



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, on page 1](#)
- [RADIUS の前提条件, on page 5](#)
- [RADIUS の注意事項と制約事項 \(5 ページ\)](#)
- [RADIUS のデフォルト設定, on page 5](#)
- [RADIUS サーバの設定, on page 6](#)
- [RADIUS 設定の確認, on page 23](#)
- [RADIUS サーバのモニタリング, on page 24](#)
- [RADIUS サーバ統計情報のクリア, on page 24](#)
- [RADIUS の設定例, on page 25](#)
- [次の作業, on page 25](#)
- [RADIUS に関する追加情報, on page 25](#)

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 デバイスで稼働し、すべてのユーザ認証情報およびネットワークサービスアクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウンティング要求を送信します。

RADIUS ネットワーク環境

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

RADIUS は、アクセスセキュリティを必要とする次のネットワーク環境で使

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク。たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。RADIUS を使用した Cisco 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 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセスコントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。
- 認証プロファイルをサポートするネットワーク。ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルを設定アップできます。ユーザごとのプロファイルにより、Cisco NX-OS デバイスは、既存の RADIUS ソリューションを使用してポートを容易に管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル契約（SLA）を提供できます。

RADIUS の動作

ユーザが RADIUS を使用して Cisco NX-OS デバイスへのログインおよび認証を試行すると、次のプロセスが実行されます。

- 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 応答または REJECT 応答には、EXEC 許可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 認可を使用するには、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。

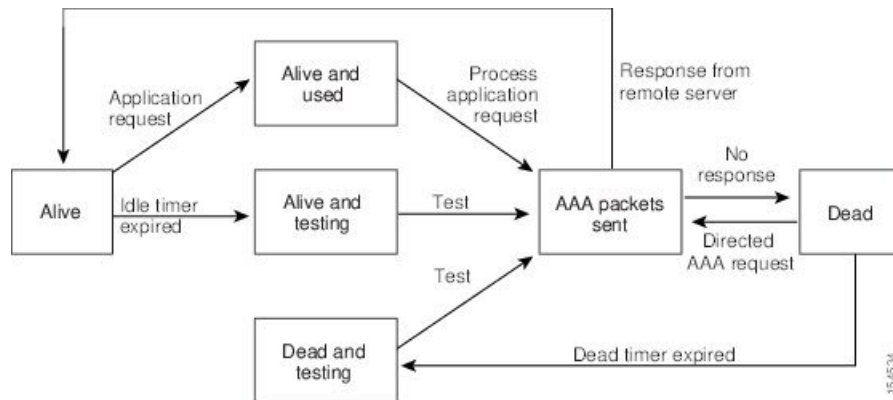
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリアトランスポート（LAT）接続、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセスリスト、ユーザ タイムアウト）

RADIUS サーバのモニタリング

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 要求の処理時間を節約するために、定期的に RADIUS サーバをモニタリングし、RADIUS サーバが応答を返す（アライブ）かどうかを調べるよう、Cisco NX-OS デバイスを設定できます。Cisco NX-OS デバイスは、応答を返さない RADIUS サーバをデッド（dead）としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。Cisco NX-OS デバイスは定期的にデッド RADIUS サーバをモニタリングし、それらが応答を返したら、アライブ状態に戻します。この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 サーバの状態がデッドまたはアライブに変わると、簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OS デバイスによって、障害が発生したことを知らせるエラーメッセージが表示されます。

Figure 1: RADIUS サーバの状態

次の図に、RADIUS サーバモニタリングの状態を示します。



Note

アライブサーバとデッドサーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバモニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワークアクセスサーバと RADIUS サーバの間での 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。ベンダーは VSA を使用して、一般的な用途には適さ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 デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、Cisco 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 ソフトウェアでは、次の属性がサポートされています。

