RadSec の設定

この章では、RadSec over Transport Layer Security（TLS）および Datagram Transport Layer Security（DTLS）サーバーを設定する方法について説明します。

RadSec の設定に関する制限事項

RadSec 機能には、次のような制限事項が適用されます。

- RADIUS クライアントは、送信元ポートとして一時ポートを使用します。この送信元ポートは、UDP、データグラムトランスポート層セキュリティ（DTLS）、およびトランスポート層セキュリティ（TLS）に同時に使用しないでください。
- 設定上の制限はありませんが、認証、認可、およびアカウンティング（AAA）サーバーグループ内のサーバーには、同じタイプ（TLS のみまたは DTLS のみ）を使用することをお勧めします。
- RadSec は、IPv4 接続でのみサポートされます。

RadSec に関する情報

RadSec の設定方法

次のセクションでは、RadSec の設定を構成するさまざまな作業について説明します。

RadSec over TLS の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *radius-server-name*
4. **tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *radius-server-name* 例： `Device(config)# radius server R1`	RADIUS サーバー設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバー設定モードを開始します。

ステップ 4	**tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name*	**server** *trustpoint name*}]
		例：
		`Device(config-radius-server)# tls connectiontimeout 10`
		`Device(config-radius-server)# tls idletimeout 75`
		`Device(config-radius-server)# tls retries 15`
		`Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1`
		`Device(config-radius-server)# tls ip vrf forwarding table-1`
		`Device(config-radius-server)# tls port 10`
		`Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660`
			TLS パラメータを設定します。次のパラメータを設定できます:
			• **connectiontimeout**：TLS 接続タイムアウト値を設定します。デフォルトは 5 秒です。
			• **idletimeout**：TLS アイドルタイムアウト値を設定します。デフォルトは 60 秒です。
			• **ip**：IP 送信元パラメータを設定します。
			• **port**：TLS ポート番号を設定します。デフォルトは 2083 です。
			• **retries**：TLS 接続再試行の回数を設定します。デフォルトは 5 です。
			• **trustpoint**：クライアントとサーバーに TLS トラストポイントを設定します。クライアントとサーバーの TLS トラストポイントが同じ場合、

	コマンドまたはアクション	目的
	`Device(config-radius-server)# tls trustpoint server isetp`	トラストポイント名も両方で同じである必要があります。
ステップ 5	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

TLS CoA の動的認可の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client {ip-addr | hostname}** [**tls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `デバイス# 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 3	**aaa server radius dynamic-author** 例： `デバイス(config)# aaa server radius dynamic-author`	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サーバーとして設定し、外部ポリシー サーバーとの連携を可能にする。
ステップ 4	**client {ip-addr | hostname}** [**tls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*] 例： `デバイス(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise`	AAA サーバー 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。次のオプションのパラメータを設定できます。 • **tls**：クライアントの TLS を有効にします。

	コマンドまたはアクション	目的
	server-tp tls_client	• **client-tp**：クライアント トラストポイントを設定します。 • **idletimeout**：DTLS アイドルタイムアウト値を設定します。 • **server-tp**：サーバートラストポイントを設定します。 • **vrf**：クライアントの Virtual Routing and Forwarding（VRF）ID。
ステップ 5	**end** 例： デバイス(config-radius-server)# end	ダイナミック認可ローカル サーバー コンフィギュレーション モードから特権 EXEC モードに戻ります。

RadSec over DTLS の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *radius-server-name*
4. **dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device> enable	特権 EXEC モードを有効にします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： Device# 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 3	**radius server** *radius-server-name* 例： Device(config)# radius server R1	RADIUS サーバー設定の名前を Protected Access Credential（PAC）のプロビジョニング用に指定し、RADIUS サーバー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

ステップ 4	**dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*}] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
	例：
	`Device(config-radius-server)# dtls connectiontimeout 10`
	`Device(config-radius-server)# dtls idletimeout 75`
	`Device(config-radius-server)# dtls retries 15`
	`Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1`
	`Device(config-radius-server)# dtls ip vrf forwarding table-1`
	`Device(config-radius-server)# dtls port 10`
	`Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660`
	`Device(config-radius-server)# dtls trustpoint server isetp`
		DTLS パラメータを設定します。次のパラメータを設定できます。
		• **connectiontimeout**：DTLS 接続タイムアウト値を設定します。デフォルトは 5 秒です。
		• **idletimeout**：DTLS アイドルタイムアウト値を設定します。デフォルトは 60 秒です。
		• **ip**：IP 送信元パラメータを設定します。
		• **port**：DTLS ポート番号を設定します。デフォルトは 2083 です。
		• **retries**：DTLS 接続再試行の回数を設定します。デフォルトは 5 です。
		• **trustpoint**：クライアントとサーバーに DTLS トラストポイントを設定します。クライアントとサーバーの DTLS トラストポイントが同じ場合、トラストポイント名も両方で同じである必要があります。

