RADIUS の設定

この章は、次の項で構成されています。

RADIUS の設定

RADIUS の概要

Remote Access Dial-In User Service（RADIUS）分散クライアント/サーバー 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 Nexus デバイスで稼働し、すべてのユーザー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 サーバー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 Nexus デバイスをネットワークに追加できます。この作業は、AAA サーバー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。ユーザーごとのプロファイルにより、Cisco Nexus 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 レベル契約を提供できます。

RADIUS の操作について

ユーザーがログインを試行し、RADIUS を使用してCisco Nexus デバイスに対する認証を行う際には、次のプロセスが実行されます。

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：ユーザーが認証されたことを表します。
   - REJECT：ユーザーは認証されず、ユーザー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サーバーによってチャレンジが発行されます。チャレンジは、ユーザーから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバーからユーザー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 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。

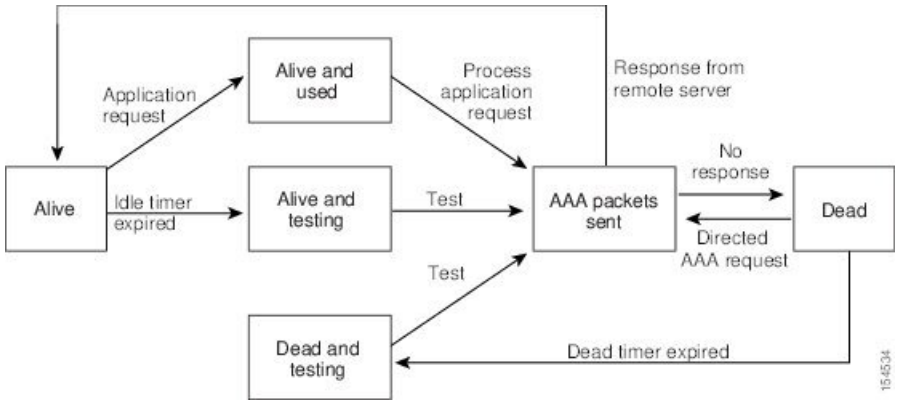
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリアトランスポート（LAT）接続、ポイントツーポイントプロトコル（PPP）、シリアルラインインターネットプロトコル（SLIP）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザー タイムアウトなどの接続パラメータ

RADIUS サーバのモニタリング

応答を返さない RADIUS サーバーがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するために、定期的に RADIUS サーバーをモニタリングし、RADIUS サーバーが応答を返す（アライブ状態である）かどうかを調べるよう、スイッチを設定できます。スイッチは、応答を返さない RADIUS サーバーをデッド（dead）状態としてマークし、デッド RADIUS サーバーには AAA 要求を送信しません。また、定期的にデッド RADIUS サーバーをモニタリングし、それらが応答を返したらアライブ状態に戻します。このプロセスにより、RADIUS サーバーが稼働状態であることを確認してから、実際の AAA 要求がサーバーに送信されます。RADIUS サーバー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、障害が発生したことを知らせるエラーメッセージがスイッチによって表示されます。

