



## RADIUS の設定

---

この章では、Cisco NX-OS デバイスで Remote Access Dial-In User Service (RADIUS) 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。

- [RADIUS について, 1 ページ](#)
- [RADIUS のライセンス要件, 6 ページ](#)
- [RADIUS の前提条件, 7 ページ](#)
- [RADIUS の注意事項と制約事項, 7 ページ](#)
- [RADIUS のデフォルト設定, 7 ページ](#)
- [RADIUS サーバの設定, 8 ページ](#)
- [RADIUS 設定の確認, 34 ページ](#)
- [RADIUS サーバのモニタリング, 35 ページ](#)
- [RADIUS サーバ統計情報のクリア, 35 ページ](#)
- [RADIUS の設定例, 36 ページ](#)
- [次の作業, 36 ページ](#)
- [RADIUS に関する追加情報, 36 ページ](#)
- [RADIUS の機能の履歴, 37 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トिंग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設定アップできます。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 Cisco 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。

- 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。
- 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。
- 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

ユーザが認証されました。

### 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、新しいパスワードを選択するよう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。

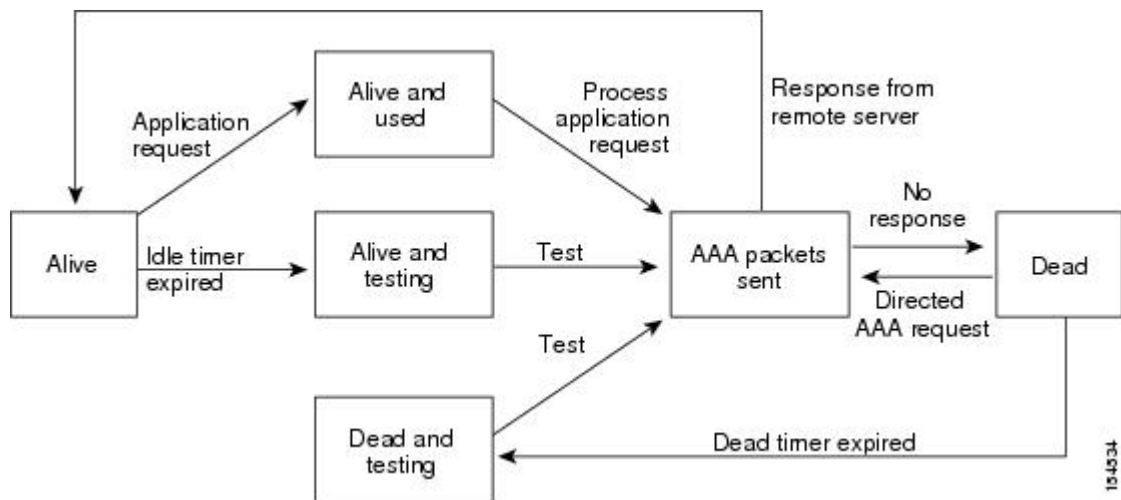
- ユーザがアクセス可能なサービス (Telnet、rlogin、または local-area transport (LAT; ローカルエリアトランスポート) 接続、PPP (ポイントツーポイントプロトコル)、シリアルラインインターネットプロトコル (SLIP)、EXEC サービスなど)
- 接続パラメータ (ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセスリスト、ユーザ タイムアウト)

# 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、定期的に RADIUS サーバをモニタして RADIUS サーバが応答している (アライブ) かどうかを調べるように、Cisco NX-OS を設定できます。Cisco NX-OS デバイスは、応答の遅い 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。Cisco NX-OS デバイスは、デッド RADIUS 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、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、Cisco NX-OS デバイスは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、RADIUS サーバ モニタリングの状態を示します。

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。

## RADIUS 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 RADIUS 設定を配布できます。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。RADIUS 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、RADIUS 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 RADIUS に対する CFS 配布をイネーブルにした後、最初に入力した RADIUS 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。
- RADIUS 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 RADIUS 設定をロックします。
- RADIUS 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 RADIUS 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 RADIUS 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 RADIUS サーバグループの設定または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。

