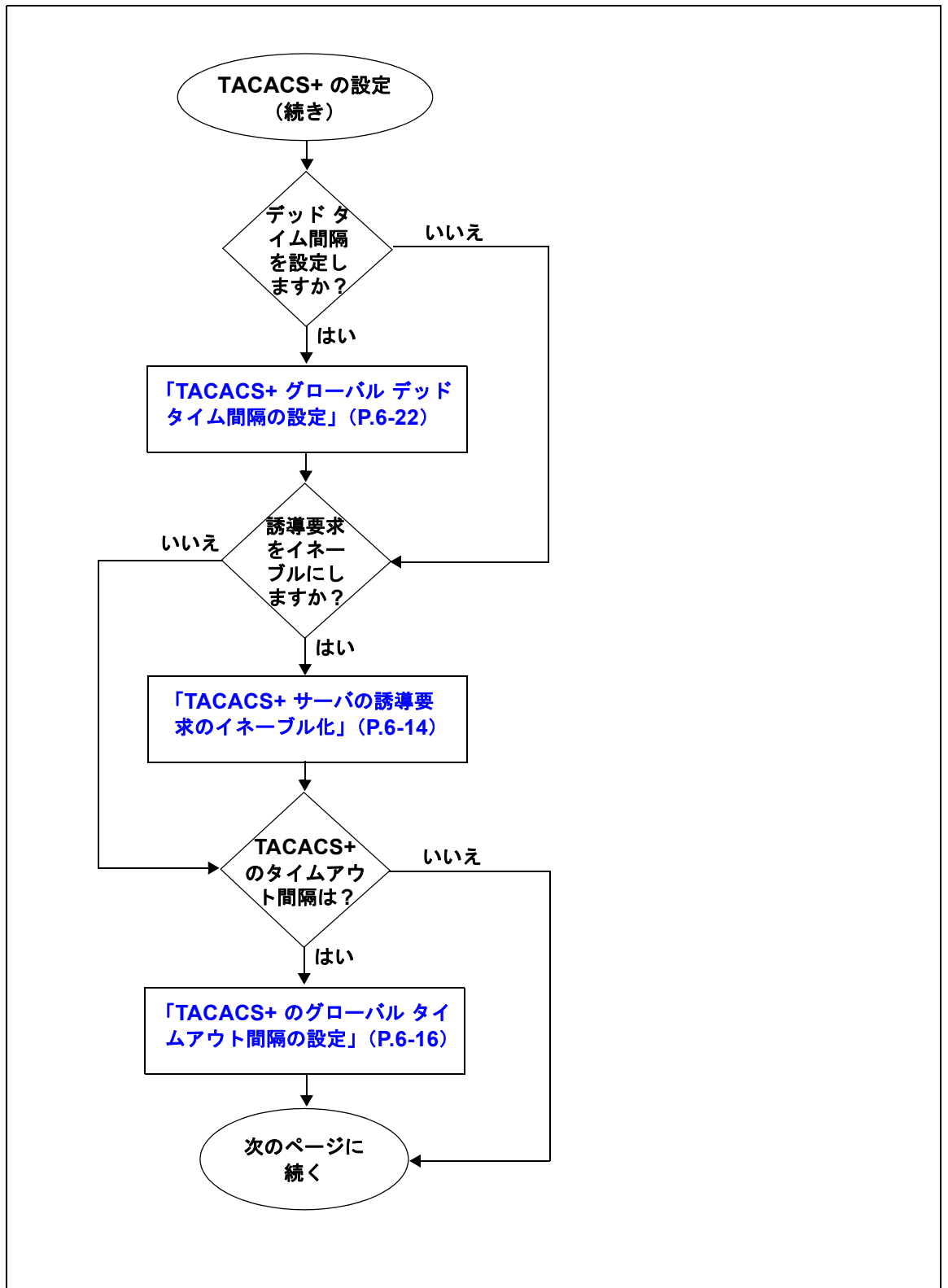
(注) Cisco Nexus 1000V のコマンドは Cisco IOS のコマンドと異なる場合があります。ご注意ください。

