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

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 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セットアップできます。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。

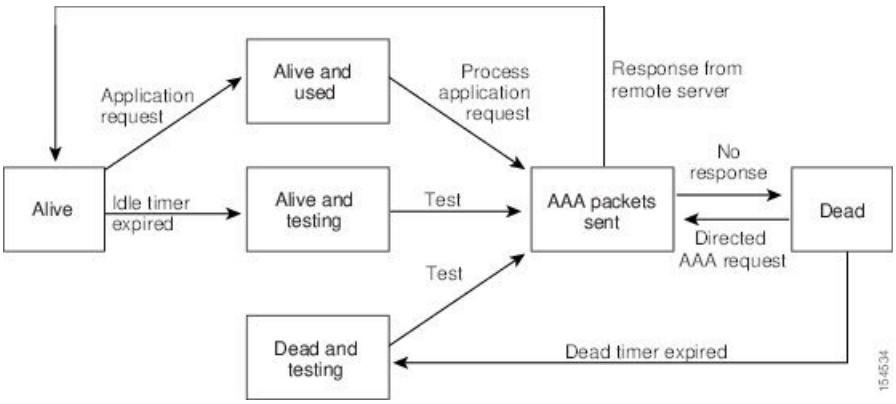
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリア トランスポート（LAT）接続、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト）

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 認可変更について

標準RADIUSインターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリが送信されたサーバが応答するプル モデルで使用されます。Cisco NX-OS ソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS Change of Authorization（CoA）要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、認可、およびアカウンティング（AAA）またはポリシー サーバからの動的なセッション再設定が可能になります。

Dot1x が有効の場合、ネットワーク デバイスはオーセンティケータとして機能し、セッションごとのダイナミック COA を処理します。

次の要求がサポートされています。

- セッション再認証
- セッションの終了

セッション再認証

セッションの再認証を開始するには、認証、認可、およびアカウンティング（AAA）サーバは、Cisco VSA および 1 個以上のセッションの ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は Cisco:Avpair=“subscriber:command=reauthenticate” の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1x によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN（EAPoL）-RequestId メッセージをサーバに送信することで応答します。
- 現在、セッションが MAC 認証バイパス（MAB）で認証されている場合は、デバイスはサーバにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

- デバイスがコマンドを受信する際にセッションの認証が行われている場合、デバイスはプロセスを終了し、認証シーケンスを再起動して、最初に試行されるように設定された方式を開始します。

セッションの終了

CoA 接続解除要求は、ホスト ポートを無効にせずにセッションを終了します。CoA 接続解除：終了の要求によって、指定したホストのオーセンティケータ ステート マシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。

セッションが見つからない場合、デバイスは「Session Context Not Found」エラー コード属性を使用して Disconnect-NAK メッセージを返します。

セッションが見つかったが、何らかの内部エラーのために NAS がセッションを削除できなかった場合、デバイスは「Session Context Not Removable」エラー コード属性を持つ Disconnect-NAK メッセージを返します。

セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

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。
- N9K-X9636C-R および N9K-X9636Q-R ラインカードおよび N9K-C9508-FM-R ファブリック モジュールの場合、特殊文字を含むユーザ名の RADIUS 認証は失敗します。

- 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。
- Cisco NX-OS リリース 10.3(1)F 以降、RADIUS は Cisco Nexus 9808 プラットフォーム スイッチでサポートされます。
  - Cisco NX-OS リリース 10.4(1)F 以降、RADIUS は、Cisco Nexus X98900CD-A および X9836DM-A ライン カードを搭載した 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、RADIUS は、X98900CD-A および X9836DM-A ライン カードを搭載した Cisco Nexus 9804 スイッチでサポートされます。
- **radius-server key コマンド** および **radius-server host***hostname***key** コマンドの **key** の値は、引用符の付かないものか（例：secret）、または正しく引用符を付けたもの（例："secret"）である必要があります。以下は許可されません。
  - **先頭または末尾の片方だけに引用符が付いたもの**（例：a"、"abc）。
  - **語の途中に引用符が含まれたもの**： 前後の引用符なし（例：ab"cd）、または前後に引用符あり（例："ab"cd"）。
- Cisco NX-OSリリース 10.4(4) 以降、radius-server CLIでは、タイムアウトと再送信のパラメータに値 0 を使用できます。

