認証、許可、アカウンティング コマンド

ここでは、認証、許可、アカウンティング（AAA）サービスを設定するために使用されるコマンドについて説明します。

AAA の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Configuring AAA Services on* 」モジュールを参照してください。

aaa accounting

アカウンティングの方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa accounting** コマンドを使用します。 システムからリスト名を削除するには、このコマンドの **no** 形式を使用します。

aaa accounting {**commands**| **exec**| **network**} {**default**| **list-name**} {**start-stop**| **stop-only**} {**none**| **method**}

no aaa accounting {**commands**| **exec**| **network**} {**default**| **list-name**}

構文の説明

commands	EXEC シェル コマンドに対してアカウンティングをイネーブルにします。
exec	EXEC セッションのアカウンティングをイネーブルにします。
network	Internet Key Exchange（IKE; インターネットキー交換）や Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）など、すべてのネットワーク関連サービス要求に対するアカウンティングをイネーブルにします。
default	このキーワードに続くアカウンティング方式のリストをアカウンティング サービスのデフォルト方式リストとして使用します。
list-name	アカウンティング方式リストの名前の指定に使用する文字列です。
start-stop	プロセスの開始時に「start accounting」通知を送信し、プロセスの終了時に「stop accounting」通知を送信します。 要求されたユーザ プロセスは、「start accounting」通知がアカウンティング サーバで受信されたかどうかに関係なく開始されます。
stop-only	要求されたユーザ プロセスの終了時に「stop accounting」通知を送信します。
none	アカウンティングを使用しません。
method	AAA システム アカウンティングのイネーブル化に使用する方式です。 値は、次のいずれかになります。 • **group tacacs+**：すべての TACACS+ サーバのリストをアカウンティングに使用します。 • **group radius**：すべての RADIUS サーバのリストをアカウンティングに使用します。 • **group** *named-group*：**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットをアカウンティングに使用します。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa accounting コマンドを使用して、回線単位またはインターフェイス単位で使用できる、特定のアカウンティング方式を定義するデフォルトまたは名前付き方式リストを作成します。 方式リストには方式を 4 つまで指定できます。 リスト名を回線（console、aux、または vty テンプレート）に適用して、その回線でアカウンティングをイネーブルにすることができます。

Cisco IOS XR ソフトウェアは、アカウンティングに TACACS+ 方式と RADIUS 方式の両方をサポートします。 ルータからセキュリティ サーバにアカウンティング レコードの形でユーザ アクティビティが報告され、そのレコードはセキュリティ サーバに保存されます。

アカウンティング方式リストには、アカウンティングの実行方法が定義されます。このリストを使用して、特定のタイプのアカウンティング サービスに固有の回線またはインターフェイスに使用する特定のセキュリティ プロトコルを指定できます。

最小限のアカウンティングを行うには、要求されたユーザ プロセスのあとで「stop accounting」通知を送信するよう、**stop-only** キーワードを付加します。 さらに詳細なアカウンティングを行うには、TACACS+ が要求されたプロセスの開始時に「start accounting」通知を送信し、プロセスのあとで「stop accounting」通知を送信するよう、**start-stop** キーワードを付加できます。 アカウンティング レコードは、TACACS+ サーバだけに保存されます。

要求されたユーザ プロセスは、「start accounting」通知がアカウンティング サーバで受信されたかどうかに関係なく開始されます。

（注） このコマンドは、TACACS または拡張 TACACS には使用できません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、デフォルトの commands アカウンティング方式リストを定義する例を示します。この例では、TACACS+ セキュリティ サーバにより、stop-only 制限付きのアカウンティング サービスが提供されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting commands default stop-only group tacacs+
```

関連コマンド

コマンド	説明
aaa authorization, （16 ページ）	許可の方式リストを作成します。

aaa accounting system default

認証、許可、アカウンティング（AAA）システム アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting system default** コマンドを使用します。システム アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting system default {**start-stop**| **stop-only**} {**none**| **method**}

no aaa accounting system default

構文の説明

start-stop	システム起動時に「start accounting」通知を送信し、システム シャットダウンまたはリロード時に「stop accounting」通知を送信します。
stop-only	システム シャットダウンまたはリロード時に「stop accounting」通知を送信します。
none	アカウンティングを使用しません。
method	AAA システム アカウンティングのイネーブル化に使用する方式です。 値は、次のいずれかになります。 • **group tacacs+**：すべての TACACS+ サーバのリストをアカウンティングに使用します。 • **group radius**：すべての RADIUS サーバのリストをアカウンティングに使用します。 • **group** *named-group*：**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットをアカウンティングに使用します。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

システムアカウンティングには、名前付きアカウンティング リストは使用されません。定義できるのは、デフォルト リストだけです。

デフォルトの方式リストが、自動的にすべてのインターフェイスまたは回線に適用されます。 デフォルトの方式リストが定義されていない場合、アカウンティングは実行されません。

方式リストには方式を 4 つまで指定できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ルータの最初の起動時に「start accounting」レコードが TACACS+ サーバに送信されるようにする例を示します。 また、ルータのシャットダウンまたはリロード時には「stop accounting」レコードが送信されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting system default start-stop group tacacs+
```

関連コマンド

コマンド	説明
aaa authentication, （13 ページ）	認証の方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。

aaa accounting system rp-failover

RP フェールオーバーまたは RP スイッチオーバー開始または停止アカウンティング メッセージを送信するためのアカウンティング リストを作成するには、**aaa accounting system rp-failover** コマンドをグローバル コンフィギュレーション モードで使用します。 RP フェールオーバーに対するシステム アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting system rp-failover {*list_name* {**start-stop**| **stop-only**}| **default** {**start-stop**| **stop-only**}}

no aaa accounting system rp-failover {*list_name* {**start-stop**| **stop-only**}| **default** {**start-stop**| **stop-only**}}

構文の説明

list_name	アカウンティング リスト名を指定します。
default	デフォルトのアカウンティング リストを指定します。
start-stop	開始および停止のレコードをイネーブルにします。
stop-only	停止レコードだけをイネーブルにします。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 4.2.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、デフォルトのアカウンティング リストに対して **aaa accounting system rp-failover** コマンドを設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# aaa accounting system rp-failover default start-stop none
```

関連コマンド

コマンド	説明
aaa attribute format	AAA 属性形式の名前を作成します。

aaa accounting update

定期的な中間アカウンティング レコードがアカウンティング サーバに送信されるようにするには、グローバル コンフィギュレーション モードで **aaa accounting update** コマンドを使用します。中間アカウンティングのアップデートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting update {**newinfo**| **periodic** *minutes*}

no aaa accounting update

構文の説明

newinfo	（任意）当該のユーザに関して報告する新しいアカウンティング情報があるときは常に、中間アカウンティング レコードをアカウンティング サーバに送信します。
periodic *minutes*	（任意）*minutes* 引数によって定義されているとおりに、中間アカウンティング レコードを定期的にアカウンティング サーバに送信します。この引数は、分数を指定する整数です。 範囲は、1 ～ 35791394 分です。

コマンド デフォルト

AAA のアカウンティングのアップデートはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

newinfo キーワードを使用すると、報告する新しいアカウンティング情報があるたびに中間アカウンティング レコードがアカウンティング サーバに送信されます。 たとえば、IP Control Protocol（IPCP; IP 制御プロトコル）がリモート ピアとの IP アドレス ネゴシエーションを完了した時点でこのようなレポートが送信されます。 中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。

periodic キーワードを使用すると、中間アカウンティング レコードは *minutes* 引数で定義されているとおりに定期的に送信されます。 中間アカウンティング レコードには、アカウンティング レコードが送信される時点までにそのユーザに関して記録されたすべてのアカウンティング情報が含まれます。

newinfo キーワードと **periodic** キーワードを両方使用すると、報告する新しいアカウンティング情報があるたびに中間アカウンティング レコードがアカウンティング サーバに送信され、さらに *minutes* 引数で定義されているとおりにアカウンティング レコードが定期的にアカウンティング サーバに送信されます。 たとえば、**aaa accounting update** コマンドに **newinfo** キーワードと **periodic** キーワードを設定すると、現在ログインしているすべてのユーザによって定期的な中間アカウンティング レコードの生成が続けられると同時に、新たにユーザがログインすると、newinfo アルゴリズムに基づいてアカウンティング レコードが生成されます。

注意 多数のユーザがネットワークにログインしているときに **aaa accounting update** コマンドに **periodic** キーワードを指定すると、大きな輻輳が生じる場合があります。

periodic キーワードと **newinfo** キーワードは相互に排他的であるため、一度に設定できるキーワードはいずれか 1 つです。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、定期的な中間アカウンティング レコードを 30 分間隔で RADIUS サーバに送信する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting update periodic 30
```

次に、報告する新しいアカウンティング情報があるときに、中間アカウンティング レコードを RADIUS サーバに送信する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa accounting update newinfo
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。

aaa authentication

認証の方式リストを作成するには、グローバル コンフィギュレーション モードまたは管理コンフィギュレーション モードで **aaa authentication** コマンドを使用します。 この認証方式をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {**login**| **ppp**} {**default**| *list-name*| **remote**} *method-list*

no aaa authentication {**login**| **ppp**} {**default**| *list-name*| **remote**} *method-list*

構文の説明

login	ログインの認証を設定します。
ppp	ポイントツーポイント プロトコルの認証を設定します。
default	このキーワードに続く認証方式のリストを認証のデフォルト方式リストとして使用します。
list-name	認証方式リストの名前の指定に使用する文字列です。
remote	このキーワードに続く認証方式リストを、所有者なしのリモートのセキュア ドメイン ルータにおける管理認証のデフォルト方式リストとして使用します。 **remote** キーワードは **login** キーワードと一緒に使用できますが、**ppp** キーワードとは一緒に使用できません。 （注） **remote** キーワードは管理プレーンだけで使用できます。
method-list	AAA システム アカウンティングのイネーブル化に使用する方式です。 値は、次のいずれかになります。 • **group tacacs+**：設定されたすべての TACACS+ サーバのリストを認証に使用する方式リストを指定します。 • **group radius**：設定されたすべての RADIUS サーバのリストを認証に使用する方式リストを指定します。 • **group** *named-group*：**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを認証に使用する方式リストを指定します。 • **local**：ローカル ユーザ名データベース方式を認証に使用する方式リストを指定します。 ユーザ名がローカル グループで定義されていない場合、AAA 方式がローカル方式以外にロールオーバーされます。 • **line**：回線パスワードを認証に使用する方式リストを指定します。

コマンド デフォルト

グローバルでは、すべてのポートにローカル認証が適用されます。

管理コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa authentication コマンドを使用して、一連の認証方式、つまり方式リストを作成します。 方式リストには方式を 4 つまで指定できます。 *method list* は、一連の認証方式（TACACS+ または RADIUS など）を示す名前付きリストです。 後続の認証方式は、最初の方式が失敗した場合ではなく、使用不可能な場合にだけ使用されます。

別の名前付き方式リストが明示的に指定されている場合を除き、すべてのインターフェイスの認証にデフォルトの方式リストが適用されます。別のリストが明示的に指定されている場合は、デフォルト リストが上書きされます。