## 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 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。

Cisco NX-OS デバイス上の認証に 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。

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、RADIUS 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 Access Control Server (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\
```



(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 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 のバーチャライゼーション サポート

RADIUS 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 RADIUS 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。

# RADIUS 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	<p>RADIUS 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。</p> <p>Cisco NX-OS ライセンス方式の詳細については、『<i>Cisco NX-OS Licensing Guide</i>』を参照してください。</p>

## 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 IP アドレスまたはホスト名を取得していること。
- RADIUS サーバからキーを取得すること。
- Cisco NX-OS 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を確認します。

## RADIUS の注意事項と制約事項

RADIUS 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 RADIUS 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。
- ワンタイムパスワードをサポートするのは RADIUS プロトコルだけです。

## 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: **RADIUS** パラメータのデフォルト設定

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

パラメータ	デフォルト
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
認証ポート	1812
アカウンティング ポート	1813
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

ここでは、Cisco NX-OS デバイスで RADIUS サーバ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りますので注意してください。

## RADIUS サーバの設定プロセス

- 1 必要に応じて、RADIUS のための CFS 配布機能をイネーブルにします。
- 2 RADIUS サーバと Cisco NX-OS デバイスの接続を確立します。
- 3 RADIUS サーバの RADIUS 秘密キーを設定します。
- 4 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。
- 5 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
  - ユーザ ログイン時の RADIUS サーバの指定の許可
  - タイムアウト間隔
  - TCP ポート



- 6 （任意）RADIUS 設定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 RADIUS 設定をコミットします。

#### 関連トピック

[RADIUS サーバ ホストの設定, \(10 ページ\)](#)

[グローバル RADIUS キーの設定, \(12 ページ\)](#)

## RADIUS 設定の配布のイネーブル化

RADIUS 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 RADIUS 設定変更の配布に参加できます。

#### 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. **radius distribute**
3. **exit**
4. （任意） **show radius 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	<b>configure terminal</b>  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	<b>radius distribute</b>  例 : switch(config)# radius distribute	RADIUS 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	<b>exit</b>  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 4	<b>show radius status</b>  例 : <pre>switch(config)# show radius status</pre>	(任意) RADIUS CFS 配布の設定を表示します。
ステップ 5	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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。

## RADIUS サーバホストの設定

リモートの RADIUS サーバにアクセスするには、RADIUS サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の RADIUS サーバを設定できます。



(注) RADIUS 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 RADIUS サーバはデフォルトの RADIUS サーバグループに追加されます。RADIUS サーバを別の RADIUS 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

サーバがすでにサーバグループのメンバーとして設定されていることを確認します。

サーバが RADIUS トラフィックを認証するよう設定されていることを確認します。

Cisco NX-OS 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を確認します。

### 手順の概要

1. **configure terminal**
2. **radius-server host {ipv4-address | ipv6-address | host-name}**
3. (任意) **show radius {pending | pending-diff}**
4. (任意) **radius commit**
5. **exit**
6. (任意) **show radius-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	<b>configure terminal</b>  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	<b>radius-server host {ipv4-address   ipv6-address   host-name}</b>  例： switch(config)# radius-server host 10.10.1.1	認証に使用する 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	<b>show radius {pending   pending-diff}</b>  例： switch(config)# show radius pending	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	<b>radius commit</b>  例： switch(config)# radius 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 RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 5	<b>exit</b>  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	<b>show radius-server</b>  例： switch# show radius-server	(任意) RADIUS サーバの設定を表示します。
ステップ 7	<b>copy running-config startup-config</b>  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

[特定の RADIUS サーバ用のキーの設定, \(13 ページ\)](#)

## グローバル RADIUS キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバの RADIUS キーを設定できます。RADIUS キーは、Cisco NX-OS デバイスと RADIUS サーバホストの間の共有秘密テキストストリングです。



(注) CFS では RADIUS キーは配布しません。

