TACACS+ の設定

この章では、Cisco NX-OS デバイス上で 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、次の項で構成されています。

TACACS+ について

TACACS+ は、Cisco NX-OS 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。Cisco NX-OS 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+ 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+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。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 NX-OS 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 NX-OS 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。

ユーザ ログインにおける TACACS+ の動作

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 NX-OS 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。

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。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項目を求めることもできます。

1. Cisco NX-OS 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、ユーザ名とパスワードを取得します。
2. Cisco NX-OS デバイスは、最終的に 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 NX-OS デバイスがユーザ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。
   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 NX-OS 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 NX-OS デバイスが ERROR 応答を受信すると、Cisco NX-OS デバイスは代替方式でユーザ認証を試行します。

   認証が終了し、Cisco NX-OS デバイスで許可がイネーブルになっていれば、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、Cisco NX-OS 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 または IPv6）、アクセス リスト、ユーザ タイムアウト）

デフォルトの TACACS+ サーバ暗号化タイプおよび秘密キー

スイッチを TACACS+ サーバに対して認証するには、TACACS+ 秘密キーを設定する必要があります。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバ 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 NX-OS デバイス上のすべての TACACS+サーバ設定で使用されるグローバルな秘密キーを設定できます。

グローバルな秘密キーの設定は、個々の 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

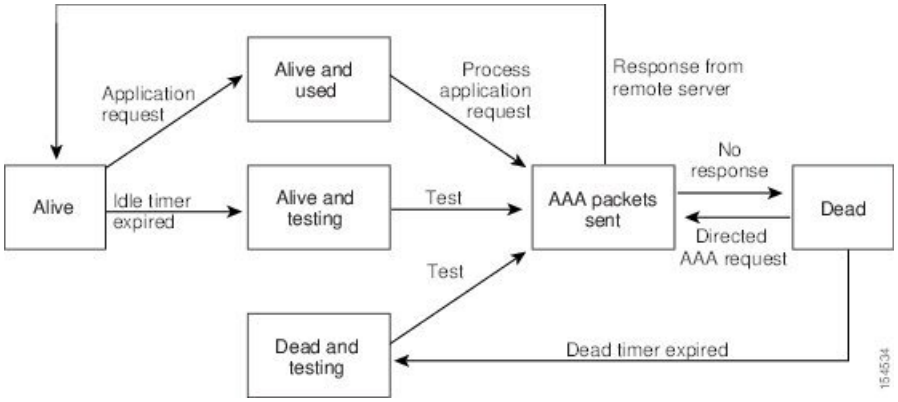
デフォルトでは、認証されたユーザがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

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 NX-OS デバイスは定期的に TACACS+ サーバをモニタリングし、TACACS+ サーバが応答を返す（アライブ）かどうかを調べることができます。Cisco NX-OS デバイスは、応答を返さない TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。また、Cisco NX-OS デバイスは、定期的にデッド TACACS+ サーバをモニタリングし、それらが応答を返したら、アライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、TACACS+ サーバが稼働状態であることを確認します。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 NX-OS 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。

Figure 1: TACACS+ サーバの状態

次の図に、TACACS+ サーバ モニタリングのサーバの状態を示します。



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。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。

TACACS+ 用の Cisco 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。

Cisco NX-OS デバイスでの認証に TACACS+ サーバを使用した場合、TACACS+ プロトコルは TACACS+ サーバに対し、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、Cisco NX-OS ソフトウェアで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。

Cisco NX-OS ソフトウェアでは、次の属性が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。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが network-operator および network-admin のロールに属している場合、値フィールドは network-operator network-admin となります。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。次に、Cisco ACS でサポートされるロール属性の例を示します。

```
shell:roles=network-operator network-admin

shell:roles*network-operator network-admin
```

Note VSA を shell:roles*"network-operator network-admin" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

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+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること。
- TACACS+ サーバから秘密キーを取得すること（ある場合）。
- Cisco NX-OS デバイスが、AAA サーバの TACACS+ クライアントとして設定されていること。