コンソールおよび vty のアクセスについては、認証が設定されていない場合、デフォルトのローカル方式が適用されます。

（注）

- このコマンドの **group tacacs+**、**group radius**、および **group** *group-name* の各形式は、あらかじめ定義された一連の TACACS+ サーバまたは RADIUS サーバを指します。
- ホスト サーバを設定するには、**tacacs-server host** コマンドまたは **radius-server host** コマンドを使用します。
- サーバの名前付きサブセットを作成するには、**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドを使用します。
- **login** キーワード、**remote** キーワード、**local** オプション、および **group** オプションは、管理コンフィギュレーション モードでだけ使用できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、グローバルコンフィギュレーションモードでデフォルトの認証方式リストを指定し、コンソールの認証をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authentication login default group tacacs+
```

次に、管理コンフィギュレーション モードでリモートの認証方式リストを指定し、コンソールの認証をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# admin
RP/0/RSP0/CPU0:router (admin)# configure
RP/0/RSP0/CPU0:router(admin-config)# aaa authentication login remote local group tacacs+
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。
aaa group server radius, （22 ページ）	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
aaa group server tacacs+, （25 ページ）	各種の TACACS+ サーバ ホストを別個のリストと別個の方式にグループ化します。
login authentication, （45 ページ）	ログインに対する AAA 認証をイネーブルにします。
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

aaa authorization

許可の方式リストを作成するには、グローバル コンフィギュレーション モードで **aaa authorization** コマンドを使用します。 機能に対する許可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization {**commands**| **eventmanager**| **exec**| **network**} {**default**| *list-name*} {**none**| **local**| **group** {**tacacs+**| **radius**| *group-name*}}

no aaa authorization {**commands**| **eventmanager**| **exec**| **network**} {**default**| *list-name*}

構文の説明

commands	すべての EXEC シェル コマンドに対する許可を設定します。
eventmanager	イベント マネージャ（障害マネージャ）を許可するための許可方式を適用します。
exec	対話型（EXEC）セッションに対する許可を設定します。
network	PPP やインターネットキー交換（IKE）などのネットワーク サービスに対する許可を設定します。
default	このキーワードに続く許可方式のリストを許可のデフォルト方式リストとして使用します。
list-name	許可方式リストの名前の指定に使用する文字列です。
none	許可を使用しません。 **none** を指定すると、後続の許可方式は試行されません。 ただし、タスク ID の許可は常に必要であり、ディセーブルにはできません。
local	ローカルの許可を使用します。 この許可方式は、コマンドの許可には使用できません。
group tacacs+	設定されているすべての TACACS+ サーバのリストを許可に使用します。
group radius	設定されているすべての RADIUS サーバのリストを許可に使用します。 この許可方式は、コマンドの許可には使用できません。
group *group-name*	**aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドで定義されているとおりに、TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを許可に使用します。

コマンド デフォルト

すべてのアクションに対する許可がディセーブルになります（**none** キーワードと同等）。

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa authorization コマンドを使用して、回線単位またはインターフェイス単位で使用できる特定の許可方式を定義する方式リストを作成します。 方式リストには方式を 4 つまで指定できます。

（注） ここに示すコマンドの許可は、タスクに基づいた許可ではなく、外部の AAA サーバで実行される許可に適用します。

許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。 方式リストは、一連の許可方式（TACACS+ など）を記述した名前付きリストです。 方式リストを使用して、許可に 1 つまたは複数のセキュリティ プロトコルを指定し、最初の方式が失敗した場合のバックアップ システムを確保することができます。 Cisco IOS XR ソフトウェアでは、特定のネットワーク サービスに対してユーザを許可するために、リスト内の最初の方式が使用されます。この方式が応答に失敗すると、Cisco IOS XR ソフトウェアでは方式リスト内の次の方式が選択されます。 このプロセスは、リスト内の許可方式との通信に成功するまで、または定義されている方式を使い果たすまで続行されます。

（注） Cisco IOS XR ソフトウェアでは、前の方式から応答がない（障害ではない）場合にだけ、次に指定された方式を使って許可が試みられます。 このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティ サーバまたはローカル ユーザ名データベースからユーザ サービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

Cisco IOS XR ソフトウェアは、次の許可方式をサポートします。

- **none**：ルータから許可情報の要求はありません。この回線やインターフェイスに対する許可は行われません。
- **local**：ローカル データベースを許可に使用します。
- **group tacacs+**：設定されているすべての TACACS+ サーバのリストを許可に使用します。
- **group radius**：設定されているすべての RADIUS サーバのリストを許可に使用します。
- **group group-name**：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを許可に使用します。

方式リストは、要求されている許可のタイプによって異なります。 Cisco IOS XR ソフトウェアは、次の 4 つのタイプの AAA 許可をサポートします。

- **コマンドの許可**：ユーザが実行する EXEC モード コマンドに適用されます。 コマンドの許可では、すべての EXEC モード コマンドに対する許可が試みられます。

  （注） 「コマンド」の許可は、認証時に設定されたタスク プロファイルに基づく「タスクベース」の許可とは異なります。

- **EXEC の許可**：EXEC セッションの開始に対する許可が適用されます。

  （注） **exec** キーワードは、障害マネージャ サービスの許可に使用されなくなりました。 障害マネージャ サービスの許可には、**eventmanager** キーワード（障害マネージャ）を使用します。 **exec** キーワードは、EXEC の許可に使用します。

- **ネットワークの許可**：IKE などのネットワーク サービスの許可が適用されます。
- **イベント マネージャの許可**：イベント マネージャ（障害マネージャ）を許可するための許可方式が適用されます。 TACACS+ を使用することも、locald を使用することもできます。

  （注） イベント マネージャ（障害マネージャ）を許可するには、**exec** キーワードの代わりに **eventmanager** キーワード（障害マネージャ）を使用します。

名前付き方式リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。 方式リストを定義した場合、定義した方式のいずれかを実行するには、まず特定の回線またはインターフェイスに方式リストを適用する必要があります。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、TACACS+ の許可を使用するように指定する listname1 というネットワーク許可方式リストを定義する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authorization commands listname1 group tacacs+
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。

aaa default-taskgroup

リモートの TACACS+ 認証と RADIUS 認証の両方のタスク グループを指定するには、グローバル コンフィギュレーション モードで **aaa default-taskgroup** コマンドを使用します。 このデフォルト タスク グループを削除するには、このコマンドの **no** 形式を入力します。

aaa default-taskgroup *taskgroup-name*

no aaa default-taskgroup

構文の説明

taskgroup-name	既存のタスク グループの名前です。

コマンド デフォルト

リモート認証には、デフォルトのタスク グループは割り当てられません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa default-taskgroup コマンドを使用して、リモート TACACS+ 認証に既存のタスク グループを指定します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、リモート TACACS+ 認証のデフォルト タスク グループとして taskgroup1 を指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa default-taskgroup taskgroup1
```

aaa group server radius

各種の RADIUS サーバ ホストを別個のリストにグループ化するには、グローバル コンフィギュレーション モードで **aaa group server radius** コマンドを使用します。 コンフィギュレーション リストからグループ サーバを削除するには、このコマンドの **no** 形式を入力します。

aaa group server radius *group-name*

no aaa group server radius *group-name*

構文の説明

group-name	サーバ グループの名前の指定に使用する文字列です。

コマンド デフォルト

このコマンドはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa group server radius コマンドを使用して、既存のサーバ ホストをグループ化します。そうすることにより、設定されているサーバ ホストのサブセットを選択し、それらのホストを特定のサービスに使用できます。 サーバ グループは、グローバル サーバ ホスト リストと併せて使用されます。 サーバ グループは、選択されているサーバ ホストの IP アドレスまたはホスト名を示します。

また、サーバ グループには、各エントリが一意の ID を持っていれば、同一サーバに複数のホスト エントリを組み込むことができます。 IP アドレスとユーザ データグラム プロトコル（UDP）ポート番号を組み合わせることで、一意の ID が作成されます。この情報を使用して、固有の認証、許可、アカウンティング（AAA）サービスを提供する RADIUS ホストとして各ポートを個別に定義できます。 つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。 たとえば、同一の RADIUS サーバの 2 つの異なるホスト エントリを同一のサービスに対して設定すると、2 つ目のホスト エントリは最初のホスト エントリをバックアップする自動

スイッチオーバーとして機能します。 この場合、最初のホストエントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じデバイス上の 2 つ目のホストエントリでアカウンティング サービスを試行します。 RADIUS ホストエントリは、サーバ グループに設定された順序で試行されます。

サーバ グループのメンバはすべて同じタイプ、つまり RADIUS であることが必要です。

サーバ グループには、radius や tacacs の名前を付けることはできません。

このコマンドを実行すると、サーバ グループ コンフィギュレーション モードが開始されます。server コマンドを使用して、特定の RADIUS サーバを定義済みのサーバ グループに関連付けることができます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、3 つのメンバ サーバからなる radgroup1 という AAA グループ サーバを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius radgroup1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.5 auth-port 1700 acct-port 1701
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.10 auth-port 1702 acct-port 1703
RP/0/RSP0/CPU0:router(config-sg-radius)# server 10.0.0.20 auth-port 1705 acct-port 1706
```

（注） **auth-port** *port-number* および **acct-port** *port-number* キーワードおよび引数が指定されていない場合、**auth-port** キーワードの *port-number* 引数のデフォルト値は 1645、**acct-port** キーワードの *port-number* 引数のデフォルト値は 1646 です。

関連コマンド

コマンド	説明
key（RADIUS）, （41 ページ）	ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定します。
radius source-interface, （66 ページ）	RADIUS で、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスが使用されるようにします。

コマンド	説明
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
server（RADIUS）, （73 ページ）	RADIUS サーバを定義済みのサーバ グループに関連付けます。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。

aaa group server tacacs+

各種の TACACS+ サーバ ホストを別個のリストにグループ化するには、グローバル コンフィギュレーション モードで **aaa group server tacacs+** コマンドを使用します。 コンフィギュレーション リストからサーバ グループを削除するには、このコマンドの **no** 形式を入力します。

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

構文の説明

group-name	サーバ グループの名前の指定に使用する文字列です。

コマンド デフォルト

このコマンドはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

AAA サーバグループ機能により、既存のサーバ ホストをグループ化する手段が追加されます。 この機能を使用して、設定されているサーバ ホストのサブセットを選択し、それらのホストを特定のサービスに使用できます。

aaa group server tacacs+ コマンドを実行すると、サーバ グループ コンフィギュレーション モードが開始されます。 **server** コマンドを実行すると、特定の TACACS+ サーバが定義済みのサーバ グループに関連付けることができます。

サーバ グループは、特定のタイプのサーバ ホストのリストです。 サポートされているサーバ ホストのタイプは、TACACS+ サーバ ホストです。 サーバ グループは、グローバル サーバ ホストのリストと一緒に使用します。 サーバ グループは、選択されているサーバ ホストの IP アドレスまたはホスト名を示します。

サーバ グループには、radius や tacacs の名前を付けることはできません。

（注） グループ名方式では、定義済みの一連の TACACS+ サーバを参照します。 ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、3 つのメンバ サーバからなる tacgroup1 という AAA グループ サーバを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ tacgroup1
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.226
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.227
RP/0/RSP0/CPU0:router(config-sg-tacacs)# server 192.168.200.228
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authentication, （13 ページ）	認証の方式リストを作成します。
aaa authorization, （16 ページ）	許可の方式リストを作成します。
server（TACACS+）, （76 ページ）	外部 TACACS+ サーバのホスト名または IP アドレスを指定します。
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

accounting（回線）

特定の回線または回線グループに対して認証、許可、アカウンティング（AAA）アカウンティング サービスをイネーブルにするには、回線テンプレート コンフィギュレーション モードで **accounting** コマンドを使用します。 AAA アカウンティング サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

accounting {**commands**| **exec**} {**default**| *list-name*}

no accounting {**commands**| **exec**}

構文の説明

commands	すべての EXEC シェル コマンドに対して、選択した回線におけるアカウンティングをイネーブルにします。
exec	EXEC セッションのアカウンティングをイネーブルにします。
default	**aaa accounting** コマンドで作成されるデフォルトの方式リストの名前です。
list-name	使用するアカウンティング方式リストの名前を指定します。 リストは、**aaa accounting** コマンドで作成されます。

コマンド デフォルト

アカウンティングはディセーブルです。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa accounting コマンドをイネーブルにして、特定のタイプのアカウンティングに対して名前付きアカウンティング方式リストを定義（またはデフォルトの方式リストを使用）したあと、アカウンティング サービスを実行する該当の回線に、定義済みのリストを適用する必要があります。 **accounting** コマンドを使用して、選択した回線または回線グループに指定の方式リストを適用し

ます。 このように方式リストを指定しないと、選択した回線または回線グループにアカウンティングが適用されません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、回線テンプレート *configure* でアカウンティング方式リスト *listname2* を使用するコマンド アカウンティング サービスをイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template configure
RP/0/RSP0/CPU0:router(config-line)# accounting commands listname2
```

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。

authorization

特定の回線または回線グループに対して認証、許可、アカウンティング（AAA）の許可をイネーブルにするには、回線テンプレート コンフィギュレーション モードで **authorization** コマンドを使用します。 許可をディセーブルにするには、このコマンドの **no** 形式を使用します。

authorization {**commands**| **exec**} {**default**| *list-name*}

no authorization {**commands**| **exec**}

構文の説明

commands	選択した回線におけるすべてのコマンドの許可をイネーブルにします。
exec	対話型（EXEC）セッションに対する許可をイネーブルにします。
default	**aaa authorization** コマンドで作成されたデフォルトの方式リストを適用します。
list-name	使用する許可方式リストの名前を指定します。 リスト名を指定しない場合は、デフォルト名が使用されます。 リストは **aaa authorization** コマンドで作成されます。

コマンド デフォルト

許可はディセーブルになります。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

aaa authorization コマンドを使用して、特定のタイプの許可に対して名前付き許可方式リストを定義（またはデフォルトの方式リストを使用）したあと、許可を実行する該当の回線に、定義済みのリストを適用する必要があります。 **authorization** コマンドを使用して、指定の方式リスト

（または、方式リストを指定していない場合はデフォルトの方式リスト）を選択した回線または回線グループに適用します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、回線テンプレート *configure* で方式リスト *listname4* を使用するコマンド許可をイネーブルにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template configure
RP/0/RSP0/CPU0:router(config-line)# authorization commands listname4
```

関連コマンド

コマンド	説明
aaa authorization, （16 ページ）	許可の方式リストを作成します。

deadtime（サーバグループ コンフィギュレーション）

RADIUS サーバ グループ レベルでデッドタイム値を設定するには、サーバグループ コンフィギュレーション モードで **deadtime** コマンドを使用します。 デッドタイムを 0 に設定するには、このコマンドの **no** 形式を使用します。

deadtime *minutes*

no deadtime

構文の説明

minutes	RADIUS サーバがトランザクション要求によってスキップされる時間を最長 1440（24 時間）まで分単位で表したものです。 指定できる範囲は 1 ～ 1440 です。

コマンド デフォルト

デッドタイムは 0 に設定されます。

コマンド モード

サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

サーバ グループに設定されたデッドタイム値は、グローバルに設定されたデッドタイム値を上書きします。 サーバグループ コンフィギュレーションでデッドタイムを省略した場合は、マスターリストの値が継承されます。 サーバグループを設定しない場合、グループ内のすべてのサーバにデフォルト値 0 が適用されます。 デッドタイムを 0 に設定すると、サーバに dead のマークは付きません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、RADIUS サーバ グループ group1 が認証要求への応答に失敗したときの **deadtime** コマンドに対して、1 分のデッドタイムを指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 1.1.1.1 auth-port 1645 acct-port 1646
RP/0/RSP0/CPU0:router(config-sg-radius)# server 2.2.2.2 auth-port 2000 acct-port 2001
RP/0/RSP0/CPU0:router(config-sg-radius)# deadtime 1
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
radius-server dead-criteria time, （50 ページ）	RADIUS サーバに dead マークを付けるための 1 つまたは両方の基準を強制的に使用します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間を分単位で定義します。

description（AAA）

設定時にタスク グループまたはユーザ グループの説明を作成するには、タスク グループ コンフィギュレーション モードまたはユーザ グループ コンフィギュレーション モードで **description** コマンドを使用します。 タスク グループの説明またはユーザ グループの説明を削除するには、このコマンドの **no** 形式を使用します。

description *string*

no description

構文の説明

string	タスク グループまたはユーザ グループを説明する文字列です。

コマンド デフォルト

なし

コマンド モード

タスク グループ コンフィギュレーション

ユーザ グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスクまたはユーザ グループ コンフィギュレーション サブモードで **description** コマンドを使用して、タスクまたはユーザ グループの説明をそれぞれ定義します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タスク グループの説明を作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup alpha
RP/0/RSP0/CPU0:router(config-tg)# description this is a sample taskgroup
```