TACACS+ を設定するには、次のフローチャートを使用します。

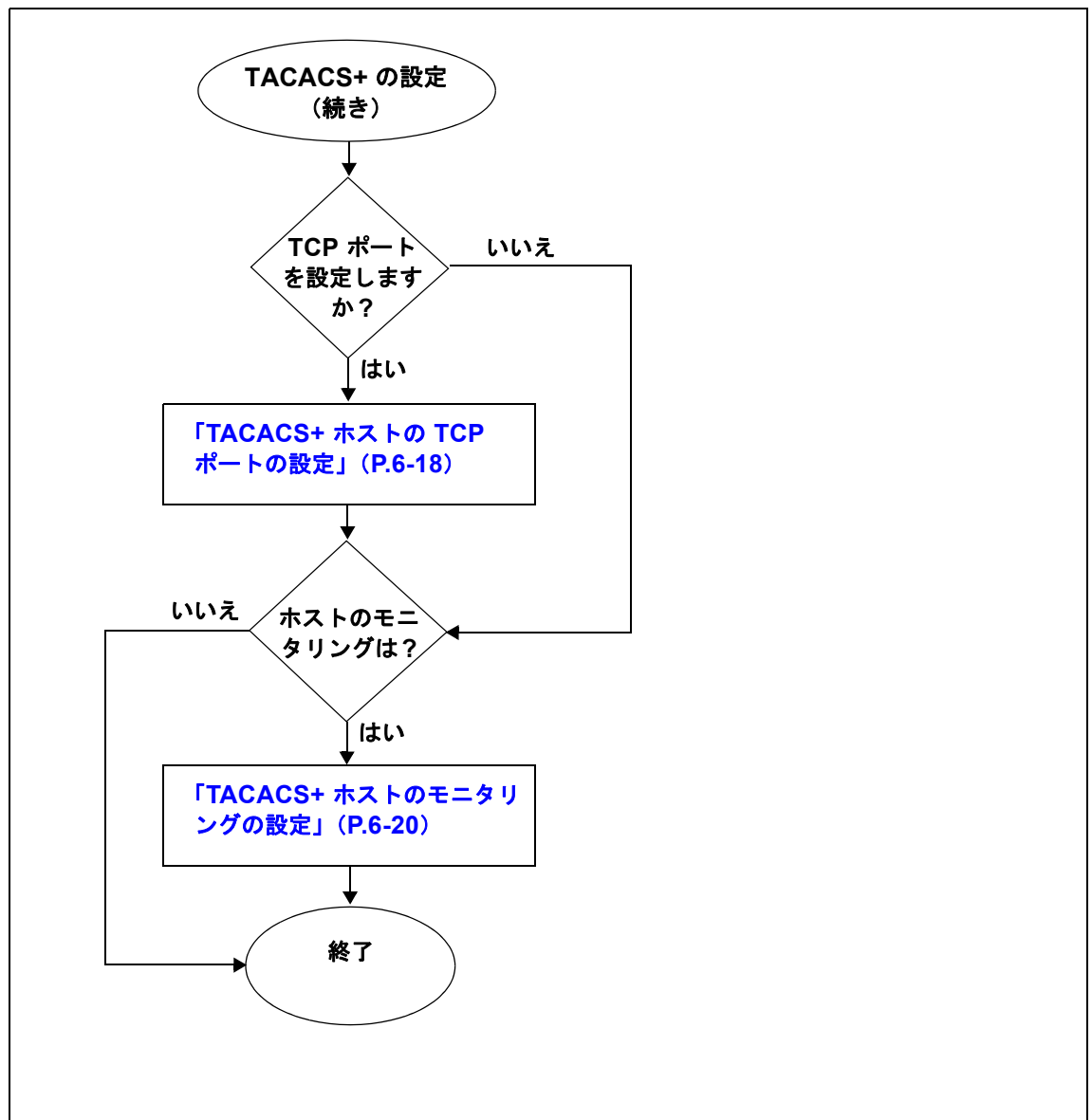
フローチャート： TACACS+ の設定



フローチャート：TACACS+ の設定（続き）



フローチャート：TACACS+ の設定（続き）



TACACS+ のイネーブル化またはディセーブル化

TACACS+ をイネーブルまたはディセーブルにするには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- EXEC モードで CLI にログインしています。
- 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設定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、すべての関連する設定は自動的に破棄されます。

