CHAPTER 3

RADIUS の設定

この章では、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。

ここでは、次の内容を説明します。

RADIUS の概要

RADIUS 分散型クライアント / 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することができます。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。

ここでは、次の内容について説明します。

RADIUS のネットワーク環境

RADIUS は、リモート ユーザのネットワーク アクセスを維持すると同時に高度なレベルのセキュリティを必要とするさまざまなネットワーク環境に実装できます。

RADIUS は、アクセスのセキュリティが必要な次のネットワーク環境で使用できます。

- 複数のベンダーのネットワーク装置で構成され、それぞれが RADIUS をサポートするネットワーク。たとえば複数のベンダーのネットワーク装置が、1 つの 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 を使用しているネットワーク。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。これが AAA サーバへ移行する最初のステップにもなります。
- リソースの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 認証や認可と無関係に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始と終了の時点にデータを送信し、そのセッション中に使用されたリソース（時間、パケット、バイトなど）の量を示すことができます。Internet service provider（ISP; インターネット サービス プロバイダー）は、RADIUS アクセス制御およびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、セキュリティおよび課金の独自ニーズを満たすこともできます。
- 認証プロファイルをサポートするネットワーク。ネットワークに RADIUS サーバを導入すると、AAA 認証を設定しユーザ単位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. プロンプトが表示され、ユーザはユーザ名およびパスワードを入力します。
2. ユーザ名と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 — ユーザの認証が失敗し、ユーザ名およびパスワードの再入力を要求されるか、またはアクセスが拒否されます。
   - CHALLENGE — RADIUS サーバによりチャレンジが送信されます。チャレンジによってユーザから追加データが収集されます。
   - CHANGE PASSWORD — ユーザは新しいパスワードを選択するように RADIUS サーバから要求が送信されます。

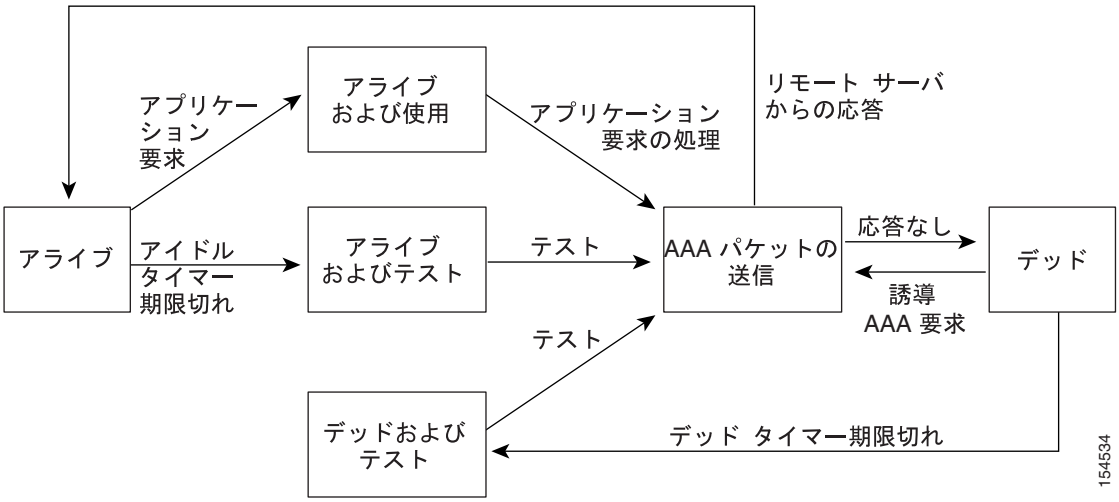
ACCEPT または REJECT 応答には、EXEC またはネットワーク許可に使用される追加データが含まれています。ユーザは RADIUS 認証が完了しないうちは RADIUS 許可を使用できません。ACCEPT または REJECT パケットに含まれる追加データには、次のものがあります。

- Telnet、rlogin、または Local-Area Transport（LAT; ローカルエリア トランスポート）、および Point-to-Point Protocol（PPP）、Serial Line Internet Protocol（SLIP）、または EXEC サービスなどといった、ユーザがアクセスできるサービス
- ホストまたはクライアントの IPv4/IPv6 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

