CHAPTER 5

RADIUS の設定

この章では、Cisco NX-OS デバイスで 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、次の内容で構成されています。

RADIUS の概要

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 デバイス上で稼動します。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、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。

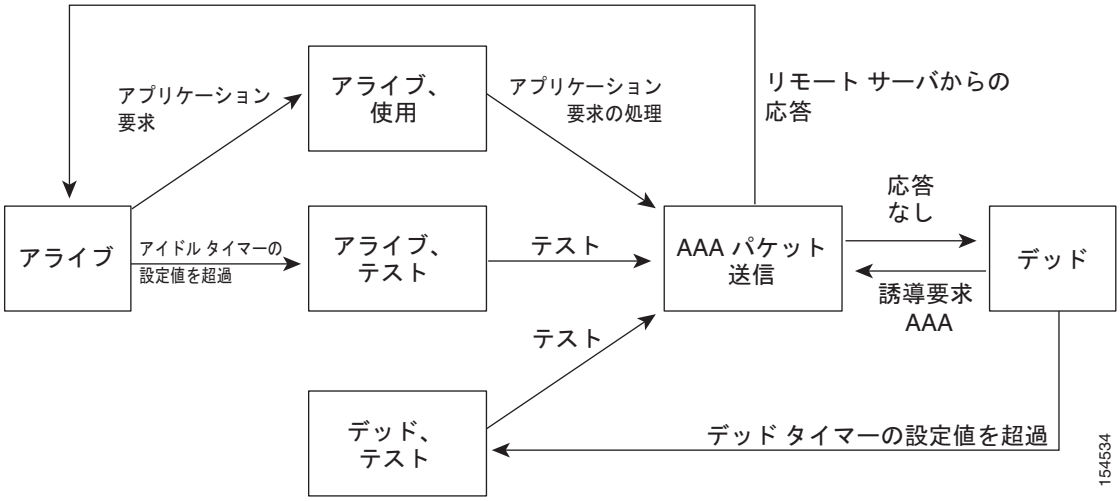
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカルエリア トランスポート）接続、PPP（ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

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 プロセスにより、RADIUS サーバが稼動状態であることを確認してから、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 Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）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。図 5-1 を参照してください。

図 5-1　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（VSA）

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）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 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属性です。separator は、必須属性の場合は =（等号）、任意の属性の場合は *（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。

次に、サポートされる VSA プロトコル オプションを示します。

- 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。

次に、サポートされる属性を示します。

- 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 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 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 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 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。

注意事項および制約事項

RADIUS に関する注意事項と制約事項は次のとおりです。

- 最大 64 の RADIUS サーバを設定できます。

デフォルト設定

表 5-1 に、RADIUS のデフォルト設定を示します。

表 5-1　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

ここでは、次の内容について説明します。

- 「RADIUS サーバ ホストの設定」（P.5-6）
- 「RADIUS グローバル キーの設定」（P.5-7）
- 「RADIUS サーバ キーの設定」（P.5-8）
- 「RADIUS サーバ グループの設定」（P.5-9）
- 「RADIUS サーバの誘導要求のイネーブル化」（P.5-11）
- 「すべての RADIUS サーバのグローバル タイムアウトの設定」（P.5-12）
- 「すべての RADIUS サーバのグローバル リトライ回数の設定」（P.5-13）
- 「単一 RADIUS サーバのタイムアウト間隔の設定」（P.5-14）
- 「単一 RADIUS サーバのリトライ回数の設定」（P.5-15）
- 「RADIUS アカウンティング サーバの設定」（P.5-16）
- 「RADIUS 認証サーバの設定」（P.5-17）
- 「RADIUS サーバの定期モニタリングの設定」（P.5-19）
- 「グローバル デッド タイム間隔の設定」（P.5-20）
- 「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」（P.5-21）

（注） この機能に対応する Cisco NX-OS コマンドは、Cisco IOS で使用されているコマンドと異なる場合があるので注意してください。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} 例： `n1000v(config)# radius-server host 10.10.1.1`	RADIUS サーバの IP アドレスまたはホスト名を定義します。

ステップ 3	**exit**
	
	例：
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 4	**show radius-server** 例： `n1000v# 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： `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS グローバル キーの設定

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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- RADIUS サーバ認証に使用されるグローバル キーがわかっています。

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**

手順の詳細

グローバル事前共有キーを設定するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server key** [**0** | **7**] *key-value* **例：** `n1000v(config)# radius-server key 0 QsEfThUkO`	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	**exit**
	
	例：
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show radius-server** 例： n1000v# 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	**copy running-config startup-config** 例： n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- リモート RADIUS ホストに使用されるキーを取得しています。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value* 例： n1000v(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg	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	目的
ステップ 3	**exit** 例： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** 例： n1000v# 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	**copy running-config startup-config** 例： n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。
- 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。

手順の概要

1. **config t**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *server-name*}
4. **deadtime** *minutes*
5. **use-vrf** *vrf-name*
6. （任意）**source-interface** {*interface-type*} {*interface-number*}
7. （任意）show radius-server groups [*group-name*]
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa group server radius** *group-name* 例： n1000v(config)# aaa group server radius RadServer n1000v(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 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	**server** {*ipv4-address* | *server-name*} 例： n1000v(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	**deadtime** *minutes* 例： n1000v(config-radius)# deadtime 30	（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）** 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（「グローバル デッド タイム間隔の設定」（P.5-20）を参照）。
ステップ 5	**use-vrf** *vrf-name* 例： n1000v(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	**source-interface** {*interface-type*} {*interface-number*} 例： n1000v(config-radius)# source-interface mgmt0 n1000v(config-radius)#	（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。 • loopback = 0 ～ 1023 の仮想インターフェイス番号 • 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

