



## RADIUS の設定

---

この章の内容は、次のとおりです。

- [RADIUS の設定, 1 ページ](#)

## RADIUS の設定

### RADIUS について

Remote Access Dial-In User Service (RADIUS) 分散クライアント/サーバシステムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントは Cisco Nexus 5000 シリーズ スイッチで稼働し、すべてのユーザ認証情報およびネットワーク サービスアクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウントング要求を送信します。

### RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモートユーザのネットワークアクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセスセキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク  
たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。

RADIUS を使用した Cisco Nexus 5000 シリーズ スイッチをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。

- リソース アカウンティングが必要なネットワーク。

RADIUS アカウンティングは、RADIUS 認証または RADIUS 許可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネットサービスプロバイダー（ISP）は、RADIUS アクセスコントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。

- 認証プロファイルをサポートするネットワーク

ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルを設定アップできます。ユーザごとのプロファイルにより、Nexus 5000 シリーズスイッチは、既存の RADIUS ソリューションを使用してポートを管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル アグリーメントを提供できます。

## RADIUS の操作について

ユーザがログインを試行し、RADIUS を使用して Cisco Nexus 5000 シリーズスイッチに対する認証を行う際には、次のプロセスが実行されます。

- 1 ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
- 2 ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
- 3 ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
  - ACCEPT : ユーザが認証されたことを表します。
  - REJECT : ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
  - CHALLENGE : RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。
  - CHANGE PASSWORD : RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

ACCEPT または REJECT 応答には、EXEC またはネットワーク認可に使用される追加データが含まれています。RADIUS 許可を使用するには、まず RADIUS 認証を完了する必要があります。

ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

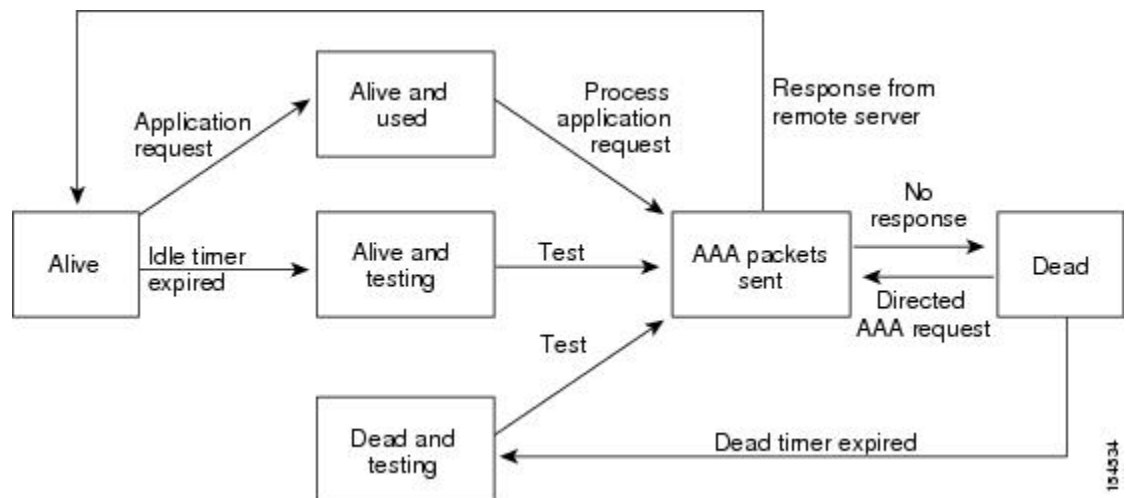
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカルエリアトランスポート）接続、PPP（ポイントツーポイントプロトコル）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセスリスト、ユーザタイムアウト）

## RADIUS サーバ モニタリング

応答を返さないRADIUS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、定期的にRADIUSサーバをモニタリングし、RADIUSサーバが応答を返す（アライブ）かどうかを調べるよう、スイッチを設定できます。スイッチは、応答を返さないRADIUSサーバをデッド（dead）としてマークし、デッドRADIUSサーバにはAAA要求を送信しません。また、定期的にデッドRADIUS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。このプロセスにより、RADIUSサーバが稼働状態であることを確認してから、実際のAAA要求がサーバに送信されます。RADIUS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、スイッチによって、障害が発生したことを知らせるエラーメッセージが表示されます。

次の図には、さまざまなRADIUSサーバの状態を示します。

図 1: RADIUS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。RADIUSサーバモニタリングを実行するには、テスト認証要求をRADIUSサーバに送信します。

## ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワークアクセスサーバとRADIUSサーバの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成しています。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RADIUS実装は、この仕様で推奨される形式を使用して、1つのベンダー固有オプションを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 *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号 (=) で、アスタリスク (\*) は任意属性を示します。

Cisco Nexus 5000 シリーズ スイッチでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。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 Nexus 5000 シリーズ スイッチ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ます。
- **Accounting** : `accounting-request` パケットで使用されます。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 Nexus 5000 シリーズ スイッチは、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。
- **accountinginfo** : 標準の RADIUS アカウンティングプロトコルで処理される属性に加えて、アカウンティング情報が格納されます。この属性は、スイッチ上の RADIUS クライアントからの `Account-Request` フレームの VSA 部分だけに送信されます。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。

## RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6 アドレスまたはホスト名を取得こと。
- RADIUS サーバから事前共有キーを取得すること。
- Cisco Nexus 5000 シリーズ スイッチが、AAA サーバの RADIUS クライアントとして設定されていること。

## RADIUS の注意事項と制約事項

RADIUS 設定時の注意事項と制限事項は次のとおりです。

- Cisco Nexus 5000 シリーズ スイッチ上に設定できる RADIUS サーバの最大数は 64 です。

## RADIUS サーバの設定

ここでは、RADIUS サーバの設定方法について説明します。

### 手順

- 
- ステップ 1** Cisco Nexus 5000 シリーズ スイッチと RADIUS サーバとの接続を確立します。
- ステップ 2** RADIUS サーバの事前共有秘密キーを設定します。
- ステップ 3** 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバグループを設定します。
- ステップ 4** 必要に応じて、次のオプションのパラメータを設定します。
- デッドタイム間隔
  - ログイン時に RADIUS サーバの指定を許可
  - 送信リトライ回数とタイムアウト間隔
  - アカウンティングおよび認証属性
- ステップ 5** 必要に応じて、定期的に RADIUS サーバをモニタリングするよう設定します。
- 

## RADIUS サーバホストの設定

認証に使用する各 RADIUS サーバについて、IP アドレス (IPv4 または IPv6)、あるいはホスト名を設定する必要があります。すべての RADIUS サーバホストは、デフォルトの RADIUS サーバグループに追加されます。最大 64 の RADIUS サーバを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> }	RADIUS サーバの IPv4 または IPv6 アドレス、またはホスト名を指定します。
ステップ 3	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、RADIUS サーバとしてホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS のグローバルな事前共有キーの設定

Cisco Nexus 5000 シリーズ 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 レベルで事前共有キーを設定できます。事前共有キーとは、スイッチと RADIUS サーバホスト間の共有秘密テキストストリングです。

### はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>radius-server key [0   7]</b> <i>key-value</i>	すべての RADIUS サーバで使用する事前共有キーを指定します。クリア テキスト形式 (0) または暗号化形式 (7) の事前共有キーを指定できます。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、事前共有キーは設定されません。
ステップ 3	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS 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
		(注) 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、 <b>show running-config</b> コマンドを使用します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、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事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS サーバの事前共有キーの設定

事前共有キーとは、Cisco Nexus デバイスと RADIUS サーバホスト間の共有秘密テキストストリングです。

### はじめる前に

リモートの RADIUS サーバの事前共有キー値を取得していること。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>key</b> [0   7] <i>key-value</i>	特定の RADIUS サーバの事前共有キーを指定します。クリアテキスト形式 (0) または暗号化形式 (7) の事前共有キーを指定できます。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。  この事前共有キーがグローバル事前共有キーの代わりに使用されます。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。  (注) 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、 <b>show running-config</b> コマンドを使用します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、RADIUS 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

## RADIUS 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 サーバによる認証を指定できます。グループのメンバーはすべて、RADIUS 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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch (config)# <b>aaa group server radius group-name</b>	RADIUS サーバグループを作成し、そのグループの RADIUS サーバグループ コンフィギュレーション サブモードを開始します。  <i>group-name</i> 引数は、最大 127 文字の英数字のストリングで、大文字小文字が区別されます。
ステップ 3	switch (config-radius)# <b>server {ipv4-address   ipv6-address   server-name}</b>	RADIUS サーバを、RADIUS サーバグループのメンバーとして設定します。