### はじめる前に

リモート RADIUS サーバの RADIUS キーの値を取得します。

リモート RADIUS サーバに RADIUS キーを設定します。

### 手順の概要

1. **configure terminal**
2. **radius-server key [0 | 6 | 7] key-value**
3. **exit**
4. (任意) **show radius-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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server key [0   6   7] key-value</b>  例 : <pre>switch(config)# radius-server key 0 QsEfThUkO</pre>	すべての RADIUS サーバ用の RADIUS キーを指定します。 <i>key-value</i> 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、RADIUS キーは設定されません。
ステップ 3	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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 4	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。  (注) RADIUS 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 RADIUS 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	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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

- [RADIUS サーバ グループの設定, \(15 ページ\)](#)
- [RADIUS 設定の配布, \(4 ページ\)](#)
- [AES パスワード暗号化およびマスター暗号キー](#)

## 特定の RADIUS サーバ用のキーの設定

Cisco NX-OS デバイスで特定の RADIUS サーバ用のキーを設定できます。RADIUS キーは、Cisco NX-OS デバイスと特定の RADIUS サーバとの間で共有する秘密テキスト スtring です。

#### はじめる前に

- 1 つまたは複数の RADIUS サーバ ホストを設定します。
- リモート RADIUS サーバのキーの値を取得します。
- RADIUS サーバにキーを設定します。

#### 手順の概要

1. **configure terminal**
2. **radius-server host {ipv4-address | ipv6-address | host-name} key [0 | 6 | 7] key-value**
3. **exit**
4. (任意) **show radius-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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server host {ipv4-address   ipv6-address   host-name} key [0   6   7] key-value</b>  例 : <pre>switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg</pre>	<p>特定の RADIUS サーバ用の RADIUS キーを指定します。  <i>key-value</i> 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。</p> <p>この RADIUS キーが グローバル RADIUS キーの代わりに使用されます。</p>
ステップ 3	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	<p>(任意)            RADIUS サーバの設定を表示します。</p> <p>(注) RADIUS 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 RADIUS キーを表示するには、<b>show running-config</b> コマンドを使用します。</p>
ステップ 5	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	<p>(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。</p>

## 関連トピック

[RADIUS サーバ ホストの設定, \(10 ページ\)](#)

[AES パスワード暗号化およびマスター暗号キー](#)

## 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。VDC には最大 100 のサーバグループを設定できます。

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 RADIUS サーバグループの設定は配布しません。

### はじめる前に

グループ内のすべてのサーバが RADIUS サーバであることを確認します。

### 手順の概要

1. **configure terminal**
2. **aaa group server radius group-name**
3. **server {ipv4-address | ipv6-address | host-name}**
4. (任意) **deadtime minutes**
5. (任意) **server {ipv4-address | ipv6-address | host-name}**
6. (任意) **use-vrf vrf-name**
7. **exit**
8. (任意) **show radius-server groups [group-name]**
9. (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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>aaa group server radius group-name</b>  例 : <pre>switch(config)# aaa group server radius RadServer switch(config-radius)#</pre>	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。

	コマンドまたはアクション	目的
ステップ 3	<b>server</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> }  例 : <pre>switch(config-radius)# server 10.10.1.1</pre>	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。  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	<b>deadtime</b> <i>minutes</i>  例 : <pre>switch(config-radius)# deadtime 30</pre>	(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	<b>server</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> }  例 : <pre>switch(config-radius)# server 10.10.1.1</pre>	(任意) 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、 <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 6	<b>use-vrf</b> <i>vrf-name</i>  例 : <pre>switch(config-radius)# use-vrf vrf1</pre>	(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 7	<b>exit</b>  例 : <pre>switch(config-radius)# exit switch(config)#</pre>	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	<b>show radius-server groups</b> [ <i>group-name</i> ]  例 : <pre>switch(config)# show radius-server groups</pre>	(任意) RADIUS サーバグループの設定を表示します。
ステップ 9	<b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	(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

[RADIUS デッドタイム間隔の設定, \(29 ページ\)](#)



## 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。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 radius source-interface *interface***
3. **exit**
4. (任意) **show radius-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	<b>configure terminal</b>  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	<b>ip radius source-interface <i>interface</i></b>  例 : switch(config)# ip radius source-interface mgmt 0	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。