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 NX-OS デバイスに設定できる TACACS+ サーバの最大数は 64 です。

- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- グループ内に6台以上のサーバが設定されている場合は、デッドタイム間隔を設定することを推奨します。6 台以上のサーバを設定する必要がある場合は、デッド タイム間隔を 0 より大きな値に設定し、テスト ユーザ名とテスト パスワードを設定することで、デッド サーバのモニタリングを有効にしてください。
- TACACS+ サーバでのコマンド認証は、コンソール セッションに使用できます。
- Cisco NX-OS スイッチは、ユーザー名/パスワードプロンプトのカスタマイズをサポートしていません。スイッチでカスタムプロンプトを設定した場合、それらは無視されます。

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値を示します。

***Table 1: TACACS+* パラメータのデフォルト設定**

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
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
TACACS+ 許可の特権レベル サポート	ディセーブル

ワンタイム パスワード サポート

ワンタイム パスワード サポート（OTP）は、1回のログイン セッションまたはトランザクションに有効なパスワードです。OTP は、通常の（スタティック）パスワードに関連する多数の欠点を回避します。OTP は攻撃をリプレイするリスクはありません。すでにサービスへのログインまたは操作の実行に使用された OTP を侵入者が記録しようとしても、OTP は有効ではなくなっているため、悪用されません。

OTP は RADIUS や TACACS プロトコル デーモンに対してのみ適用できます。RADIUS プロトコル デーモンの場合は、ASCII 認証モードを無効にする必要があります。TACACS +プロトコル デーモンの場合は、ASCII 認証モードを有効にする必要があります。TACACS+ サーバでパスワードの ASCII 認証を有効にするには、 **aaa authentication login ascii-authentication** コマンドを使用します。

TACACS+ の設定

ここでは、Cisco NX-OS デバイスで TACACS+ サーバを設定する手順を説明します。

Note Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

TACACS+ サーバの設定プロセス

Procedure

ステップ 1 TACACS+ をイネーブルにします。

ステップ 2 TACACS+ サーバと Cisco NX-OS デバイスとの接続を確立します。

ステップ 3 TACACS+ サーバの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+ サーバのサブセットを使用して TACACS+ サーバ グループを設定します。

ステップ 5 （任意）TCP ポートを設定します。

ステップ 6 （任意）必要に応じて、TACACS+ サーバの定期モニタリングを設定します。

ステップ 7 （任意）TACACS+ の配布がイネーブルになっている場合は、ファブリックに対して TACACS+ 設定をコミットします。

Related Topics

TACACS+ のイネーブル化 （7 ページ）

TACACS+ のイネーブル化

デフォルトでは、Cisco NX-OS デバイスの TACACS+ 機能はディセーブルに設定されています。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。

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	**feature tacacs+** **Example:** `switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **copy running-config startup-config** **Example:** `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 NX-OS デバイス上でその TACACS+ サーバの IP アドレスかホスト名を設定する必要があります。最大 64 の TACACS+ サーバを設定できます。

Note TACACS+ サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスに設定するとき、デフォルトでは TACACS+ サーバはデフォルトの TACACS+ サーバ グループに追加されます。TACACS+ サーバは別の TACACS+ サーバ グループに追加することもできます。

Before you begin

TACACS+ を有効にします。

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。

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	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **Example:** `switch(config)# tacacs-server host 10.10.2.2`	TACACS+ サーバの IP アドレス（IPv4 または IPv6）、またはホスト名を指定します。
ステップ 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。

ステップ 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）
TACACS+ サーバ グループの設定 （12 ページ）

グローバル TACACS+ キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバについて、グローバル レベルで秘密 TACACS+ キーを設定できます。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