	コマンドまたはアクション	目的
		指定した RADIUS サーバが見つからない場合は、 <b>radius-server host</b> コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	<code>switch (config-radius)# deadtime minutes</code>	(任意) モニタリング 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 1 ~ 1440 です。  (注) RADIUS サーバグループのデッドタイム間隔が 0 より大きい場合は、この値がグローバルなデッドタイム値より優先されます。
ステップ 5	<code>switch(config-radius)# source-interface interface</code>	(任意) 特定の RADIUS サーバグループに発信元インターフェイスを割り当てます。  サポートされているインターフェイスのタイプは管理および VLAN です。  (注) <b>source-interface</b> コマンドを使用して、 <b>ip radius source-interface</b> コマンドによって割り当てられたグローバルソースインターフェイスを上書きします。
ステップ 6	<code>switch(config-radius)# exit</code>	コンフィギュレーション モードを終了します。
ステップ 7	<code>switch(config)# show radius-server group [group-name]</code>	(任意) RADIUS サーバグループの設定を表示します。
ステップ 8	<code>switch(config)# copy running-config startup-config</code>	(任意) リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、RADIUS サーバグループを設定する例を示します。

```
switch# configure terminal
switch (config)# aaa group server radius RadServer
switch (config-radius)# server 10.10.1.1
switch (config-radius)# deadtime 30
switch (config-radius)# use-vrf management
switch (config-radius)# exit
switch (config)# show radius-server group
switch (config)# copy running-config startup-config
```

### 次の作業

AAA サービスに RADIUS サーバグループを適用します。

## RADIUS 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

RADIUS サーバグループにアクセスする際に使用する、RADIUS 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 RADIUS 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。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>ip radius source-interface interface</b>	このデバイスで設定されているすべての RADIUS 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。発信元インターフェイスは、管理または VLAN インターフェイスにすることができます。
ステップ 3	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定情報を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(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。

次に、RADIUS サーバグループのグローバル発信元インターフェイスとして、`mgmt 0` インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip radius source-interface mgmt 0
switch(config)# exit
switch# copy running-config startup-config
```

## ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時にユーザによる RADIUS サーバの指定を許可できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>radius-server directed-request</b>	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。デフォルトはディセーブルです。
ステップ 3	switch(config)# <b>exit</b>	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	switch# <b>show radius-server directed-request</b>	(任意) directed request の設定を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(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。

次に、ネットワークにログインしたときに、ユーザが RADIUS サーバを選択できるようにする例を示します。

```
switch# configure terminal
switch(config)# radius-server directed-request
switch# exit
switch# copy running-config startup-config
```

## グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。デフォルトでは、スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔は、Cisco Nexus 5000 シリーズスイッチがタイムアウトエラーを宣言する前に、RADIUS サーバからの応答を待機する時間を決定します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>radius-server retransmit count</b>	すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ~ 5 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# <b>radius-server timeout seconds</b>	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ~ 60 秒です。
ステップ 4	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。
ステップ 6	switch# <b>copy running-config startup-config</b>	(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。

次に、RADIUS サーバで、リトライ回数を 3、伝送タイムアウト間隔を 5 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server retransmit 3
switch(config)# radius-server timeout 5
switch(config)# exit
switch# copy running-config startup-config
```

## サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

デフォルトでは、Cisco Nexus スイッチはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。スイッチが、タイムアウトエラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# <b>radius-server host {ipv4-address   ipv6-address   host-name} retransmit count</b>	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。  (注) 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	switch(config)# <b>radius-server host {ipv4-address   ipv6-address   host-name} timeout seconds</b>	特定のサーバの送信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。

	コマンドまたはアクション	目的
		(注) 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS 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 4	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。
ステップ 6	switch# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、RADIUS ホストサーバ server1 で、RADIUS 送信リトライ回数を 3、タイムアウト間隔を 10 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# copy running-config startup-config
```

## RADIUS サーバのアカウントिंगおよび認証属性の設定

RADIUS サーバをアカウントング専用、または認証専用に指定できます。デフォルトでは、RADIUS サーバはアカウントングと認証の両方に使用されます。RADIUS のアカウントングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>acct-port udp-port</b>	(任意) RADIUS アカウントングのメッセージに使用する UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。  指定できる範囲は 0 ~ 65535 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>accounting</b>	(任意) 特定の RADIUS サーバをアカウントング用のみ使用することを指定します。デフォルトでは、アカウントングと認証の両方に使用されます。
ステップ 4	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>auth-port</b> <i>udp-port</i>	(任意) RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。 指定できる範囲は 0 ~ 65535 です。
ステップ 5	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>authentication</b>	(任意) 特定の RADIUS サーバを認証用のみ使用することを指定します。デフォルトでは、アカウントングと認証の両方に使用されます。
ステップ 6	switch(config)# <b>exit</b>	コンフィギュレーションモードを終了します。
ステップ 7	switch(config)# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。
ステップ 8	switch(config)# <b>copy</b> <b>running-config startup-config</b>	リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、RADIUS サーバのアカウントング属性と認証属性を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch # exit
switch # copy running-config startup-config
switch #
```