次に、ユーザ グループの説明を作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup alpha
RP/0/RSP0/CPU0:router(config-ug)# description this is a sample user group
```

関連コマンド

コマンド	説明
taskgroup, （125 ページ）	タスク グループ コンフィギュレーション モードにアクセスし、一連のタスク ID に関連付けることでタスク グループを設定します。
usergroup, （133 ページ）	ユーザ グループ コンフィギュレーション モードにアクセスし、一連のタスク グループに関連付けることでユーザ グループを設定します。

group（AAA）

ユーザをグループに追加するには、ユーザ名コンフィギュレーション モードで **group** コマンドを使用します。 グループからユーザを削除するには、このコマンドの **no** 形式を使用します。

group {**root-system**| **root-lr**| **netadmin**| **sysadmin**| **operator**| **cisco-support**| **serviceadmin**| *group-name*}**no group** {**root-system**| **root-lr**| **netadmin**| **sysadmin**| **operator**| **cisco-support**| **serviceadmin**| *group-name*}

構文の説明

root-system	事前定義された root-system グループにユーザを追加します。 root-system 権限を持つユーザだけがこのオプションを使用できます。
root-lr	事前定義された root-lr グループにユーザを追加します。 root-system 権限または root-lr 権限を持つユーザだけがこのオプションを使用できます。
netadmin	事前定義されたネットワーク管理者グループにユーザを追加します。
sysadmin	事前定義されたシステム管理者グループにユーザを追加します。
operator	事前定義されたオペレータ グループにユーザを追加します。
cisco-support	事前定義されたシスコ サポート担当者グループにユーザを追加します。
serviceadmin	事前定義されたサービス管理者グループにユーザを追加します。
group-name	すでに **usergroup** コマンドで定義されている名前付きユーザ グループにユーザを追加します。

コマンド デフォルト

なし

コマンド モード

ユーザ名コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

定義済みの root-system グループは、root-system ユーザだけが管理の設定時に指定できます。

ユーザ名コンフィギュレーション モードで **group** コマンドを使用します。 ユーザ名コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで username,（135 ページ） コマンドを使用します。

管理コンフィギュレーション モードで **group** コマンドを使用する場合に指定できるキーワードは、root-system および cisco-support に限られます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザ グループ operator を user1 というユーザに割り当てる例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# group operator
```

関連コマンド

コマンド	説明
password（AAA）, （47 ページ）	ユーザのログイン パスワードを作成します。
usergroup, （133 ページ）	ユーザ グループを設定し、そのユーザ グループを一連のタスク グループに関連付けます。
username, （135 ページ）	ユーザ名コンフィギュレーションモードにアクセスし、新しいユーザにユーザ名を設定して、そのユーザのパスワードとアクセス許可を設定します。

inherit taskgroup

タスク グループで別のタスク グループのアクセス許可を取得できるようにするには、タスク グループ コンフィギュレーション モードで **inherit taskgroup** コマンドを使用します。

inherit taskgroup {*taskgroup-name*| **netadmin**| **operator**| **sysadmin**| **cisco-support**| **root-lr**| **root-system**| **serviceadmin**}

構文の説明

taskgroup-name	アクセス許可を継承する元のタスク グループの名前です。
netadmin	ネットワーク管理者タスク グループからアクセス許可を継承します。
operator	オペレータ タスク グループからアクセス許可を継承します。
sysadmin	システム管理者タスク グループからアクセス許可を継承します。
cisco-support	Cisco サポート タスク グループからアクセス許可を継承します。
root-lr	root-lr タスク グループからアクセス許可を継承します。
root-system	root-system タスク グループからアクセス許可を継承します。
serviceadmin	サービス管理者タスク グループからアクセス許可を継承します。

コマンド デフォルト

なし

コマンド モード

タスク グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

inherit taskgroup コマンドを使用して、あるタスク グループから別のタスク グループにアクセス許可（タスク ID）を継承します。 継承元のタスク グループが変更されると、ただちに継承元のグループ内に反映されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タスク グループ tg2 のアクセス許可がタスク グループ tg1 に継承される例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup tg1
RP/0/RSP0/CPU0:router(config-tg)# inherit taskgroup tg2
RP/0/RSP0/CPU0:router(config-tg)# end
```

inherit usergroup

ユーザ グループで別のユーザ グループの特性を取得できるようにするには、ユーザ グループ コンフィギュレーション モードで **inherit usergroup** コマンドを使用します。

inherit usergroup *usergroup-name*

構文の説明

usergroup-name	アクセス許可が継承される元のユーザ グループの名前です。

コマンド デフォルト

なし

コマンド モード

ユーザ グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

各ユーザ グループは、そのグループのユーザに適用できる一連のタスク グループが関連付けられます。 タスク グループは、タスク ID の集合によって定義されます。 タスク グループには、各アクション クラスに対応したタスク ID リストが含まれます。 ユーザに対するタスク アクセス許可は、そのユーザが属するユーザ グループに関連付けられたタスク グループから（EXEC または XML セッションの開始時に）取得されます。

ユーザ グループは、別のユーザ グループからの継承をサポートします。 **inherit usergroup** コマンドを使用して、あるユーザ グループから別のユーザ グループにアクセス許可（タスク ID 属性）をコピーします。「コピー先」のユーザ グループは継承元のグループのプロパティを継承し、これらのグループに指定されているすべてのタスク ID の集合を形成します。 たとえば、ユーザ グループ A がユーザ グループ B を継承すると、ユーザ グループ A のタスク マップは A と B の集合になります。 循環インクルードは検出され、拒否されます。 ユーザ グループは、root-system ユーザ、root-sdr ユーザ、netadmin ユーザなどの事前定義されたグループからプロパティを継承できません。 継承元のユーザグループが変更されると、継承元のグループ内にただちに反映されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、purchasing ユーザ グループが sales ユーザ グループのプロパティを継承できるようにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup purchasing
RP/0/RSP0/CPU0:router(config-ug)# inherit usergroup sales
```

関連コマンド

コマンド	説明
description（AAA）, （33 ページ）	タスク グループ コンフィギュレーション モードでタスク グループの説明を作成するか、ユーザ グループ コンフィギュレーション モードでユーザ グループの説明を作成します。
taskgroup, （125 ページ）	一連のタスク ID に関連付けるように、タスク グループを設定します。
usergroup, （133 ページ）	一連のタスク グループに関連付けるように、ユーザ グループを設定します。

key（RADIUS）

ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定するには、RADIUS サーバグループ プライベート コンフィギュレーション モードで **key**（**RADIUS**）コマンドを使用します。

key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

no key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
clear-text-key	暗号化されていない（クリアテキスト）ユーザ パスワードを指定します。

コマンド デフォルト

サブモードの **key** コマンドでは、定義されている場合はデフォルトでグローバル コンフィギュレーション モードの **radius-server key** コマンドが使用されます。 グローバル キーも定義されていない場合、この設定は完了しません。

コマンド モード

RADIUS サーバグループ プライベート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、暗号キーを anykey に設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# key anykey
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の RADIUS サーバ ホストを別個のリストにグループ化します。
radius-server key, （60 ページ）	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。

key（TACACS+）

AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定するには、TACACS ホスト コンフィギュレーション モードで **key（TACACS+）** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

no key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
auth-key	AAA サーバと TACACS+ サーバ間の暗号化されていないキーを指定します。

コマンド デフォルト

なし

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

TACACS+ パケットは、キーを使って暗号化されます。このキーは、TACACS+ デーモンで使用されるキーと一致する必要があります。 このキーを指定すると、このサーバに限り、**tacacs-server key** コマンドで設定されているキーが上書きされます。

このキーを使用して、TACACS+ から発信されるパケットを暗号化します。パケットが正しく復号化されるよう、このキーは外部 TACACS+ サーバに設定されているキーと一致している必要があります。 一致しない場合は、復号化に失敗します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、暗号キーを anykey に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# key anykey
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。
tacacs-server key, （117 ページ）	ルータと TACACS+ デーモン間のすべての TACACS+通信に使用される認証および暗号キーをグローバルに設定します。

login authentication

ログインに対する認証、許可、アカウンティング（AAA）の認証をイネーブルにするには、回線テンプレート コンフィギュレーション モードで **login authentication** コマンドを使用します。 デフォルトの認証設定に戻すには、このコマンドの **no** 形式を使用します。

login authentication {**default**| *list-name*}

no login authentication

構文の説明

default	**aaa authentication login** コマンドで設定されている、デフォルトの AAA 認証方式リストです。
list-name	認証に使用する方式リストの名前です。 このリストは、**aaa authentication login** コマンドで指定します。

コマンド デフォルト

このコマンドでは、**aaa authentication login** コマンドで設定されたデフォルトが使用されます。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

login authentication コマンドは、ログイン時に試行される AAA 認証方式のリスト名を指定した AAA と一緒に使用する、回線単位のコマンドです。

⚠ **注意** **aaa authentication login** コマンドで設定されていない *list-name* 値を使用した場合、その設定は拒否されます。

login authentication コマンドの **no** 形式を入力すると、このコマンドに **default** キーワードを使用した場合と同じ結果になります。

このコマンドを実行する前に、**aaa authentication login** グローバル コンフィギュレーション コマンドを使用して認証プロセスのリストを作成します。

タスク ID

タスク ID	操作
aaa	read, write
tty-access	read, write

例

次に、回線テンプレート *template1* にデフォルトの AAA 認証を使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template template1
RP/0/RSP0/CPU0:router(config-line)# login authentication default
```

次に、回線テンプレート *template2* に AAA 認証リスト *list1* を使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template template2
RP/0/RSP0/CPU0:router(config-line)# login authentication list1
```

関連コマンド

コマンド	説明
aaa authentication, （13 ページ）	認証の方式リストを作成します。

password（AAA）

ユーザにログインパスワードを作成するには、ユーザ名コンフィギュレーションモードまたは回線テンプレート コンフィギュレーション モードで **password** コマンドを使用します。 パスワードを削除するには、このコマンドの **no** 形式を使用します。

password {**[0]**| **7** *password*}

no password {**0**| **7** *password*}

構文の説明

0	（任意）暗号化されていないクリアテキスト パスワードが続くことを指定します。
7	暗号化パスワードが続くことを指定します。
password	「lab」など、ログインするユーザが入力する暗号化されていないパスワードのテキストを指定します。 暗号化が設定されている場合、パスワードはユーザに表示されません。 最長で 253 文字まで入力できます。

コマンド デフォルト

パスワードは暗号化されていないクリア テキストです。

コマンド モード

ユーザ名コンフィギュレーション

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

パスワードは暗号化かクリア テキストのいずれかのタイプを指定できます。

パスワードで保護された回線で EXEC プロセスが開始されると、パスワードの入力を求められます。ユーザが正しいパスワードを入力すると、プロンプトが実行されます。ユーザがパスワードの入力に 3 回失敗すると、プロセスは終了し、端末がアイドル状態に戻ります。

パスワードは双方向に暗号化されており、復号化できるパスワードを必要とする PPP などのアプリケーションに使用する必要があります。

（注） **show running-config** コマンドに **0** オプションが使用されていると、クリアテキストのログインパスワードが常に暗号化形式で表示されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザに暗号化されていないパスワード *pwd1* を設定する例を示します。 **show** コマンドの出力には、パスワードが暗号化形式で表示されます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# password 0 pwd1
RP/0/RSP0/CPU0:router(config-un)# commit
RP/0/RSP0/CPU0:router(config-un)# show running-config
Building configuration...
username user1
 password 7 141B1309
```

関連コマンド

コマンド	説明
group（AAA）, （35 ページ）	ユーザをグループに追加します。
usergroup, （133 ページ）	ユーザ グループ コンフィギュレーション モードにアクセスし、ユーザ グループを設定して一連のタスク グループに関連付けます。
username, （135 ページ）	ユーザ名コンフィギュレーションモードにアクセスし、新しいユーザにユーザ名とパスワードを設定し、そのユーザのアクセス許可を付与します。

コマンド	説明
line	指定された回線テンプレートの回線テンプレート コンフィギュレーション モードが開始されます。 詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference*』を参照してください。

radius-server dead-criteria time

ルータが RADIUS サーバから有効なパケットを最後に受信してから、サーバに dead マークが付くまでに最低限経過する必要のある時間を秒単位で指定するには、グローバル コンフィギュレーション モードで **radius-server dead-criteria time** コマンドを使用します。 設定された基準をディセーブルにするには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria time *seconds*

no radius-server dead-criteria time *seconds*

構文の説明

seconds	秒単位の時間です。 範囲は、1 ～ 120 秒です。 *seconds* 引数を設定していない場合、サーバのトランザクション レートによって 10 ～ 60 秒になります。 （注） 時間基準は、dead マークを付けるサーバについて満たす必要があります。

コマンド デフォルト

seconds 引数を設定していない場合、サーバのトランザクション レートによって 10 ～ 60 秒になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

（注） **radius-server deadtime** コマンドの前に **radius-server dead-criteria time** コマンドを設定すると、**radius-server dead-criteria time** コマンドが実行されない場合があります。

ルータが起動してからパケットの受信がなく、タイムアウトになると、時間基準は満たされたものとして処理されます。

seconds 引数を指定していない場合、時間はデフォルトに設定されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**radius-server dead-criteria time** コマンドに対し、RADIUS サーバに dead マークを付けるための dead-criteria 条件として時間を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server dead-criteria time 5
```

関連コマンド

コマンド	説明
radius-server dead-criteria tries, （52 ページ）	ルータで連続何回タイムアウトが発生したら、RADIUS サーバに dead マークを付けるかを指定します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間の長さを分単位で定義します。
show radius dead-criteria, （99 ページ）	dead サーバの検出基準の情報を表示します。

radius-server dead-criteria tries

RADIUS サーバに dead マークが付くまでにルータで発生する連続タイムアウト回数を指定するには、グローバル コンフィギュレーション モードで **radius-server dead-criteria tries** コマンドを使用します。 設定された基準をディセーブルにするには、このコマンドの **no** 形式を使用します。

radius-server dead-criteria *tries*

no radius-server dead-criteria *tries*

構文の説明

tries	1 ～ 100 のタイムアウト回数。 *tries* 引数を設定しない場合は、サーバのトランザクション レートと設定されている再送信回数によって、連続タイムタウト回数は 10 ～ 100 となります。 （注） 試行基準は、dead マークを付けるサーバについて満たす必要があります。

コマンド デフォルト

tries 引数を設定しない場合は、サーバのトランザクション レートと設定されている再送信回数によって、連続タイムタウト回数は 10 ～ 100 となります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

サーバが認証とアカウンティングの両方を実行する場合、両方のパケットのタイプが数値に含まれます。 構造が適切でないパケットは、タイムアウトされたものとしてカウントされます。 最初の送信と再送信を含むすべての送信がカウントされます。