TACACS+ を有効にします。

リモート TACACS+ サーバの秘密キーの値を取得します。

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	**tacacs-server key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# tacacs-server key 0 QsEfThUkO`	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、実行コンフィギュレーション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。 デフォルトでは、秘密キーは設定されていません。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。 **Note** 秘密キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された秘密キーを表示するには、**show running-config** コマンドを使用します。

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

Related Topics

TACACS+ のイネーブル化 （7 ページ）
AES パスワード暗号化およびプライマリ暗号キーについて

特定の TACACS+ サーバ用のキーの設定

TACACS+サーバの秘密キーを設定できます。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

TACACS+ を有効にします。

リモート TACACS+ サーバの秘密キーの値を取得します。

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	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value* **Example:** `switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg`	特定の TACACS+ サーバの秘密キーを指定します。*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、実行コンフィギュレーション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。 グローバル秘密キーではなく、この秘密キーが使用されます。
ステップ 3	**exit** **Example:**	設定モードを終了します。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 4	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。 **Note** 秘密キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された秘密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) **copy running-config startup-config** **Example:** `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。

Related Topics

AES パスワード暗号化およびプライマリ暗号キーについて

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+ を有効にします。

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 group server tacacs+** *group-name* **Example:**	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。

	Command or Action	Purpose
	`switch(config)# aaa group server tacacs+ TacServer` `switch(config-tacacs+)#`	
ステップ 3	**server** {*ipv4-address* | *ipv6-address* | *hostname*} **Example:** `switch(config-tacacs+)# server 10.10.2.2`	TACACS+ サーバを、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、このコマンドを再試行します。

ステップ 4	**exit**
	Example:
	`switch(config-tacacs+)# exit`
	`switch(config)#`
		TACACS+ サーバ グループ 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) **show tacacs-server groups** **Example:** `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 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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）
リモート AAA サービス
TACACS+ サーバ ホストの設定 （8 ページ）
TACACS+ デッド タイム間隔の設定 （22 ページ）

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。デフォルトでは、Cisco NX-OS ソフトウェアは、使用可能なあらゆるインターフェイスを使用します。

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	**ip tacacs source-interface** *interface* **Example:** `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 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。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show tacacs-server** **Example:** `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** **Example:** `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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）
TACACS+ サーバ グループの設定 （12 ページ）

ユーザによるログイン時の TACACS+ サーバ指定の許可

スイッチ上で directed-request（誘導要求）オプションを有効にすることにより、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なります。デフォルトでは、Cisco NX-OS 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。このオプションを有効にすると、ユーザは *username@vrfname:hostname* としてログインできます。ここで *vrfname* は使用する VRF で、*hostname* は設定された TACACS+ サーバの名前です。

Note directed-request オプションをイネーブルにすると、Cisco NX-OS デバイスでは認証に TACACS+ 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。

Note 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。

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	**tacacs-server directed-request** **Example:** `switch(config)# tacacs-server directed-request`	ログイン時にユーザが認証要求の送信先となる TACACS+ サーバ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	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。

ステップ 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	(Optional) **show tacacs-server directed-request** **Example:** `switch# show tacacs-server directed-request`	TACACS+ の directed request の設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）

TACACS+ サーバのタイムアウト間隔の設定

Cisco NX-OS 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。タイムアウト間隔には、Cisco NX-OS デバイスがTACACS+サーバ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。

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	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **timeout** *seconds* **Example:** `switch(config)# tacacs-server host server1 timeout 10`	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。
ステップ 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。

ステップ 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	Command or Action	Purpose
ステップ 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）

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 NX-OS デバイスはすべての TACACS+ 要求にポート 49 を使用します。

Before you begin

TACACS+ を有効にします。

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	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **port** *tcp-port* **Example:** `switch(config)# tacacs-server host 10.10.1.1 port 2`	サーバに送る TACACS+ メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 49 です。値の範囲は 1 ～ 65535 です。
ステップ 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ distribution pending`	配布するために保留状態になっている TACACS+ 設定を表示します。