次の図に、さまざまな RADIUS サーバーの状態を示します。

***Figure 1: RADIUS* サーバーの状態**



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 サーバーと RADIUS サーバーの間でのベンダー固有属性（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 *
```

プロトコルは、特定のタイプの許可用のシスコ属性です。必須属性の区切り文字は等号（=）で、アスタリスク（*）は任意属性を示します。

Cisco Nexus デバイスでの認証に RADIUS サーバーを使用する場合は、認証結果とともに許可情報などのユーザー属性を返すよう、RADIUS プロトコルが RADIUS サーバーに指示します。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 Nexus デバイスでサポートされています。

- Shell：ユーザー プロファイル情報を提供する access-accept パケットで使用されます。
- Accounting：accounting-request パケットで使用されます。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 Nexus デバイスでは、次の属性がサポートされています。

- roles：ユーザー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複数のロール名をリストするストリングです。
- 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 サーバーの IPv4 アドレスまたはホスト名を取得すること。
- RADIUS サーバーから事前共有キーを取得すること。
- Cisco Nexus デバイスが、AAA サーバーの 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 設定時の注意事項と制限事項は次のとおりです。

- Cisco Nexus デバイスに設定できる RADIUS サーバーの最大数は 64 です。
- ASCII（PAP）認証は RADIUS サーバーではサポートされていません。

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 サーバの設定

ここでは、RADIUS サーバーの設定方法について説明します。

SUMMARY STEPS

1. Cisco Nexus デバイスと RADIUS サーバーとの接続を確立します。
2. RADIUS サーバーの事前共有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。
5. 必要に応じて、定期的に RADIUS サーバーをモニタリングするよう設定します。

DETAILED STEPS

Procedure

ステップ 1 Cisco Nexus デバイスと RADIUS サーバーとの接続を確立します。

ステップ 2 RADIUS サーバーの事前共有秘密キーを設定します。

ステップ 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。

ステップ 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
- ログイン時に RADIUS サーバーの指定を許可

- 送信リトライ回数とタイムアウト間隔
- アカウンティングおよび認証属性

ステップ 5 必要に応じて、定期的に RADIUS サーバーをモニタリングするよう設定します。

RADIUS サーバ ホストの設定

認証に使用する各 RADIUS サーバーについて、IPv4 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 サーバー ホストは、デフォルトの RADIUS サーバー グループに追加されます。最大 64 の RADIUS サーバーを設定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *host-name*}
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server host** {*ipv4-address* | *host-name*}	RADIUS サーバーの IPv4 アドレスまたはホスト名を指定します。
ステップ 3	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、RADIUS サーバーとしてホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
```

```
switch(config)# exit
switch# copy running-config startup-config
```

RADIUS のグローバルな事前共有キーの設定

Cisco Nexus デバイスで使用するすべてのサーバーについて、グローバル レベルで事前共有キーを設定できます。事前共有キーとは、スイッチと RADIUS サーバー ホスト間の共有秘密テキスト ストリングです。

Before you begin

リモートの RADIUS サーバーの事前共有キー値を取得していること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server key** [**0** | **7**] *key-value*
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server key** [**0** | **7**] *key-value*	すべての RADIUS サーバー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**）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	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。 **Note** 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。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、デバイスで使用するすべてのサーバーについて、グローバル レベルで事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# copy running-config startup-config
```

RADIUS サーバーの事前共有キーの設定

事前共有キーとは、Cisco Nexus デバイスと RADIUS サーバー ホスト間の共有秘密テキスト ストリングです。

Before you begin

リモートの RADIUS サーバーの事前共有キー値を取得していること。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の RADIUS サーバー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**）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 文字です。

	Command or Action	Purpose
		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。
ステップ 3	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。 **Note** 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	(Optional) switch# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、RADIUS 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch (config)# **aaa group server radius** *group-name*
3. switch (config-radius)# **server** {*ipv4-address* |*server-name*}
4. (Optional) switch (config-radius)# **deadtime** *minutes*
5. (Optional) switch(config-radius)# **source-interface** *interface*
6. switch(config-radius)# **exit**
7. (Optional) switch(config)# **show radius-server group** [*group-name*]
8. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch (config)# **aaa group server radius** *group-name*	RADIUS サーバー グループを作成し、そのグループの RADIUS サーバー 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	switch (config-radius)# **server** {*ipv4-address* |*server-name*}	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	(Optional) switch (config-radius)# **deadtime** *minutes*	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) switch(config-radius)# **source-interface** *interface*	特定の RADIUS サーバー グループに発信元インターフェイスを割り当てます。 サポートされているインターフェイスのタイプは管理および VLAN です。 **Note** source-interface コマンドを使用して、ip radius source-interface コマンドによって割り当てられたグローバル ソース インターフェイスをオーバーライドします。
ステップ 6	switch(config-radius)# **exit**	設定モードを終了します。
ステップ 7	(Optional) switch(config)# **show radius-server group** [*group-name*]	RADIUS サーバー グループの設定を表示します。

	Command or Action	Purpose
ステップ 8	(Optional) switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、RADIUS サーバー グループを設定する例を示します。