（注） **radius-server deadtime** コマンドの前に **radius-server dead-criteria tries** コマンドを設定すると、**radius-server dead-criteria tries** コマンドが実行されない場合があります。

tries 引数が指定されていない場合、試行回数はデフォルトに設定されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**radius-server dead-criteria tries** コマンドに対し、RADIUS サーバに dead マークを付けるための dead-criteria 条件として試行回数を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server dead-criteria tries 4
```

関連コマンド

コマンド	説明
radius-server dead-criteria time, （50 ページ）	ルータが RADIUS サーバから有効なパケットを最後に受信してから、サーバに dead マークが付くまでに経過する必要のある時間を秒単位で定義します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間の長さを分単位で定義します。
show radius dead-criteria, （99 ページ）	dead サーバの検出基準の情報を表示します。

radius-server deadtime

一部のサーバが使用できない場合に RADIUS の応答時間を短縮し、使用できないサーバがただちにスキップされるようにするには、グローバル コンフィギュレーション モードで **radius-server deadtime** コマンドを使用します。 デッドタイムを 0 に設定するには、このコマンドの **no** 形式を使用します。

radius-server deadtime *value*

no radius-server deadtime *value*

構文の説明

value	RADIUS サーバがトランザクション要求によってスキップされる時間を最長 1440（24 時間）まで分単位で表したものです。 指定できる範囲は 1 ～ 1440 です。 デフォルト値は 0 です。

コマンド デフォルト

デッド タイムは 0 に設定されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

他すべてのサーバに dead マークが付いている場合、また、ロールオーバー方式が存在しない場合以外は、指定の時間内に追加要求が発生すると、dead マークの付いた RADIUS サーバはスキップされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**radius-server deadtime** コマンドに対し、認証要求への応答に失敗した RADIUS サーバのデッドタイムを 5 分に指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server deadtime 5
```

radius-server host

RADIUS サーバ ホストを指定するには、グローバル コンフィギュレーション モードで **radius-server host** コマンドを使用します。 指定した RADIUS ホストを削除するには、このコマンドの **no** 形式を使用します。

radius-server host {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no radius-server host {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

hostname	RADIUS サーバ ホストのドメイン ネーム システム（DNS）名です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対してユーザ データグラム プロトコル（UDP）宛先ポートを指定します。0 に設定すると、そのホストは認証に使用されません。 指定しない場合、ポート番号はデフォルトの 1645 になります。
acct-port *port-number*	（任意）アカウンティング要求に対して UDP 宛先ポートを指定します。0 に設定すると、そのホストはアカウンティングに使用されません。 指定しない場合、ポート番号はデフォルトの 1646 になります。
timeout *seconds*	（任意）ルータが RADIUS サーバの応答を待機し、再送信するまでの時間間隔（秒単位）です。 この設定によって、**radius-server timeout** コマンドのグローバル値は上書きされます。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。 1 ～ 1000 の範囲の値を入力します。 デフォルトは 5 です。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数です。 この設定によって、**radius-server retransmit** コマンドのグローバル設定は上書きされます。 再送信値が指定されていない場合は、グローバル値が使用されます。 1 ～ 100 の範囲の値を入力します。 デフォルトは 3 です。

key *string*	（任意）ルータと RADIUS サーバ間で使用される認証および暗号キーを指定します。 この設定によって、**radius-server key** コマンドのグローバル設定は上書きされます。 キー文字列を指定しない場合、グローバル値が使用されます。 キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。 キーは常に、**radius-server host** コマンド構文の最後の項目として設定します。 これは、先頭のスペースは無視されますが、キーの中と末尾のスペースは使用されるためです。 キーにスペースを使用する場合は、引用符自体がキーの一部でない限り、そのキーを引用符で囲まないでください。

コマンド デフォルト

RADIUS ホストは指定されません。グローバルの**radius-server** コマンド値を使用します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

複数の **radius-server host** コマンドを使用して、複数のホストを指定できます。 Cisco IOS XR ソフトウェアにより、指定の順序でホストが検索されます。

ホスト固有のタイムアウト値、再送信値、またはキー値が指定されていない場合は、グローバル値が各ホストに適用されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、*host1* を RADIUS サーバとして設定し、アカウンティングと認証の両方にデフォルト ポートを使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host host1host1
```

次に、host1 という RADIUS ホストで認証要求の宛先ポートとしてポート 1612 を設定し、アカウンティング要求の宛先ポートとしてポート 1616 を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host host1 auth-port 1612 acct-port 1616
```

回線を入力するとすべてのポート番号がリセットされるため、ホストを指定し、1 つの回線のアカウンティング ポートと認証ポートを設定する必要があります。

次に、RADIUS サーバとして IP アドレス 172.29.39.46 のホストを設定し、許可ポートおよびアカウンティング ポートとしてポート 1612 と 1616 を使用し、タイムアウト値を 6、再送信値を 5 にそれぞれ設定して、さらに RADIUS サーバのキーと一致する暗号キーとして「rad123」を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server host 172.29.39.46 auth-port 1612 acct-port
1616 timeout 6 retransmit 5 key rad123
```

アカウンティングと認証に別個のサーバを使用するには、適宜 0 ポート値を使用します。

次に、RADIUS サーバ host1 を認証には使用せずにアカウンティングに使用するように設定し、RADIUS サーバ host2 をアカウンティングには使用せずに認証に使用するように指定する例を示します。

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config)#radius-server host host1.example.com auth-port 0
RP/0/RSP0/CPU0:router(config)#radius-server host host2.example.com acct-port 0
```

関連コマンド

コマンド	説明
aaa accounting subscriber	アカウンティングの方式リストを作成します。
aaa authentication subscriber	認証の方式リストを作成します。
aaa authorization subscriber	許可の方式リストを作成します。
radius-server key, （60 ページ）	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。
radius-server retransmit, （62 ページ）	Cisco IOS XR ソフトウェアからサーバにパケットを再送信する回数を指定します。

コマンド	説明
radius-server timeout, （64 ページ）	サーバホストが応答するまでルータが待機する間隔を設定します。

radius-server key

ルータと RADIUS デーモン間のすべての RADIUS 通信に対して認証および暗号キーを設定するには、グローバル コンフィギュレーション モードで **radius-server key** コマンドを使用します。 キーをディセーブルにするには、このコマンドの **no** 形式を使用します。

radius-server key {**0** *clear-text-key*| **7** *encrypted-key*| *clear-text-key*}

no radius-server key

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
clear-text-key	暗号化されていない（クリアテキスト）共有キーを指定します。

コマンド デフォルト

認証および暗号キーはディセーブルになります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

入力したキーは、RADIUS サーバで使用されるキーと一致する必要があります。 先頭のスペースはすべて無視されますが、キーの中間および末尾のスペースは使用できます。 キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。

タスク ID

タスク ID	操作
aaa	read, write

例

次の例では、クリアテキスト キーを「samplekey」に設定する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 0 samplekey
```

次の例では、暗号化共有キーを「anykey」に設定する方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server key 7 anykey
```

radius-server retransmit

Cisco IOS XR ソフトウェアからサーバにパケットを再送信する回数を指定するには、グローバル コンフィギュレーション モードで **radius-server retransmit** コマンドを使用します。 再送信をディセーブルにするには、このコマンドの **no** 形式を使用します。

radius-server retransmit *retries*

no radius-server retransmit

構文の説明

retries	再送信の最大試行回数です。 範囲は 1 ～ 100 です。 デフォルトは 3 です。

コマンド デフォルト

RADIUS サーバには 3 回まで、または応答が受信されるまで再送信されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

RADIUS クライアントでは、すべてのサーバに対して再送信が試みられ、それぞれがタイムアウトになってから再送信カウントが増加します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、再送信カウンタ値を 5 回に指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server retransmit 5
```

関連コマンド

コマンド	説明
radius-server key, （60 ページ）	ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。

radius-server timeout

タイムアウトになるまでルータがサーバ ホストの応答を待機する間隔を設定するには、グローバル コンフィギュレーション モードで **radius-server timeout** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

radius-server timeout *seconds*

no radius-server timeout

構文の説明

seconds	タイムアウトの間隔を指定する秒数です。 範囲は、1 ～ 1000 です。

コマンド デフォルト

radius-server timeout のデフォルト値は 5 秒です。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

radius-server timeout コマンドを使用して、タイムアウトになるまでルータがサーバ ホストの応答を待機する秒数を設定します。

タスク ID

タスク ID	操作
aaa	read, write

例

この例では、インターバル タイマーを 10 秒に変更します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius-server timeout 10
```

radius source-interface

すべての発信 RADIUS パケットに対して RADIUS が指定されたインターフェイスまたはサブインターフェイスの IP アドレスを使用するようにするには、グローバル コンフィギュレーション モードで **radius source-interface** コマンドを使用します。 指定されたインターフェイスだけがデフォルトにならないようにし、すべての発信 RADIUS パケットに使用されないようにするには、このコマンドの **no** 形式を使用します。

radius source-interface *interface* [**vrf** *vrf_name*]

no radius source-interface *interface*

構文の説明

interface-name	RADIUS がすべての発信パケットに使用するインターフェイスの名前です。
vrf *vrf-id*	割り当てられている VRF の名前を指定します。

コマンド デフォルト

特定のソース インターフェイスが設定されていない場合、インターフェイスがダウン状態にある場合、またはインターフェイスに IP アドレスが設定されていない場合は、IP アドレスが自動的に選択されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.2.0	このコマンドが BNG でサポートされました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

radius source-interface コマンドを使用して、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスを設定します。 インターフェイスまたはサブインターフェイスがアップ状態である限り、このアドレスが使用されます。 このように、RADIUS

サーバでは IP アドレスのリストを保持する代わりに、すべてのネットワーク アクセス クライアントに対して 1 つの IP アドレス エントリを使用できます。

指定されたインターフェイスまたはサブインターフェイスには、IP アドレスが関連付けられている必要があります。指定のインターフェイスまたはサブインターフェイスにIPアドレスが設定されていないか、そのインターフェイスがダウン状態にある場合、RADIUS はデフォルトに戻ります。これを回避するには、インターフェイスまたはサブインターフェイスにIPアドレスを追加するか、そのインターフェイスをアップ状態にします。

特に、ルータに多数のインターフェイスやサブインターフェイスがあり、特定のルータからのすべての RADIUS パケットに同じ IP アドレスが含まれるようにする場合は、**radius source-interface** コマンドが役立ちます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、すべての発信 RADIUS パケットに対して RADIUS がサブインターフェイス s2 の IP アドレスを使用するようにする例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# radius source-interface Loopback 10 vrf vrf-1
```

retransmit（RADIUS）

サーバが応答しない場合や、応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定するには、RADIUS サーバグループ プライベート コンフィギュレーション モードで **retransmit** コマンドを使用します。

retransmit *retries*

no retransmit *retries*

構文の説明

retries	*retries* 引数は、再送信値を指定します。 範囲は 1 ～ 100 です。 再送信値が指定されていない場合は、グローバル値が使用されます。

コマンド デフォルト

デフォルト値は 3 です。

コマンド モード

RADIUS サーバグループ プライベート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、再送信値を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
```

```
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# retransmit 100
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の RADIUS サーバ ホストを別個のリストにグループ化します。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。

secret

Message Digest 5（MD5）で暗号化されたシークレットを設定して暗号化されたユーザ名に関連付けるには、ユーザ名コンフィギュレーション モードまたは回線テンプレート コンフィギュレーション モードで **secret** コマンドを使用します。 セキュア シークレットを削除するには、このコマンドの **no** 形式を使用します。

secret {**[0]** *secret-login*| **5** *secret-login*}

no secret {**0**| **5**} *secret-login*

構文の説明

0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。 MD5 暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。 それ以外の場合、パスワードは暗号化されません。
5	暗号化された MD5 パスワード（シークレット）が続くことを指定します。
secret-login	ユーザのログイン ID と一緒に MD5 で暗号化されたパスワードとして保存される、ユーザが入力する英数字のテキスト文字列です。 最長で 253 文字まで入力できます。 （注） 入力する文字は、MD5 暗号化標準に準拠する必要があります。

コマンド デフォルト

パスワードは指定されません。

コマンド モード

ユーザ名コンフィギュレーション

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

Cisco IOS XR ソフトウェアでは、ログインに使用するユーザ名とパスワードに Message Digest 5（MD5）暗号化を設定できます。 MD5 暗号化は、暗号化されたパスワードの逆送信を不可能にする一方向ハッシュ関数であり、強力な暗号化保護を可能にします。 MD5 暗号化を使用すると、クリアテキストパスワードを取得できません。 したがって、MD5 で暗号化されたパスワードは、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）など、クリアテキスト パスワードの取得を必要とするプロトコルと一緒には使用できません。

セキュア シークレット ID のタイプは暗号化（5）とクリア テキスト（0）のいずれかを指定できます。 0 も 5 も選択しなかった場合、入力したクリアテキスト パスワードは暗号化されません。

パスワードで保護された回線で EXEC プロセスが開始されると、シークレットの入力を求めるプロンプトが表示されます。 ユーザが正しいシークレットを入力すると、プロンプトが実行されます。 ユーザがシークレットの入力に 3 回失敗すると、端末はアイドル状態に戻ります。

シークレットは一方向の暗号化なので、復号可能なシークレットを必要としないログイン アクティビティに使用します。

MD5 パスワードの暗号化がイネーブルであることを確認するには、**show running-config** コマンドを使用します。 コマンド出力に「username name secret 5」という行が表示された場合は、拡張パスワード セキュリティがイネーブルです。

（注） **0** オプションを使用して暗号化されていないパスワードを指定すると、**show running-config** コマンドを実行してもログイン パスワードはクリアテキストで表示されません。 「例」の項を参照してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザ *user2* にクリアテキスト シークレット「lab」を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# username user2
RP/0/RSP0/CPU0:router(config-un)# secret 0 lab
RP/0/RSP0/CPU0:router(config-un)# commit
RP/0/RSP0/CPU0:router(config-un)# show running-config
Building configuration...
username user2
 secret 5 $1$DTmd$q7C6fhzje7Cc7Xzmu2Frx1
!
end
```

関連コマンド

コマンド	説明
group（AAA）， （35 ページ）	ユーザをグループに追加します。

コマンド	説明
password（AAA）, （47 ページ）	ユーザのログイン パスワードを作成します。
usergroup, （133 ページ）	ユーザ グループ コンフィギュレーション モードにアクセスし、ユーザ グループを設定して一連のタスク グループに関連付けます。
username, （135 ページ）	ユーザ名コンフィギュレーションモードにアクセスし、新しいユーザにユーザ名とパスワードを設定し、そのユーザのアクセス許可を付与します。

server（RADIUS）

特定の RADIUS サーバを定義済みのサーバ グループに関連付けるには、RADIUS サーバグループ コンフィギュレーションモードで **server** コマンドを使用します。 関連付けられたサーバをサーバ グループから削除するには、このコマンドの **no** 形式を使用します。

server {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

no server {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポートを指定します。 *port-number* 引数は、認証要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストは認証に使用されません。 デフォルトは 1645 です。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。 *port-number* 引数は、アカウンティング要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。 デフォルトは 1646 です。

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

RADIUS サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server コマンドを使用して、特定の RADIUS サーバを定義済みのサーバ グループに関連付けることができます。

