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 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する。
- 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する。 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

TACACS+を使用するCisco NX-OSデバイスに対して、ユーザがパスワード認証プロトコル（PAP）ログインを試みると、次の処理が行われます。

（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項目を求めることもできます。

1. Cisco NX-OSデバイスは接続が確立されると、ユーザ名とパスワードを取得するためにTACACS+デーモンに接続します。
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得ます。

   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 デバイスがユーザ許可を必要とする場合は、許可処理が始まります。

   REJECT

   ユーザ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 デバイスは ERROR 応答を受信した場合、別の方法でユーザの認証を試行します。

認証が終了し、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 デバイスは再び TACACS+ デーモンに接続します。デーモンから ACCEPT または REJECT 応答が返されます。 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、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（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。 秘密キーは、Cisco NX-OS 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）。 Cisco NX-OS デバイス上のすべての TACACS+ サーバの設定には、グローバル事前共有キーを使用できます。

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無効にできます。

TACACS+ サーバのコマンド許可サポート

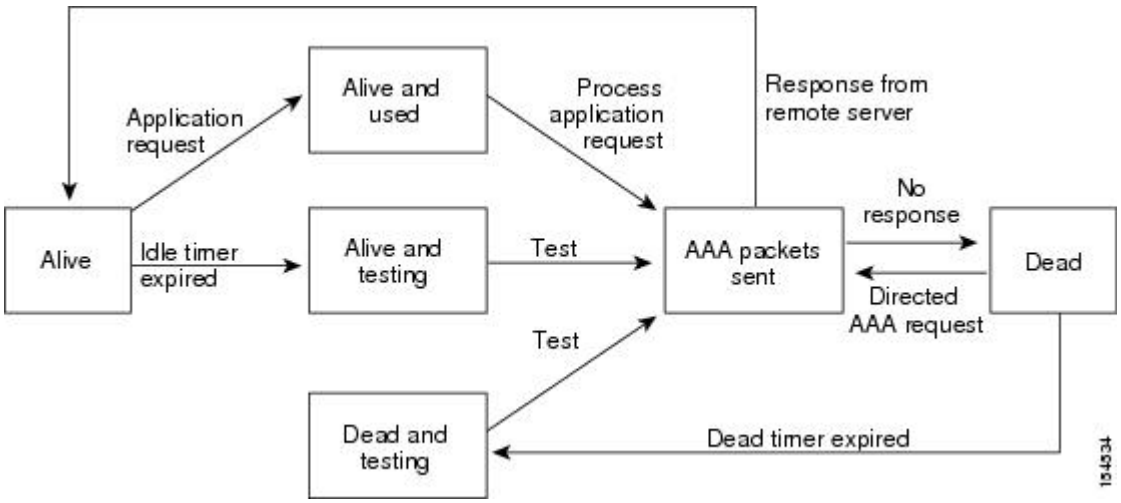
デフォルトでは、認証されたユーザがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。 また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

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 要求の処理時間を短縮するために、TACACS+ サーバを定期的にモニタして TACACS+ サーバが応答している（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、応答の遅い 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。 Cisco NX-OS デバイスはデッド TACACS+ サーバを定期的にモニタし、応答があれば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+ サーバがデッドまたはアライブの状態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 デバイスは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エラー メッセージで表示します。

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。

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。

TACACS+ 設定の配布

Cisco Fabric Services（CFS）を使用すると、Cisco NX-OS デバイスからネットワーク上の他の Cisco NX-OS デバイスに TACACS+ 設定および権限ロールを配布できます。 使用しているデバイスにおいて、ある機能に対して CFS 配布をイネーブルにすると、そのデバイスは CFS 領域に属します。この CFS 領域には、その機能に対して CFS 配布をイネーブルにしているネットワーク上の他のデ

バイスが含まれます。 TACACS+ に対する CFS 配布はデフォルトではディセーブルになっています。

（注） 設定変更を配布する場合は、TACACS+ に対する CFS を各デバイスで明示的にイネーブルにする必要があります。

使用している Cisco NX-OS デバイスで TACACS+ に対する CFS 配布をイネーブルにした後、最初に入力した TACACS+ コンフィギュレーション コマンドによって、Cisco NX-OS ソフトウェアで次の処理が行われます。

