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。

この章は、次の内容で構成されています。

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、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、およびアカウンティング 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。

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

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。

   サービスには次が含まれます。
   - 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）、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

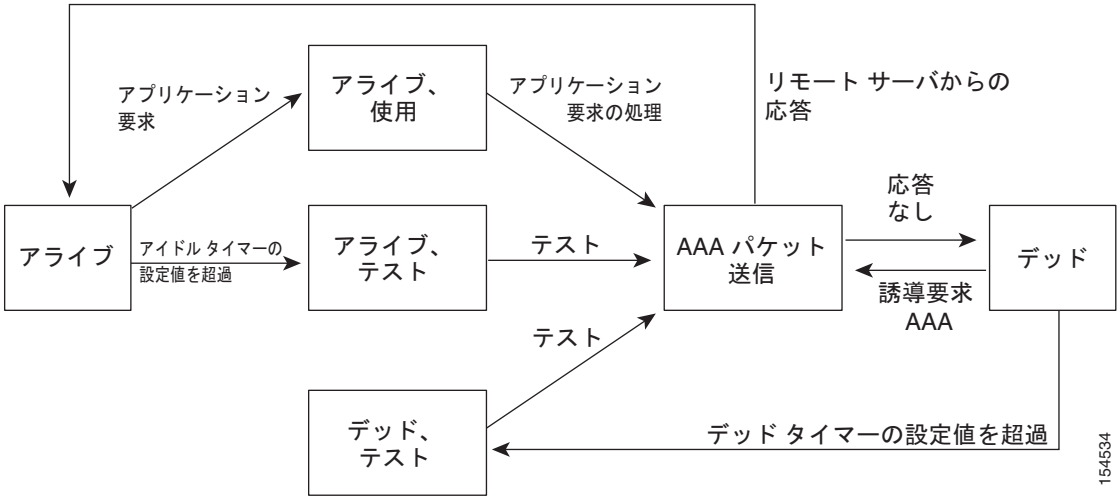
TACACS+ サーバに認証するには、TACACS+ 事前共有キーを設定する必要があります。事前共有キーは、デバイスと TACACS+ サーバ ホストの間で共有される秘密テキスト ストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。すべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

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 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（VSA）

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、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）、任意の属性の場合は *（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ている場合は、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属性を示します。

- 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 Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

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。
- 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+ に関する注意事項と制約事項は次のとおりです。