サーバを識別する方法は、AAA サービスを提供する方法に応じて 2 種類あります。 IP アドレスを使用して単純にサーバを識別する方法と、オプションの **auth-port** キーワードおよび **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを識別する方法があります。

オプションのキーワードを使用すると、ネットワーク アクセス サーバにより、IP アドレスと特定の UDP ポート番号に基づいてグループ サーバに関連付けられている RADIUS セキュリティ サーバおよびホスト インスタンスが識別されます。 IP アドレスと UDP ポート番号の組み合わせによって一意の ID を作成し、特定の AAA サービスを提供する RADIUS ホスト エントリとして各ポートを個々に定義できます。 たとえば、同一の RADIUS サーバの 2 つの異なるホスト エントリを同一のサービス（アカウンティングなど）に対して設定すると、2 番目に設定したホスト エントリは最初のホスト エントリをバックアップする自動スイッチオーバーとして機能します。 この場合、最初のホストエントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します （試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、同一のサービス、つまり認証とアカウンティングに設定されている同一の RADIUS サーバ上の 2 つの異なるホスト エントリを使用する例を示します。 2 番目に設定されているホスト エントリは、最初のホスト エントリをバックアップするスイッチオーバーとして機能します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server 1.1.1.1 auth-port 1645 acct-port 1646
RP/0/RSP0/CPU0:router(config-sg-radius)# server 2.2.2.2 auth-port 2000 acct-port 2001
```

関連コマンド

コマンド	説明
aaa group server radius, （22 ページ）	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。

コマンド	説明
deadtime（サーバグループ コンフィギュレーション），（31 ページ）	RADIUS サーバ グループ レベルでデッドタイム値を設定します。
server-private（RADIUS），（78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

server（TACACS+）

特定の TACACS+ サーバを定義済みのサーバ グループに関連付けるには、TACACS+ サーバグループ コンフィギュレーション モードで **server** コマンドを使用します。 関連付けられたサーバをサーバ グループから削除するには、このコマンドの **no** 形式を使用します。

server {*hostname*| *ip-address*}

no server {*hostname*| *ip-address*}

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	サーバ ホストの IP アドレスです。

コマンド デフォルト

なし

コマンド モード

TACACS+ サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server コマンドを使用して、特定の TACACS+ サーバを定義済みのサーバ グループに関連付けることができます。 サーバは設定時にアクセス可能である必要はありません。 あとで、認証、許可、アカウンティング（AAA）の設定に使用される方式リストから、設定済みのサーバ グループを参照できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、IP アドレス 192.168.60.15 の TACACS+ サーバをサーバ グループ tac1 に関連付ける例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ tac1
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の TACACS+ サーバ ホストを別個のリストにグループ化します。

server-private（RADIUS）

グループ サーバに対して、プライベート RADIUS サーバの IP アドレスを設定するには、RADIUS サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。 関連付けられたプライベート サーバを AAA グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private {*hostname*| *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（任意）認証要求に対するユーザデータグラムプロトコル（UDP）宛先ポートを指定します。 *port-number* 引数は、認証要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストは認証に使用されません。 デフォルト値は 1645 です。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。 *port-number* 引数は、アカウンティング要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。 デフォルト値は 1646 です。
timeout *seconds*	（任意）再送信するまでにルータが RADIUS サーバの応答を待機する秒数を指定します。 この設定によって、**radius-server timeout** コマンドのグローバル値は上書きされます。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。 *seconds* 引数は、タイムアウト値を秒単位で指定します。 範囲は 1 ～ 1000 です。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。 この設定によって、**radius-server transmit** コマンドのグローバル設定は上書きされます。 *retries* 引数は、再送信値を指定します。 範囲は 1 ～ 100 です。 再送信値が指定されていない場合は、グローバル値が使用されます。

key *string*	（任意）ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定します。 この設定によって、**radius-server key** コマンドのグローバル設定は上書きされます。 キー文字列を指定しない場合、グローバル値が使用されます。

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

RADIUS サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 VRF インスタンス間では IP アドレスの重複が可能です。 プライベート サーバ（プライベート アドレスを持つサーバ）はサーバ グループ内で定義して、他のグループからは非表示のままにすることができます。一方、グローバル プール（デフォルトの RADIUS サーバグループなど）内のサーバは、IP アドレスとポート番号を使って参照できます。 このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

auth-port キーワードと **acct-port** キーワードのどちらを使用しても、RADIUS サーバグループ プライベート コンフィギュレーション モードが開始されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、group1 RADIUS グループ サーバを定義して、これにプライベート サーバを関連付け、RADIUS サーバグループ プライベート コンフィギュレーション モードを開始する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 timeout 5
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 retransmit 3
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 key coke
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# exit
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 timeout 5
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 retransmit 3
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 key coke
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)#
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	複数の RADIUS サーバ ホストを別々のリストと別々の方式にグループ分けします。
radius-server key, （60 ページ）	ルータと RADIUS デーモン間のすべての RADIUS 通信に対する認証および暗号キーを設定します。
radius-server retransmit, （62 ページ）	Cisco IOS XR ソフトウェアからサーバにパケットを再送信する回数を指定します。
radius-server timeout, （64 ページ）	タイムアウトになるまでにルータがサーバホストの応答を待機する間隔を設定します。
key（RADIUS）, （41 ページ）	ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定します。
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
timeout（RADIUS）, （127 ページ）	ルータが RADIUS サーバの応答を待機する秒数を指定します。この秒数を過ぎると、再送信されます。
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。

server-private（TACACS+）

グループ サーバに対して、プライベートTACACS+サーバのIPアドレスを設定するには、TACACS+サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。 関連付けられたプライベート サーバを AAA グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private {*hostname*| *ip-address*} [**port** *port-number*] [**timeout** *seconds*] [**key** *string*]

no server-private {*hostname*| *ip-address*}

構文の説明

hostname	サーバ ホスト名の指定に使用する文字列です。
ip-address	TACACS+ サーバ ホストの IP アドレスです。
port *port-number*	（任意）サーバのポート番号を指定します。 この設定によって、デフォルトのポート 49 は上書きされます。 有効なポート番号の範囲は 1 ～ 65535 です。
timeout *seconds*	（任意）認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を秒で指定します。 このオプションによって、**tacacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。 範囲は 1 ～ 1000 です。 デフォルト値は 5 です。
key *string*	（任意）ルータと TACACS+ サーバ上で稼働する TACACS+ デーモン間で使用される認証および暗号キーを指定します。 このキーは **tacacs-server key** コマンドのグローバル設定を書き換えます。 キー文字列を指定しない場合、グローバル値が使用されます。

コマンド デフォルト

port-name 引数が指定されていない場合、標準ポート 49 がデフォルトで使用されます。

seconds 引数が指定されていない場合、5 秒がデフォルトで使用されます。

コマンド モード

TACACS+ サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 4.1.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 VRF インスタンス間では IP アドレスの重複が可能です。 プライベート サーバ（プライベート アドレスを持つサーバ）はサーバ グループ内で定義して、他のグループからは非表示のままにすることができます。一方、グローバルプール（デフォルトの TACACS+ サーバグループなど）内のサーバは、IP アドレスとポート番号を使って参照できます。 このように、サーバグループ内のサーバのリストには、グローバルコンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、myserver TACACS+ グループ サーバを定義して、プライベート サーバを関連付け、TACACS+ サーバグループ プライベート コンフィギュレーション モードを開始する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 timeout 5
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 key a_secret
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 port 51
RP/0/RSP0/CPU0:router(config-sg-tacacs-private)# exit
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 timeout 5
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 key coke
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 port 300
RP/0/RSP0/CPU0:router(config-sg-tacacs-private)#
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の TACACS+ サーバ ホストを別個のリストと別個の方式にグループ化します。
tacacs-server key, （117 ページ）	ルータと TACACS+ デーモン間のすべての TACACS+ 通信に使用される認証および暗号キーを設定します。
tacacs-server timeout, （119 ページ）	タイムアウトになるまでにルータがサーバ ホストの応答を待機する間隔を設定します。

コマンド	説明
key（TACACS+），（43 ページ）	AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。
timeout（TACACS+），（129 ページ）	認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。
vrf（TACACS+），（143 ページ）	AAA TACACS+ サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照情報を設定します。

show aaa

インターネットキー交換（IKE）セキュリティプロトコルグループ、ユーザグループ、ローカルユーザ、ログイントレース、タスクグループに関する情報を表示したり、システム内のすべてのIKEグループ、ユーザグループ、ローカルユーザ、タスクグループに関連付けられたすべてのタスクIDを一覧表示したり、指定のIKEグループ、ユーザグループ、ローカルユーザ、タスクグループのすべてのタスクIDを一覧表示したりするには、EXECモードで**show aaa コマンド**を使用します。

show aaa {**ikegroup** *ikegroup-name*| **login trace**| **usergroup** [*usergroup-name*]| **trace**| **userdb** [*username*]| **task supported**| **taskgroup** [**root-lr**| **netadmin**| **operator**| **sysadmin**| **root-system**| **service-admin**| **cisco-support**| **t** *askgroup-name*]}

構文の説明

ikegroup	すべてのIKEグループの詳細を表示します。
ikegroup-name	（任意）詳細が表示されるIKEグループです。
login trace	ログイン サブシステムに関するトレース データを表示します。
usergroup	すべてのユーザ グループの詳細を表示します。
root-lr	（任意）ユーザグループ名です。
netadmin	（任意）ユーザグループ名です。
operator	（任意）ユーザグループ名です。
sysadmin	（任意）ユーザグループ名です。
root-system	（任意）ユーザグループ名です。
cisco-support	（任意）ユーザグループ名です。
usergroup-name	（任意）ユーザグループ名です。
trace	AAAサブシステムに関するトレース データを表示します。
userdb	すべてのローカル ユーザと各ユーザが属するユーザグループの詳細を表示します。
username	（任意）詳細を表示する対象のユーザです。
task supported	使用可能なすべてのAAAタスクIDを表示します。

taskgroup	すべてのタスク グループの詳細を表示します。 （注） taskgroup のキーワードについては、オプションの usergroup name キーワード リストを参照してください。
taskgroup-name	（任意）詳細を表示する対象のタスク グループ。

コマンド デフォルト

引数を入力しない場合は、すべてのユーザ グループ、すべてのローカルユーザ、またはすべてのタスク グループの詳細が表示されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

システム内のすべての IKE グループ、ユーザ グループ、ローカル ユーザ、またはタスク グループの詳細を表示するには、**show aaa** コマンドを使用します。 オプションの *ikegroup-name*、*usergroup-name*、*username*、または *taskgroup-name* 引数を使用して、それぞれ指定の IKE グループ、ユーザ グループ、ユーザ、またはタスク グループの詳細を表示します。

タスク ID

タスク ID	操作
aaa	read

例

次に、**ikegroup** キーワードを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa ikegroup

IKE Group ike-group
        Max-Users = 50
IKE Group ikeuser
        Group-Key = test-password
        Default Domain = cisco.com
IKE Group ike-user
```

次に、**usergroup** コマンドを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa usergroup operator

User group 'operator'
  Inherits from task group 'operator'
User group 'operator' has the following combined set
of task IDs (including all inherited groups):
Task:       basic-services  : READ    WRITE    EXECUTE DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

次に、タスク グループ netadmin に対して **taskgroup** キーワードを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa taskgroup netadmin

Task group 'netadmin'

Task group 'netadmin' has the following combined set
  of task IDs (including all inherited groups):

Task:                  aaa  : READ
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                admin  : READ
Task:                 ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cgn  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ
Task:                 dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                  eem  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:    ethernet-services  : READ
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:                l2vpn  : READ    WRITE    EXECUTE    DEBUG
Task:                   li  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ
Task:             mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:          mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:            multicast  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:             pkg-mgmt  : READ
Task:              pos-dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ                              (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ                              (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、オペレータに対して **taskgroup** キーワードを使用した **show aaa** コマンドの出力例を示します。 タスク グループ operator には、次に示すように、継承されるすべてのグループを含む一連のタスク ID が組み合わされています。

```
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ
Task:                 diag  : READ
Task:           ext-access  : READ             EXECUTE
Task:              logging  : READ
```

次に、ルート システムに対して **taskgroup** キーワードを使用した **show aaa** コマンドの出力例を示します。 タスク グループ root system には次に示すように、継承されるすべてのグループを含む一連のタスク ID が組み合わされています。

```
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa acl  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  admin atm  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services           bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp boot  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot bundle  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle    cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp cef  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt services  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services           crypto  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto   diag  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  drivers  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access     fabric  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem         fr  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  host-services  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services           hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  interface  : READ    WRITE    EXECUTE    DEBUG
Task:            interface inventory  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services         ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4 ipv6  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:                 ipv6 isis  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  logging  : READ    WRITE    EXECUTE    DEBUG
Task:              logging     lpts  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static te  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow network  : READ    WRITE    EXECUTE    DEBUG
Task:              network     ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf ouni  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:             pkg  pos-mgmt dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG
Task:          root-system  : READ    WRITE    EXECUTE    DEBUG
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、**userdb** キーワードを使用した **show aaa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show aaa userdb

Username lab (admin plane)
User group root-system
User group cisco-support
Username acme
User group root-system
```

次に、**task supported** キーワードを使用した **show aaa** コマンドの出力例を示します。 タスク ID はアルファベット順に表示されます。

```
RP/0/RP0/CPU0:router# show aaa task supported

aaa
acl
admin
atm
basic-services
bcdl
bfd
bgp
boot
bundle
cdp
cef
cisco-support
config-mgmt
config-services
crypto
diag
disallowed
drivers
eigrp
ext-access
fabric
fault-mgr
```

```
filesystem
firewall
fr
hdlc
host-services
hsrp
interface
inventory
ip-services
ipv4
ipv6
isis
logging
lpts
monitor
mpls-ldp
mpls-static
mpls-te
multicast
netflow
network
ospf
ouni
pkg-mgmt
pos-dpt
ppp
qos
rib
rip
User group root-systemlr
root-system
route-map
route-policy
sbc
snmp
sonet-sdh
static
sysmgr
system
transport
tty-access
tunnel
universal
vlan
vrrp
```

関連コマンド

コマンド	説明
show user, （108 ページ）	現在ログインしているユーザに対してイネーブルになっているタスク ID を表示します。

show radius

システムに設定されている RADIUS サーバの情報を表示するには、EXEC モードで **show radius** コマンドを使用します。

show radius

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

RADIUS サーバが設定されていない場合、出力は表示されません。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show radius コマンドを使用して、設定されている RADIUS サーバごとの統計情報を表示します。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius

Global dead time: 0 minute(s)

Server: 1.1.1.1/1645/1646  is UP
  Timeout: 5 sec, Retransmit limit: 3
  Authentication:
    0 requests, 0 pending, 0 retransmits
```

```
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
  Accounting:
    0 requests, 0 pending, 0 retransmits
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt

Server: 2.2.2.2/1645/1646  is UP
  Timeout: 10 sec, Retransmit limit: 3
  Authentication:
    0 requests, 0 pending, 0 retransmits
    0 accepts, 0 rejects, 0 challenges
    0 timeouts, 0 bad responses, 0 bad authenticators
    0 unknown types, 0 dropped, 0 ms latest rtt
  Accounting:
    0 requests, 0 pending, 0 retransmits
    0 responses, 0 timeouts, 0 bad responses
    0 bad authenticators, 0 unknown types, 0 dropped
    0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *1*：*show radius* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート/アカウンティング要求の UDP 宛先ポートです。
Timeout	タイムアウトになるまでにルータがサーバホストの応答を待機する秒数です。
Retransmit limit	Cisco IOS XR ソフトウェアで RADIUS サーバホストのリストを検索する回数です。

関連コマンド

コマンド	説明
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。
radius-server retransmit, （62 ページ）	Cisco IOS XR ソフトウェアで RADIUS サーバホストのリストを検索する回数を指定します。
radius-server timeout, （64 ページ）	サーバホストが応答するまでルータが待機する間隔を設定します。

show radius accounting

RADIUS アカウンティング サーバとポートの情報および詳細な統計情報を取得するには、EXEC モードで **show radius accounting** コマンドを使用します。

show radius accounting

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

RADIUS サーバがルータに設定されていない場合、出力は空になります。 カウンタ（要求や保留など）に対するデフォルト値の場合、RADIUS サーバは定義されただけでまだ使用されていないため、値はすべてゼロになります。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read

例

次に、サーバ単位で表示される **show radius accounting** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius accounting

Server: 12.26.25.61, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt
```

```
Server: 12.26.49.12, port: 1813
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt

Server: 12.38.28.18, port: 29199
0 requests, 0 pending, 0 retransmits
0 responses, 0 timeouts, 0 bad responses
0 bad authenticators, 0 unknown types, 0 dropped
0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *2*：*show radius accounting* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート、アカウンティング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authentication, （13 ページ）	認証の方式リストを作成します。
show radius authentication, （95 ページ）	RADIUS 認証サーバおよびポートの情報と詳細な統計情報を取得します。

show radius authentication

RADIUS 認証サーバおよびポートの情報と詳細な統計情報を取得するには、EXEC モードで **show radius authentication** コマンドを使用します。

show radius authentication

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

RADIUS サーバがルータに設定されていない場合、出力は空になります。 カウンタ（要求や保留など）に対するデフォルト値の場合、RADIUS サーバは定義されただけでまだ使用されていないため、値はすべてゼロになります。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius authentication** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius authentication

Server: 12.26.25.61, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
```

```
Server: 12.26.49.12, port: 1812
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt

Server: 12.38.28.18, port: 21099
0 requests, 0 pending, 0 retransmits
0 accepts, 0 rejects, 0 challenges
0 timeouts, 0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *3*：*show radius authentication* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート、アカウンティング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
aaa accounting, （4 ページ）	アカウンティングの方式リストを作成します。
aaa authentication, （13 ページ）	認証の方式リストを作成します。
show radius accounting, （93 ページ）	RADIUS アカウンティング サーバおよびポートの情報と詳細な統計情報を取得します。

show radius client

Cisco IOS XR ソフトウェアで RADIUS クライアントの一般情報を取得するには、EXEC モードで **show radius client** コマンドを使用します。

show radius client

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

カウンタ（無効なアドレスなど）のデフォルト値は 0 です。 Network Access Server（NAS; ネットワーク アクセス サーバ）の ID は、ルータで定義されているホスト名です。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show radius client コマンドを実行すると、NAS に認識されないサーバなど、無効な RADIUS サーバから受信した認証およびアカウンティングの応答が表示されます。 また、**show radius client** コマンドによって、RADIUS 認証クライアント、アカウンティング クライアント、またはその両方のホスト名または NAS ID が表示されます。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius client** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius client
```

```
Client NAS identifier:                          miniq
Authentication responses from invalid addresses:      0
Accounting responses from invalid addresses:          0
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *4* : ***show radius client*** フィールドの説明

フィールド	説明
Client NAS identifier	RADIUS 認証クライアントの NAS ID を識別します。

関連コマンド

コマンド	説明
server（RADIUS）, （73 ページ）	特定の RADIUS サーバを定義済みのサーバ グループに関連付けます。
show radius, （91 ページ）	システムに設定されている RADIUS サーバの情報を表示します。

show radius dead-criteria

デッド サーバの検出基準に関する情報を取得するには、EXEC モードで **show radius dead-criteria** コマンドを使用します。

show radius dead-criteria host *ip-addr* [**auth-port** *auth-port*] [**acct-port** *acct-port*]

構文の説明

host *ip-addr*	設定されている RADIUS サーバの名前または IP アドレスを指定します。
auth-port *auth-port*	（任意）RADIUS サーバに対する認証ポートを指定します。 デフォルト値は 1645 です。
acct-port *acct-port*	（任意）RADIUS サーバに対するアカウンティング ポートを指定します。 デフォルト値は 1646 です。

コマンド デフォルト

時間と試行回数のデフォルト値は、1 つの値に固定されません。時間の場合は 10 ～ 60 秒、試行回数の場合は 10 ～ 100 回の範囲で算出されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show radius dead-criteria** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius dead-criteria host 12.26.49.12 auth-port 11000 acct-port
 11001

Server: 12.26.49.12/11000/11001
Dead criteria time: 10 sec (computed) tries: 10 (computed)
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 5：***show radius dead-criteria*** **フィールドの説明**

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート/アカウンティング要求の UDP 宛先ポートです。
Timeout	タイムアウトになるまでにルータがサーバホストの応答を待機する秒数です。
Retransmits	Cisco IOS XR ソフトウェアで RADIUS サーバホストのリストを検索する回数です。

関連コマンド

コマンド	説明
radius-server dead-criteria time, （50 ページ）	RADIUS サーバに dead マークを付けるための 1 つまたは両方の基準を強制的に使用します。
radius-server deadtime, （54 ページ）	RADIUS サーバに dead マークを付けたままにする時間を分単位で定義します。

show radius server-groups

システムに設定されている RADIUS サーバ グループの情報を表示するには、EXEC モードで **show radius server-groups** コマンドを使用します。

show radius server-groups [*group-name* **[detail]**]

構文の説明

group-name	（任意）サーバ グループの名前です。プロパティが表示されます。
detail	（任意）すべてのサーバ グループのプロパティを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show radius server-groups コマンドを使用して、グループ名、グループ内のサーバ数、名前付きサーバ グループ内のサーバのリストなど、設定されている各 RADIUS サーバ グループの情報を表示します。 設定されているすべての RADIUS サーバのグローバル リストも、認証およびアカウンティングのポート番号と一緒に表示されます。

タスク ID

タスク ID	操作
aaa	read

例

このグループに対してグループ レベルのデッドタイムが定義されていない場合、継承されるグローバルメッセージが表示されます。グループ レベルのデッドタイム値が定義されている場合はその値が表示され、このメッセージは省略されます。 次に、**show radius server-groups** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius server-groups

Global list of servers
  Contains 2 server(s)
    Server 1.1.1.1/1645/1646
    Server 2.2.2.2/1645/1646

Server group 'radgrp1' has 2 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 2 server(s)
    Server 1.1.1.1/1645/1646
    Server 2.2.2.2/1645/1646

Server group 'radgrp-priv' has 1 server(s)
  Dead time: 0 minute(s) (inherited from global)
  Contains 1 server(s)
    Server 3.3.3.3/1645/1646 [private]
```

次に、グループ「radgrp1」に含まれるすべてのサーバ グループのプロパティの出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius server-groups radgrp1 detail

Server group 'radgrp1' has 2 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 2 server(s)
      Server 1.1.1.1/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
      Server 2.2.2.2/1645/1646
    Authentication:
      0 requests, 0 pending, 0 retransmits
      0 accepts, 0 rejects, 0 challenges
      0 timeouts, 0 bad responses, 0 bad authenticators
      0 unknown types, 0 dropped, 0 ms latest rtt
    Accounting:
      0 requests, 0 pending, 0 retransmits
      0 responses, 0 timeouts, 0 bad responses
      0 bad authenticators, 0 unknown types, 0 dropped
      0 ms latest rtt
```

次に、グループ「raddgrp-priv」に含まれるすべてのサーバ グループのプロパティの詳細な出力例を示します。

```
RP/0/RSP0/CPU0:router# show radius server-groups radgrp-priv detail

Server group 'radgrp-priv' has 1 server(s)
    VRF default (id 0x60000000)
    Dead time: 0 minute(s) (inherited from global)
    Contains 1 server(s)
      Server 3.3.3.3/1645/1646 [private]
```

```
Authentication:
  0 requests, 0 pending, 0 retransmits
  0 accepts, 0 rejects, 0 challenges
  0 timeouts, 0 bad responses, 0 bad authenticators
  0 unknown types, 0 dropped, 0 ms latest rtt
Accounting:
  0 requests, 0 pending, 0 retransmits
  0 responses, 0 timeouts, 0 bad responses
  0 bad authenticators, 0 unknown types, 0 dropped
  0 ms latest rtt
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *6*：*show radius server-groups* フィールドの説明

フィールド	説明
Server	サーバの IP アドレス/認証要求の UDP 宛先ポート/アカウンティング要求の UDP 宛先ポートです。

関連コマンド

コマンド	説明
vrf（RADIUS）, （141 ページ）	AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VRF; VPN ルーティングおよび転送）参照情報を設定します。

show tacacs

システムに設定されている TACACS+ サーバの情報を表示するには、EXEC モードで **show tacacs** コマンドを使用します。

show tacacs

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show tacacs コマンドを使用して、設定されている各 TACACS+ サーバの統計情報を表示します。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show tacacs** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show tacacs

Server:1.1.1.1/21212 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

Server:2.2.2.2/21232 opens=0 closes=0 aborts=0 errors=0
```

```
        packets in=0 packets out=0
        status=up single-connect=false
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *7* : ***show tacacs*** フィールドの説明

フィールド	説明
Server	サーバの IP アドレス。
opens	外部サーバに対して開くソケットの数です。
closes	外部サーバに対して閉じるソケットの数です。
aborts	途中で中断された TACACS+ 要求の数です。
errors	外部サーバからのエラー応答の数です。
packets in	外部サーバから受信した TCP パケットの数です。
packets out	外部サーバに送信された TCP パケットの数です。

show tacacs server-groups

システムに設定されている TACACS+ サーバ グループの情報を表示するには、EXEC モードで **show tacacs server-groups** コマンドを使用します。

show tacacs server-groups

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show tacacs server-groups コマンドを使用して、グループ名、グループ内のサーバ数、名前付きサーバ グループ内のサーバのリストなど、設定されている各 TACACS+ サーバ グループの情報を表示します。 設定されているすべての TACACS+ サーバのグローバル リストも表示されます。

タスク ID

タスク ID	操作
aaa	read

例

次に、**show tacacs server-groups** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show tacacs server-groups

Global list of servers
  Server 12.26.25.61/23456
  Server 12.26.49.12/12345
```

```
  Server 12.26.49.12/9000
  Server 12.26.25.61/23432
  Server 5.5.5.5/23456
  Server 1.1.1.1/49
Server group 'tac100' has 1 servers
Server 12.26.49.12
```

次の表に、この出力で表示される重要なフィールドの説明を示します。

表 *8*：***show tacacs server-groups*** フィールドの説明

フィールド	説明
Server	サーバの IP アドレス。

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

show user

現在ログインしているユーザに関連付けられているすべてのユーザ グループとタスク ID を表示するには、EXEC モードで **show user** コマンドを使用します。

show user [**all**| **authentication**| **group**| **tasks**]

構文の説明

all	（任意）現在ログインしているユーザに関するすべてのユーザ グループとタスク ID を表示します。
authentication	（任意）現在ログインしているユーザの認証方式パラメータを表示します。
group	（任意）現在ログインしているユーザに関連付けられているユーザ グループを表示します。
tasks	（任意）現在ログインしているユーザに関連付けられているタスク ID を表示します。 **tasks** キーワードを使用した出力例では、予約済みのタスクが示されています。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

show user コマンドを使用して、現在ログインしているユーザに関連付けられているすべてのユーザ グループとタスク ID を表示します。

タスク ID

タスク ID	操作
none	—

例

次に、**show user** コマンドの認証方式パラメータの出力例を示します。

```
RP/0/RSP0/CPU0:router# show user authentication

local
```

次に、**show user** コマンドのグループの出力例を示します。

```
RP/0/RSP0/CPU0:router# show user group

root-system
```

次に、**show user** コマンドのグループとタスクに関するすべての情報の出力例を示します。

```
RP/0/RSP0/CPU0:router# show user all
Username: lab
Groups: root-system
Authenticated using method local
User lab has the following Task ID(s):

Task:                 aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                 aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                 acl  : READ    WRITE    EXECUTE    DEBUG
Task:                 admin  : READ    WRITE    EXECUTE    DEBUG
Task:                 atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                 bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                 bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                boot  : READ    WRITE    EXECUTE    DEBUG
Task:              bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                 cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                 cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:               drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:             pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                  ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                  qos  : READ    WRITE    EXECUTE    DEBUG
Task:                  rib  : READ    WRITE    EXECUTE    DEBUG
Task:                  rip  : READ    WRITE    EXECUTE    DEBUG
Task:              root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:          root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                  sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                 snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、**show user** コマンドのタスクの一覧とどのタスクが予約されているかの出力例を示します。

```
RP/0/RSP0/CPU0:router# show user tasks

Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  aaa  : READ    WRITE    EXECUTE    DEBUG
Task:                  acl  : READ    WRITE    EXECUTE    DEBUG
Task:                 admin  : READ    WRITE    EXECUTE    DEBUG
Task:                  atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:               drivers  : READ    WRITE    EXECUTE    DEBUG
Task:                eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:            fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:           filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:             firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                   fr  : READ    WRITE    EXECUTE    DEBUG
Task:                 hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:            interface  : READ    WRITE    EXECUTE    DEBUG
Task:            inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                 ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                 isis  : READ    WRITE    EXECUTE    DEBUG
Task:              logging  : READ    WRITE    EXECUTE    DEBUG
Task:                 lpts  : READ    WRITE    EXECUTE    DEBUG
Task:              monitor  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:              mpls-static  : READ    WRITE    EXECUTE    DEBUG
```