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 `network-admin` のロールに属している場合、値フィールドは `network-operator network-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 network-admin
shell:roles*"network-operator network-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 network-admin\
Cisco-AVPair = shell:roles*\network-operator network-admin\
```



Note

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

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6 アドレスまたはホスト名を取得していること。
- 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。

RADIUS の注意事項と制約事項

RADIUS には次のガイドラインおよび制限事項があります。

- Cisco NX-OS デバイスに設定できる RADIUS サーバの最大数は 64 です。
- 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。
- Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

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。

Table 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	認証とアカウンティング

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
アカウントिंग 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	テスト

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。



Note

Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。



Note

Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。

RADIUS サーバの設定プロセス

1. Cisco NX-OS デバイスと RADIUS サーバとの接続を確立します。
2. RADIUS サーバの RADIUS 秘密キーを設定します。
3. 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。
4. 必要に応じて、次のオプションのパラメータを設定します。
 - デッドタイム間隔
 - 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

5. (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。

Related Topics

[RADIUS サーバホストの設定](#) (7 ページ)

[グローバル RADIUS キーの設定](#) (8 ページ)

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。



Note 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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	radius-server host {ipv4-address ipv6-address hostname} Example: <pre>switch(config)# radius-server host 10.10.1.1</pre>	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	exit Example:	設定モードを終了します。

	Command or Action	Purpose
	<code>switch(config)# exit</code> <code>switch#</code>	
ステップ 4	(Optional) show radius-server Example: <code>switch# show radius-server</code>	RADIUS サーバの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	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。

Related Topics

[特定の RADIUS サーバ用のキーの設定](#) (9 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 キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	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 6 7] key-value Example: <code>switch(config)# radius-server key 0 QsEfThUkO</code>	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 テキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) 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

	Command or Action	Purpose
		リア テキストです。最大で 63 文字です。 デフォルトでは、RADIUS キーは設定されません。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。 Note 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、 show running-config コマンドを使用します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	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。

Related Topics[RADIUS サーバ グループの設定 \(11 ページ\)](#)[AES パスワード暗号化およびプライマリ暗号キーについて](#)

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 ストリングです。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	radius-server host {ipv4-address ipv6-address hostname} key [0 6 7] key-value Example: <pre>switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg</pre>	特定の RADIUS サーバ用の RADIUS キーを指定します。key-value がクリア テキスト形式 (0) か、タイプ 6 暗号化形式 (6) か、タイプ 7 暗号化形式 (7) 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。 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。
ステップ 3	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。 Note 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、show running-config コマンドを使用します。
ステップ 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	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。

Related Topics

[RADIUS サーバ ホストの設定 \(7 ページ\)](#)

[AES パスワード暗号化およびプライマリ暗号キーについて](#)

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。

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。

Before you begin

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	aaa group server radius group-name Example: <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。 RADIUS サーバグループを削除するには、このコマンドの no 形式を使用します。 Note デフォルトのシステム生成デフォルトグループ (RADIUS) は削除できません。
ステップ 3	server {ipv4-address ipv6-address hostname} Example: <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、 radius-server host コマンドを実行し、このコマンドを再試行します。
ステップ 4	(Optional) deadtime minutes Example: <pre>switch(config-radius)# deadtime 30</pre>	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。 Note

	Command or Action	Purpose
		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	(Optional) server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } Example: <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。 Tip 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 6	(Optional) use-vrf <i>vrf-name</i> Example: <pre>switch(config-radius)# use-vrf vrf1</pre>	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	exit Example: <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	(Optional) show radius-server groups [<i>group-name</i>] Example: <pre>switch(config)# show radius-server groups</pre>	RADIUS サーバグループの設定を表示します。
ステップ 9	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

Related Topics

[RADIUS デッドタイム間隔の設定](#) (21 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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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	ip radius source-interface interface Example: 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	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: switch# show radius-server	RADIUS サーバの設定情報を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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。

Related Topics

[RADIUS サーバ グループの設定](#) (11 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の AAA 認証方式に基づいて認証要求を転送します。VRF と認証要求送信先 RADIUS サーバをユーザが指定できるように Cisco NX-OS デバイスを設定するには、directed-request オプションを有効にします。このオプションを有効にした場合、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。



Note

directed-request オプションを有効にすると、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。



Note 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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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	radius-server directed-request Example: 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。デフォルトでは無効になっています。
ステップ 3	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) show radius-server directed-request Example: switch# show radius-server directed-request	directed request の設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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 デバイスはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔には、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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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	radius-server retransmit count Example: 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、範囲は 0 ～ 5 です。
ステップ 3	radius-server timeout seconds Example: 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、範囲は 1 ～ 60 秒です。
ステップ 4	exit Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: switch# show radius-server	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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。