  Cisco NX-OSリリース 10.4(4) 以降では、 **show running-config** 出力にもタイムアウトと再送信の値 0 が表示されます。

  リリース 10.4(4) と 9.3(11) 以降の間のダウングレード中に、これらの修正を行わないと、タイムアウト値 0 または再送信値 0 を使用する RADIUS サーバー構成が失われるか、機能しない可能性があります。構成の一貫性を確保するために、影響を受けるリリース間での移行時にこれらのパラメータの値として 0 を使用しないでください。または、ソースとターゲットの両方のリリースでこれらの値がサポートされていることを確認してください。

RadSec の注意事項と制約事項

RadSec には、次の注意事項と制約事項 があります。

- Cisco NX-OS リリース 10.3(1)F 以降、トランスポート層での RADIUS/TCP ピア間の通信を保護するために、RADIUS Secure（RadSec）サポートが Cisco Nexus スイッチで提供されます。
- RadSec はスイッチ レベルで有効/無効にする必要があります。これは、異なるトランスポート プロトコル（つまり、UDP と TCP-with-TLS）を持つサーバーの組み合わせが不可能であるためです。

- **radius-serverdirected-request** コマンドは、RadSec 機能ではサポートされていません。
- **test aaa server radius** コマンドは RadSec サーバーではサポートされていません。RadSec でサポートされるのは **test aaa group** コマンドだけです。
- Dot1x は RadSec で公式にサポートされていません。
- RADIUS サーバーの監視は、RadSec サーバーではサポートされていません。
- RADIUS サーバーの再送信とタイムアウトは、UDP ベースの RADIUS モードに適用されますが、RadSec サーバーに対してはサポートされません。
- Cisco NX-OS リリース 10.4(3)F 以降、TLS バージョン 1.3 および 1.2 が、Cisco Nexus スイッチでサポートされています。TLS v1.1 は廃止されました。

RADIUS の認可変更の注意事項と制約事項

RADIUS の認可変更に関する注意事項と制約事項は次のとおりです。

- RADIUS の認可変更は FEX によりサポートされています。
- RADIUS の認可変更は VXLAN EVPN によりサポートされています。

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
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	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 （9 ページ）
グローバル RADIUS キーの設定 （11 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:
	`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 host** {*ipv4-address* | *ipv6-address* | *hostname*} **Example:** `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	**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

特定の RADIUS サーバ用のキーの設定 （12 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:
	`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 key** [**0** | **6** | **7**] *key-value*
	Example:
	`switch(config)# radius-server key 0 QsEfThUkO`
	Example:
	`switch(config)# radius-server key 7 "fewhg"`
		すべての 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。
		デフォルトでは、RADIUS キーは設定されません。
		Note
		generate type7_encrypted_secret を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。詳細については、RADIUS または TACACS+ の共有秘密の設定を参照してください。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	Command or Action	Purpose
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。 **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:** `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 （19 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:
	`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 host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **6** | **7**] *key-value* **Example:**	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**）

	Command or Action	Purpose

	`switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg`
	Example:
	`switch(config)# radius-server host 10.10.1.1 key 7 "fewhg"`
		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。
		Note
		generate type7_encrypted_secret を使用してすでに共有秘密を設定している場合 コマンドを使用して、二番目の例に示すように引用符に入力します。詳細については、RADIUS または TACACS+ の共有秘密の設定を参照してください。

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。 **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:** `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 （9 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 属性メッセージ オーセンティケータの構成

Cisco NX-OS スイッチを使用するすべてのサーバに RADIUS 属性メッセージ オーセンティケータを構成できます。RADIUS 属性は、Extended Access Protocol（EAP; 拡張アクセス プロトコル）パケットをカプセル化して、スイッチが HMAC-MD5 を使用して EAP 経由でダイヤルイン ユーザを認証できるようにします。

（注） Cisco Fabric Services（CFS）は、RADIUS 属性メッセージ オーセンティケータを配信しません。

Cisco NX-OS リリース 10.2(9)M 以降、Cisco Nexus 9000 スイッチでは、**radius-server attribute message-authenticator** コマンドが導入されています。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	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	**radius-server attribute message-authenticator** 例： `switch(config)# radius-server attribute message-authenticator`	すべての RADIUS サーバに RADIUS 属性 message-authenticaton を指定します。 デフォルトでは、RADIUS 属性の message-authenticator は無効になっています。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	（任意） **show radius-server**
	例：
	`switch# show radius-server`
	`etransmission count:1`
	`timeout value:5`
	`deadtime value:0`
	`message-authenticator attribute:enabled`
	`source interface:any available`
	`total number of servers:4`
	
