



Per VRF for TACACS+ Servers

Per VRF for TACACS+ Servers 機能により、TACACS+ サーバで Per Virtual Route Forwarding (Per VRF; Per Virtual ルーティングおよび転送) の Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング) を設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「[Per VRF for TACACS+ Servers の機能情報 \(P.8\)](#)」を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

この章の構成

- 「[Per VRF for TACACS+ Servers の前提条件](#)」 (P.1)
- 「[Per VRF for TACACS+ Servers の制約事項](#)」 (P.2)
- 「[Per VRF for TACACS+ Servers について](#)」 (P.2)
- 「[Per VRF for TACACS+ Servers の設定方法](#)」 (P.2)
- 「[Per VRF for TACACS+ Server の設定例](#)」 (P.5)
- 「[その他の参考資料](#)」 (P.6)

Per VRF for TACACS+ Servers の前提条件

- TACACS+ サーバ アクセスが必要です。
- TACACS+、AAA および Per VRF AAA、およびグループ サーバ設定の経験が必要です。

Per VRF for TACACS+ Servers の制約事項

- Per VRF for TACACS+ Servers を設定する前に、VRF インスタンスを指定する必要があります。

Per VRF for TACACS+ Servers について

Per VRF for TACACS+ Servers 機能を設定するには、次の概念を理解しておく必要があります。

- 「[Per VRF for TACACS+ Servers の概要](#)」(P.2)

Per VRF for TACACS+ Servers の概要

Per VRF for TACACS+ Servers 機能により、TACACS+ サーバで Per VRF AAA を設定できます。Cisco IOS Release 12.3(7)T よりも前のリリースでは、この機能は、RADIUS サーバ上だけで使用可能でした。

Per VRF for TACACS+ Servers の設定方法

ここでは、次の各手順について説明します。

- 「[TACACS+ サーバ上の Per VRF の設定](#)」(P.2) (必須)
- 「[Per VRF for TACACS+ Servers の確認](#)」(P.4) (任意)

TACACS+ サーバ上の Per VRF の設定

この手順の最初のステップは、AAA およびサーバグループの設定、VRF ルーティングテーブルの作成、およびインターフェイスの設定に使用されます。ステップ 10～13 は、TACACS+ サーバ機能上での Per VRF の設定に使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf vrf-name**
4. **rd route-distinguisher**
5. **exit**
6. **interface interface-name**
7. **ip vrf forwarding vrf-name**
8. **ip address ip-address mask [secondary]**
9. **exit**
10. **aaa group server tacacs+ group-name**
11. **server-private {ip-address | name} [nat] [single-connection] [port port-number] [timeout seconds] [key [0 | 7] string]**

12. `ip vrf forwarding vrf-name`13. `ip tacacs source-interface subinterface-name`14. `exit`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • 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	<code>configure terminal</code> 例： Router# 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	<code>ip vrf vrf-name</code> 例： Router (config)# ip vrf cisco	VRF テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	<code>rd route-distinguisher</code> 例： Router (config-vrf)# rd 100:1	VRF インスタンスに対するルーティングおよびフォワーディング テーブルを作成します。
ステップ 5	<code>exit</code> 例： Router (config-vrf)# exit	VRF コンフィギュレーション モードを終了します。
ステップ 6	<code>interface interface-name</code> 例： Router (config)# interface Loopback0	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	<code>ip vrf forwarding vrf-name</code> 例： Router (config-if)# ip vrf forwarding cisco	インターフェイスに VRF を設定します。
ステップ 8	<code>ip address ip-address mask [secondary]</code> 例： Router (config-if)# ip address 10.0.0.2 255.0.0.0	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 9	<code>exit</code> 例： Router (config-if)# exit	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	<code>aaa group server tacacs+ group-name</code> 例： Router (config)# aaa group server tacacs+ tacacs1	異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、 <code>server-group</code> コンフィギュレーション モードを開始します。