```
switch# configure terminal
switch (config)# aaa group server radius RadServer
switch (config-radius)# server 10.10.1.1
switch (config-radius)# deadtime 30
switch (config-radius)# use-vrf management
switch (config-radius)# exit
switch (config)# show radius-server group
switch (config)# copy running-config startup-config
```

What to do next

AAA サービスに RADIUS サーバー グループを適用します。

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip radius source-interface** *interface*
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **ip radius source-interface** *interface*	このデバイスで設定されているすべての RADIUS サーバー 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。発信元インターフェイス

	Command or Action	Purpose
		は、管理またはVLANインターフェイスにすることができます。
ステップ 3	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show radius-server**	RADIUS サーバーの設定情報を表示します。
ステップ 5	(Optional) 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。

Example

次に、RADIUS サーバー グループのグローバル発信元インターフェイスとして、mgmt 0 インターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# ip radius source-interface mgmt 0
switch(config)# exit
switch# copy running-config startup-config
```

ログイン時にユーザによる RADIUS サーバの指定を許可

ログイン時に RADIUS サーバーを指定することをユーザーに許可できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server directed-request**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server directed-request**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server directed-request**	ログイン時にユーザーが認証要求の送信先となる RADIUS サーバー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	switch(config)# **exit**	コンフィグレーション モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) switch# **show radius-server directed-request**	directed request の設定を表示します。
ステップ 5	(Optional) 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。

Example

次に、ネットワークにログインしたときに、ユーザーが RADIUS サーバーを選択できるようにする例を示します。

```
switch# configure terminal
switch(config)# radius-server directed-request
switch# exit
switch# copy running-config startup-config
```

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。

手順の概要

1. **configure terminal**
2. **radius-server secure tls**
3. **radius-server host t** {*ipv4-address* | *ipv6-address*| *hostname*} **key** {*key*} **auth-port 2083 acct-port 2083 authentication accounting**
4. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **tls client-trustpoint** *trustpoint*
5. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **tls idle-timeout** *value*

手順の詳細

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。
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： `switch(config)# radius-server secure dtls`	スイッチで RADIUS with DTLS プロトコルを有効にします。
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。

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サーバー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、スイッチはローカル認証に戻す前に、RADIUSサーバーへの送信を1回だけ再試行します。このリトライの回数は、サーバーごとに最大5回まで増やすことができます。タイムアウト間隔は、Cisco Nexus デバイスがタイムアウト エラーを宣言する前に、RADIUS サーバーからの応答を待機する時間を決定します。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server retransmit** *count*
3. switch(config)# **radius-server timeout** *seconds*
4. switch(config)# **exit**
5. (Optional) switch# **show radius-server**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server retransmit** *count*	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	switch(config)# **radius-server timeout** *seconds*	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	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 6	(Optional) 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。

Example

次に、RADIUS サーバーで、リトライ回数を 3、伝送タイムアウト間隔を 5 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server retransmit 3
switch(config)# radius-server timeout 5
switch(config)# exit
switch# copy running-config startup-config
```

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 Nexus スイッチはローカル認証に戻す前に、RADIUS サーバーへの送信を 1 回だけ再試行します。このリトライの回数は、サーバーごとに最大 5 回まで増やすことができます。また、スイッチがタイムアウト エラーを宣言する前に RADIUS サーバーからの応答を待機するタイムアウト間隔を設定することもできます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count*
3. switch(config)#**radius-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*
4. switch(config)# **exit**
5. (Optional) switch# **show radius-server**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **retransmit** *count*	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**

	Command or Action	Purpose
		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	switch(config)#**radius-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*	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	switch(config)# **exit**	グローバル 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	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、RADIUS ホスト サーバー server1 で、RADIUS 送信リトライ回数を 3、タイムアウト間隔を 10 秒に設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# copy running-config startup-config
```

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。RADIUS のアカウンティングおよび認証メッセージの宛先 UDP ポート番号も指定できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. (Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*
3. (Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **accounting**
4. (Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **auth-port** *udp-port*
5. (Optional) switch(config)# **radius-server host** {*ipv4-address* |*host-name*} **authentication**
6. switch(config)# **exit**