	`following RADIUS servers are configured:`
	`10.10.1.1:`
	`available for`
		RADIUS サーバの設定を表示します。

	コマンドまたはアクション	目的
	`authentication on port:1812 available for accounting on port:1813 RADIUS shared secret:******** timeout:60`	
ステップ 5	（任意） **copy running-config startup-config** 例： `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。

RadSec の設定

RadSec は、TLS 経由で RADIUS データグラムを転送するためのプロトコルです。

この手順では、スイッチで RadSec を有効または無効にする方法について説明します。

始める前に

- サーバーのクライアント ID 証明書と CA 証明書がスイッチにインストールされていることを確認します。
- サーバー証明書のサブジェクト名が、スイッチで構成されているサーバーのホスト名/IP アドレスと一致していることを確認してください。
- RadSec サーバーを使用するように AAA 認証とアカウンティングを設定する前に、**test aaa group** コマンドを使用して、RadSec 認証が成功することを確認します。
- スイッチからの頻繁な TLS セッションの再試行を避けるために、RadSec サーバーで TLS アイドル タイムアウトを最大値に設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	コンフィギュレーション モードに入ります。
ステップ 2	**radius-server secure tls** 例： `switch# radius-server secure tls`	グローバル レベルで有効にします。 （注） この CLI は、RadSec に使用されるポート番号を変更または影響しません。

	コマンドまたはアクション	目的
ステップ 3	**radius-server host t** {*ipv4-address* | *ipv6-address*| *hostname*} **key** {*key*} **auth-port 2083 acct-port 2083 authentication accounting** 例： `switch# radius-server host 10.105.222.161 key radsec auth-port 2083 acct-port 2083 authentication accounting`	認証およびアカウンティング ポートとともに共有秘密キーを使用して RadSec サーバーを構成します。 （注） サーバーの場合、認証とアカウンティングのデフォルトの RadSec ポートは「2083」で、キーは「radsec」です。スイッチの場合、RadSec ポートとキーのデフォルト設定はありません。サーバーで定義されているように、この設定を明示的に追加してください。
ステップ 4	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **tls client-trustpoint** *trustpoint* 例： `switch# radius-server host 10.105.222.161 tls client-trustpoint rad1`	クライアント ID 証明書がインストールされている TLS クライアント トラストポイントを設定します。
ステップ 5	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **tls idle-timeout** *value* 例： `switch# radius-server host 10.105.222.161 tls idle-timeout 80`	TLS アイドル タイムアウトを設定します。デフォルト値は 600 秒です。 （注） RadSec クライアントからのトランザクションがない場合、サーバーはタイムアウト値に基づいて接続を閉じることができます。クライアントの TLS アイドル タイムアウトは、このリリースではサポートされていません。クライアントは自分自身で接続を閉じません。

（注） リモートユーザーがログインすると、約20秒間のログインの遅延が見られることがあります。つまり、スイッチと RadSec サーバーの間で TLS セッションの確立が初めて行われるときです。TLS セッションが起動すると、連続したリモート ログインで遅延は見られません。

（注） RadSec クライアントで、証明書が存在しない、または無効な証明書がサーバーと交換されているなどの証明書関連の問題が発生している場合、`show run` コマンドで遅延が発生する可能性があります。

DTLS を使用した RADIUS について

Cisco NX-OS リリース 10.4(1)F から、DTLS プロトコルを使用した RADIUS が導入されました。このプロトコルは、UDP を使用してセキュア チャネルを介して RADIUS データグラムを転送するためのものです。

RADIUS と DTLS は、トランスポート層での RADIUS ピア間のセキュアな通信を可能にします。このプロトコルは、さまざまな管理ドメインや疑わしい、安全でないネットワークを介してセキュアな RADIUS パケット転送を行いたい場合に役立ちます。