ステップ 3	<b>exit</b>  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	<b>show radius-server</b>  例 : switch# show radius-server	(任意) RADIUS サーバの設定情報を表示します。
ステップ 5	<b>copy running-config startup config</b>  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

[RADIUS サーバ グループの設定, \(15 ページ\)](#)

## ログイン時にユーザによる RADIUS サーバの指定を許可

デフォルトでは、Cisco NX-OS デバイスはデフォルト AAA 認証方式に基づいて認証要求を転送します。Cisco NX-OS デバイス上で `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 VRF および RADIUS サーバをユーザが指定できるようになります。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 RADIUS 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 RADIUS 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。

## 手順の概要

1. `configure terminal`
2. `radius-server directed-request`
3. (任意) `show radius {pending | pending-diff}`
4. (任意) `radius commit`
5. `exit`
6. (任意) `show radius-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	<b><code>configure terminal</code></b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server directed-request</b>  例： switch(config)# radius-server directed-request	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	<b>show radius {pending   pending-diff}</b>  例： switch(config)# show radius pending	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	<b>radius commit</b>  例： switch(config)# radius 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 RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 5	<b>exit</b>  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	<b>show radius-server directed-request</b>  例： switch# show radius-server directed-request	(任意) directed request の設定を表示します。
ステップ 7	<b>copy running-config startup-config</b>  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

[RADIUS 設定の配布, \(4 ページ\)](#)

## 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、Cisco NX-OS デバイスは RADIUS サーバに 1 回だけ送信を再試行してから、ローカル認証に切り換えます。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。タイムアウト間隔には、Cisco NX-OS デバイスが RADIUS 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。

## 手順の概要

1. **configure terminal**
2. **radius-server retransmit *count***
3. **radius-server timeout *seconds***
4. (任意) **show radius {pending | pending-diff}**
5. (任意) **radius commit**
6. **exit**
7. (任意) **show radius-server**
8. (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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server retransmit <i>count</i></b>  例 : <pre>switch(config)# radius-server retransmit 3</pre>	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。
ステップ 3	<b>radius-server timeout <i>seconds</i></b>  例 : <pre>switch(config)# radius-server timeout 10</pre>	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	<b>show radius {pending   pending-diff}</b>  例 : <pre>switch(config)# show radius pending</pre>	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 5	<b>radius commit</b>  例 : <pre>switch(config)# radius commit</pre>	(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 RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 6	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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 7	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。
ステップ 8	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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

[RADIUS 設定の配布, \(4 ページ\)](#)

## 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 NX-OS デバイスは RADIUS サーバに 1 回だけ送信を再試行してから、ローカル認証に切り換えます。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。Cisco NX-OS デバイスが RADIUS サーバからの応答を待つタイムアウト間隔も設定できます。これを過ぎるとタイムアウトエラーになります。

#### はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

#### 手順の概要

1. **configure terminal**
2. **radius-server host {ipv4-address | ipv6-address | host-name} retransmit count**
3. **radius-server host {ipv4-address | ipv6-address | host-name} timeout seconds**
4. (任意) **show radius {pending | pending-diff}**
5. (任意) **radius commit**
6. **exit**
7. (任意) **show radius-server**
8. (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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server host {ipv4-address   ipv6-address   host-name} retransmit count</b>  例 : <pre>switch(config)# radius-server host server1 retransmit 3</pre>	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	<b>radius-server host {ipv4-address   ipv6-address   host-name} timeout seconds</b>  例 : <pre>switch(config)# radius-server host server1 timeout 10</pre>	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。  (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	<b>show radius {pending   pending-diff}</b>  例 : <pre>switch(config)# show radius pending</pre>	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 5	<b>radius commit</b>  例 : <pre>switch(config)# radius commit</pre>	(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 RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 6	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。