- Cisco NX-OS デバイスで CFS セッションを作成します。
- TACACS+ に対する CFS がイネーブルにされている CFS 領域で、すべての Cisco NX-OS デバイスの TACACS+ 設定をロックします。
- TACACS+ の設定変更を Cisco NX-OS デバイスの一時バッファに保存します。

この変更は、CFS 領域にあるデバイスに対して配布するよう明示的にコミットするまで、Cisco NX-OS デバイスの一時バッファに存在します。 変更をコミットすると、Cisco NX-OS ソフトウェアが次の処理を実行します。

- Cisco NX-OS デバイスの実行コンフィギュレーションに変更を適用します。
- 更新された TACACS+ 設定を CFS 領域内にある他の Cisco NX-OS デバイスに配布します。
- CFS 領域内にある他のデバイスの TACACS+ 設定のロックを解除します。
- CFS セッションを終了します。

CFS では TACACS+ サーバ グループの設定、定期的な TACACS+ サーバのテスト設定、およびサーバ キーとグローバル キーは配布しません。 キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

CFS の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

TACACS+ のベンダー固有属性

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、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。

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、必須属性の場合に =（等号）、オプションの属性の場合に *（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。

Cisco NX-OS ソフトウェアでは次の VSA プロトコル オプションをサポートしています。

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 ソフトウェアは、次の属性をサポートしています。

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 vdc-admin のロールに属している場合、値フィールドは network-operator vdc-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 vdc-admin
```

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

（注） VSA を shell:roles*"network-operator vdc-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 Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

TACACS+ のバーチャライゼーション サポート

TACACS+ の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。 VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

Cisco NX-OS デバイスは、仮想ルーティング/転送（VRF）インスタンスを使用して TACACS+ サーバにアクセスします。 VRF の詳細情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

TACACS+ のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	TACACS+ にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

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 デバイス上には最大 64 の TACACS+ サーバを設定できます。
- 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。
- Cisco NX-OS Release 4.x および 5.x の場合、TACACS+ サーバ上のコマンド許可は、コンソール以外のセッションでのみ使用可能です。 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。 Cisco NX-OS Release 6.0 から、TACACS+ サーバ上のコマンド許可は、コンソール セッションとコンソール以外のセッションの両方で使用可能になりました。

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。

表 *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	test
TACACS+ 許可の特権レベル サポート	ディセーブル

TACACS+ の設定

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

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

TACACS+ サーバの設定プロセス

ステップ 1 TACACS+ をイネーブルにします。
ステップ 2 必要であれば、TACACS+ のための CFS 配布機能をイネーブルにします。
ステップ 3 TACACS+ サーバと Cisco NX-OS デバイスの接続を確立します。
ステップ 4 TACACS+ サーバの秘密キーを設定します。
ステップ 5 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 6 （任意）TCP ポートを設定します。
ステップ 7 （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 8 （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。

関連トピック

TACACS+ のイネーブル化，（9 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なっています。 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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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。

	コマンドまたはアクション	目的
ステップ 2	**feature tacacs+** 例： `switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# 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+ 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。

（注） 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。

はじめる前に

TACACS+ をイネーブルにします。

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。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**] 例： `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。 単一の TACACS+ 接続を設定することでパフォーマンスを改善するには、**single-connection** オプションを使用します。通信が必要になるたびに、デバイスを開き、デーモンへの TCP 接続を閉じるのではなく、このオプションによって、デバイスとデーモン間の単一のオープンな接続を保守します。
ステップ 3	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 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	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ 設定の配布のイネーブル化，（42 ページ）
TACACS+ サーバ グループの設定，（15 ページ）

グローバル TACACS+ キーの設定

Cisco NX-OS デバイスで使用されるすべてのサーバ用の秘密 TACACS+ キーをグローバル レベルで設定できます。 秘密キーは、Cisco NX-OS デバイスと TACACS+ サーバ ホストのと間の共有秘密テキスト ストリングです。

（注） CFS ではグローバル TACACS+ キーを配布しません。 キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

はじめる前に

TACACS+ をイネーブルにします。

リモート TACACS+ サーバの秘密キーの値を取得します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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* 例： `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（**0**）の形式か、タイプ 6 暗号化（**6**）形式か、タイプ 7 暗号化（**7**）形式かを指定できます。 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 文字の長さまで指定可能です。 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**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。 （注） 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	**copy running-config startup-config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ 設定の配布のイネーブル化，（42 ページ）
AES パスワード暗号化およびマスター暗号キー

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。 秘密キーは、Cisco NX-OS デバイスと TACACS+ サーバ ホストとの間の共有秘密テキスト ストリングです。

（注） CFS では TACACS+ サーバのキーを配布しません。 キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

はじめる前に

TACACS+ をイネーブルにします。

リモート TACACS+ サーバの秘密キーの値を取得します。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. （任意） **show tacacs-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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* 例： `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（**0**）の形式か、タイプ 6 暗号化（**6**）形式か、タイプ 7 暗号化（**7**）形式かを指定できます。 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**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。 （注） 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	**copy running-config startup-config** 例： `switch# 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。

関連トピック

AES パスワード暗号化およびマスター暗号キー

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。

（注） CFS では TACACS+ サーバ グループの設定は配布しません。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
3. **aaa group server tacacs+** *group-name*
4. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
5. **exit**
6. （任意） **show tacacs-server groups**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
	
	例：
	`switch(config)# tacacs-server host 10.10.2.2`
	`switch(config-tacacs+)#`
		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。
		
		単一の TACACS+ 接続を設定することでパフォーマンスを改善するには、**single-connection** オプションを使用します。 通信が必要になるたびに、デバイスを開き、デーモンへの TCP 接続を閉じるのではなく、このオプションによって、デバイスとデーモン間の単一のオープンな接続を保守します。

ステップ 3	**aaa group server tacacs+** *group-name*
	
	例：
	`switch(config)# aaa group server tacacs+ TacServer`
	`switch(config-tacacs+)#`
		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。

ステップ 4	**server** {*ipv4-address* | *ipv6-address* | *host-name*} 例： `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 5	**exit**
	