```
Task:              mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:              multicast  : READ    WRITE    EXECUTE    DEBUG
Task:              netflow  : READ    WRITE    EXECUTE    DEBUG
Task:              network  : READ    WRITE    EXECUTE    DEBUG
Task:                 ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                 ouni  : READ    WRITE    EXECUTE    DEBUG
Task:            pkg-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:                 ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                 qos  : READ    WRITE    EXECUTE    DEBUG
Task:                 rib  : READ    WRITE    EXECUTE    DEBUG
Task:                 rip  : READ    WRITE    EXECUTE    DEBUG
Task:             root-lr  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:          root-system  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:            route-map  : READ    WRITE    EXECUTE    DEBUG
Task:         route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                 sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                snmp  : READ    WRITE    EXECUTE    DEBUG
Task:            sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:               static  : READ    WRITE    EXECUTE    DEBUG
Task:               sysmgr  : READ    WRITE    EXECUTE    DEBUG
Task:               system  : READ    WRITE    EXECUTE    DEBUG
Task:            transport  : READ    WRITE    EXECUTE    DEBUG
Task:           tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:               tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:            universal  : READ    WRITE    EXECUTE    DEBUG (reserved)
Task:                 vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                 vrrp  : READ    WRITE    EXECUTE    DEBUG
```

関連コマンド

コマンド	説明
show aaa, （85 ページ）	選択されているユーザ グループ、ローカル ユーザ、またはタスク グループに関するタスク マップを表示します。

single-connection

単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信するには、TACACS ホスト コンフィギュレーション モードで **single-connection** コマンドを使用します。 別個の接続を使用するすべての新しいセッションに対して単一の TCP 接続をディセーブルにするには、このコマンドの **no** 形式を使用します。

single-connection

no single-connection

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

デフォルトでは、セッションごとに別個の接続が使用されます。

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

single-connection コマンドを使用すると、複数の TCP 接続を使用してサーバに要求が送信された場合に可能な数よりも、多くの TACACS 操作を TACACS+ サーバで処理することができます。

この機能をイネーブルにするには、使用されている TACACS+ サーバが単一接続モードをサポートしている必要があります。それ以外の場合はネットワーク アクセス サーバと TACACS+ サーバ間の接続がロックアップするか、非認証のエラーが発生します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、TACACS+ サーバ（IP アドレス 209.165.200.226）との単一の TCP 接続を設定し、すべての認証、許可、アカウンティング要求でこのTCP接続が使用されるようにする例を示します。 この設定は、TACACS+ サーバも単一接続モードで設定されている場合に限り機能します。 TACACS+ サーバを単一接続モードで設定する方法については、各サーバのマニュアルを参照してください。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# single-connection
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

tacacs-server host

TACACS+ホストサーバを指定するには、グローバルコンフィギュレーションモードで**tacacs-server host**コマンドを使用します。 指定された名前またはアドレスを削除するには、このコマンドの**no**形式を使用します。

tacacs-server host host-name [**port port-number**] [**timeout seconds**] [**key** [**0**| **7**] **auth-key**] **[single-connection]**

no tacacs-server host *host-name* [*port port-number*]

構文の説明

host-name	TACACS+ サーバのホスト名またはドメイン名または IP アドレス。
port *port-number*	（任意）サーバのポート番号を指定します。 この設定によって、デフォルトのポート 49 は上書きされます。 有効なポート番号の範囲は 1 ～ 65535 です。
timeout *seconds*	（任意）認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。 この設定によって、**acacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。 有効なタイムアウトの範囲は、1 ～ 1000 秒です。 デフォルトは 5 です。
key [**0** | **7**] *auth-key*	（任意）AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。 TACACS+ パケットは、このキーを使って暗号化されます。 このキーはTACACS+デーモンで使用されるキーと一致する必要があります。 このキーを指定すると、このサーバに限り、**tacacs-server key** コマンドで設定されているキーが上書きされます。 （任意）**0** の入力により、暗号化されていない（クリアテキスト）キーが続くことを指定します。 （任意）**7** の入力により、暗号キーが続くことを指定します。 *auth-key* 引数は、AAA サーバと TACACS+ サーバ間の暗号化されていないキーを指定します。
single-connection	（任意）単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信します。 デフォルトでは、セッションごとに別個の接続が使用されます。

コマンド デフォルト

TACACS+ ホストは指定されません。

port-name 引数が指定されていない場合、標準ポート 49 がデフォルトで使用されます。
seconds 引数が指定されていない場合、5 秒がデフォルトで使用されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

key キーワードには文字列（改行のないテキスト）ではなく行（改行付きのテキスト）が使用されるため、このキーワードは最後に入力する必要があります。 ユーザが Enter キーを押すまでのテキストと改行は、キーの一部として使用されます。

複数の **tacacs-server host** コマンドを使用して、追加のホストを指定できます。 Cisco IOS XR ソフトウェアでは、指定の順序でホストが検索されます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、IP アドレス 209.165.200.226 の TACACS+ ホストを指定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)#
```

次に、**show run** コマンドによって、**tacacs-server host** コマンドのデフォルト値を表示する例を示します。

```
RP/0/RSP0/CPU0:router# show run

Building configuration...
!! Last configuration change at 13:51:56 UTC Mon Nov 14 2005 by lab
!
tacacs-server host 209.165.200.226 port 49
 timeout 5
!
```

次に、ルータがポート番号 51 の TACACS+ サーバ ホスト host1 を参照するように指定する例を示します。 この接続における要求のタイムアウト値は 30 秒で、暗号キーは a_secret です。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host host1 port 51 timeout 30 key a_secret
```

関連コマンド

コマンド	説明
key（TACACS+），（43 ページ）	AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。
single-connection,（112 ページ）	単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信します。
tacacs-server key,（117 ページ）	ルータと TACACS+ デーモン間のすべての TACACS+通信に使用される認証および暗号キーをグローバルに設定します。
tacacs-server timeout,（119 ページ）	ルータがサーバホストの応答を待機する間隔をグローバルに設定します。
timeout（TACACS+），（129 ページ）	認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。

tacacs-server key

ルータと TACACS+ デーモン間のすべての TACACS+ 通信に対して認証および暗号キーを設定するには、グローバル コンフィギュレーション モードで **tacacs-server key** コマンドを使用します。キーをディセーブルにするには、このコマンドの **no** 形式を使用します。

tacacs-server key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

no tacacs-server key {**0** *clear-text-key*| **7** *encrypted-key*| *auth-key*}

構文の説明

0 *clear-text-key*	暗号化されていない（クリアテキスト）共有キーを指定します。
7 *encrypted-key*	暗号化共有キーを指定します。
auth-key	AAA サーバと TACACS+ サーバ間の暗号化されていないキーを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

入力するキー名は、TACACS+ デーモンで使用するキーと一致する必要があります。 キー名は、個別にキーが指定されていないすべてのサーバに適用されます。 すべての先頭のスペースは無視されますが、キーの中と後続のスペースは使用されます。 キーにスペースを使用する場合、引用符をキーに含める場合を除き、引用符でキーを囲まないでください。

キー名は、次のガイドラインに沿っている場合に限り有効です。

- *clear-text-key* 引数のあとに **0** キーワードを指定する必要があります。

- *encrypted-key* 引数のあとに **7** キーワードを指定する必要があります。

TACACS サーバ キーは、個々の TACACS サーバにキーが設定されていない場合に限り使用されます。 個々のTACACSサーバにキーを設定すると、このグローバルなキー設定は常に上書きされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、認証および暗号キーを key1 に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server key key1
```

関連コマンド

コマンド	説明
key（TACACS+）, （43 ページ）	AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

tacacs-server timeout

サーバがサーバホストの応答を待機する間隔を設定するには、グローバルコンフィギュレーション モードで **tacacs-server timeout** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

構文の説明

seconds	タイムアウトの間隔（秒単位）を指定する 1 ～ 1000 の整数です。

コマンド デフォルト

5 秒

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

この TACACS+ サーバのタイムアウトは、個々の TACACS+ サーバにタイムアウトが設定されていない場合に限り使用されます。 個々の TACACS+ サーバにタイムアウトの間隔が設定されている場合は常に、このグローバルなタイムアウト設定が上書きされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、インターバル タイマーを 10 秒に変更する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server timeout 10
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

tacacs source-interface

すべての発信 TACACS+ パケットに対して選択したインターフェイスの送信元 IP アドレスを指定するには、グローバル コンフィギュレーション モードで **tacacs source-interface** コマンドを使用します。 指定したインターフェイス IP アドレスをディセーブルにするには、このコマンドの **no** 形式を使用します。

tacacs source-interface *type path-id* [**vrf** *vrf-id*]

no tacacs source-interface *type path-id*

構文の説明

type	インターフェイス タイプ。 詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
path-id	物理インターフェイスまたは仮想インターフェイス。 （注） EXEC モードで **show interfaces** コマンドを使用して、現在ルータに設定されているすべてのインターフェイスのリストを表示します。 ルータ構文の詳細については、疑問符（**?**）を使用してオンライン ヘルプを参照してください。
vrf *vrf-id*	割り当てられている VRF の名前を指定します。

コマンド デフォルト

特定のソース インターフェイスが設定されていない場合、インターフェイスがダウン状態にある場合、またはインターフェイスに IP アドレスが設定されていない場合は、IP アドレスが自動的に選択されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。
リリース 4.1.0	**vrf** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

radius source-interface コマンドを使用して、すべての発信 TACACS+ パケットに対して指定するインターフェイスの IP アドレスを設定します。 インターフェイスがアップ状態である限り、このアドレスが使用されます。 このように、TACACS+ サーバでは IP アドレスのリストを保持する代わりに、ネットワーク アクセス クライアントに関連付けられた 1 つの IP アドレス エントリを使用できます。

特に、ルータに多数のインターフェイスがあり、特定のルータからのすべての TACACS+ パケットに同一の IP アドレスが含まれるようにする場合は、このコマンドが役立ちます。

指定したインターフェイスに IP アドレスが設定されていないか、そのインターフェイスがダウン状態にある場合、TACACS+ は、送信元インターフェイスの設定が使用されないものとして処理します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、すべての発信 TACACS+ パケットに指定するインターフェイスの IP アドレスを設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# tacacs source-interface GigabitEthernet 0/0/0/29 vrf abc
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種のサーバ ホストを別個のリストと別個の方式にグループ化します。

task

タスク ID をタスク グループに追加するには、タスク グループ コンフィギュレーション モードで **task** コマンドを使用します。 タスク グループからタスク ID を削除するには、このコマンドの **no** 形式を使用します。

task {**read**| **write**| **execute**| **debug**} *taskid-name*

no task {**read**| **write**| **execute**| **debug**} *taskid-name*

構文の説明

read	名前付きタスク ID に対して読み取り専用特権をイネーブルにします。
write	名前付きタスク ID に対して書き込み特権をイネーブルにします。「write」という用語には read の意も含まれます。
execute	名前付きタスク ID に対して実行特権をイネーブルにします。
debug	名前付きタスク ID に対してデバッグ特権をイネーブルにします。
taskid-name	タスク ID の名前です。

コマンド デフォルト

新しく作成したタスク グループには、タスク ID は割り当てられません。

コマンド モード

タスク グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク グループ コンフィギュレーション モードで **task** コマンドを使用します。 タスク グローバル コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードで **taskgroup** コマンドを使用します。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、config-services タスク ID に対して実行特権をイネーブルにし、そのタスク ID をタスク グループ taskgroup1 に関連付ける例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup taskgroup1
RP/0/RSP0/CPU0:router(config-tg)# task execute config-services
```

関連コマンド

コマンド	説明
taskgroup, （125 ページ）	一連のタスク ID に関連付けるように、タスク グループを設定します。

taskgroup

タスク グループを一連のタスク ID に関連付けるように設定するには、また、タスク グローバル コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **taskgroup** コマンドを使用します。 タスク 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。

taskgroup *taskgroup-name* [**description** *string*| **task** {**read**| **write**| **execute**| **debug**} *taskid-name*| **inherit taskgroup** *taskgroup-name*]

no taskgroup *taskgroup-name*

構文の説明

taskgroup-name	特定のタスク グループの名前です。
description	（任意）名前付きタスク グループの説明を作成できます。
string	（任意）タスク グループの説明に使用する文字列です。
task	（任意）タスク ID が名前付きタスク グループに関連付けられることを指定します。
read	（任意）名前付きタスク ID で読み取りアクセスだけが許可されることを指定します。
write	（任意）名前付きタスク ID で読み取りおよび書き込みアクセスだけが許可されることを指定します。
execute	（任意）名前付きタスク ID で実行アクセスが許可されることを指定します。
debug	（任意）名前付きタスク ID でデバッグ アクセスだけが許可されることを指定します。
taskid-name	（任意）タスクの名前：タスク ID です。
inherit taskgroup	（任意）名前付きタスク グループからアクセス許可をコピーします。
taskgroup-name	（任意）アクセス許可を継承する元のタスク グループの名前です。

コマンド デフォルト

デフォルトでは、事前定義された 5 つのユーザ グループが使用可能になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク グループには、アクション タイプごとに一連のタスク ID が設定されます。 システムでまだ参照されているタスク グループを削除すると、警告が表示され、削除は拒否されます。

グローバル コンフィギュレーション モードから、設定されているすべてのタスク グループを表示できます。 ただし、タスク グループ コンフィギュレーション モードでは、設定されているすべてのタスク グループを表示できるとは限りません。

キーワードや引数なしで **taskgroup** コマンドを入力すると、タスク グループ コンフィギュレーション モードが開始されます。このモードでは、**description**、**inherit**、**show**、および **task** の各コマンドを使用できます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、BGP 読み取りアクセス権をタスク グループ alpha に割り当てる例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# taskgroup alpha
RP/0/RSP0/CPU0:router(config-tg)# task read bgp
```

関連コマンド

コマンド	説明
description（AAA）, （33 ページ）	タスク コンフィギュレーション モードでタスク グループの説明を作成します。
task, （123 ページ）	タスク ID をタスク グループに追加します。

timeout（RADIUS）

ルータが RADIUS サーバの応答を待機し、再送信するまでの秒数を指定するには、RADIUS サーバグループ プライベート コンフィギュレーション モードで **timeout** コマンドを使用します。 このコマンドをディセーブルにして、デフォルトのタイムアウト値の 5 秒に戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout *seconds*