DTLS を使用する RADIUS の構成

始める前に

- スイッチの IP アドレス/DNS ホスト名と同じサブジェクトと代替名を使用してクライアントアイデンティティ証明書を作成してください。トラストポイントを使用して、スイッチにクライアント アイデンティティ証明書をインストールします。
- DTLS/RADIUS に使用される ISE サーバのサーバ証明書がスイッチにインストールされていることを確認します。
- クライアント アイデンティティ証明書の署名に使用される CA 証明書が ISE サーバーの信頼できる証明書ストアにインストールされていることを確認します。
- サーバー証明書のサブジェクト名が、スイッチで構成されているサーバーのホスト名/IPアドレスと同じであることを確認します。
- RADIUS サーバーを使用するように AAA 認証およびアカウンティンググループを構成する前に、test aaa group コマンドで RADIUS 認証が成功することを確認します。
- スイッチ レベルで RADIUS と DTLS プロトコルを有効にする必要があります。
- DTLS と TLS など、異なるトランスポートプロトコルを使用するように RADIUS サーバーを組み合わせて構成することはサポートされていません。一度に 1 つのプロトコルを構成できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**radius-server secure dtls** 例：	スイッチで RADIUS with DTLS プロトコルを有効にします。

	コマンドまたはアクション	目的
	`switch(config)# radius-server secure dtls`	
ステップ 3	**radius-server host** {*ipv4-address* | *ipv6-address*| *hostname*} **key** {*radius/dtls*} **auth-port 2083 acct-port 2083 authentication accounting** 例： `switch(config)# radius-server host 10.105.222.161 key radius/dtls auth-port 2083 acct-port 2083 authentication accounting`	共有秘密キー、および認証ポートとアカウンティングポートを使用して、RADIUS サーバを構成します。 （注） 認証およびアカウンティングのデフォルトの接続先 DTLS ポートは **UDP/2083** です。RFC に従って、DTLS のデフォルトのサーバー キーはありません。サーバーで定義されているように、この構成を明示的に追加してください。ISE サーバーは、その時点で「radius/dtls」キーで事前設定されている必要があります。ISE サーバーで DTLS を構成するときに、Nexus スイッチでキーを確認して追加します。
ステップ 4	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **dtls client-trustpoint** *trustpoint* 例： `switch(config)# radius-server host 10.105.222.161 dtls client-trustpoint rad1`	スイッチ ID 証明書がインストールされているトラストポイントで、DTLS client-trustpoint パラメータを構成します。*rad1* は、クライアントアイデンティティ証明書が必要なスイッチ上のトラストポイントです。
ステップ 5	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **dtls idle-timeout** *value* 例： `switch# radius-server host 10.105.222.161 dtls idle-timeout 80`	DTLS アイドル タイムアウトを設定します。デフォルト値は 600 秒です。 （注） RADIUS クライアントからのトランザクションがない場合、サーバは定義されたタイムアウト値に従い接続を閉じます。クライアントの DTLS アイドル タイムアウトは、このリリースではサポートされていません。クライアントは自分自身で接続を閉じません。

（注）
- リモートユーザーがログインすると、約20秒の遅延が発生することがあります。これは、スイッチとRADIUSサーバの間でTLSセッションが初めて確立されるときに発生します。いったん TLS セッションが確立されれば、後続のリモートログインで遅延は発生しません。
- RADIUSクライアントで、証明書が存在しない、または無効な証明書がサーバと交換されているなどの証明書関連の問題が発生している場合、`show run` コマンドで遅延が発生する可能性があります。

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:
	`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	**aaa group server radius** *group-name*
	Example:
	`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

	Command or Action	Purpose
		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:** `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。 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:** `switch(config-radius)# deadtime 30`	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** 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** {*ipv4-address* | *ipv6-address* | *hostname*} **Example:** `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。 **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** *vrf-name* **Example:** `switch(config-radius)# use-vrf vrf1`	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:
	`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。

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

	Command or Action	Purpose
ステップ 9	(Optional) **copy running-config startup-config** **Example:** `switch(config)# 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 デッド タイム間隔の設定 （30 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。

	Command or Action	Purpose
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 （19 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。

	Command or Action	Purpose
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。

	Command or Action	Purpose
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:
	`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 host** {*ipv4-address* | *ipv6-address* | *hostname*} **retransmit** *count* **Example:** `switch(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。 **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:** `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。 **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

	Command or Action	Purpose
		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:
	`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。

Related Topics

RADIUS サーバ ホストの設定 （9 ページ）

RADIUS サーバのアカウンティングおよび認証属性の設定

RADIUS サーバをアカウンティング専用、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:
	`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	(Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **acct-port** *udp-port* **Example:**	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 1813 です。範囲は 0 ～ 65535 です。