手順の概要

1. `config t`
2. `[no] tacacs+ enable`
3. `exit`
4. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>config t</code> 例： n1000v# <code>config t</code> n1000v(config)#	CLI 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>[no] tacacs+ enable</code> 例： n1000v(config)# <code>tacacs+ enable</code> n1000v(config)# 例： n1000v(config)# <code>no tacacs+ enable</code> n1000v(config)#	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	<code>exit</code> 例： n1000v(config)# <code>exit</code> n1000v#	CLI 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	<code>copy running-config startup-config</code> 例： n1000v# <code>copy running-config startup-config</code>	(任意) 行った変更を、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。

共有鍵の設定

次のものを設定するには、次の手順を実行します。

- グローバル鍵 (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)
- 鍵 (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)

■ TACACS+ の設定

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
 (「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。
- TACACS+ サーバ ホストの鍵がわかっています。
- デフォルトでは、グローバル鍵は設定されません。

手順の概要

1. `config t`
2. `tacacs-server key [0 | 7] global_key`
3. `exit`
4. `show tacacs-server`
5. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>config t</code> 例: n1000v# config t n1000v(config)#	CLI 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	Do one of the following: <ul style="list-style-type: none"> • すべての TACACS+ サーバ ホストのグローバル鍵を設定する場合は、次のステップに進みます。 • 単一の TACACS+ サーバ ホストの鍵を設定する場合は、ステップ 5に進みます。 	
ステップ 3	<code>tacacs-server key [0 7] global_key</code> 例: n1000v(config)# tacacs-server key 0 QsEFtkI# n1000v(config)#	Cisco Nexus 1000V と TACACS+ サーバ ホストの間で共有されるグローバル鍵を指定します。 0 : 使用するクリア テキスト ストリング (鍵) を指定します (デフォルト)。 7 : 使用する暗号化ストリング (鍵) 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、グローバル鍵は設定されません。
ステップ 4	ステップ 6 に進みます。	
ステップ 5	<code>tacacs-server host {ipv4-address host-name} key [0 7] shared_key</code> 例: n1000v(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg n1000v(config)#	Cisco Nexus 1000V と指定した TACACS+ サーバ ホストの間で共有される鍵を指定します。 0 : 使用するクリア テキスト ストリング (鍵) を指定します (デフォルト)。 7 : 使用する暗号化ストリング (鍵) を指定します。 global_key : 最大 63 文字のストリングです。 グローバル共有鍵ではなく、この共有鍵が使用されます。

	コマンド	目的
ステップ6	exit 例: n1000v(config)# exit n1000v#	CLI 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7	show tacacs-server 例: n1000v# 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	(任意) TACACS+ サーバの設定を表示します。 (注) グローバル共有鍵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。鍵を表示するには、 show running-config コマンドを使用します。
ステップ8	copy running-config startup-config 例: n1000v# copy running-config startup-config	(任意) これらの実行コンフィギュレーションの変更内容を、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

TACACS+ サーバを TACACS+ ホストとして設定するには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
(「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。
- 次の手順に従って、共有鍵がすでに設定されています。
「共有鍵の設定」の手順 (P.6-9)
- 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ます。
- 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。

手順の概要

1. **config t**
2. **tacacs-server host {ipv4-address | host-name}**
3. **exit**
4. **show tacacs-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	config t 例: n1000v# config t n1000v(config)#	CLI 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 host {ipv4-address host-name} 例: n1000v(config)# tacacs-server host 10.10.2.2	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	exit 例: n1000v(config)# exit n1000v#	CLI 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	show tacacs-server 例: n1000v# 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 n1000v#	(任意) TACACS+ サーバの設定を表示します。
ステップ 5	copy running-config startup-config 例: n1000v# copy running-config startup-config	(任意) これらの実行コンフィギュレーションの変更内容を、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。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- TACACS+ サーバグループに追加されたすべてのサーバは、TACACS+ プロトコルを使用する必要があります。
- 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。
- 認証用に TACACS+ がイネーブルになっています
(「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。