■ Per VRF for TACACS+ Servers の設定方法

	コマンドまたはアクション	目的
ステップ 11	<pre>server-private {ip-address name} [nat] [single-connection] [port port-number] [timeout seconds] [key [0 7] string]</pre> <p>例： Router (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco</p>	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。
ステップ 12	<pre>ip vrf forwarding vrf-name</pre> <p>例： Router (config-sg-tacacs+)# ip vrf forwarding cisco</p>	AAA TACACS+ サーバ グループの VRF リファレンスを設定します。
ステップ 13	<pre>ip tacacs source-interface subinterface-name</pre> <p>例： Router (config-sg-tacacs+)# ip tacacs source-interface Loopback0</p>	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ステップ 14	<pre>exit</pre> <p>例： Router (config-sg-tacacs)# exit</p>	server-group コンフィギュレーション モードを終了します。

Per VRF for TACACS+ Servers の確認

Per VRF TACACS+ 設定を確認するには、次の手順を実行します。



(注) **debug** コマンドは、任意の実行順序で使用できます。

手順の概要

1. **enable**
2. **debug tacacs authentication**
3. **debug tacacs authorization**
4. **debug tacacs accounting**
5. **debug tacacs packets**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： Router> enable	特権 EXEC モードをイネーブルにします。 • 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	<code>debug tacacs authentication</code> 例： Router# debug tacacs authentication	AAA/TACACS+ 認証に関する情報を表示します。
ステップ 3	<code>debug tacacs authorization</code> 例： Router# debug tacacs authorization	AAA/TACACS+ 認可に関する情報を表示します。
ステップ 4	<code>debug tacacs accounting</code> 例： Router# debug tacacs accounting	説明可能なイベントが発生したときに、その情報を表示します。
ステップ 5	<code>debug tacacs packets</code> 例： Router# debug tacacs packets	TACACS+ パケットに関する情報を表示します。

Per VRF for TACACS+ Server の設定例

ここでは、次の設定例について説明します。

- 「Per VRF for TACACS+ Servers の設定 : 例」 (P.5)

Per VRF for TACACS+ Servers の設定 : 例

次の出力例では、Per VRF AAA サービスにグループ サーバ **tacacs1** が設定されています。

```
aaa group server tacacs+ tacacs1
  server-private 10.1.1.1 port 19 key cisco
  ip vrf forwarding cisco
  ip tacacs source-interface Loopback0

ip vrf cisco
  rd 100:1

interface Loopback0
  ip address 10.0.0.2 255.0.0.0
  ip vrf forwarding cisco
```

その他の参考資料

ここでは、Per VRF for TACACS+ Servers に関する関連資料について説明します。

関連資料

内容	参照先
TACACS+ の設定	「 Configuring TACACS+ 」 モジュール
Per VRF AAA	「 Per VRF AAA 」 モジュール
セキュリティ コマンド	『 Cisco IOS Security Command Reference 』

規格

規格	タイトル
この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能がサポートする新規 RFC または改訂 RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
<p>右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。</p> <p>以下を含むさまざまな作業にこの Web サイトが役立ちます。</p> <ul style="list-style-type: none">・テクニカル サポートを受ける・ソフトウェアをダウンロードする・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける・ツールおよびリソースへアクセスする<ul style="list-style-type: none">- Product Alert の受信登録- Field Notice の受信登録- Bug Toolkit を使用した既知の問題の検索・Networking Professionals (NetPro) コミュニティで、技術関連のディスカッションに参加する・トレーニング リソースへアクセスする・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する <p>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Per VRF for TACACS+ Servers の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンドリファレンスマニュアルを参照してください。

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 を使用すると、Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。



(注) 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1 Per VRF for TACACS+ Servers の機能情報

機能名	リリース	機能情報
Per VRF for TACACS+ Servers	12.3(7)T 12.2(33)SRA 1 12.2(33)SXI 12.2(33)SXH 4 12.2(54)SG	Per VRF for TACACS+ Servers 機能により、TACACS+ サーバで Per Virtual Route Forwarding (Per VRF; Per Virtual ルーティングおよび転送) の Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウントティング) を設定できます。 この機能は、Cisco IOS Release 12.3(7)T で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRA1 に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXI に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH4 に統合されました。 この機能により、次のコマンドが導入または変更されました。 ip tacacs source-interface 、 ip vrf forwarding (server-group) 、 server-private (TACACS+) 。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2004-2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2004–2011, シスコシステムズ合同会社.
All rights reserved.