	例：
	`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。

	コマンドまたはアクション	目的
ステップ 6	**show tacacs-server groups** 例： `switch(config)# 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 7	**copy running-config startup-config** 例： `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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
リモート AAA サービス
TACACS+ サーバ ホストの設定，（10 ページ）
TACACS+ デッド タイム間隔の設定，（29 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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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* 例： `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**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定情報を表示します。
ステップ 5	**copy running-config startup config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ サーバ グループの設定，（15 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）オプションをイネーブルにすることにより、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 デバイスは認証要求を、デフォルト AAA 認証方式に基づいて転送します。 このオプション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。ここで、*vrfname* は使用する VRF、*hostname* は設定された TACACS+ サーバの名前です。

（注） 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。

（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

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server directed-request**
3. （任意） **show tacacs+ {pending | pending-diff}**
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server directed-request**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** 例： `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。 デフォルトではディセーブルになっています。
ステップ 3	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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

	コマンドまたはアクション	目的
		適用して、TACACS+ 設定を他の NX-OS デバイスに配布します。

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

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

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ 設定の配布のイネーブル化，（42 ページ）

グローバルな TACACS+ タイムアウト間隔の設定

デバイスがすべての TACACS+ サーバからの応答を待つグローバルなタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。 タイムアウト間隔には、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。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. [Feature Selector] ペインで、[Security] > [AAA] > [Server Groups] を選択します。
2. [Summary] ペインで、デバイスをダブルクリックしてサーバ グループを表示します。
3. [Default TACACS Server Group] をクリックします。
4. [Details] ペインで、[Global Settings] タブをクリックします。
5. [Time out(secs)] フィールドに、タイムアウト間隔の秒数を入力します。
6. メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

手順の詳細

ステップ 1 [Feature Selector] ペインで、[Security] > [AAA] > [Server Groups] を選択します。

ステップ 2 [Summary] ペインで、デバイスをダブルクリックしてサーバ グループを表示します。

ステップ 3 [Default TACACS Server Group] をクリックします。

ステップ 4 [Details] ペインで、[Global Settings] タブをクリックします。

ステップ 5 [Time out(secs)] フィールドに、タイムアウト間隔の秒数を入力します。
デフォルトは 5 秒です。

ステップ 6 メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ 設定の配布のイネーブル化，（42 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 TACACS+ サーバからの応答を待つタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。 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。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout** *seconds*
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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*} **timeout** *seconds* 例： `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。 （注） 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	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 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	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

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

ステップ 6	**show tacacs-server** 例： `switch# 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 7	**copy running-config startup-config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ 設定の配布のイネーブル化，（42 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+ 要求に対しポート 49 を使用します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port*
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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。

	コマンドまたはアクション	目的
ステップ 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* 例： `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。有効な範囲は 1 ～ 65535 です。
ステップ 3	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ distribution pending`	（任意） 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	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ 設定の配布のイネーブル化，（42 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。

（注） 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+ サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。 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。

（注） テスト パラメータは、Cisco NX-OS Release 5.x 以降が稼動している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動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。

（注） 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。

（注） 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

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server 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. （任意） **show tacacs-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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*]]} 例： `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。 （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： `switch(config)# tacacs-server dead-time 5`	以前に応答の遅かった TACACS+ サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。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**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs-server** 例： `switch# show tacacs-server`	（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： `switch# 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。

関連トピック

各 TACACS+ サーバの定期モニタリングの設定, （26 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+ サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。 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。

（注） 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。

（注） 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。

（注） 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。

（注） テスト パラメータは、Cisco NX-OS Release 5.x が稼働している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。

はじめる前に

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。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-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. （任意） **show tacacs-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} 例： `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。 （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： `switch(config)# tacacs-server dead-time 5`	以前に応答の遅かった TACACS+ サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。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**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs-server** 例： `switch# show tacacs-server`	（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： `switch# 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。