- 次の手順に従って、事前共有鍵がすでに設定されています。
「共有鍵の設定」の手順 (P.6-9)
- TACACS+ サーバグループは、1つ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することができます。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。これと同じように、複数のサーバグループが相互にフェールオーバーを提供できます。

手順の概要

1. `config t`
2. `aaa group server tacacs+ group-name`
3. `server {ipv4-address | host-name}`
4. `deadtime minutes`
5. `use-vrf vrf-name`
6. `exit`
7. `show tacacs-server groups`
8. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ1	<code>config t</code> 例: n1000v# config t n1000v(config)#	CLI 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>aaa group server tacacs+ group-name</code> 例: n1000v(config)# aaa group server tacacs+ TacServer n1000v(config-tacacs)#	指定した名前で作成した TACACS+ サーバグループの TACACS+ コンフィギュレーション モードを開始します。
ステップ3	<code>server {ipv4-address host-name}</code> 例: n1000v(config-tacacs)# server 10.10.2.2 n1000v(config-tacacs)#	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。 ヒント 指定した TACACS+ サーバが検出されなかった場合、 <code>tacacs-server host</code> コマンドを使用してサーバを設定し、再度このコマンドを実行してください。
ステップ4	<code>deadtime minutes</code> 例: n1000v(config-tacacs)# deadtime 30 n1000v(config-tacacs)#	(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。有効な範囲は 0 ~ 1440 です。 (注) デッドタイム間隔がゼロ (0) より大きい TACACS+ サーバグループの場合は、その値がグローバル デッドタイム値に優先します (「TACACS+ グローバル デッドタイム間隔の設定」の手順 (P.6-22) を参照)。

	コマンド	目的
ステップ 5	<pre>use-vrf vrf-name</pre> <p>例: n1000v(config-tacacs+)# use-vrf management n1000v(config-tacacs+)#</p>	(任意) このサーバグループとの接続に使用する Virtual Routing and Forwarding (VRF; 仮想ルーティングおよび転送) インスタンスを指定します。
ステップ 6	<pre>exit</pre> <p>例: n1000v(config-tacacs+)# exit n1000v(config)#</p>	TACACS+ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	<pre>exit</pre> <p>例: n1000v(config)# exit n1000v#</p>	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 8	<pre>show tacacs-server groups</pre> <p>例: n1000v# show tacacs-server groups total number of groups:1</p> <p>following TACACS+ server groups are configured: group TacServer: server 10.10.2.2 on port 49 deadtime is 30 vrf is management n1000v#</p>	(任意) TACACS+ サーバグループの設定を表示します。
ステップ 9	<pre>copy running-config startup-config</pre> <p>例: n1000v(config)# copy running-config startup-config</p>	(任意) 実行コンフィギュレーションで行ったこれらの変更内容を、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。

```
例:
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# server 10.10.2.2
n1000v(config-tacacs+)# deadtime 30
n1000v(config-tacacs+)# use-vrf management
n1000v(config-tacacs+)# exit
n1000v(config)# exit
n1000v# 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
n1000v#
```

TACACS+ サーバの誘導要求のイネーブル化

認証要求の送信先の TACACS+ サーバをユーザが指定できるようにするには、次の手順を実行します。これは directed-request (誘導要求) と呼ばれます。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
 (「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。



(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。

- 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せん (vrfname は使用する VRF、hostname は設定された TACACS+ サーバの名前)。

手順の概要

1. `config t`
2. `tacacs-server directed-request`
3. `exit`
4. `show tacacs-server directed-request`
5. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>config t</code> 例: n1000v# config t n1000v(config)#	CLI 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>tacacs-server directed-request</code> 例: n1000v(config)# tacacs-server directed-request n1000v(config)#	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。デフォルトはディセーブルです。
ステップ 3	<code>exit</code> 例: n1000v(config)# exit n1000v#	CLI 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	<code>show tacacs-server directed-request</code> 例: n1000v# show tacacs-server directed-request enabled n1000v#	(任意) TACACS+ の誘導要求の設定を表示します。
ステップ 5	<code>copy running-config startup-config</code> 例: n1000v# 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。