	Command or Action	Purpose
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。

ステップ 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）

TACACS+ サーバのグローバルな定期モニタリングの設定

各サーバに個別にテストパラメータを設定しなくても、すべての TACACS+ サーバの可用性をモニタリングできます。テスト パラメータが設定されていないサーバは、グローバル レベルのパラメータを使用してモニタリングされます。

Note 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

グローバル コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS 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定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

Note テスト パラメータは、すべてのスイッチに配布されます。ファブリック内に旧リリースが稼働しているスイッチが 1 つでもある場合は、ファブリック内のすべてのスイッチにテスト パラメータが配布されなくなります。

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。

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。

Before you begin

TACACS+ を有効にします。

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	**tacacs-server test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3`	グローバルなサーバ 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* **Example:** `switch(config)# tacacs-server dead-time 5`	Cisco NX-OS デバイスが、前回応答しなかった TACACS+ サーバ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 分です。有効な範囲は 0 ～ 1440 分です。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

各 TACACS+ サーバの定期モニタリングの設定 （20 ページ）

各 TACACS+ サーバの定期モニタリングの設定

各TACACS+サーバの可用性をモニタリングできます。コンフィギュレーションパラメータには、サーバで使用するユーザ名とパスワード、およびアイドルタイマーなどがあります。アイドルタイマーには、TACACS+サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS 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定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

Note 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

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。

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。

Note テスト パラメータは、すべてのスイッチに配布されます。テスト パラメータは、ファブリック内のスイッチには配信されません。

Before you begin

TACACS+ をイネーブルにします。

1 つまたは複数の TACACS+ サーバ ホストを追加します。

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	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は 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* **Example:** `switch(config)# tacacs-server dead-time 5`	Cisco NX-OS デバイスが、前回応答しなかった TACACS+ サーバ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 分です。有効な範囲は 0 ～ 1440 分です。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `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。

Related Topics

TACACS+ サーバ ホストの設定 （8 ページ）

TACACS+ サーバのグローバルな定期モニタリングの設定 （18 ページ）

TACACS+ デッド タイム間隔の設定

すべてのTACACS+サーバ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 NX-OS 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。

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	**tacacs-server deadtime** *minutes* **Example:** `switch(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	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	保留状態になっている TACACS+設定を表示します。
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+の設定変更を実行コンフィギュレーションに適用します。

ステップ 5	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	Command or Action	Purpose
ステップ 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

ASCII 認証の設定

TACACS+ サーバで ASCII 認証をイネーブルにできます。

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 authentication login ascii-authentication** **Example:** `switch(config)# aaa authentication login ascii-authentication`	ASCII 認証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	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。
ステップ 5	**exit** **Example:**	設定モードを終了します。

	Command or Action	Purpose
	`switch(config)# exit` `switch#`	
ステップ 6	(Optional) **show tacacs-server** **Example:** `switch# show tacacs-server`	TACACS+サーバの設定を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `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。

Caution 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。

Note コンソールを使用してサーバにログインすると、コマンド認可はディセーブルになります。認証は、非コンソール セッションとコンソール セッションの両方に使用できます。デフォルトでは、コマンド許可はデフォルト（非コンソール）セッション用に設定されていても、コンソールセッションに対してディセーブルです。コンソールセッションでコマンド許可をイネーブルにするには、コンソールの AAA グループを明示的に設定する必要があります。

Note デフォルトでは、状況依存ヘルプおよびコマンドのタブ補完に表示されるのは、割り当てられたロールでユーザに対するサポートが定義されているコマンドだけです。コマンド許可をイネーブルにすると、Cisco NX-OS ソフトウェアでは、ユーザに割り当てられているロールに関係なく、状況依存ヘルプおよびタブ補完にすべてのコマンドが表示されるようになります。