- 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
タイムアウト間隔	5 秒

パラメータ	デフォルト
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

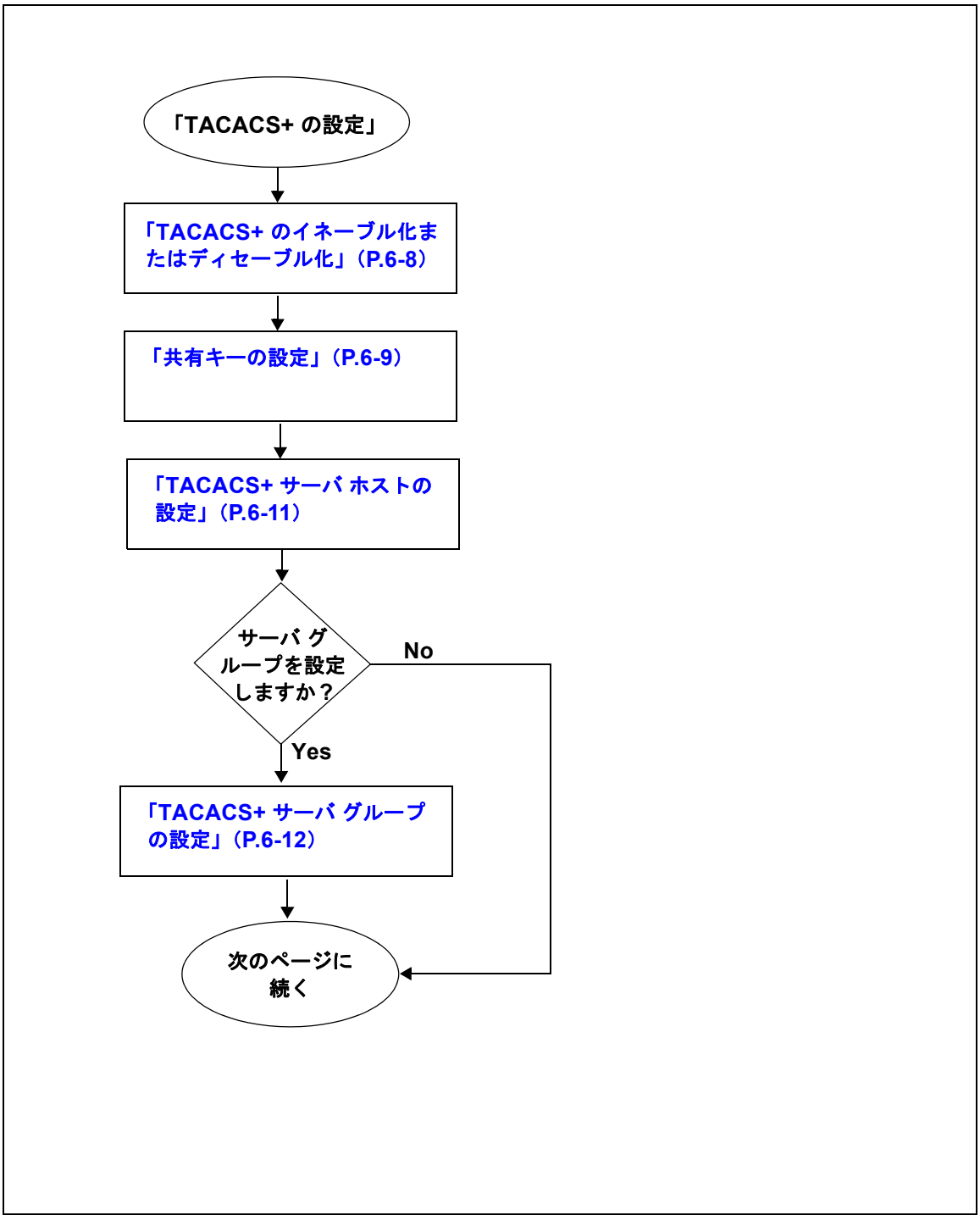