ステップ 8	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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

[RADIUS サーバ ホストの設定, \(10 ページ\)](#)[RADIUS 設定の配布, \(4 ページ\)](#)

## RADIUS サーバのアカウントティングおよび認証属性の設定

RADIUS サーバをアカウントティング専用、または認証専用に使用するかを指定できます。デフォルトでは、RADIUS サーバはアカウントティングと認証の両方に使用されます。また、デフォルトのポートとの競合が発生する場合は、RADIUS アカウントティング メッセージと認証メッセージの送信先である宛先 UDP ポート番号を指定することもできます。

## はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

## 手順の概要

1. **configure terminal**
2. (任意) **radius-server host {ipv4-address | ipv6-address | host-name} acct-port udp-port**
3. (任意) **radius-server host {ipv4-address | ipv6-address | host-name} accounting**
4. (任意) **radius-server host {ipv4-address | ipv6-address | host-name} auth-port udp-port**
5. (任意) **radius-server host {ipv4-address | ipv6-address | host-name} authentication**
6. (任意) **show radius {pending | pending-diff}**
7. (任意) **radius commit**
8. **exit**
9. (任意) **show radius-server**
10. (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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server host {ipv4-address   ipv6-address   host-name} acct-port udp-port</b>  例 : <pre>switch(config)# radius-server host 10.10.1.1 acct-port 2004</pre>	(任意) RADIUS アカウントティ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 1813 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	<b>radius-server host {ipv4-address   ipv6-address   host-name} accounting</b>  例 : <pre>switch(config)# radius-server host 10.10.1.1 accounting</pre>	(任意) RADIUS サーバをアカウントिंगだけに使用することを指定します。デフォルトでは、アカウントINGと認証の両方に使用されます。
ステップ 4	<b>radius-server host {ipv4-address   ipv6-address   host-name} auth-port udp-port</b>  例 : <pre>switch(config)# radius-server host 10.10.2.2 auth-port 2005</pre>	(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	<b>radius-server host {ipv4-address   ipv6-address   host-name} authentication</b>  例 : <pre>switch(config)# radius-server host 10.10.2.2 authentication</pre>	(任意) RADIUS サーバを認証だけに使用することを指定します。デフォルトでは、アカウントINGと認証の両方に使用されます。
ステップ 6	<b>show radius {pending   pending-diff}</b>  例 : <pre>switch(config)# show radius pending</pre>	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 7	<b>radius commit</b>  例 : <pre>switch(config)# radius commit</pre>	(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 RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 8	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	コンフィギュレーション モードを終了します。
ステップ 9	<b>show radius-server</b>  例 : <pre>switch(config)# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。
ステップ 10	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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

[RADIUS サーバ ホストの設定, \(10 ページ\)](#)[RADIUS 設定の配布, \(4 ページ\)](#)

## RADIUS 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 RADIUS 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、RADIUS 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) CFS ではグローバル RADIUS サーバグループの設定は配布しません。



(注) ネットワークのセキュリティを保護するために、RADIUS データベースの既存のユーザ名と同じもの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。アイドルタイムインターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

### はじめる前に

RADIUS をイネーブルにします。

## 手順の概要

1. **configure terminal**
2. **radius-server test {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}**
3. **radius-server deadtime minutes**
4. **exit**
5. (任意) **show radius-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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server test {idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]}</b>  例 : <pre>switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3</pre>	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 <b>test</b> 、デフォルトのパスワードは <b>test</b> 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) 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	<b>radius-server deadtime minutes</b>  例 : <pre>switch(config)# radius-server deadtime 5</pre>	以前に応答の遅かった RADIUS 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	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。
ステップ 6	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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 RADIUS サーバの定期モニタリングの設定, \(27 ページ\)](#)

## 各 RADIUS サーバの定期モニタリングの設定

各 RADIUS 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、RADIUS 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) 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。



