RADIUS の設定

この章の内容は、次のとおりです。

- RADIUS について，1 ページ
- RADIUS の前提条件，5 ページ
- 注意事項と制限事項，5 ページ
- デフォルト設定，5 ページ
- RADIUS サーバの設定，6 ページ
- RADIUS 設定の確認，20 ページ
- RADIUS サーバ統計情報の表示，20 ページ
- RADIUS の設定例，20 ページ
- RADIUS の機能の履歴，21 ページ

RADIUS について

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 NX-OS デバイス上で稼働します。認証要求とアカウンティング要求は、すべてのユーザ認証情報とネットワーク サービスアクセス情報が格納されている中央の RADIUS サーバに送信されます。

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 機能を持つ Cisco NX-OS デバイス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セットアップできます。 ユーザ単位のプロファイルにより、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービス レベル契約を提供できるようになります。

RADIUS の動作

RADIUS を使用する NX-OS デバイスにユーザがログインおよび認証を試みると、次の処理が行われます。

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許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。

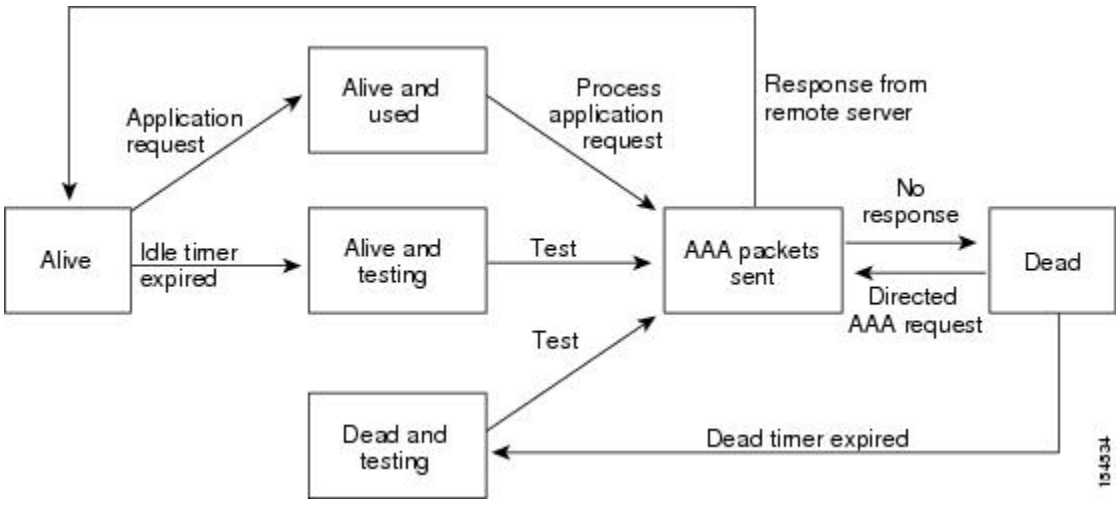
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカル エリア トランスポート）接続、PPP（ポイントツーポイントプロトコル）、シリアルライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

RADIUS サーバ モニタリング

応答しない RADIUS サーバがあると、AAA 要求の処理が遅れることがあります。 AAA 要求の処理時間を短縮するために、RADIUS サーバを定期的にモニタして RADIUS 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。 応答しない RADIUS サーバはデッド（dead）としてマークされ、AAA 要求は送信されません。 デッド RADIUS サーバは定期的にモニタされ、応答があればアライブ状態に戻されます。 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、RADIUS サーバが稼働状態であることを確認します。 RADIUS 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、障害が発生していることを示すエラー メッセージが表示されます。

（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。

図 *1*：*RADIUS* サーバの状態



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 *
```

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。

認証に RADIUS サーバを使用した場合、RADIUS プロトコルでは RADIUS サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。 この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが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。

次の属性がサポートされます。

- 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、ユーザが属しているロールが network-operator と vdc-admin ならば、値フィールドは「network-operator vdc-admin」となります。この属性は、RADIUS サーバから送信される Access-Accept フレームの VSA 部分に格納されます。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 Access Control System（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"
  ```

  次に、FreeRADIUS でサポートされるロール属性の例を示します。

  ```
  Cisco-AVPair = "shell:roles=\"network-operator vdc-admin\""
  ```

  ```
  Cisco-AVPair = "shell:roles*\"network-operator vdc-admin\""
  ```

  Cisco ACS を使用していて、Cisco Nexus 1000V 認証と Cisco UCS 認証の両方に同じ ACS グループを使用する場合は、次のロール属性を使用します。

  ```
  cisco-av-pair*shell:roles="network-admin admin"
  ```

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

RADIUS の前提条件

- RADIUS サーバの IP アドレスまたはホスト名がわかっていること。
- ネットワーク内での RADIUS 通信を保護するために使用されるキーがわかっていること。
- デバイスが AAA サーバの RADIUS クライアントとして設定されていること。