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

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	radius-server host {ipv4-address ipv6-address hostname} retransmit count Example: <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。 Note 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	radius-server host {ipv4-address ipv6-address hostname} timeout seconds Example: <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。 Note 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	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	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。

Related Topics

[RADIUS サーバ ホストの設定 \(7 ページ\)](#)

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。

Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	(Optional) radius-server host {ipv4-address ipv6-address hostname} acct-port udp-port Example: <pre>switch(config)# radius-server host 10.10.1.1 acct-port 2004</pre>	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。範囲は 0 ～ 65535 です。
ステップ 3	(Optional) radius-server host {ipv4-address ipv6-address hostname} accounting Example: <pre>switch(config)# radius-server host 10.10.1.1 accounting</pre>	RADIUS サーバをアカウントティングだけに使用することを指定します。デフォルトでは、アカウントティングと認証の両方に使用されます。
ステップ 4	(Optional) radius-server host {ipv4-address ipv6-address hostname} auth-port udp-port Example: <pre>switch(config)# radius-server host 10.10.2.2 auth-port 2005</pre>	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。範囲は 0 ～ 65535 です。
ステップ 5	(Optional) radius-server host {ipv4-address ipv6-address hostname} authentication Example: <pre>switch(config)# radius-server host 10.10.2.2 authentication</pre>	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、アカウントティングと認証の両方に使用されます。
ステップ 6	exit Example:	設定モードを終了します。

	Command or Action	Purpose
	switch(config)# exit switch#	
ステップ 7	(Optional) show radius-server Example: switch# show radius-server	RADIUS サーバの設定を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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。

Related Topics

[RADIUS サーバ ホストの設定](#) (7 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。



Note 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 サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテスト パケットを送信するかを指定します。このオプションを設定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。



Note 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。



Note 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。

Before you begin

RADIUS をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	radius-server test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]} Example: <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 test、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。 Note 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	radius-server deadtime minutes Example: <pre>switch(config)# radius-server deadtime 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	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。

Related Topics

[各 RADIUS サーバの定期モニタリングの設定](#) (20 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 サーバがどのくらいの期間要求を受信しなかった場合に Cisco NX-OS スイッチがテスト パケットを送信するかを指定します。このオプションを設定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。



Note 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。



Note 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。



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

Before you begin

RADIUS を有効にします。

1 つまたは複数の RADIUS サーバ ホストを追加します。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <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	radius-server host {ipv4-address ipv6-address hostname} test {idle-time minutes password password [idle-time minutes] username name [password password [idle-time minutes]]} Example:	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 test、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。

	Command or Action	Purpose
	<pre>switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	Note 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	radius-server deadtime minutes Example: <pre>switch(config)# radius-server deadtime 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 4	exit Example: <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	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。

Related Topics

[RADIUS サーバ ホストの設定](#) （7 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](#) （18 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。デッドタイム間隔には、Cisco NX-OS デバイスが、RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを確認するためにテスト パケットを送信するまでの間隔を指定します。デフォルト値は 0 分です。



Note

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。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: 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	radius-server deadtime minutes Example: 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 Example: switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) show radius-server Example: switch# show radius-server	RADIUS サーバの設定を表示します。
ステップ 5	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	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。

Related Topics

[RADIUS サーバ グループの設定](#) (11 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。



Note

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。

Before you begin

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 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。

Procedure

	Command or Action	Purpose
ステップ 1	test aaa server radius {ipv4-address ipv6-address hostname} [vrf vrf-name] username password Example: <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	test aaa group group-name username password Example: <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
show radius {status pending pending-diff}	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。
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 [hostname ipv4-address ipv6-address] [directed-request groups sorted statistics]	設定済みのすべての RADIUS サーバのパラメータを表示します。

RADIUS サーバのモニタリング

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します。

Before you begin

1 つまたは複数の RADIUS サーバホストを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	show radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# show radius-server statistics 10.10.1.1	RADIUS 統計情報を表示します。

Related Topics

[RADIUS サーバホストの設定](#) (7 ページ)

[RADIUS サーバ統計情報のクリア](#) (24 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。

Before you begin

Cisco NX-OS デバイスの RADIUS サーバを設定します。

Procedure

	Command or Action	Purpose
ステップ 1	(Optional) show radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# show radius-server statistics 10.10.1.1	Cisco NX-OS デバイスの RADIUS サーバ統計情報を表示します。
ステップ 2	clear radius-server statistics {hostname ipv4-address ipv6-address} Example: switch# clear radius-server statistics 10.10.1.1	RADIUS サーバ統計情報をクリアします。

Related Topics

[RADIUS サーバホストの設定](#)（7 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 "ToIkLhPg"
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	マニュアル タイトル
Cisco NX-OS ライセンス設定	『Cisco NX-OS ライセンス ガイド』

関連項目	マニュアル タイトル
VRF コンフィギュレーション	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

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。	—

MIB

MIB	MIB のリンク
RADIUS に関連する MIB	サポートされている 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。 ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。