構文の説明

seconds	タイムアウト値（秒単位）です。 範囲は 1 ～ 1000 です。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。

コマンド デフォルト

seconds：5

コマンド モード

RADIUS サーバグループ プライベート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タイムアウト値の秒数を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RSP0/CPU0:router(config-sg-radius-private)# timeout 500
```

関連コマンド

コマンド	説明
radius-server timeout, （64 ページ）	タイムアウトになるまでにルータがサーバホストの応答を待機する間隔を設定します。
retransmit（RADIUS）, （68 ページ）	サーバが応答しない、または応答が遅い場合に、RADIUS 要求を再送信する回数を指定します。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

timeout（TACACS+）

認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定するには、TACACS ホスト コンフィギュレーション モードで **timeout**（TACACS+）コマンドを使用します。 このコマンドをディセーブルにして、デフォルトのタイムアウト値の 5 秒に戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout *seconds*

構文の説明

seconds	タイムアウト値（秒単位）です。 範囲は 1 ～ 1000 です。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。

コマンド デフォルト

seconds：5

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

timeout（TACACS+）コマンドによって、**tacacs-server timeout** コマンドで設定されたグローバルのタイムアウト値が、このサーバに限り上書きされます。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、タイムアウト値の秒数を設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RSP0/CPU0:router(config-tacacs-host)# timeout 500
```

関連コマンド

コマンド	説明
tacacs-server host, （114 ページ）	TACACS+ ホストを指定します。

timeout login response

サーバがログインに対する応答を待機する間隔を設定するには、回線テンプレート コンフィギュレーション モードで **timeout login response** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

timeout login response *seconds*

no timeout login response *seconds*

構文の説明

seconds	タイムアウトの間隔（秒単位）を指定する 0 ～ 300 の整数です。

コマンド デフォルト

seconds：30

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

回線テンプレート コンフィギュレーション モードで **timeout login response** コマンドを使用して、タイムアウト値を設定します。 このタイムアウト値は、入力した回線テンプレートが適用されるすべての端末回線に適用されます。 このタイムアウト値は、コンソール回線にも適用できます。 タイムアウト値の時間が経過すると、ユーザに再びプロンプトが表示されます。 再試行は 3 回まで可能です。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、インターバル タイマーを 20 秒に変更する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# line template alpha
RP/0/RSP0/CPU0:router(config-line)# timeout login response 20
```

関連コマンド

コマンド	説明
login authentication, （45 ページ）	ログインに対する AAA 認証をイネーブルにします。

usergroup

ユーザ グループを設定し、そのグループを一連のタスク グループに関連付けるには、また、ユーザ グループ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **usergroup** コマンドを使用します。 ユーザ グループを削除するには、またはタスク グループと指定されたユーザ グループとの関連付けを削除するには、このコマンドの **no** 形式を使用します。

usergroup *usergroup-name*

no usergroup *usergroup-name*

構文の説明

usergroup-name	ユーザ グループの名前です。 *usergroup-name* 引数には 1 つの単語だけ使用できます。 スペースと引用符は使用できません。

コマンド デフォルト

デフォルトでは、事前定義された 5 つのユーザ グループが使用可能になります。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ユーザ グループは、タスク グループなど一連のユーザに対するコマンド パラメータによって設定されます。 特定のユーザ グループを削除するには、**usergroup** コマンドの **no** 形式を使用します。 ユーザ グループ自体を削除するには、このコマンドをパラメータなしの **no** 形式で実行します。 システムでまだ参照されているユーザ グループを削除すると、警告が表示され、削除は拒否されます。

別のユーザ グループからアクセス権をコピーするには、inherit usergroup, （39 ページ） コマンドを使用します。 ユーザ グループは親グループに継承され、これらのグループに指定されているすべてのタスク ID の集合を形成します。 循環インクルードは検出され、拒否されます。 ユーザ グ

ループは、root-system や owner-sdr などの事前定義されたグループのプロパティを継承できません。

グローバル コンフィギュレーション モードから、設定されているすべてのユーザ グループを表示できます。 ただし、ユーザグループ コンフィギュレーション モードでは、設定されているすべてのユーザ グループを表示できるとは限りません。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、ユーザ グループ beta からユーザ グループ alpha にアクセス権を追加する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# usergroup alpha
RP/0/RSP0/CPU0:router(config-ug)# inherit usergroup beta
```

関連コマンド

コマンド	説明
description（AAA）, （33 ページ）	設定時にタスク グループの説明を作成します。
inherit usergroup, （39 ページ）	ユーザ グループが別のユーザ グループからアクセス権を取得できるようにします。
taskgroup, （125 ページ）	一連のタスク ID に関連付けるように、タスク グループを設定します。

username

新しいユーザにユーザ名とパスワードを設定し、そのユーザに対してアクセス権を付与するには、また、ユーザ名コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードまたは管理コンフィギュレーション モードで **username** コマンドを使用します。データベースからユーザを削除するには、このコマンドの **no** 形式を使用します。

username *user-name* [**password** {**[0]| 7**} *password*| **secret** {**[0]| 5**} *password*| **group** *usergroup-name*]

no username *user-name* [**password** {**0| 7**} *password*| **secret** {**0| 5**} *password*| **group** *usergroup-name*]

構文の説明

user-name	ユーザ名。 *user-name* 引数に指定できるのは、1 つの単語だけです。 スペースと引用符は使用できません。
password	（任意）名前付きユーザにパスワードを作成できます。
0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。 シスコ独自の暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。
7	（任意）暗号化パスワードが続くことを指定します。
password	（任意）「*lab*」など、ログインするユーザが入力する暗号化されていないパスワードのテキストを指定します。 暗号化が設定されている場合、パスワードはユーザに表示されません。 最長で 253 文字まで入力できます。
secret	（任意）名前付きユーザに対して、MD5 で保護されたパスワードを作成できます。
0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。 MD5 暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。
5	（任意）暗号化パスワードが続くことを指定します。
group	（任意）名前付きユーザをユーザ グループに関連付けることができます。
usergroup-name	（任意）**usergroup** コマンドで定義されているとおりのユーザ グループの名前。

コマンド デフォルト

グローバルにユーザ名は定義されません。

管理コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

（注） 1 人のユーザが、単独のグループとしてシスコ サポート特権を持つことはできません。

username コマンドを使用して、ユーザを識別し、ユーザ名コンフィギュレーション モードを開始します。 パスワードとユーザ グループの割り当ては、グローバル コンフィギュレーション モードかユーザ名コンフィギュレーションサブモードのいずれかで実行できます。 アクセス権（タスク ID）を割り当てるには、定義されている 1 つまたは複数のユーザ グループにユーザを関連付けます。

グローバルコンフィギュレーションモードから、設定されているすべてのユーザ名を表示できます。 ただし、ユーザ名コンフィギュレーションモードでは、設定されているすべてのユーザ名を表示できるとは限りません。

各ユーザは、管理ドメイン内で一意のユーザ名によって識別されます。 各ユーザは、少なくとも 1 つのユーザ グループのメンバーであることが必要です。 ユーザ グループを削除すると、そのグループに関連付けられたユーザが孤立する場合があります。 AAA サーバでは孤立したユーザも認証されますが、ほとんどのコマンドは許可されません。

デフォルトでは、ローカル ログイン認証用に **username** コマンドが特定のユーザに関連付けられます。 また、TACACS+ ログイン認証用に TACACS+ サーバのデータベースにユーザとパスワードを設定することもできます。 詳細については、aaa authentication, （13 ページ） コマンドの説明を参照してください。

事前定義された root-system グループは、管理の設定時に root-system ユーザだけが指定できます。

（注） ローカル ネットワーキング デバイスをリモートのチャレンジ ハンドシェーク認証プロトコル（CHAP）の要求に応答できるようにするには、一方の **username** コマンド エントリを、他方のネットワーキング デバイスにすでに割り当てられているホスト名エントリと同一にする必要があります。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、グローバル コンフィギュレーション モードで **username** コマンドを実行したあとに使用できるコマンドの例を示します。

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# ?
```

clear	コミットされていない設定をクリアします。
commit	設定変更を実行コンフィギュレーションにコミットします。
describe	実際に処理を行わず、コマンドについて説明します。
do	exec コマンドを実行します。
exit	このサブモードを終了します。
group	このユーザがメンバであるユーザ グループです。
no	コマンドを無効にするか、またはデフォルト値を設定します。
password	このユーザのパスワードを指定します。
pwd	現在のサブモードを開始するために使用するコマンドです。
root	グローバル コンフィギュレーション モードに戻ります。
secret	このユーザの安全なパスワードを指定します。
show	設定内容を表示します。

```
RP/0/RSP0/CPU0:router(config-un)#
```

次に、グローバル コンフィギュレーション モードでユーザ名 *user1* にクリアテキスト パスワード *password1* を設定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# username user1
RP/0/RSP0/CPU0:router(config-un)# password 0 password1
```

次に、管理コンフィギュレーション モードでユーザ *user1* に MD5 で保護されたシークレットを設定する例を示します。

```
RP/0/RSP0/CPU0:P1(admin-config)# username user1
RP/0/RSP0/CPU0:P1(admin-config-un)# secret 0 lab
RP/0/RSP0/CPU0:P1(admin-config-un)# commit
RP/0/RSP0/CPU0:May  6 13:06:43.205 : config[65723]: %MGBL-CONFIG-6-DB_COMMIT_ADMIN :
Configuration committed by user 'cisco'. Use 'show configuration commit changes 2000000005'
 to view the changes.
RP/0/RSP0/CPU0:P1(admin-config-un)# exit
RP/0/RSP0/CPU0:P1(admin-config)# show run username
username user1 secret 5 $1$QB03$3H29k3ZT.0PMQ8GQQKXCF0
!
```

関連コマンド

コマンド	説明
aaa authentication, （13 ページ）	認証の方式リストを定義します。
group（AAA）, （35 ページ）	ユーザをグループに追加します。
password（AAA）, （47 ページ）	ユーザのログイン パスワードを作成します。
secret, （70 ページ）	ユーザに対してセキュア ログイン用のシークレットを作成します。

users group

ユーザ グループとその特権を回線に関連付けるには、回線テンプレート コンフィギュレーション モードで **users group** コマンドを使用します。 ユーザ グループと回線の関連付けを削除するには、このコマンドの **no** 形式を使用します。

users group {*usergroup-name*| **cisco-support**| **netadmin**| **operator**| **root-lr**| **root-system**| **sysadmin**}

no users group {*usergroup-name*| **cisco-support**| **netadmin**| **operator**| **root-lr**| **root-system**| **serviceadim**| **sysadmin**}

構文の説明

usergroup-name	ユーザ グループの名前です。 *usergroup-name* 引数には 1 つの単語だけ使用できます。 スペースと引用符は使用できません。
cisco-support	その回線を介してログインしているユーザにシスコ サポート担当者の特権を与えることを指定します。
netadmin	その回線を介してログインしているユーザにネットワーク管理者の特権を与えることを指定します。
operator	その回線を介してログインしているユーザにオペレータの特権を与えることを指定します。
root-lr	その回線を介してログインしているユーザにルート論理ルータ（LR）の特権を与えることを指定します。
root-system	その回線を介してログインしているユーザにルート システムの特権を与えることを指定します。
serviceadmin	その回線を介してログインしているユーザにサービス管理者グループの特権を与えることを指定します。
sysadmin	その回線を介してログインしているユーザにシステム管理者の特権を与えることを指定します。

コマンド デフォルト

なし

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

users group コマンドを使用して、ユーザ グループとその特権を回線に関連付けます。つまり、その回線にログインしているユーザには、特定のユーザ グループの特権が与えられます。

タスク ID

タスク ID	操作
aaa	read, write

例

次の例では、回線テンプレート *vty* を使って vty-pool が作成された場合、vty を介してログインしているユーザにオペレータの特権が与えられます。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa authen login vty-authen line
RP/0/RSP0/CPU0:router(config)# commit
RP/0/RSP0/CPU0:router(config)# line template vty
RP/0/RSP0/CPU0:router(config-line)# users group operator
RP/0/RSP0/CPU0:router(config-line)# login authentication
```

vrf（RADIUS）

AAA RADIUS サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照を設定するには、RADIUS サーバグループ コンフィギュレーション モードで **vrf** コマンドを使用します。 サーバ グループがグローバル（デフォルト）ルーティング テーブルを使用できるようにするには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf *vrf-name*

構文の説明

vrf-name	VRF に割り当てる名前です。

コマンド デフォルト

デフォルトの VRF が使用されます。

コマンド モード

RADIUS サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

vrf コマンドを使用して、AAA RADIUS サーバ グループに VRF を指定し、ダイヤルアップ ユーザが異なるルーティング ドメインの AAA サーバを使用できるようにします。

タスク ID

タスク ID	操作
aaa	read, write

例

次の例では、**vrf** コマンドの使用方法を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server radius group1
RP/0/RSP0/CPU0:router(config-sg-radius)# vrf wal-mart
```

関連コマンド

コマンド	説明
radius source-interface, （66 ページ）	RADIUS で、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスが使用されるようにします。
server-private（RADIUS）, （78 ページ）	グループ サーバに対するプライベート RADIUS サーバの IP アドレスを設定します。

vrf（TACACS+）

AAA TACACS+ サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照を設定するには、TACACS+ サーバグループ コンフィギュレーション モードで **vrf** コマンドを使用します。 サーバ グループがグローバル（デフォルト）ルーティング テーブルを使用できるようにするには、このコマンドの **no** 形式を使用します。

vrf *vrf-name*

no vrf *vrf-name*

構文の説明

vrf-name	VRF に割り当てる名前です。

コマンド デフォルト

デフォルトの VRF が使用されます。

コマンド モード

TACACS+ サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 4.1.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

vrf コマンドを使用して、AAA TACACS+ サーバ グループに VRF を指定し、ダイヤルアップ ユーザが異なるルーティング ドメインの AAA サーバを使用できるようにします。

タスク ID

タスク ID	操作
aaa	read, write

例

次に、**vrf** コマンドを使用する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# server 9.27.10.6
RP/0/RSP0/CPU0:router(config-sg-tacacs+)# vrf abc
```

関連コマンド

コマンド	説明
aaa group server tacacs+, （25 ページ）	各種の TACACS+ サーバ ホストを別個のリストと別個の方式にグループ化します。
server（TACACS+）, （76 ページ）	すべての発信 TACACS+ パケットに対して、選択したインターフェイスの発信元 IP アドレスを指定します。
server-private（TACACS+）, （82 ページ）	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。