注意事項と制限事項

最大 64 の RADIUS サーバを設定できます。

デフォルト設定

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	認証とアカウンティング
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

RADIUS サーバの設定

RADIUS サーバ ホストの設定

認証に使用される各 RADIUS サーバの IP アドレスまたはホスト名を設定するには、次の手順を実行します。 次の情報を知っている必要があります。

- 最大 64 の RADIUS サーバを設定できます。
- すべての RADIUS サーバ ホストは自動的にデフォルトの RADIUS サーバ グループに追加されます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** {*ipv4-address* | *host-name*}	RADIUS サーバの IP アドレスまたはホスト名、または RADIUS サーバのドメイン ネーム サーバ（DNS）名を定義します。 ホスト名は英数字（大文字と小文字を区別）で、最大文字数は 256 です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	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。

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

RADIUS グローバル キーの設定

この手順を使用して、すべての RADIUS サーバが Cisco Nexus 1000V での認証に使用するキーを設定します。

RADIUS サーバ認証に使用されるグローバル キーを知っている必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server key** [**0** | **7**]*key-value*	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)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（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、show running-config コマンドを使用します。
ステップ 5	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。

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

RADIUS サーバ キーの設定

単一の RADIUS サーバ ホストのキーを設定するには、次の手順を実行します。

リモート RADIUS ホストで使用されるキーを取得している必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	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 文字です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（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、show running-config コマンドを使用します。
ステップ 5	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。

```
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

メンバー サーバが認証機能を共有する RADIUS サーバ グループを設定するには、次の手順を実行します。

グループ内のサーバへのアクセスは、サーバを設定した順番で行われます。

はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- RADIUS サーバ グループ内のすべてのサーバが、同じ RADIUS プロトコルに属しています。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **aaa group server radius** *group-name*	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 モードを開始します。 group-name 引数は、最大 127 文字の長さ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)# **server** {*ipv4-address* | *server-name*}	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。 **ヒント** 指定した RADIUS サーバが見つからない場合は、radius-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 4	switch(config-radius)# **deadtime** *minutes*	（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	switch(config-radius)# **use-vrf** *vrf-name*	（任意） サーバ グループ内のサーバとの接続に使用する VRF を指定します。
ステップ 6	switch(config-radius)# **source-interface** {*interface-type*} {*interface-number*}	（任意） RADIUS サーバに到達するために使用される送信元インターフェイスを指定します。 インターフェイス タイプおよびインターフェイス番号は、次のように定義されています。 • loopback = 0 ～ 1023 の仮想インターフェイス番号

	コマンドまたはアクション	目的
		• mgmt = 管理インターフェイス 0 • null = ヌル インターフェイス 0 • port-channel = 1 ～ 4096 のポート チャネル番号
ステップ 7	switch(config-radius)# **show radius-server groups** [*group-name*]	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 8	switch(config-radius)# **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。

```
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 vrf1
switch(config-radius)# source-interface mgmt0
switch(config-radius)# show radius-server group
total number of groups:2

following RADIUS server groups are configured:
        group Radserver:
                server: 10.10.1.1
                deadtime is 30
        group test:
                deadtime is 30
switch(config-radius)# copy running-config startup-config
```

RADIUS サーバの誘導要求のイネーブル化

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することができます。 これは、誘導要求と呼ばれます。

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* は使用するルーティングおよび転送（VRF）、*hostname* は設定された RADIUS サーバの名前です。

デフォルトでは、誘導要求はディセーブルです。

（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

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server directed-request**	誘導要求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	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch(config)# **show radius-server directed-request**	（任意） directed request の設定を表示します。
ステップ 5	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。

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

すべての RADIUS サーバのグローバル タイムアウトの設定

ここでは、RADIUS サーバからの応答を待つ時間を指定するグローバル タイムアウト間隔の設定手順を説明します。この時間が経過すると、タイムアウト障害となります。

「単一RADIUSサーバのタイムアウト間隔の設定」で指定したタイムアウトは、RADIUSのグローバル タイムアウトに優先します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server timeout** *seconds*	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 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 3	switch(config-radius)# **exit**	EXEC モードに戻ります。
ステップ 4	switch(config-radius)# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch(config-radius)# **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。

```
switch# configure terminal
switch(config)# n1000v(config)# radius-server timeout 101
switch(config-radius)# exit
switch(config-radius)# show radius-server
switch(config-radius)# copy running-config startup-config
```

すべての RADIUS サーバのグローバル リトライ回数の設定

ローカル認証に切り換える前に RADIUS サーバへの送信を再試行する最大回数を設定するには、次の手順を実行します。この設定はすべての RADIUS サーバに適用されます。

デフォルトでは、ローカル認証に切り換える前に、RADIUS サーバへの再送信を 1 回だけ試行します。

リトライ回数は最大 5 回まで増やすことができます。

「単一 RADIUS サーバのリトライ回数の設定」で単一の RADIUS サーバに指定したリトライ回数は、このグローバル設定よりも優先されます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server retransmit***count*	ローカル認証に切り換える前に許可する再送信回数を定義します。 このグローバル設定はすべての RADIUS サーバに適用されます。 デフォル

	コマンドまたはアクション	目的
		トの再送信回数は 1 です。有効な範囲は 0 ～ 5 です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	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。