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となります。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
 (「[TACACS+ のイネーブル化またはディセーブル化](#)」の[手順 \(P.6-8\)](#)を参照)。
- 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。
 個別サーバのタイムアウトの設定については、「[個別 TACACS+ ホストのタイムアウト間隔の設定](#)」の[手順 \(P.6-17\)](#)を参照してください。

手順の概要

1. `config t`
2. `tacacs-server timeout seconds`
3. `exit`
4. `show tacacs-server`
5. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>config t</code> 例: n1000v# config t n1000v(config)#	CLI 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>tacacs-server timeout seconds</code> 例: n1000v(config)# tacacs-server timeout 10	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	<code>exit</code> 例: n1000v(config)# exit n1000v#	CLI 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。

	コマンド	目的
ステップ4	<pre>show tacacs-server</pre> <p>例:</p> <pre>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 n1000v#</pre>	(任意) TACACS+ サーバの設定を表示します。
ステップ5	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>n1000v# copy running-config startup-config</pre>	(任意) 実行コンフィギュレーションで行ったこれらの変更内容を、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。

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となります。この設定は TACACS+ ホスト単位で設定します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
(「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。
- 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。

手順の概要

1. `config t`
2. `tacacs-server host {ipv4-address | host-name} timeout seconds`
3. `exit`
4. `show tacacs-server`
5. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	config t 例: n1000v# config t n1000v(config)#	CLI 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 host {ipv4-address host-name} timeout seconds 例: n1000v(config)# tacacs-server host 10.10.2.2 timeout 10 n1000v(config)#	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。 詳細については、「 TACACS+ のグローバル タイムアウト間隔の設定 」の手順 (P.6-16) を参照してください。
ステップ 3	exit 例: n1000v(config)# exit n1000v#	CLI 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	show tacacs-server 例: 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 n1000v#	(任意) TACACS+ サーバの設定を表示します。
ステップ 5	copy running-config startup-config 例: n1000v# copy running-config startup-config	(任意) 実行コンフィギュレーションで行ったこれらの変更内容を、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+ 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。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
(「[TACACS+ のイネーブル化またはディセーブル化](#)」の手順 (P.6-8) を参照)。
- 「[TACACS+ サーバ ホストの設定](#)」の手順 (P.6-11) に従って TACACS+ サーバが設定されています。

手順の概要

1. `config t`
2. `tacacs-server host {ipv4-address | host-name} port tcp-port`
3. `exit`
4. `show tacacs-server`
5. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ1	<code>config t</code> 例: n1000v# config t n1000v(config)#	CLI 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>tacacs-server host {ipv4-address host-name} port tcp-port</code> 例: n1000v(config)# tacacs-server host 10.10.2.2 port 2 n1000v(config)#	使用する TCP ポートを指定します。 有効な範囲 : 1 ~ 65535 デフォルト : 49
ステップ3	<code>exit</code> 例: n1000v(config)# exit n1000v#	CLI 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	<code>show tacacs-server</code> 例: 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:2 timeout:10 n1000v#	(任意) TACACS+ サーバの設定を表示します。
ステップ5	<code>copy running-config startup-config</code> 例: n1000v# 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。

TACACS+ ホストのモニタリングの設定

TACACS+ ホストの定期モニタリングを設定するには、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
 (「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。
- TACACS+ サーバが設定されています
 (「TACACS+ サーバホストの設定」の手順 (P.6-11) を参照)。
- 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。