TACACS+ の設定

ここでは、次の内容について説明します。

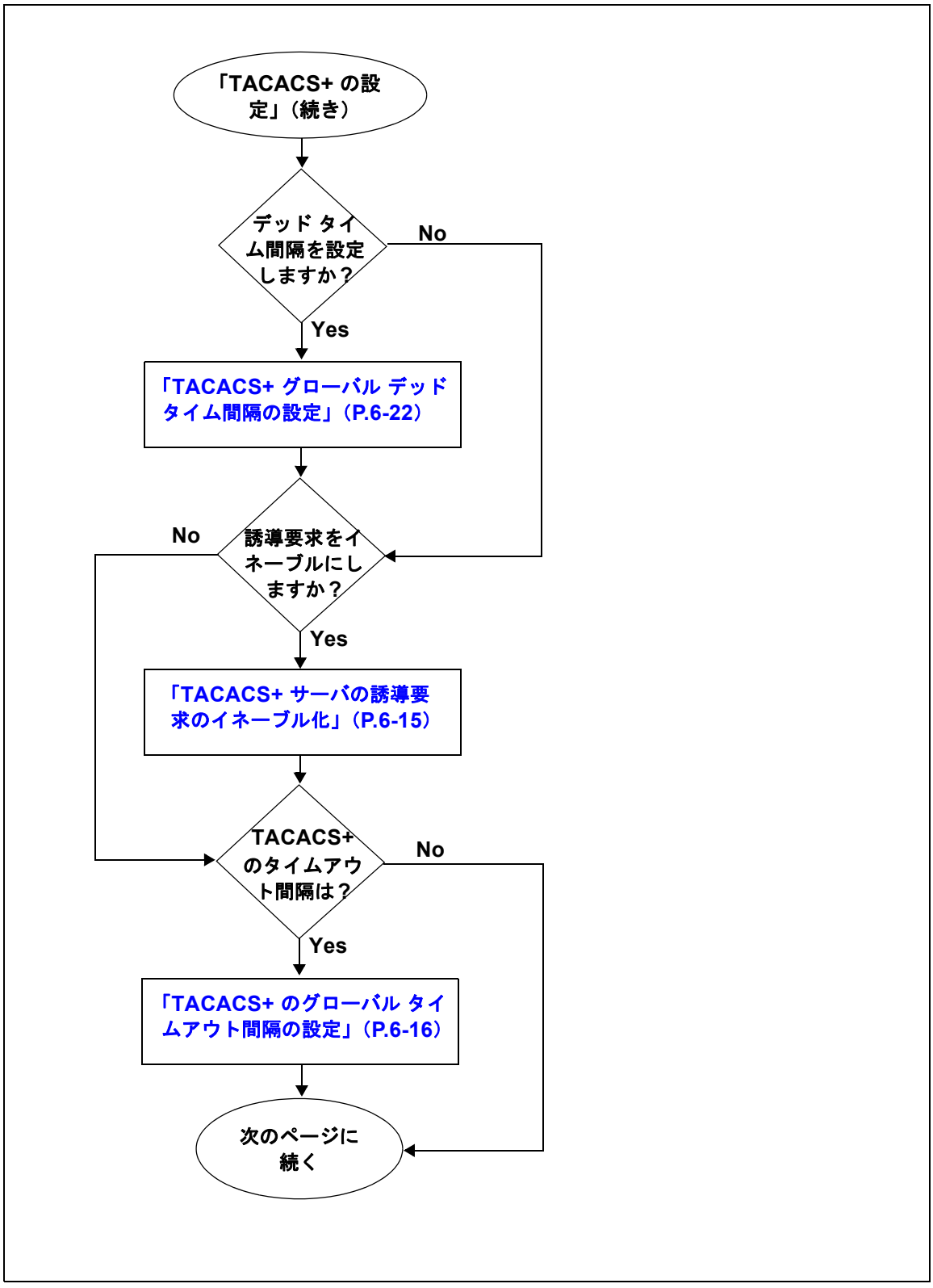
（注）　Cisco Nexus 1000V のコマンドは Cisco IOS のコマンドと異なる場合があることに注意してください。