RADIUS サーバの応答が遅いと、AAA 要求の処理が遅れる原因にもなります。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）かどうかを調べる設定ができます。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。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 プロセスにより、RADIUS サーバが稼働状態であることが確認されてから、実際の AAA 要求が送信されます。RADIUS サーバがデッドまたはアライブの状態に変わると SNMP トラップが生成され、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。図 3-1 を参照してください。

図 3-1　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 モニタリングは、テスト認証要求を RADIUS サーバに送信して行われます。

VSA

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 RADIUS サーバの間で VSA（vendor-specific attribute; 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 はアトリビュート 26 を使用しています。VSA を使用すると、ベンダーは一般的な用途に適さない独自の拡張アトリビュートをサポートできます。シスコの RADIUS 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 で、サポートするオプションはベンダー タイプ 1、名前は 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アトリビュートです。separator は、必須アトリビュートの場合に =（等号）、オプションのアトリビュートの場合に *（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 アトリビュートを返すように指示します。この権限付与情報は、VSA を通じて指定されます。

次の VSA プロトコル オプションが Cisco NX-OS ソフトウェアでサポートされています。

- shell — ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル
- Accounting — accounting-request パケットで使用されるプロトコル。値にスペースが含まれる場合は、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、次のアトリビュートをサポートしています。

- roles — ユーザが属しているすべてのロールをリストします。値フィールドは、ロール名をスペースで区切ったストリングです。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。このサブアトリビュートは 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。このアトリビュートはシェル 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 アトリビュートの例を示します。

  ```
  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 アトリビュートの例を示します。

  ```
  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 アトリビュートとしてフラグ設定され、他のシスコ製装置はこのアトリビュートを無視します。

- accountinginfo — 標準の RADIUS アカウンティング プロトコルに含まれるアトリビュートとともにアカウンティング情報を格納します。このアトリビュートは、スイッチ上の RADIUS 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。このアトリビュート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）とだけ併用できます。

バーチャライゼーション サポート

RADIUS の設定と操作は、Virtual Device Context（VDC）に対してローカルです。VDC の詳細については、『*Cisco NX-OS Virtual Device Context Configuration Guide, Release 4.0*』を参照してください。

NX-OS デバイスは、Virtual Routing and Forwarding instance（VRF）を使用して TACACS+ サーバをアクセスします。VRF の詳細については、『*Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0*』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
NX-OS	RADIUS に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、無償で提供されます。NX-OS のライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide, Release 4.0*』を参照してください。

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すること
- RADIUS サーバから事前共有鍵を取得すること
- 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

注意事項および制限事項

RADIUS には、次の注意事項と制限事項があります。

- 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。

RADIUS サーバの設定

ここでは、次の内容について説明します。

（注）　Cisco IOS CLI の知識があるユーザは、この機能に関する Cisco NX-OS のコマンドが Cisco IOS のコマンドで使用されるものと異なる場合があることに注意してください。

RADIUS サーバの設定プロセス

RADIUS サーバの設定には、次の作業を行います。

ステップ 1　RADIUS サーバと NX-OS デバイスの接続を確立します（「RADIUS サーバ ホストの設定」[p.3-7] を参照）。

ステップ 2　RADIUS サーバの事前共有秘密鍵を設定します（「グローバル事前共有鍵の設定」[p.3-7] を参照）。

ステップ 3　必要な場合は、AAA 認証方式に、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（「ログイン時の RADIUS サーバの指定をユーザに許可する」[p.3-11] および「AAA の設定」[p.2-8] を参照）。

ステップ 4　必要な場合は、次のオプション パラメータを設定します。

- デッド タイム間隔（「デッド タイム間隔の設定」[p.3-17] を参照）
- ログイン時の RADIUS サーバの指定の許可（「ログイン時の RADIUS サーバの指定をユーザに許可する」[p.3-11] を参照）
- 送信リトライ回数およびタイムアウト間隔（「RADIUS のグローバル送信リトライ回数およびタイムアウト間隔の設定」[p.3-12] を参照）
- アカウンティングおよび認証のアトリビュート（「RADIUS サーバのアカウンティングおよび認証アトリビュートの設定」[p.3-14] を参照）