```
switch# configure terminal
switch(config)# radius-server retransmit 31
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

単一 RADIUS サーバのタイムアウト間隔の設定

ここでは、RADIUS サーバからの応答を待つ時間を設定する手順を説明します。この時間が経過すると、タイムアウト障害となります。

単一の RADIUS サーバに指定したタイムアウトは、「すべての RADIUS サーバのグローバル タイムアウトの設定」の項で定義したタイムアウトに優先します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** { *ipv4-address* | *host-name* } **timeout** *seconds*	特定のサーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。 （注） 単一の RADIUS サーバに指定したタイムアウトは、RADIUS のグローバル タイムアウトに優先します。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	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。

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

単一 RADIUS サーバのリトライ回数の設定

ローカル認証に切り換える前に RADIUS サーバへの送信を再試行する最大回数を設定するには、次の手順を実行します。この設定は単一の RADIUS サーバに適用され、グローバル リトライ回数に優先します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

次のことを知っている必要があります。

- デフォルトでは、ローカル認証に切り換える前に、RADIUS サーバへの再送信を 1 回だけ試行します。
- リトライ回数は最大 5 回まで増やすことができます。
- 単一の RADIUS サーバに指定したリトライ回数は、すべての RADIUS サーバ用に作成されるグローバル設定に優先します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** {*ipv4-address* |*host-name*} **retransmit** *count*	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） この単一 RADIUS サーバの再送信回数は、すべての RADIUS サーバ用のグローバル設定に優先します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	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。

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

RADIUS アカウンティング サーバの設定

アカウンティング機能を実行するサーバを設定するには、次の手順を実行します。

デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。

はじめる前に

この手順を開始する前に

- EXEC モードで CLI にログインする必要があります。
- RADIUS アカウンティング メッセージの宛先 UDP ポート番号を知っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*	（任意） 特定のホストに RADIUS アカウンティング メッセージを受信する UDP ポートを関連付けます。デフォルトの UDP ポートは 1812 です。 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)# **radius-server host** {*ipv4-address* | *host-name*} **accounting**	（任意） 特定の RADIUS ホストをアカウンティング サーバとして指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	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。

```
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)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS 認証サーバの設定

認証機能を実行するサーバを設定するには、次の手順を実行します。

デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。

はじめる前に

この手順を開始する前に

- EXEC モードで CLI にログインする必要があります。
- RADIUS 認証メッセージの宛先 UDP ポート番号を知っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** {*ipv4-address* | *hostname*} **auth-port** *udp-port*	（任意） 特定のホストに RADIUS 認証メッセージを受信する UDP ポートを関連付けます。 デフォル

	コマンドまたはアクション	目的
		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 3	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **authentication**	（任意） 特定の RADIUS ホストを認証サーバとして指定します。 デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	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。

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

RADIUS サーバの定期的モニタリングの設定

RADIUS サーバのモニタリングを設定するには、次の手順を実行します。

テスト アイドル タイマーには、応答しない RADIUS サーバにテスト パケットが送信されるまでの経過時間を指定します。

デフォルトのアイドル タイマー値は 0 分です。 アイドル時間の間隔が 0 分の場合、Cisco NX-OS デバイスは RADIUS サーバの定期モニタリングを実行しません。

（注） セキュリティ上の理由から、RADIUS データベースに存在するユーザ名をテスト ユーザ名として設定しないでください。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time***minutes*]]}	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。 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)# **radius-server dead-time** *minutes*	デッドと宣言された RADIUS サーバにテスト パケットを送信するまで待機する分数を指定します。 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)# **exit**	EXEC モードに戻ります。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	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。

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

グローバル デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定するには、次の手順を実行します。 デッド タイム間隔には、RADIUS サーバをデッドであると宣言したあと、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待機する時間を指定します。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、デット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。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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)# **radius-server deadtime** *minutes*	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)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	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。

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# show radius-server
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

RADIUS サーバまたはサーバ グループにテスト メッセージを手動で送信するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password*	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(config)# **test aaa group** *group-name username password*	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。

```
switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

RADIUS 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	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。
show radius-server [*server-name* | *ipv4-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

RADIUS サーバのアクティビティに関する統計情報を表示するには、次のコマンドを使用します。

show radius-server statistics { *hostname* | *ipv4-address* }

RADIUS の設定例

次に、グローバル RADIUS キーと RADIUS サーバ ホスト キー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 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
    server 10.10.1.1
```

RADIUS の機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
RADIUS	4.0(4)SV1(1)	この機能が導入されました。