	Command or Action	Purpose
	`switch(config)# radius-server host 10.10.1.1 acct-port 2004`	
ステップ 3	(Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **accounting** **Example:** `switch(config)# radius-server host 10.10.1.1 accounting`	RADIUS サーバをアカウン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:** `switch(config)# radius-server host 10.10.2.2 auth-port 2005`	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:** `switch(config)# radius-server host 10.10.2.2 authentication`	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、アカウンティングと認証の両方に使用されます。

ステップ 6	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

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 （9 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:
	`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 test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3`	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。

	Command or Action	Purpose
ステップ 3	**radius-server deadtime** *minutes* **Example:** `switch(config)# radius-server deadtime 5`	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:
	`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。

Related Topics

各 RADIUS サーバの定期モニタリングの設定 （28 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:
	`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 host** {*ipv4-address* | *ipv6-address* | *hostname*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]} **Example:** `switch(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。 **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:** `switch(config)# radius-server deadtime 5`	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:
	`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。

	Command or Action	Purpose
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。

Related Topics

RADIUS サーバ ホストの設定 （9 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 （26 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、デットとしてマークされません。RADIUS サーバ グループに対するデッド タイム間隔を設定できます。

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。

	Command or Action	Purpose
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 （19 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:** `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可用性を確認します。
ステップ 2	**test aaa group** *group-name username password* **Example:** `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可用性を確認します。

Dynamic Author Server の有効化または無効化

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	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	**aaa server radius dynamic-author** 例： `switch(config)# aaa server radius dynamic-author`	RADIUS dynamic author server を有効にします。このコマンドのno形式を使用すれば、RADIUS dynamic author server を無効にできます。

RADIUS 認可変更の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	[**no**] **aaa server radius dynamic-author** 例： `switch(config)# aaa server radius dynamic-author`	スイッチを AAA サーバとして設定し、外部ポリシー サーバとの連携を促進します。このコマンドの no 形式を使用して、RADIUS ダイナミック オーサーと、関連付けられたクライアントを無効にできます。
ステップ 3	[**no**] **client** {*ip-address* | **hostname** } [**server-key** [**0** | **7**] *string*] 例： `switch(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1`	AAA サーバ クライアントの IP アドレスまたはホスト名を設定します。オプションの server-key キーワードと string 引数を使用して、「クライアント」レベルでサーバ キーを設定します。クライアント サーバを削除するには、このコマンドの no 形式を使用します。 （注） クライアント レベルでサーバ キーを設定すると、グローバル レベルで設定されたサーバ キーが上書きされます。
ステップ 4	[**no**] **port** *port-number* 例： `switch(config-locsvr-da-radius)# port 3799`	設定された RADIUS クライアントからの RADIUS 要求をデバイスが受信するポートを指定します。ポート範囲は 1 ～ 65535 です。デフォルトのポートに戻すには、このコマンドの no 形式を使用します。 （注） パケット オブ ディスコネクトのデフォルト ポートは 1700 です。
ステップ 5	[**no**] **server-key** [**0** | **7**] *string*	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。サーバ キーを削除するには、このコマンドの no 形式を使用します。

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 認可変更の設定の検証

RADIUS 認可変更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 running-config dot1x	実行コンフィギュレーションの dot1x 設定を表示します。
show running-config aaa	実行コンフィギュレーションの AAA 設定を表示します。
show running-config radius	実行コンフィギュレーションの RADIUS 設定を表示します。
show aaa server radius statistics	ローカルの RADIUS サーバ統計情報を表示します。
show aaa client radius statistics {*ip address* | *hostname* }	ローカルの RADIUS クライアント統計情報を表示します。
clear aaa server radius statistics	ローカルの RADIUS サーバ統計情報をクリアします。
clear aaa client radius statistics {*ip address* | *hostname* }	ローカルの RADIUS クライアント統計情報をクリアします。

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 （9 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。

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 （9 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 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

RADIUS 認可変更の設定例

次に、RADIUS の認可変更を設定する方法の例を示します。

```
radius-server host 10.77.143.170 key 7 "fewhg123" authentication accounting
aaa server radius dynamic-author
    client 10.77.143.170 vrf management server-key 7 "fewhg123"
```

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』
VRF コンフィギュレーション	『*Cisco Nexus 9000* シリーズ *NX-OS* ユニキャスト ルーティング設定ガイド』

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。 https://cisco.github.io/cisco-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。