(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。

### はじめる前に

RADIUS をイネーブルにします。

1 つまたは複数の RADIUS サーバ ホストを追加します。

### 手順の概要

1. **configure terminal**
2. **radius-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. **radius-server deadtime minutes**
4. **exit**
5. (任意) **show radius-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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>radius-server host {ipv4-address   ipv6-address   host-name} test {idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]}</b>  例 : <pre>switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	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 <b>test</b> 、デフォルトのパスワードは <b>test</b> 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) 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	<b>radius-server deadtime minutes</b>  例 : <pre>switch(config)# radius-server deadtime 5</pre>	以前に応答の遅かった RADIUS 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 1 ～ 1440 分です。
ステップ 4	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。
ステップ 6	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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

[RADIUS サーバ ホストの設定, \(10 ページ\)](#)

[RADIUS サーバのグローバルな定期モニタリングの設定, \(25 ページ\)](#)

## RADIUS 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。デッドタイム間隔では、Cisco NX-OS デバイスが RADIUS 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。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。

### 手順の概要

1. **configure terminal**
2. **radius-server deadtime *minutes***
3. (任意) **show radius {pending | pending-diff}**
4. (任意) **radius commit**
5. **exit**
6. (任意) **show radius-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	<b>configure terminal</b>  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	<b>radius-server deadtime <i>minutes</i></b>  例 : switch(config)# radius-server deadtime 5	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	<b>show radius {pending   pending-diff}</b>  例 : switch(config)# show radius pending	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	<b>radius commit</b>  例 : switch(config)# radius 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 RADIUS の設定変更を実行コンフィギュレーションに適用して、

	コマンドまたはアクション	目的
		RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 5	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 6	<b>show radius-server</b>  例 : <pre>switch# show radius-server</pre>	(任意) RADIUS サーバの設定を表示します。
ステップ 7	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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

[RADIUS サーバ グループの設定, \(15 ページ\)](#)

[RADIUS 設定の配布, \(4 ページ\)](#)

## ワンタイムパスワードの設定

RSA SecurID トークン サーバを使用することで、Cisco NX-OS デバイスでワンタイムパスワード (OTP) をサポートできます。この機能を使用すると、ユーザは、暗証番号 (ワンタイムパスワード) とその時点で RSA SecurID トークンに表示されるトークンコードの両方を入力することで、Cisco NX-OS デバイスに対する認証を実行できます。



(注) Cisco NX-OS デバイスにログインするために使用されるトークンコードは、60 秒ごとに変更されます。デバイス検出に関する問題を防ぐために、Cisco Secure ACS 内部データベースに存在する異なるユーザ名を使用することを推奨します。

#### はじめる前に

Cisco NX-OS デバイスで、RADIUS サーバホストとデフォルトのリモートログイン認証を設定します。

次のものがインストールされていることを確認します。

- Cisco Secure Access Control Server (ACS) Version 4.2

- RSA Authentication Manager Version 7.1 (RSA SecurID トークン サーバ)
- RSA ACE Agent/Client

ワンタイムパスワードをサポートするために、Cisco NX-OS デバイスで (RADIUS サーバ ホスト とリモート認証以外の) 設定を行う必要はありません。ただし、Cisco Secure ACS を次のように設定する必要があります。

- 1 RSA SecurID トークン サーバ認証をイネーブルにします。
- 2 RSA SecurID トークン サーバを不明ユーザ ポリシー データベースに追加します。

## RADIUS 情報の配布のコミット

一時バッファに保存されている RADIUS のグローバル設定およびサーバ特有の設定を、ファブリック内のすべてのデバイス (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。

### 手順の概要

1. **configure terminal**
2. (任意) **show radius {pending | pending-diff}**
3. **radius commit**
4. **exit**
5. (任意) **show role session 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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>show radius {pending   pending-diff}</b>  例 : <pre>switch(config)# show radius pending</pre>	(任意) 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 3	<b>radius commit</b>  例 : <pre>switch(config)# radius commit</pre>	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 RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 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	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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	<b>show role session status</b>  例 : <pre>switch# show role session status</pre>	(任意) ユーザ ロールについての CSF セッションのステータスを表示します。
ステップ 6	<b>copy running-config startup-config</b>  例 : <pre>switch# copy running-config startup-config</pre>	(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。

## RADIUS の配布セッションの廃棄

RADIUS 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。