ステップ 5　必要な場合、RADIUS サーバの定期モニタリングの設定（「RADIUS サーバの定期モニタリングの設定」[p.3-15] を参照）

RADIUS サーバ ホストの設定

認証に使用する各 RADIUS サーバの IPv4 または IPv6 アドレスまた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 ホストをデフォルトの RADIUS サーバ グループに追加します。最大 64 の RADIUS サーバを設定できます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **例：** `switch(config)# radius-server host 10.10.1.1`	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	**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 radius-server** **例：** `switch# show radius-server`	（任意）RADIUS サーバ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。

グローバル事前共有鍵の設定

NX-OS デバイスで使用されるすべてのサーバの事前共有鍵をグローバル レベルで設定できます。事前共有鍵は、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

リモート RADIUS サーバの事前共有鍵の値を取得します。

手順の概要

1. **config t**
2. **radius-server key** [**0** | **7**] *key-value*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**radius-server key** [**0** | **7**] *key-value* **例**： `switch(config)# radius-server key 0 QsEfThUkO`	すべての RADIUS サーバの事前共有鍵を指定します。クリア テキスト（**0**）または暗号化（**7**）の事前共有鍵を指定します。デフォルト形式はクリア テキストです。最大長は 63 文字です。 デフォルトでは、事前共有鍵は設定されません。

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 radius-server** **例**： `switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。 **（注）** 事前共有鍵は実行コンフィギュレーションに暗号化形式で保存されます。暗号化事前共有鍵を表示するには、**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。

RADIUS サーバの事前共有鍵の設定

RADIUS サーバの事前共有鍵を設定できます。事前共有鍵は、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

リモート RADIUS サーバの事前共有鍵の値を取得します。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** *key-value*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value* **例：** `switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg`	特定の RADIUS サーバの事前共有鍵を指定します。クリア テキスト（**0**）または暗号化（**7**）の事前共有鍵を指定します。デフォルト形式はクリア テキストです。最大長は 63 文字です。 グローバル事前共有鍵ではなく、この事前共有鍵が使用されます。

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 radius-server** **例：** `switch# show radius-server`	（任意）RADIUS サーバの設定を表示します。 **（注）** 事前共有鍵は実行コンフィギュレーションに暗号化形式で保存されます。暗号化事前共有鍵を表示するには、**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。

RADIUS サーバ グループの設定

認証にサーバ グループを使用して 1 つまたは複数のリモート AAA サーバを指定できます。グループ内のすべてのメンバーは同じ RADIUS プロトコルに属する必要があります。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。VDC には最大 100 のサーバ グループを設定できます。

サーバ グループはいつでも設定できますが、AAA サービスに適用したときにしか有効になりません。AAA サービスについては、「リモート AAA サービス」（p.2-3）を参照してください。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *ipv6-address* | *server-name*}
4. **deadtime** *minutes*
5. **use-vrf** *vrf-name*
6. **exit**
7. **show radius-server groups** [*group-name*]
8. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		コンフィギュレーション モードを開始します。

ステップ 2	**aaa group server radius** *group-name*
	
	例：
	`switch(config)# aaa group server radius RadServer`
	`switch(config-radius)#`
		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。*group-name* 引数は、最大 127 文字の英数字ストリングで、大文字と小文字は区別されます。

ステップ 3	**server** {*ipv4-address* | *ipv6-address* | *server-name*} **例：** `switch(config-radius)# server 10.10.1.1`	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 サーバが検出されなかった場合、**radius-server host** コマンドを使用してサーバを設定し、再度このコマンドを実行してください。
ステップ 4	**deadtime** *minutes* **例：** `switch(config-radius)# deadtime 30`	（任意）モニタリングのデッド タイムを設定します。デフォルト値は 0 分です。有効値の範囲は 1 ～ 1440 です。 **（注）**　デッド タイム間隔がゼロ（0）より大きい RADIUS サーバ グループの場合は、その値がグローバル デット タイム値に優先します（「デッド タイム間隔の設定」[p.3-17] を参照）。
ステップ 5	**use-vrf** *vrf-name* **例：** `switch(config-radius)# use-vrf vrf1`	（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	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 7	**show radius-server groups** [*group-name*] **例：** `switch(config)# show radius-server group`	（任意）RADIUS サーバ グループの設定を表示します。
ステップ 8	**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。