ステップ 5	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DTLS CoA の動的認可の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client {ip-addr | hostname}** [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*]
5. **dtls** {**ip radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*}
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	デバイス> enable	
ステップ 2	**configure terminal** 例： デバイス# 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 3	**aaa server radius dynamic-author** 例： デバイス(config)# aaa server radius dynamic-author	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更（CoA）を受け入れ、要求を取り外すRADIUS クライアントを指定します。デバイスを AAA サーバーとして設定し、外部ポリシー サーバーとの連携を可能にする。
ステップ 4	**client {ip-addr | hostname}** [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id*] 例： デバイス(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp dtls_ise server-tp dtls_client	AAA サーバー 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。次のオプションのパラメータを設定できます。 • **dtls**：クライアントの DTLS を有効にします。 • **client-tp**：クライアント トラストポイントを設定します。 • **idletimeout**：DTLS アイドルタイムアウト値を設定します。 • **server-tp**：サーバートラストポイントを設定します。 • **vrf**：クライアントの Virtual Routing and Forwarding（VRF）ID。
ステップ 5	**dtls** {**ip radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*} 例： デバイス(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24 デバイス(config-locsvr-da-radius)# dtls port 100	RADIUS CoA サーバを設定します。次のパラメータを設定できます。 • **ip radius source-interface** *interface-name*：RADIUS CoA サーバーの送信元アドレスのインターフェイスを指定します。 • **port** *radius-dtls-server-port-number*：ローカル DTLS RADIUS サーバーがリッスンするポートを指定します。
ステップ 6	**end** 例： デバイス(config-radius-server)# end	ダイナミック認可ローカル サーバー コンフィギュレーション モードから特権 EXEC モードに戻ります。

RadSec のモニタリング

次のコマンドを使用して、TLS および DTLS サーバーの統計を監視します。

表 *1 : TLS* および *DTLS* サーバー統計コマンドの監視

コマンド	目的
show aaa servers	TLS および DTLS サーバーに関連する情報を表示します。
clear aaa counters servers radius {*server id* | **all**}	RADIUS TLS 固有または DTLS 固有の統計情報をクリアします。
debug radius radsec	RADIUS RadSec デバッグを有効にします。

RadSec の設定例

次の例は、RadSec の設定を理解するのに役立ちます。

例：RadSec over TLS の設定

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# tls connectiontimeout 10
Device(config-radius-server)# tls idletimeout 75
Device(config-radius-server)# tls retries 15
Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1
Device(config-radius-server)# tls ip vrf forwarding table-1
Device(config-radius-server)# tls port 10
Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660
Device(config-radius-server)# tls trustpoint server isetp
Device(config-radius-server)# end
```

例：TLS CoA の動的認可の設定

```
Device> enable
Device# configure terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise
 server-tp tls_client
Device(config-locsvr-da-radius)# dtls port 100
Device(config-radius-server)# end
```

例：RadSec over DTLS の設定

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# dtls idletimeout 75
Device(config-radius-server)# dtls retries 15
Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1
Device(config-radius-server)# dtls ip vrf forwarding table-1
Device(config-radius-server)# dtls port 10
Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660
Device(config-radius-server)# dtls trustpoint server isetp
Device(config-radius-server)# end
```

例：DTLS CoA の動的認可の設定

```
Device> enable
Device# configure terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp
dtls_ise server-tp dtls_client
Device(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24
Device(config-locsvr-da-radius)# dtls port 100
Device(config-radius-server)# end
```

RadSec 設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	RadSec over DTLS の設定	RadSec over DTLS は、安全なトンネルを介して転送される RADIUS サーバー上で暗号化サービスを提供します。
Cisco IOS XE Fuji 16.9.1	RadSec over TLS の設定	RadSec over TLS は、安全なトンネルを介して転送される RADIUS サーバー上で暗号化サービスを提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。