7. (Optional) switch(config)# **show radius-server**
8. switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*	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。 範囲は 0 ～ 65535 です。
ステップ 3	(Optional) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **accounting**	特定の RADIUS サーバーをアカウンティング用にのみ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) switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **auth-port** *udp-port*	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) switch(config)# **radius-server host** {*ipv4-address* |*host-name*} **authentication**	特定の RADIUS サーバーを認証用にのみ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	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 7	(Optional) switch(config)# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 8	switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、RADIUS サーバーのアカウンティング属性と認証属性を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch # exit
switch # copy running-config startup-config
switch #
```

RADIUS サーバーの定期的モニタリングの設定

RADIUSサーバーの可用性をモニタリングできます。パラメータとして、サーバーに使用するユーザー名とパスワード、およびアイドル タイマーがあります。アイドル タイマーには、RADIUSサーバーがどのくらいの期間要求を受信しなかった場合にスイッチがテスト 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することで、サーバーを定期的にテストできます。

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ー名と同じテスト ユーザー名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 サーバーがどのくらいの期間要求を受信しなかった場合にスイッチがテスト パケットを送信するかを指定します。

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、スイッチは RADIUS サーバーの定期的なモニタリングを実行しません。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **test** { **idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}
3. switch(config)# **radius-server deadtime** *minutes*
4. switch(config)# **exit**
5. (Optional) switch# **show radius-server**
6. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **test** { **idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	サーバー 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ー名は 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。 有効な範囲は、0 ～ 1440 分です。 **Note** RADIUSサーバー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	switch(config)# **radius-server deadtime** *minutes*	スイッチが、前回応答しなかったRADIUSサーバー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	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 5	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 6	(Optional) switch# **copy running-config startup-config**	リブートおよびリスタート時に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て、変更を継続的に保存します。

Example

次に、ユーザー名（user1）およびパスワード（Ur2Gd2BH）と、3 分のアイドル タイマーおよび 5 分のデッドタイムで、RADIUS サーバー ホスト 10.10.1.1 を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# copy running-config startup-config
```

デッド タイム間隔の設定

すべての RADIUS サーバーのデッド タイム間隔を設定できます。デッド タイム間隔には、Cisco Nexus デバイスが RADIUS サーバーをデッド状態であると宣言した後、そのサーバーがアライブ状態に戻ったかどうかを判断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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **radius-server deadtime**
3. switch(config)# **exit**
4. (Optional) switch# **show radius-server**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **radius-server deadtime**	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	switch(config)# **exit**	コンフィグレーション モードを終了します。
ステップ 4	(Optional) switch# **show radius-server**	RADIUS サーバーの設定を表示します。
ステップ 5	(Optional) 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。

Example

次に、RADIUS サーバーに 5 分間のデッドタイムを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config# exit
switch# copy running-config startup-config
```

RADIUS サーバまたはサーバ グループの手動モニタリング

SUMMARY STEPS

1. switch# **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password* **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password*
2. switch# **test aaa group** *group-name username password*

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password* **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password*	RADIUS サーバーにテスト メッセージを送信して可用性を確認します。
ステップ 2	switch# **test aaa group** *group-name username password*	RADIUS サーバー 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。

Example

次に、可用性を確認するために、RADIUS サーバーとサーバー グループにテスト メッセージを送信する例を示します。

```
switch# test aaa server radius 10.10.1.1 user 1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

RADIUS サーバー統計情報の表示

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

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 サーバーのアクティビティに関する統計情報を表示します。

始める前に

Cisco NX-OS デバイスに RADIUS サーバーを設定します。

手順の概要

1. （任意） switch# **show radius-server statistics** {*hostname* | *ipv4-address*}
2. switch# **clear radius-server statistics** {*hostname* | *ipv4-address*}

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） switch# **show radius-server statistics** {*hostname* | *ipv4-address*}	Cisco NX-OS デバイスでの RADIUS サーバー統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 2	switch# **clear radius-server statistics** {*hostname* | *ipv4-address*}	RADIUS サーバ統計情報をクリアします。

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# exit
switch(config-radius)# use-vrf management
```

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: デフォルトの ***RADIUS*** パラメータ

パラメータ	デフォルト
サーバーの役割	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	テスト

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。