手順の概要

1. `config t`
2. `tacacs-server host {ipv4-address | host-name} test {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}`
3. `tacacs-server dead-time minutes`
4. `exit`
5. `show tacacs-server`
6. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<pre>config t</pre> <p>例:</p> <pre>n1000v# config t n1000v(config)#</pre>	CLI 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	<pre>tacacs-server host {ipv4-address host-name} test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]}</pre> <p>例:</p> <pre>n1000v(config)# tacacs-server host 10.10.2.2 test username pvk2 password a3z9yjz7 idle-time 3</pre>	<p>サーバ モニタリングを設定します。</p> <p>username : デフォルトは test です。</p> <p>(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。</p> <p>password : デフォルトは test です。</p> <p>idle-time : デフォルトは 0 分です。有効な範囲は、0 ~ 1440 分です。</p> <p>(注) TACACS+ サーバの定期モニタリングの場合、アイドル タイマーの値を 0 より大きくする必要があります。</p>
ステップ 3	<pre>tacacs-server dead-time minutes</pre> <p>例:</p> <pre>n1000v(config)# tacacs-server dead-time 5</pre>	以前に回答しなかった 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	<pre>exit</pre> <p>例:</p> <pre>n1000v(config)# exit n1000v#</pre>	CLI 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	<pre>show tacacs-server</pre> <p>例:</p> <pre>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:2 timeout:10 n1000v#</pre>	(任意) TACACS+ サーバの設定を表示します。
ステップ 6	<pre>copy running-config startup-config</pre> <p>例:</p> <pre>n1000v# copy running-config startup-config</pre>	(任意) これらの実行コンフィギュレーションに行った変更内容を、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+ 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。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
 (「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。
- TACACS+ サーバが設定されています
 (「TACACS+ サーバホストの設定」の手順 (P.6-11) を参照)。
- デッド タイマー間隔が 0 分の場合、TACACS+ サーバの応答がなくても、そのサーバをデッドとしません。デッド タイマー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」の手順 (P.6-12) を参照)。

手順の概要

1. `config t`
2. `tacacs-server deadtime minutes`
3. `exit`
4. `show tacacs-server`
5. `copy running-config startup-config`

手順の詳細

	コマンド	目的
ステップ 1	<code>config t</code> 例: n1000v# <code>config t</code> n1000v(config)#	CLI 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>tacacs-server deadtime minutes</code> 例: n1000v(config)# <code>tacacs-server deadtime 5</code>	グローバル 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	<code>exit</code> 例: n1000v(config)# <code>exit</code> n1000v#	CLI 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。

	コマンド	目的
ステップ4	<code>show tacacs-server</code> 例: n1000v# show tacacs-server	(任意) TACACS+ サーバの設定を表示します。
ステップ5	<code>copy running-config startup-config</code> 例: n1000v# 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。

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、次の手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしています。
- 認証用に TACACS+ がイネーブルになっています
(「TACACS+ のイネーブル化またはディセーブル化」の手順 (P.6-8) を参照)。
- TACACS+ サーバが設定されています
(「TACACS+ サーバホストの設定」の手順 (P.6-11) を参照)。

手順の概要

1. `show tacacs-server statistics {hostname | ipv4-address}`

手順の詳細

	コマンド	目的
ステップ1	<code>show tacacs-server statistics {hostname ipv4-address}</code>	TACACS+ ホストの統計情報を表示します。

例:
n1000v# `show tacacs-server statistics 10.10.1.1`
Server is not monitored

```
Authentication Statistics
  failed transactions: 9
  successfull transactions: 2
  requests sent: 2
  requests timed out: 0
  responses with no matching requests: 0
  responses not processed: 0
  responses containing errors: 0
```

```
Authorization Statistics
  failed transactions: 1
  successfull transactions: 0
  requests sent: 0
```

■ TACACS+ 設定例

```

requests timed out: 0
responses with no matching requests: 0
responses not processed: 0
responses containing errors: 0

Accounting Statistics
failed transactions: 0
sucessfull transactions: 0
requests sent: 0
requests timed out: 0
responses with no matching requests: 0
responses not processed: 0
responses containing errors: 0

```

TACACS+ 設定例

次に、TACACS+ 設定の例を示します。

```

feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
server 10.10.2.2

```

TACACS+ 機能の履歴

ここでは、TACACS+ のリリース履歴を示します。

機能名	リリース	機能情報
TACACS+	4.0	この機能が追加されました。

その他の関連資料

TACACS+ の実装に関連する詳細情報については、次を参照してください。

- 「関連資料」 (P.6-25)
- 「標準規格」 (P.6-25)

関連資料

関連項目	マニュアル タイトル
CLI	『Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)』
システム管理	『Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