Before you begin

TACACS+ を有効にします。

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** {**commands** | **config-commands**} {**console** | **default**} {**group** *group-list* [**local**] | **local**}
	Example:
	`switch(config)# aaa authorization commands`
	`default group TacGroup`
	`Per command authorization will disable RBAC for all`
	`users. Proceed (y/n)?`
		TACACS+ サーバの特定の役割にコマンド許可方式を設定します。
		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。
		console キーワードは、コンソール セッションのコマンド許可を設定し、**default** キーワードは、非コンソール セッションのコマンド許可を設定します。
		group-list 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。このグループに属しているサーバに対して、コマンド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。
		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。デフォルトの方式は **local** です。
		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。
		確認プロンプトで **Enter** キーを押した場合のデフォルトのアクションは **n** です。

	Command or Action	Purpose
ステップ 3	(Optional) **show tacacs+** {**pending** | **pending-diff**} **Example:** `switch(config)# show tacacs+ pending`	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) **tacacs+ commit** **Example:** `switch(config)# tacacs+ commit`	一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用します。

ステップ 5	**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 6	(Optional) **show aaa authorization** [**all**] **Example:** `switch(config)# 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 7	(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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）
TACACS+ サーバでのコマンド許可のテスト （26 ページ）

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。

Note **test** コマンドでは許可に、コンソール方式ではなくデフォルト（非コンソール）方式を使用します。

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:** `switch# test aaa authorization command-type commands user TestUser command reload`	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。 **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。 **Note** *command-string* 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。

Related Topics

TACACS+ のイネーブル化 （7 ページ）
TACACS+ サーバでのコマンド許可の設定 （24 ページ）
ユーザ アカウントおよび RBAC の設定

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ー セッションまたは別のユーザー名に対して、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有効にしたり、無効にしたりすることができます。

（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： `switch# terminal verify-only`	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が Cisco NX-OS ソフトウェアによって示されます。
ステップ 2	**terminal no verify-only** [**username** *username*] 例：	コマンド許可検証をディセーブルにします。

	コマンドまたはアクション	目的
	`switch# terminal no verify-only`	

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、Role-Based Access Control（RBAC; ロールベース アクセス コントロール）を使用します。両方のタイプのデバイスを同じ 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 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	• **feature privilege** の場合の NX-OS ロールの権限 コマンドは無効です。 • 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

Important ネットワーク管理者のみがルートに権限を昇格できます。新しいセキュリティ対策により、ネットワーク オペレータ（priv-1 ユーザ）は show tech を収集できません。したがって、enable コマンドはでは権限のエスカレーションを行えません。

Note

- **feature privilege** コマンドが有効の場合、権限ロールは下位の権限ロールの権限を継承します。
- Cisco Secure Access Control Server（ACS）にも、Cisco NX-OS デバイスの特権レベルを設定する必要があります。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature privilege** **Example:** `switch(config)# feature privilege`	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:** `switch(config)# enable secret 5 def456 priv-lvl 15`	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。 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。*password* 引数に指定できる文字数は、最大 64 文字です。*priv-lvl* 引数は、1 ～ 15 です。 **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。

	Command or Action	Purpose
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。

Related Topics

権限ロールのユーザ コマンドの許可または拒否 （30 ページ）
ユーザ ロールおよびルールの作成

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:
	`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。

	Command or Action	Purpose

ステップ 2	[no] **role name priv-***n*
	Example:
	`switch(config)# role name priv-5`
	`switch(config-role)#`
		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。*n* 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:** `switch(config-role)# rule 2 permit command pwd`	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。ロールごとに最大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 つのロールが 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。 *command-string* 引数には、空白スペースを含めることができます。 **Note** 必要な規則の数だけこのコマンドを繰り返します。

ステップ 4	**exit**
	Example:
	`switch(config-role)# exit`
	`switch(config)#`
		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:** `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。

Related Topics

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 （28 ページ）
ユーザ ロールおよびルールの作成

TACACS+ サーバまたはサーバ グループの手動モニタリング

TACACS+ サーバまたはサーバ グループに、手動でテスト メッセージを送信できます。

Before you begin

TACACS+ をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	**test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *hostname*} [**vrf** *vrf-name*] *username password* **Example:** `switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH`	TACACS+ サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	**test aaa group** *group-name username password* **Example:** `switch# test aaa group TacGroup user2 As3He3CI`	TACACS+ サーバ 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。