	コマンド	目的
ステップ 7	**show radius-server groups** [*group-name*] 例： n1000v(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	（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： n1000v(config-radius)# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバの誘導要求のイネーブル化

認証要求の送信先の RADIUS サーバをユーザが指定できるようにするには、次の手順を実行します。これは directed-request（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 VRF、*hostname* は設定された RADIUS サーバの名前です。

（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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- デフォルトでは、誘導要求はディセーブルです。

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**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	n1000v(config)# radius-server directed-request 例： n1000v(config)# radius-server directed-request	誘導要求をイネーブルにします。デフォルトはディセーブルです。
ステップ 3	**exit** 例： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server directed-request** 例： n1000v# show radius-server directed-request	（任意）指定要求設定を表示します。
ステップ 5	**copy running-config startup-config** 例： n1000v# 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。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 「単一 RADIUS サーバのタイムアウト間隔の設定」（P.5-14）の手順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。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	**radius-server timeout** *seconds* 例： n1000v(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。有効な範囲は 1 ～ 60 秒です。
ステップ 3	**exit** 例： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** 例： n1000v# 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： n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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」（P.5-15）の手順で単一の 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に優先します。

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**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	**radius-server retransmit** *count* 例： n1000v(config)# radius-server retransmit 3	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。これはすべての RADIUS サーバに適用されるグローバル設定です。デフォルトの再送信回数は 1 です。有効な範囲は 0 ～ 5 です。
ステップ 3	**exit** 例： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** 例： n1000v# 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： n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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」（P.5-12）の手順で定義したタイムアウトに優先します。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **timeout** *seconds* 例： `n1000v(config)# radius-server host server1 timeout 10`	特定のサーバのタイムアウト間隔を指定します。デフォルト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	**exit**
	
	例：
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 4	**show radius-server** 例： `n1000v# 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： `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count*
3. **exit**

4. **show radius-server**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count* 例： `n1000v(config)# radius-server host server1 retransmit 3`	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。

ステップ 3	**exit**
	
	例：
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 4	**show radius-server** 例： `n1000v# 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： `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。
- RADIUS アカウンティング メッセージの宛先 UDP ポート番号がわかっています。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*
3. **radius-server host** {*ipv4-address* | *host-name*} **accounting**
4. **exit**

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

手順の詳細

RADIUS サーバの認証およびアカウンティング属性を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port* 例： n1000v(config)# radius-server host 10.10.1.1 acct-port 2004	(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。
ステップ 3	**radius-server host** {*ipv4-address* | *host-name*} **accounting** 例： n1000v(config)# radius-server host 10.10.1.1 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	**exit** 例： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 5	**show radius-server** 例： n1000v(config)# 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： n1000v# copy running-config startup-config	(任意) この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。
- RADIUS 認証メッセージの宛先 UDP ポート番号がわかっています。

手順の概要

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

手順の詳細

RADIUS サーバの認証およびアカウンティング属性を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **auth-port** *udp-port* 例： n1000v(config)# radius-server host 10.10.2.2 auth-port 2005	（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。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 3	**radius-server host** {*ipv4-address* | *host-name*} **authentication** 例： n1000v(config)# radius-server host 10.10.2.2 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	**exit** 例： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 5	**show radius-server** 例： n1000v(config)# 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： n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

RADIUS サーバの定期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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。

（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。

（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。

手順の概要

1. **config t**
2. **radius-server host** {*ipv4-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**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**radius-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **例：** `n1000v(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを指定します。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。

	コマンド	目的
ステップ 3	**radius-server dead-time** *minutes* **例：** `n1000v(config)# radius-server dead-time 5`	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	**exit**
	
	例：
	`n1000v(config)# exit`
	`n1000v#`
		CLI EXEC モードに戻ります。

ステップ 5	**show radius-server** **例：** `n1000v# 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：** `n1000v# copy running-config startup-config`	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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 グループのデッド タイム間隔を設定することもできます（「RADIUS サーバ グループの設定」（P.5-9）を参照）。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

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**

手順の詳細

RADIUS 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。

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	n1000v(config)# **radius-server deadtime** *minutes* 例： n1000v(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： n1000v(config)# exit n1000v#	CLI EXEC モードに戻ります。
ステップ 4	**show radius-server** 例： n1000v# 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： n1000v# copy running-config startup-config	（任意）この実行コンフィギュレーションの変更内容を、スタートアップ コンフィギュレーションに保存します。

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、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **test aaa server radius** {*ipv4-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	目的
ステップ 1	**test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password* **例：** `n1000v# 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可用性を確認します。
ステップ 2	**test aaa group** *group-name username password* **例：** `n1000v# 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可用性を確認します。

RADIUS 設定の確認

この項のコマンドを使用して、RADIUS 設定を確認します。show コマンド出力の詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。

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 サーバの統計情報の表示

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 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
```

その他の関連資料

RADIUS の実装に関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.5-23）
- 「標準」（P.5-23）

関連資料

関連項目	参照先
コマンド リファレンス	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

RADIUS 機能の履歴

ここでは、RADIUS のリリース履歴を示します。

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。