関連トピック

TACACS+ サーバ ホストの設定，（10 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，（24 ページ）
TACACS+ 設定の配布のイネーブル化，（42 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 タイム間隔では、Cisco NX-OS デバイスが TACACS+ サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。

（注） 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。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server deadtime** *minutes*
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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* 例： `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	**show tacacs+** {**pending**	**pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 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 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の NX-OS デバイスに配布します。

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

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

関連トピック

TACACS+ 設定の配布のイネーブル化, （42 ページ）

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。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authentication login ascii-authentication**
3. （任意） **show tacacs+ {pending | pending-diff}**
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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** 例： `switch(config)# aaa authentication login ascii-authentication`	ASCII 認証をイネーブルにします。デフォルトはディセーブルです。
ステップ 3	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs-server** 例： `switch# 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 7	**copy running-config startup-config** 例： `switch# 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+ サーバでの AAA 許可の設定

TACACS+ サーバのデフォルトの AAA 許可方式を設定できます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 ssh-certificate default** {**group** *group-list* [**none**]	**local**	**none**}
			
			例：
			`switch(config)# aaa authorization ssh-certificate`
			`default group TACACSServer1 TACACSServer2`
				TACACS+ サーバのデフォルトの AAA 許可方式を設定します。
				
				ssh-certificate キーワードは、証明書認証を使用した TACACS+ 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。
				
				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。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local**

	コマンドまたはアクション	目的
		方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA 認証が使用されないように指定します。

ステップ 3	**exit**
	
	例：
	`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 4	**show aaa authorization** [**all**] 例： `switch# show aaa authorization`	（任意） AAA 許可設定を表示します。 **all** キーワードは、デフォルト値を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）

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。

注意 コマンド許可では、デフォルト ロールを含むユーザの Role-Based Authorization Control（RBAC; ロールベース許可コントロール）がディセーブルになります。

（注） Cisco NX-OS Release 4.x および 5.x の場合、コマンド許可は、非コンソール セッションだけに使用できます。 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。 Cisco NX-OS Release 6.0 以降では、コマンド許可は、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。

（注） 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。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} {**console** | **default**}
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show aaa authorization** [**all**]
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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**}
	
	例：
	`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 キーワードは、すべての EXEC コマンドの許可ソースを設定し、**config-commands** キーワードは、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します。
		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 データベースを使用します。

	コマンドまたはアクション	目的
		設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。 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。
ステップ 3	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	例：
	`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	**show aaa authorization** [**all**] 例： `switch(config)# show aaa authorization`	（任意） AAA 許可設定を表示します。 **all** キーワードは、デフォルト値を表示します。
ステップ 7	**copy running-config startup-config** 例： `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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ サーバでのコマンド許可のテスト，（36 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。

（注） 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。

（注） **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。

はじめる前に

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。

手順の概要

1. **test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**test aaa authorization command-type** {**commands** | **config-commands**} **user** *username* **command** *command-string* 例： `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。 （注） *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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ サーバでのコマンド許可の設定，（33 ページ）
ユーザ アカウントと 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セッションまたは別のユーザ名に対して、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イネーブルにしたり、ディセーブルにしたりできます。

（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。

手順の概要

1. **terminal verify-only** [**username** *username*]
2. **terminal no verify-only** [**username** *username*]

手順の詳細

	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： `switch# terminal no verify-only`	コマンド許可検証をディセーブルにします。

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、ロールベース アクセス コントロール（RBAC）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
14	vdc-admin 権限
13 ～ 1	• スタンドアロン ロール権限（**feature privilege** コマンドがディセーブルの場合）。 • 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** コマンドがイネーブルの場合）。
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。

（注） **feature privilege** コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

（注） 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。 次の URL から入手できるマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html

手順の概要

1. **configure terminal**
2. [**no**] **feature privilege**
3. [**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**]
4. [**no**] **username** *username* **priv-lvl** *n*
5. （任意） **show privilege**
6. （任意） **copy running-config startup-config**
7. **exit**
8. **enable** *level*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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 privilege** 例： `switch(config)# feature privilege`	ロールの累積権限をイネーブルまたはディセーブルにします。 **enable** コマンドは、この機能をイネーブルにした場合しか表示されません。 デフォルトはディセーブルです。
ステップ 3	[**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**] 例： `switch(config)# enable secret 5 def456 priv-lvl 15`	特定の特権レベルのシークレット パスワードをイネーブルまたはディセーブルにします。 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。 デフォルトはディセーブルです。 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。 （注） シークレット パスワードをイネーブルにするには、**feature privilege** コマンドを入力してロールの累積権限をイネーブルにする必要があります。