## RADIUS サーバの定期的モニタリングの設定

RADIUS サーバの可用性をモニタリングできます。パラメータとして、サーバに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があります。アイドルタイマーには、RADIUS 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スイッチ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することで、サーバを定期的にテストできます。



(注) セキュリティ上の理由から、RADIUS データベース内の既存のユーザ名と同じテスト ユーザ名を設定しないことを推奨します。

テストアイドルタイマーには、RADIUS 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スイッチがテスト パケットを送信するかを指定します。

デフォルトのアイドル タイマー値は 0 分です。アイドル時間間隔が 0 分の場合、スイッチは RADIUS サーバの定期的なモニタリングを実行しません。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>test</b> { <b>idle-time</b> <i>minutes</i>   <b>password</b> <i>password</i> [ <b>idle-time</b> <i>minutes</i> ]   <b>username</b> <i>name</i> [ <b>password</b> <i>password</i> [ <b>idle-time</b> <i>minutes</i> ]]}	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 <b>test</b> 、デフォルトのパスワードは <b>test</b> です。 デフォルトのアイドル タイマー値は 0 分です。指定できる範囲は、0 ~ 1440 分です。  (注) RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# <b>radius-server deadtime</b> <i>minutes</i>	スイッチが、前回応答しなかった RADIUS 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。指定できる範囲は 1 ~ 1440 分です。
ステップ 4	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。
ステップ 6	switch# <b>copy running-config startup-config</b>	(任意) リブートおよびリスタート時に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て、変更を永続的に保存します。

次に、ユーザ名 (user1) およびパスワード (Ur2Gd2BH) と、3 分のアイドル タイマーおよび 5 分のデッドタイムで、RADIUS サーバ ホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time
3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

## デッドタイム間隔の設定

すべての RADIUS 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 Nexus 5000 シリーズ スイッチが RADIUS 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。デフォルト値は 0 分です。



(注) デッドタイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デッドとしてマークされません。RADIUS サーバグループに対するデッドタイム間隔を設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>radius-server deadtime</b>	デッドタイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ~ 1440 分です。
ステップ 3	switch(config)# <b>exit</b>	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	switch# <b>show radius-server</b>	(任意) RADIUS サーバの設定を表示します。
ステップ 5	switch# <b>copy running-config startup-config</b>	(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。

次に、RADIUS サーバに 5 分間のデッドタイムを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```



## RADIUS サーバまたはサーバグループの手動モニタリング

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>test aaa server radius</b> {ipv4-address   ipv6-address   server-name} [vrf vrf-name] <b>username password test aaa server radius</b> {ipv4-address   ipv6-address   server-name} [vrf vrf-name] <b>username password</b>	RADIUS 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	switch# <b>test aaa group group-name username password</b>	RADIUS 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。

次に、可用性を確認するために、RADIUS サーバとサーバグループにテストメッセージを送信する例を示します。

```
switch# test aaa server radius 10.10.1.1 user 1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

## RADIUS 設定の確認

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>show running-config radius [all]</b>	実行コンフィギュレーションの RADIUS 設定を表示します。
ステップ 2	switch# <b>show startup-config radius</b>	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
ステップ 3	switch# <b>show radius-server</b> [server-name   ipv4-address   ipv6-address] [directed-request   groups   sorted   statistics]	設定済みのすべての RADIUS サーバのパラメータを表示します。

## RADIUS サーバ統計情報の表示

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>show radius-server statistics</b> {hostname   ipv4-address   ipv6-address}	RADIUS 統計情報を表示します。

## RADIUS 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 RADIUS 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 RADIUS サーバを設定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	switch# <b>show radius-server statistics</b> {hostname   ipv4-address   ipv6-address}	(任意) Cisco NX-OS デバイスでの RADIUS サーバ統計情報を表示します。
ステップ 2	switch# <b>clear radius-server statistics</b> {hostname   ipv4-address   ipv6-address}	RADIUS サーバ統計情報をクリアします。

## RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhT1" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)# use-vrf management
```

## RADIUS のデフォルト設定

次の表に、RADIUS パラメータのデフォルト設定を示します。

表 1: デフォルトの RADIUS パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウントिंग
デッドタイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	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