TACACS+ を設定するには、次のフロー チャートを使用します。

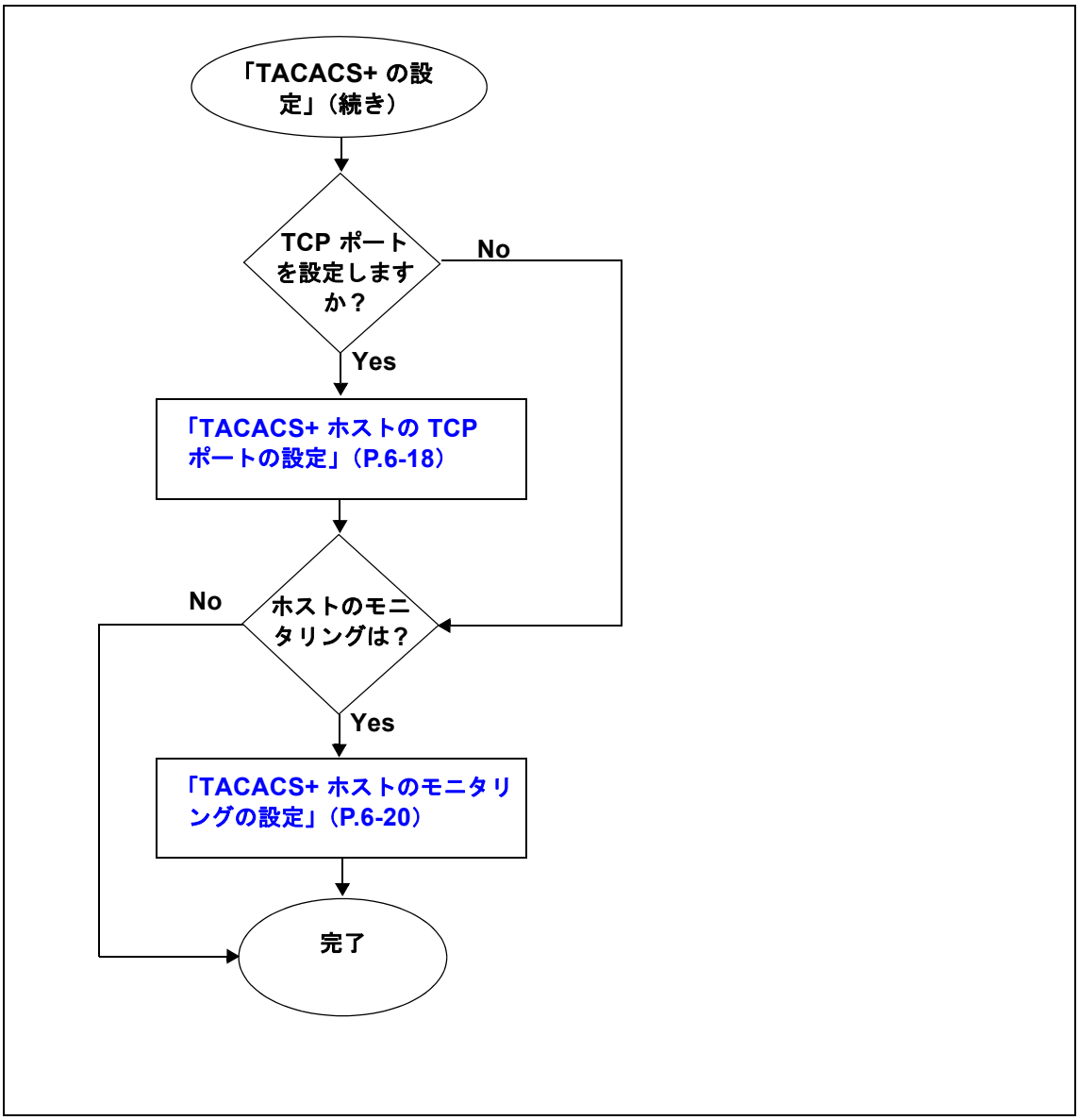
フロー チャート：「TACACS+ の設定」



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。

はじめる前に

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 にログインしていること。
- 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。

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	**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	**[no] tacacs+ enable**
	
	例：
	`n1000v(config)# tacacs+ enable`
	`n1000v(config)#`
	
	例：
	`n1000v(config)# no tacacs+ enable`
	`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	**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	**copy running-config startup-config**
	
	例：
	`n1000v# copy running-config`
	`startup-config`
		（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。

共有キーの設定

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 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

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
  「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバ ホストのキーがわかっています。
- デフォルトでは、グローバル キーは設定されません。

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	**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	次のいずれかを実行します。 • 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 5 に進みます。	

ステップ 3	**tacacs-server key** [**0** | **7**] *global_key*
	
	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 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（デフォルト）。
		7：使用する暗号化ストリング（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	ステップ 6 に進みます。	