ステップ 4	[**no**] **username** *username* **priv-lvl** *n* 例： `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イネーブルまたはディセーブルにします。 デフォルトはディセーブルです。 **priv-lvl** キーワードはユーザに割り当てる権限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	**show privilege** 例： `switch(config)# show privilege`	（任意） 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。
ステップ 6	**copy running-config startup-config** 例： `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。

	コマンドまたはアクション	目的

ステップ 7	**exit**
	
	例：
	`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* 例： `switch# enable 15`	上位の特権レベルへのユーザの昇格をイネーブルにします。 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。

関連トピック

権限ロールのユーザ コマンドの許可または拒否, （40 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**。

手順の概要

1. **configure terminal**
2. [**no**] **role name priv-***n*
3. **rule** *number* {**deny** | **permit**} **command** *command-string*
4. **exit**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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**] **role name priv-***n*
	
	例：
	`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* 例： `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 つの規則を持っている場合、規則 3 が規則 2 よりも前に適用され、規則 2 は規則 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。 （注） 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**
	
	例：
	`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	**copy running-config startup-config**
	
	例：
	`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。

関連トピック

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，（37 ページ）
ユーザ ロールおよびルールの作成

TACACS+ 設定の配布のイネーブル化

設定の配布がイネーブルになっている Cisco NX-OS デバイスだけが、CFS 領域内での TACACS+ 設定配布の変更に参加できます。

はじめる前に

CFS 配布がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **tacacs+ distribute**
3. **exit**
4. （任意） **show tacacs+ status**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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+ distribute** 例： `switch(config)# tacacs+ distribute`	TACACS+ 設定の配布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：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**show tacacs+ status** 例： `switch(config)# show tacacs+ status`	（任意） TACACS+ の CFS による配布の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# 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。

関連トピック

TACACS+ のイネーブル化，（9 ページ）
TACACS+ サーバ ホストの設定，（10 ページ）
TACACS+ サーバの設定プロセス，（9 ページ）
TACACS+ サーバ グループの設定，（15 ページ）

TACACS+ 設定の配布のコミット

一時バッファに保存されている TACACS+ のグローバル設定およびサーバ設定を、ファブリック内のすべての Cisco NX-OS デバイス（元のデバイスを含む）の実行コンフィギュレーションに適用します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show tacacs+ {pending | pending-diff}**
3. **tacacs+ commit**
4. **exit**
5. （任意） **show tacacs+ distribution status**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 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 3	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、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て、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs+ distribution status** 例： `switch(config)# show tacacs+ distribution status`	（任意） TACACS+ の配布の設定とステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# 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適用します。

関連トピック

TACACS+ 設定の配布のイネーブル化, （42 ページ）

TACACS+ の配布セッションの廃棄

TACACS+ の設定変更の一時データベースを廃棄して、CFS 配布セッションを終了します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show tacacs+ {pending | pending-diff}**
3. **tacacs+ abort**
4. **exit**
5. （任意） **show tacacs+ distribution status**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 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 3	**tacacs+ abort** 例： `switch(config)# tacacs+ abort`	一時ストレージにある TACACS+設定を廃棄して、セッションを終了します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		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	**show tacacs+ distribution status** 例： `switch(config)# show tacacs+ distribution status`	（任意） TACACS+ の配布の設定とステータスを表示します。

関連トピック

TACACS+ 設定の配布のイネーブル化, （42 ページ）

TACACS+ の配布セッションのクリア

アクティブな CFS 配布セッションをクリアして、ネットワーク内の TACACS+ 設定のロックを解除します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **clear tacacs+ session**
2. （任意） **show tacacs+ distribution status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear tacacs+ session** 例： `switch# clear tacacs+ session`	TACACS+ のための CFS セッションをクリアして、ファブリックのロックを解除します。
ステップ 2	**show tacacs+ distribution status** 例： `switch(config)# show tacacs+ distribution status`	（任意） TACACS+ の配布の設定とステータスを表示します。

関連トピック

TACACS+ 設定の配布のイネーブル化，（42 ページ）

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。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. **test aaa group** *group-name username password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password* 例： `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* 例： `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。

関連トピック

TACACS+ サーバ ホストの設定, （10 ページ）
TACACS+ サーバ グループの設定, （15 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。

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. **configure terminal**
2. **no feature tacacs+**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`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+** 例： `switch(config)# no feature tacacs+`	TACACS+ をディセーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# 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+ 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リングできます。

はじめる前に

Cisco NX-OS デバイスに TACACS+ サーバを設定します。

手順の概要

1. **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show tacacs-server statistics 10.10.1.1`	TACACS+ 統計情報を表示します。

関連トピック

TACACS+ サーバ ホストの設定，（10 ページ）
TACACS+ サーバ統計情報のクリア，（48 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。

はじめる前に

Cisco NX-OS デバイスに TACACS+ サーバを設定します。

手順の概要

1. （任意） **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. **clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show tacacs-server statistics 10.10.1.1`	（任意） Cisco NX-OS デバイスでの 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*} 例： `switch# clear tacacs-server statistics 10.10.1.1`	TACACS+ サーバ統計情報をクリアします。

関連トピック

TACACS+ サーバ ホストの設定, （10 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。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

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** コマンドを入力した後、ユーザは、**enable secret** コマンドを使用して管理者によって設定されたパスワードを入力するよう求められます。 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 ©) 2002-2009, 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 ©) 2002-2009, 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による **pwd** コマンドの実行を許可する例を示します。