Related Topics

TACACS+ サーバ ホストの設定 （8 ページ）
TACACS+ サーバ グループの設定 （12 ページ）

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	**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	**no feature tacacs+** **Example:** `switch(config)# no feature tacacs+`	TACACS+ をディセーブルにします。

	Command or Action	Purpose

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **copy running-config startup-config** **Example:** `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+ サーバのモニタリング

Cisco NX-OS デバイスが保持している TACACS+ サーバのアクティビティに関する統計情報をモニタできます。

Before you begin

Cisco NX-OS デバイスの TACACS+ サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	**show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show tacacs-server statistics 10.10.1.1`	TACACS+ 統計情報を表示します。

Related Topics

TACACS+ サーバ ホストの設定 （8 ページ）
TACACS+ サーバ統計情報のクリア （33 ページ）

TACACS+ サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している TACACS+ サーバのアクティビティに関する統計情報を表示します。

Before you begin

Cisco NX-OS デバイスの TACACS+ サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# show tacacs-server statistics 10.10.1.1`	Cisco NX-OS デバイスの TACACS+ サーバ統計情報を表示します。
ステップ 2	**clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} **Example:** `switch# clear tacacs-server statistics 10.10.1.1`	TACACS+ サーバ統計情報をクリアします。

Related Topics

TACACS+ サーバ ホストの設定 （8 ページ）

TACACS+ の設定の確認

TACACS+ の設定を表示するには、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-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての TACACS+ サーバのパラメータを表示します。
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。

TACACS+ の設定例

次に、TACACS+ サーバ ホストおよびサーバ グループを設定する例を示します。

```
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
```

次に、コマンド許可検証を設定して使用する例を示します。

```
switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                  Ch #
--------------------------------------------------------------------------------
Eth7/2        1      eth  access down    SFP not inserted           auto(D) --
```

次に、ロールの累積権限をイネーブルにし、特権レベル 2 のシークレット パスワードを設定し、特権レベル 2 の許可用に user3 を設定する例を示します。

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret def456 priv-lvl 2
switch(config)# username user3 priv-lvl 2
switch(config)# show privilege
User name: user3
Current privilege level: -2
Feature privilege: Enabled
switch(config)# copy running-config startup-config
switch(config)# exit
```

次に、user3 を priv-2 ロールから priv-15 ロールに変更する例を示します。**enable 15** コマンドを入力すると、ユーザは、管理者が **enable secret** コマンドを使用して設定したパスワードを入力するように求められます。特権レベルを 15 に設定すると、このユーザには、イネーブル モードにおける network-admin 権限が付与されます。

```
User Access Verification
login: user3
Password: ******
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

```
switch# enable 15
Password: def456
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2013, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch-enable#
```

次に、priv-5 以上のロールを持つすべてのユーザが **pwd** コマンドを実行できるようにする例を示します。

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd
```

次に、priv-5 未満のロールを持つすべてのユーザが **show running-config** コマンドを実行できないようにする例を示します。まず、このコマンドを実行する権限を priv-0 ロールから削除する必要があります。次に、ロール priv-5 でこのコマンドを許可し、priv-5 以上のロールを持つユーザにこのコマンドを実行する権限が付与されるようにする必要があります。

```
switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-config
switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-config
switch(config-role)# exit
```

次の作業

これで、サーバ グループも含めて AAA 認証方式を設定できるようになります。

TACACS+ に関する追加情報

ここでは、TACACS+ の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
VRF コンフィギュレーション	『*Cisco NX-OS 9000 Series NX-OS Unicast Routing Configuration Guide*』

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。	—

MIB

MIB	MIB のリンク
TACACS+ に関連する MIB	サポートされている MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

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。