### 手順の概要

1. **configure terminal**
2. (任意) **show radius {pending | pending-diff}**
3. **radius abort**
4. **exit**
5. (任意) **show radius session 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	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	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	<b>show radius {pending   pending-diff}</b>  例 : <pre>switch(config)# show radius pending</pre>	(任意) 配布するために保留状態になっている RADIUS 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 3	<b>radius abort</b>  例 : <pre>switch(config)# radius abort</pre>	一時ストレージにある RADIUS 設定を廃棄して、セッションを終了します。
ステップ 4	<b>exit</b>  例 : <pre>switch(config)# exit switch#</pre>	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	<b>show radius session status</b>  例 : <pre>switch# show radius session status</pre>	(任意) RADIUS CFS セッションのステータスを表示します。

## RADIUS の配布セッションのクリア

実行中の Cisco Fabric Services の配布セッション（存在する場合）をクリアして、RADIUS 機能のためのファブリックのロックを解除します。

### 手順の概要

1. **clear radius session**
2. (任意) **show radius session 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	<b>clear radius session</b>  例 : <pre>switch# clear radius session</pre>	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	<b>show radius session status</b>  例 : <pre>switch# show radius session status</pre>	(任意) RADIUS CFS セッションのステータスを表示します。

## 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 グループに対し手動でテスト メッセージを送信できます。

### 手順の概要

1. **test aaa server radius** {*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	<b>test aaa server radius</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } [ <b>vrf</b> <i>vrf-name</i> ] <i>username password</i>  例 : <pre>switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH</pre>	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	<b>test aaa group</b> <i>group-name username password</i>  例 : <pre>switch# test aaa group RadGroup user2 As3He3CI</pre>	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。

## RADIUS 設定の確認

RADIUS の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
<b>show radius</b> { <b>status</b>   <b>pending</b>   <b>pending-diff</b> }	Cisco Fabric Services の RADIUS 設定の配布状況と他の詳細事項を表示します。
<b>show running-config radius</b> [ <b>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。
<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。
<b>show radius-server</b> [ <i>host-name</i>   <i>ipv4-address</i>   <i>ipv6-address</i> ] [ <b>directed-request</b>   <b>groups</b>   <b>sorted</b>   <b>statistics</b> ]	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。

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。

## RADIUS サーバのモニタリング

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モニタリングできます。

### はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

### 手順の概要

1. **show radius-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	<b>show radius-server statistics</b> {hostname   ipv4-address   ipv6-address}  例 : switch# show radius-server statistics 10.10.1.1	RADIUS 統計情報を表示します。

### 関連トピック

[RADIUS サーバ ホストの設定, \(10 ページ\)](#)

[RADIUS サーバ統計情報のクリア, \(35 ページ\)](#)

## 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。

### 手順の概要

1. (任意) **show radius-server statistics** {hostname | ipv4-address | ipv6-address}
2. **clear radius-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	<b>show radius-server statistics</b> {hostname   ipv4-address   ipv6-address}  例 : switch# show radius-server statistics 10.10.1.1	(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	<b>clear radius-server statistics</b> {hostname   ipv4-address   ipv6-address}  例 : switch# clear radius-server statistics 10.10.1.1	RADIUS サーバ統計情報をクリアします。

## 関連トピック

[RADIUS サーバホストの設定, \(10 ページ\)](#)

## RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPgG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

## 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。

## RADIUS に関する追加情報

ここでは、RADIUS 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	<i>Cisco NX-OS ライセンス ガイド</i>
コマンド リファレンス	『 <i>Cisco Nexus 7000 Series NX-OS Security Command Reference</i> 』

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
<ul style="list-style-type: none"> <li>• CISCO-AAA-SERVER-MIB</li> <li>• CISCO-AAA-SERVER-EXT-MIB</li> </ul>	<p>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。</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p>

# RADIUS の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 2: **RADIUS** の機能の履歴

機能名	リリース	機能情報
RADIUS	6.0(1)	Release 5.2 以降、変更はありません。
RADIUS	5.2(1)	RADIUS サーバキーのタイプ 6 暗号化が追加されました。
RADIUS	5.1(1)	Release 5.0 以降、変更はありません。

機能名	リリース	機能情報
定期サーバ モニタリング	5.0(2)	RADIUS 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。
OTP	5.0(2)	ワンタイムパスワードのサポートが追加されました。