	コマンド	目的
ステップ 5	**tacacs-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *shared_key* **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（デフォルト）。 **7**：使用する暗号化ストリング（キー）を指定します。 **global_key**：最大 63 文字のストリングです。 グローバル共有キーではなく、この共有キーが使用されます。
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 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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
  「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 次の手順に従って、共有キーがすでに設定されています。
  「共有キーの設定」（P.6-9）の手順
- 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。

はじめる前に

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 にログインしていること。

- 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ること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 次の手順に従って、事前共有キーがすでに設定されています。
「共有キーの設定」（P.6-9）の手順
- 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. （任意）**source-interface** {*interface-type*} {*interface-number*}
7. （任意）**show tacacs-server groups**
8. （任意）**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	**aaa group server tacacs+** *group-name*
	
	例：
	`n1000v(config)# aaa group server tacacs+ TacServer`
	`n1000v(config-tacacs+)#`
		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。

ステップ 3	**server** {*ipv4-address* | *host-name*}
	
	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。

	コマンド	目的
ステップ 4	**deadtime** *minutes* 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。指定できる範囲は 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 デット 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」（P.6-22）の手順を参照）。
ステップ 5	**use-vrf** *vrf-name* 例： n1000v(config-tacacs+)# use-vrf management n1000v(config-tacacs+)#	（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	**source-interface** {*interface-type*} {*interface-number*} 例： n1000v(config-tacacs+)# source-interface mgmt0 n1000v(config-tacacs+)#	（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	**show tacacs-server groups**	（任意）TACACS+ サーバ グループの設定を表示します。

例：
```
n1000v(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
n1000v(config-tacacs+)#
```

ステップ 8	**copy running-config startup-config** 例： n1000v(config-tacacs+)# 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。

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+)# 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(config-tacacs+)#
```

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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。

（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す（*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	**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 directed-request**
	
	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	**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。

	コマンド	目的
ステップ 4	**show tacacs-server directed-request** 例： n1000v# show tacacs-server directed-request enabled n1000v#	（任意）TACACS+ の directed request 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が宣言されます。

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 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」（P.6-17）の手順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	**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 timeout** *seconds* 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。

	コマンド	目的

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`
	`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。

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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 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」（P.6-16）の手順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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- 「TACACS+ サーバ ホストの設定」（P.6-11）の手順に従って 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	**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*} **port** *tcp-port*
	
	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	**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:2`
	`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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバが設定されていること。
「TACACS+ サーバ ホストの設定」（P.6-11）の手順を参照してください。
- 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	**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*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **例：** `n1000v(config)# tacacs-server host 10.10.2.2 test username pvk2 password a3z9yjqz7 idle-time 3`	サーバ モニタリングを設定します。 **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。指定できる範囲は、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	**tacacs-server dead-time** *minutes* **例：** `n1000v(config)# tacacs-server dead-time 5`	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	**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 5	**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:2`
	`timeout:10`
	`n1000v#`
		（任意）TACACS+ サーバの設定を表示します。

ステップ 6	**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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバが設定されていること。
「TACACS+ サーバ ホストの設定」（P.6-11）の手順を参照してください。
- 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」（P.6-12）の手順を参照）。

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	**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 deadtime** *minutes* 例： `n1000v(config)# tacacs-server deadtime 5`	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	**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。

	コマンド	目的
ステップ 4	**show tacacs-server** **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	**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。

はじめる前に

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 にログインしていること。
- 認証用に TACACS+ がイネーブルになっていること。
「TACACS+ のイネーブル化またはディセーブル化」（P.6-8）の手順を参照してください。
- TACACS+ サーバが設定されていること。
「TACACS+ サーバ ホストの設定」（P.6-11）の手順を参照してください。

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	**show tacacs-server statistics** {*hostname* | *ipv4-address*}	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
        sucessfull 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
        sucessfull transactions: 0
        requests sent: 0
```

```
        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+ の設定例

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(4)SV1(1)	この機能が導入されました。

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」（P.6-25）

関連資料

関連項目	参照先
CLI	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』
システム管理	『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—