```
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による **show running-config** コマンドを拒否する例を示します。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	参照先
Cisco NX-OS のライセンス	*Cisco NX-OS* ライセンス ガイド
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

関連項目	参照先
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能では、新規の標準がサポートされることも、一部変更された標準がサポートされることもありません。また、既存の標準に対するサポートが変更されることもありません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	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。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

TACACS+ 機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *2* : ***TACACS+*** 機能の履歴

機能名	リリース	機能情報
TACACS+	6.2(2)	単一の TACACS+ 接続のサポートが追加されました。
TACACS+	6.0(1)	コンソール セッションのコマンド許可を設定する機能が追加されました。
TACACS+	5.2(1)	TACACS+ サーバ キーのタイプ 6 暗号化が追加されました。

機能名	リリース	機能情報
TACACS+	5.1(1)	Release 5.0 以降、変更はありません。
TACACS+ の特権レベルの許可	5.0(2)	Cisco NX-OS デバイスでローカルに設定されたユーザ ロールに対して、TACACS+ サーバでユーザ用に設定された特権レベルのマッピングをサポートするようになりました。
権限ロール	5.0(2)	権限ロールのユーザ コマンドの許可または拒否のサポートが追加されました。
定期サーバ モニタリング	5.0(2)	TACACS+ サーバのグローバルな定期モニタリングのサポートが追加されました。
AAA 許可	5.0(2)	TACACS+ サーバのデフォルトの AAA 許可方式の設定のサポートが追加されました。