ログイン時の RADIUS サーバの指定をユーザに許可する

（注）　デフォルトでは、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。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。ユーザ指定のログインは Telnet セッションでのみサポートされます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **radius-server directed-request**
3. **exit**
4. **show radius-server directed-request**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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** **例：** `switch(config)# radius-server directed-request`	ログイン時に認証要求の送信先の RADIUS サーバを指定することをユーザに許可します。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。

	コマンド	目的
ステップ 4	**show radius-server directed-request** **例：** `switch# show radius-server directed-request`	（任意）誘導要求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。

RADIUS のグローバル送信リトライ回数およびタイムアウト間隔の設定

すべての RADIUS サーバのグローバル再送信リトライ回数および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 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。この回数は各サーバにつき、最大 5 回まで再試行を増やすことができます。タイムアウト間隔には、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障害が宣言されます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **radius-server retransmission** *count*
3. **radius-server timeout** *seconds*
4. **exit**
5. **show radius-server**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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* **例：** `switch(config)# radius-server retransmit 3`	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 です。有効範囲は 0 ～ 5 です。
ステップ 3	`switch(config)#` **radius-server timeout** *seconds* **例：** `switch(config)# radius-server timeout 10`	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。有効範囲は 1 ～ 60 秒です。

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。

	コマンド	目的
ステップ 5	**show radius-server** **例：** switch# show radius-server	（任意）RADIUS 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。

個別サーバの RADIUS 送信リトライ回数およびタイムアウト間隔の設定

デフォルトでは、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。この回数は各サーバにつき、最大 5 回まで再試行を増やすことができます。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障害が宣言されます。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
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. **exit**
5. **show radius-server**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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* |*ipv6-address* | *host-name*} **retransmit** *count* **例：** switch(config)# radius-server host server1 retransmit 3	特定の RADIUS サーバの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）** RADIUS サーバに個別に指定された再送信カウント値は、ステップ 2 ですべての RADIUS サーバに指定されたカウント値に優先します。

	コマンド	目的
ステップ 3	switch(config)# **radius-server host** {*ipv4-address* |*ipv6-address* | *host-name*} **timeout** *seconds* **例：** switch(config)# radius-server host server1 timeout 10	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）** RADIUS サーバに個別に指定されたタイムアウト間隔値は、ステップ 3 ですべての RADIUS サーバに指定されたタイムアウト間隔値に優先します。
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 radius-server** **例：** switch# show radius-server	（任意）RADIUS 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。

RADIUS サーバのアカウンティングおよび認証アトリビュートの設定

RADIUS サーバをアカウンティングにのみ使用するのか、認証にのみ使用するのかを指定できます。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。また、RADIUS アカウンティング 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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port*
3. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**
4. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*
5. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**
6. **exit**
7. **show radius-server**
8. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t switch(config)#	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	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port** *udp-port* **例：** switch(config)# radius-server host 10.10.1.1 acct-port 2004	（任意）RADIUS アカウン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 1812 です。有効範囲は 0 ～ 65535 です。
ステップ 3	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting** **例：** switch(config)# radius-server host 10.10.1.1 accounting	（任意）指定した RADIUS サーバをアカウンティングにのみ使用することを指定します。デフォルトは、アカウンティングと認証の両方の用途です。
ステップ 4	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port* **例：** switch(config)# radius-server host 10.10.2.2 auth-port 2005	（任意）RADIUS 認証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。有効範囲は 0 ～ 65535 です。
ステップ 5	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication** **例：** switch(config)# radius-server host 10.10.2.2 authentication	（任意）指定した RADIUS サーバを認証にのみ使用することを指定します。デフォルトは、アカウンティングと認証の両方の用途です。
ステップ 6	**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 7	**show radius-server** **例：** switch(config)# show radius-server	（任意）RADIUS サーバの設定を表示します。
ステップ 8	**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。

RADIUS サーバの定期モニタリングの設定

RADIUS サーバが使用可能かどうかをモニタできます。パラメータには、サーバとアイドル タイマーに使用されるユーザ名とパスワードなどがあります。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 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、サーバを定期的にテストすることができます。

（注） セキュリティ上の理由から、テストのユーザ名には、RADIUS データベースの既存のユーザ名と同じもの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 NX-OS デバイスはテスト パケットを送信します。

（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、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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
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 dead-time** *minutes*
4. **exit**
5. **show radius-server**
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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	**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*]]} **例**： `switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバのモニタリングのパラメータを指定します。デフォルト ユーザ名は test で、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）　RADIUS サーバを定期モニタリングする場合には、アイドル タイマーを 0 より大きな値に設定する必要があります。
ステップ 3	**radius-server dead-time** *minutes* **例**： `switch(config)# radius-server dead-time 5`	以前に応答の遅かった RADIUS サーバを 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	**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	目的
ステップ 5	**show radius-server** **例：** `switch# show radius-server`	（任意）RADIUS 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。

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、NX-OS デバイスが 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 サーバの応答がなくても、そのサーバをデッドとしません。RADIUS サーバのデッド タイム間隔を個別に設定できます（「RADIUS サーバ グループの設定」[p.3-9] を参照）。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

1. **config t**
2. **radius-server dead-time** *minutes*
3. **exit**
4. **show radius-server**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		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* **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	**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	目的
ステップ 4	**show radius-server** **例**： switch# show radius-server	（任意）RADIUS サーバ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。

RADIUS サーバまたはサーバ グループの手動でのモニタリング

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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

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*

詳細な手順

	コマンド	目的
ステップ 1	**test aaa server radius** {*ipv4-address* | *ipv6-address* | *server-name*} [**vrf** *vrf-name*] *username password* **例**： switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH	RADIUS サーバにテスト メッセージを送信して使用可能であることを確認します。
ステップ 2	**test aaa group** *group-name username password* **例**： switch# test aaa group RadGroup user2 As3He3CI	RADIUS サーバ グループにテスト メッセージを送信して使用可能であることを確認します。

RADIUS 設定の確認

RADIUS の設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーション内の 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内の RADIUS 設定を表示します。
show radius-server [*server-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	RADIUS サーバのすべての設定済みパラメータを表示します。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

RADIUS サーバ統計情報の表示

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。

作業を開始する前に

正しい VDC にいることを確認します（または **switchto vdc** コマンドを使用）。

手順の概要

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

詳細な手順

	コマンド	目的

ステップ 1	`switch# show radius-server statistics {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。

このコマンドの出力に表示されるフィールドの詳細については、『*Cisco NX-OS Security Command Reference, Release 4.0*』を参照してください。

RADIUS 設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
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、RADIUS 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（第 2 章「AAA の設定」を参照）。

デフォルト設定

表 3-1 に、RADIUS パラメータのデフォルト設定を示します。

表 3-1　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 ロール	認証およびアカウンティング
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
定期サーバ モニタリングのユーザ名	test
定期サーバ モニタリングのパスワード	test

その他の参考資料

RADIUS の実装に関連する詳細情報については、次を参照してください。

- 関連資料（p.3-21）
- 規格（p.3-21）
- MIB（p.3-21）

関連資料

関連事項	タイトル
NX-OS ライセンス	『*Cisco NX-OS Licensing Guide, Release 4.0*』
コマンド リファレンス	『*Cisco NX-OS Security Command Reference, Release 4.0*』
VRF の設定	『*Cisco NX-OS Unicast Routing Configuration Guide, Release 4.0*』

規格

規格	タイトル
この機能によりサポートされた新規規格または改訂規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	MIB の確認とダウンロードを行うには、次の URL にアクセスします。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml