



## 認証、許可、アカウントिंग コマンド

ここでは、認証、許可、アカウントिंग（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、『*System Security Configuration Guide for Cisco NCS 5000 Series Routers*』の「Configuring AAA Services」の章を参照してください。



(注)

現在、デフォルトの VRF のみがサポートされています。VPNv4、VPNv6、および VPN ルーティング/転送（VRF）アドレスファミリは、今後のリリースでサポートされます。

- [aaa accounting](#), 4 ページ
- [aaa accounting system default](#), 7 ページ
- [aaa accounting update](#), 9 ページ
- [aaa authentication \(XR-VM\)](#), 11 ページ
- [aaa authorization \(XR-VM\)](#), 14 ページ
- [aaa default-taskgroup](#), 17 ページ
- [aaa group server radius](#), 18 ページ
- [aaa group server tacacs+](#), 20 ページ
- [accounting \(回線\)](#), 22 ページ
- [authorization \(回線\)](#), 24 ページ
- [description \(AAA\)](#), 26 ページ
- [group \(AAA\)](#), 28 ページ
- [inherit taskgroup](#), 30 ページ
- [inherit usergroup](#), 32 ページ
- [key \(TACACS+\)](#), 34 ページ

- login authentication, 36 ページ
- password (AAA) , 38 ページ
- radius-server dead-criteria time, 40 ページ
- radius-server dead-criteria tries, 42 ページ
- radius-server deadtime (BNG) , 44 ページ
- radius-server key (BNG) , 46 ページ
- radius-server retransmit (BNG) , 48 ページ
- radius-server timeout (BNG) , 50 ページ
- radius source-interface (BNG) , 51 ページ
- secret, 53 ページ
- server (RADIUS) , 55 ページ
- server (TACACS+) , 57 ページ
- server-private (RADIUS) , 59 ページ
- server-private (TACACS+) , 62 ページ
- show aaa (XR-VM) , 64 ページ
- show aaa accounting, 70 ページ
- show radius, 72 ページ
- show radius accounting, 74 ページ
- show radius authentication, 76 ページ
- show radius dead-criteria, 78 ページ
- show radius server-groups, 80 ページ
- show tacacs, 83 ページ
- show tacacs server-groups, 85 ページ
- show user, 87 ページ
- show aaa user-group, 91 ページ
- show tech-support aaa , 92 ページ
- single-connection, 93 ページ
- tacacs-server host, 95 ページ
- tacacs-server key, 97 ページ
- tacacs-server timeout, 99 ページ
- tacacs-server ipv4, 100 ページ

- [tacacs source-interface, 103 ページ](#)
- [task, 105 ページ](#)
- [taskgroup, 107 ページ](#)
- [timeout \(TACACS+\) , 109 ページ](#)
- [timeout login response, 111 ページ](#)
- [usergroup, 113 ページ](#)
- [username, 115 ページ](#)
- [users group, 119 ページ](#)

## aaa accounting

アカウントング用のメソッドリストを作成するには、XR EXEC モードで **aaa accounting** コマンドを使用します。リスト名をシステムから削除するには、このコマンドの **no** 形式を使用します。

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

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

### 構文の説明

<b>commands</b>	XR EXEC シェル コマンドのアカウントングをイネーブルにします。
<b>exec</b>	XR EXEC セッションのアカウントングをイネーブルにします。
<b>mobile</b>	モバイル IP 関連のアカウントング イベントをイネーブルにします。
<b>network</b>	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トングをイネーブルにします。
<b>system</b>	すべてのシステム関連イベントをイネーブルにします。
<b>event manager</b>	XR EXEC 用の許可リストを設定します。
<b>default</b>	このキーワードに続くアカウントングメソッドのリストをアカウントングサービスのデフォルトメソッドリストとして使用します。
<i>list-name</i>	アカウントングメソッドリストの名前の指定に使用する文字列です。
<b>start-stop</b>	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」通知がアカウント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。
<b>stop-only</b>	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。 注：これはシステムアカウントングではサポートされていません。
<b>none</b>	アカウントングを使用しません。

<i>method</i>	<p>AAA システムアカウント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。</p> <ul style="list-style-type: none"> <li>• <b>group tacacs+</b> : すべての TACACS+ サーバのリストをアカウントングに使用します。</li> <li>• <b>group radius</b> : すべての RADIUS サーバのリストをアカウントングに使用します。</li> <li>• <b>groupnamed-group</b> : <b>aaa group server tacacs+</b> コマンド、または <b>aaa group server radius</b> コマンドで定義されたアカウントング用の TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを使用します。</li> </ul>
---------------	---

**コマンド デフォルト** AAA アカウントングはディセーブルです。

**コマンド モード** XR EXEC モード

#### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

#### 使用上のガイドライン

**aaa accounting** コマンドを使用して、デフォルトまたは名前付きのメソッドリストを作成して特定のアカウントングメソッドを定義し、回線ごと、またはインターフェイスごとに使用できるようにします。メソッドリストには方式を 4 つまで指定できます。このリスト名を回線に適用し（コンソール、aux、または vty テンプレート）、その特定の回線のアカウントングをイネーブルにします。

Cisco IOS XR ソフトウェアは、アカウントングに 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ト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。

アカウントングメソッドリストには、アカウント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ト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。

最小アカウントングでは、**stop-only** キーワードを含めて、要求されたユーザプロセス後に「stop accounting」通知を送信します。さらに詳細なアカウントングでは、TACACS+ または RADIUS が要求されたプロセスの開始時に「start accounting」通知を送信し、プロセスの後に「stop

accounting」通知を送信するように **start-stop** キーワードを含めることができます。アカウントングレコードは TACACS+ または RADIUS サーバのみに格納されます。

要求されたユーザプロセスは、「start accounting」通知がアカウント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	動作
aaa	読み取り、書き込み

#### 例

次に、デフォルトの `commands` アカウントングメソッド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トングサービスが提供されます。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa accounting commands default stop-only group tacacs+
```

## aaa accounting system default

認証、許可、およびアカウントिंग（AAA）システムアカウントングをイネーブルにするには、XR 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。システムアカウント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

<b>start-stop</b>	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。
<b>stop-only</b>	システムシャットダウンまたはリロード時に「stop accounting」通知を送信しません。
<b>none</b>	アカウントングを使用しません。
<b>method</b>	AAAシステムアカウント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。 <ul style="list-style-type: none"> <li>• <b>group tacacs+</b> : すべての TACACS+ サーバのリストをアカウントングに使用します。</li> <li>• <b>group radius</b> : すべての RADIUS サーバのリストをアカウントングに使用します。</li> <li>• <b>groupnamed-group</b> : <b>aaa group server tacacs+</b> コマンド、または <b>aaa group server radius</b> コマンドで定義されたアカウントング用の TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを使用します。</li> </ul>

### コマンドデフォルト

AAA アカウントングはディセーブルです。

### コマンドモード

XR 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 6.0	このコマンドが導入されました。

**使用上のガイドライン** システムアカウントリングには、名前付きアカウントリ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。

デフォルトのメソッドリストが、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せん。デフォルトのメソッドリストが定義されていない場合、アカウントリングは実行されません。

メソッドリストには方式を4つまで指定できます。

タスク ID	タスク ID	動作
	aaa	読み取り、書き込み

**例** 次に、ルータが最初に起動したときに「start accounting」通知を TACACS+ サーバに送信す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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# aaa accounting system default start-stop group tacacs+
```



## aaa accounting update

中間アカウントングレコードがアカウントングサーバに定期的送信されるようにするには、XR 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。中間アカウントングの更新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

<b>newinfo</b>	(任意) 当該のユーザに関して報告する新しいアカウントング情報があるときは常に、中間アカウントングレコードをアカウントングサーバに送信します。
<b>periodicminutes</b>	(任意) <i>minutes</i> 引数 (分数を指定する整数) で設定したとおりに中間アカウントングレコードを定期的アカウントングサーバに送信します。範囲は、1 ~ 35791394 分です。

### コマンド デフォルト

AAA のアカウント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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**newinfo** キーワードを使用した場合は、レポートする新しいアカウントング情報が発生するたびに、中間アカウントングレコードがアカウント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。中間アカウントングレコードには、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** キーワードと一緒に使用した場合、中間アカウントングレコードは *minutes* 引数で定義したとおりに定期的送信されます。中間アカウントングレコードには、アカウント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トング情報が含まれます。

**newinfo** キーワードと **periodic** キーワードを一緒に使用すると、中間アカウントングレコードは、レポートする新しいアカウントング情報が発生するたびにアカウントングサーバに送信され、また、*minutes* 引数で定義されたとおりにアカウントングレコードがアカウントングサーバに定期的送信されます。たとえば、**aaa accounting update** コマンドと **newinfo** キーワードおよび **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は中間アカウントングレコードを定期的に生成し続け、新たにログインしたユーザは **newinfo** アルゴリズムに基づいてアカウントングレコードを生成します。



注意

**aaa accounting update** コマンドと **periodic** キーワードを使用すると、多くのユーザがネットワークにログインしている場合は大きな輻輳が発生する可能性があります。

**periodic** キーワードと **newinfo** キーワードの両方を一緒に使用することはできません。一度に設定できるのはいずれか1つのキーワードのみです。

---

**タスク ID**


---

**タスク ID**


---

**動作**

aaa

読み取り、書き込み

---

**例**

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa accounting update periodic 30
```

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

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa accounting update newinfo
```

## aaa authentication (XR-VM)

認証用のメソッドリストを作成するには、XR コンフィギュレーション モードまたはシステム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*} *method-list*

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

### 構文の説明

<b>login</b>	ログインの認証を設定します。
<b>ppp</b>	ポイントツーポイント プロトコルの認証を設定します。
<b>default</b>	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 メソッドリストとして使用します。
<i>list-name</i>	認証メソッドリストの名前の指定に使用する文字列です。
<i>method-list</i>	AAA システム アカウントिंग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。 <ul style="list-style-type: none"> <li>• <b>group tacacs+</b> : 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メソッドリストを指定します。</li> <li>• <b>group radius</b> : 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メソッドリストを指定します。</li> <li>• <b>groupnamed-group</b> : <b>aaa group server tacacs+</b> コマンド、または <b>aaa group server radius</b> コマンドで定義された認証用の TACACS+サーバまたは RADIUS サーバの名前付きサブセットを使用するメソッドリストを指定します。</li> <li>• <b>local</b> : ローカル ユーザ名データベース方式を認証に使用するメソッド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。</li> <li>• <b>line</b> : 回線パスワードを認証に使用するメソッドリストを指定します。</li> </ul>

### コマンド デフォルト

デフォルトでは、すべてのポートにローカル認証が適用されます。

### コマンド モード

XR コンフィギュレーション モードまたは システム管理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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**aaa authentication** コマンドを使用して、一連の認証方式、つまりメソッドリストを作成します。メソッドリストには方式を4つまで指定できます。メソッドリストは、認証方式（TACACS+またはRADIUS）を順番に記述した名前付きのリストです。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。

別の名前付きメソッド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メソッド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** の形式は、以前に定義した一連の TACACS+ サーバまたは RADIUS サーバを参照します。
- **tacacs-server host** コマンドまたは **radius-server host** コマンドを使用して、ホストサーバを設定します。
- **aaa group server tacacs+** コマンドまたは **aaa group server radius** コマンドを使用して、サーバの名前付きサブセットを作成します。
- **login** キーワード、**local** オプション、および **group** オプションはシステム管理コンフィギュレーションモードでのみ使用できます。

## タスク ID

タスク ID	動作
aaa	読み取り、書き込み

## 例

次に、認証用のデフォルトのメソッドリストを指定し、さらに XR コンフィギュレーションモードで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/RP0/CPU0:router# configure
```

```
RP/0/RP0/CPU0:router(config)# aaa authentication login default group tacacs+
```

次に、認証用のリモートのメソッドリストを指定し、さらにシステム管理コンフィギュレーションモードで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/RP0/CPU0:router# admin  
sysadmin-vm:0_RP0# configure  
sysadmin-vm:0_RP0(config)# aaa authentication users user lab
```

```
RP/0/RP0/CPU0:router# admin  
sysadmin-vm:0_RP0# configure  
sysadmin-vm:0_RP0(config)# aaa authentication groups group aaa-r
```

## aaa authorization (XR-VM)

許可用のメソッドリストを作成するには、XR 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。機能の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

<b>commands</b>	すべての XR EXEC モードのシェル コマンドの許可を設定します。
<b>eventmanager</b>	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。
<b>exec</b>	インタラクティブ (XR EXEC モード) セッションの許可を設定します。
<b>network</b>	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。
<b>default</b>	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 メソッド リストとして使用します。
<i>list-name</i>	許可メソッド リストの名前の指定に使用する文字列です。
<b>none</b>	許可を使用しません。 <b>none</b> を指定した場合は、後続の認証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。
<b>local</b>	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。
<b>group tacacs+</b>	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。
<b>group radius</b>	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。
<b>group group-name</b>	<b>aaa group server tacacs+</b> コマンド、または <b>aaa group server radius</b> コマンドで定義された許可用の TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを使用します。

### コマンド モデル

XR-VM の **aaa authorization** (none キーワードの方式に等価) に対する許可をディセーブルにします。

## コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**aaa authorization** コマンドを使用して、回線ごとまたはインターフェイスごとに使用できる特定の許可方式を定義するメソッドリストを作成します。メソッドリストには方式を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。

許可メソッドリストによって、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。メソッドリストは、一連の許可方式 (TACACS+ など) を記述した名前付きリストです。メソッドリストを使用して、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 ソフトウェアではメソッド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認可が失敗した場合 (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)、認可プロセスは停止し、その他の認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** : ルータから認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認可は行われません。
- **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。
- **groupgroup-name** : 許可用の TACACS+ サーバまたは RADIUS サーバの名前付きのサブセットを使用します。

メソッドリストは、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。

- **Commands authorization** : ユーザが実行する XR EXEC モード コマンドに適用します。Command authorization は、すべての XR EXEC モードのコマンドに試行されます。



(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。

- XR EXEC モード **authorization** : XR EXEC モードセッションを開始するために許可を適用します。



(注) **exec** キーワードは障害マネージャ サービスの許可には使用されていません。障害マネージャ サービスを許可するには、**eventmanager** キーワード (障害マネージャ) を使用します。EXEC 許可には、**exec** キーワードを使用します。

- **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。

- **Event manager authorization** : 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。TACACS+ を使用することも、**locald** を使用することもできます。



(注) **eventmanager** キーワード (障害マネージャ) で**exec** キーワードを置換し、イベント マネージャ (障害マネージャ) を許可します。

名前付きメソッド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メソッドリストが定義されます。メソッド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メソッドリストを適用する必要があります。

タスク ID

タスク ID	動作
aaa	読み取り、書き込み

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メソッドリストを定義する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa authorization commands listname1 group tacacs+
```



## aaa default-taskgroup

リモート TACACS+ 認証と RADIUS 認証の両方にタスク グループを指定するには、XR 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。このデフォルトのタスク 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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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

### タスク ID

タスク ID	動作
aaa	読み取り、書き込み

### 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa default-taskgroup taskgroup1
```

## aaa group server radius

異なる RADIUS サーバホストを重複のないリストにグループ化するには、XR 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。グループサーバを設定リストから削除するには、このコマンドの **no** 形式を使用します。

**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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**aaa group serverradius** 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。これにより、設定済みのサーバホストのサブセットを選択して、それらのサーバを特定のサービスに使用することができます。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、各エントリが一意的 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 User Datagram Protocol (UDP) ポート番号を組み合わせることによって、異なるポートを特定の認証、許可、およびアカウントング (AAA) サービスを提供する RADIUS ホストとして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トング 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ト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	動作
aaa	読み取り、書き込み

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius radgroup1
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.0.0.5 auth-port 1700 acct-port 1701
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.0.0.10 auth-port 1702 acct-port 1703
RP/0/RP0/CPU0:router(config-sg-radius)# server 10.0.0.20 auth-port 1705 acct-port 1706
```



(注) **auth-port***port-number* キーワードと **acct-port***port-number* キーワードおよび引数を指定しない場合は、**auth-port** キーワードの *port-number* 引数は 1645 となり、**acct-port** キーワードの *port-number* 引数のデフォルト値は 1646 になります。





(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。 **tacacs-server host** コマンドを使用して、ホストサーバを設定します。

#### タスク ID

タスク ID	動作
aaa	読み取り、書き込み

#### 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ tacgroup1
RP/0/RP0/CPU0:router(config-sg-tacacs)# server 192.168.200.226
RP/0/RP0/CPU0:router(config-sg-tacacs)# server 192.168.200.227
RP/0/RP0/CPU0:router(config-sg-tacacs)# server 192.168.200.228
```

## accounting (回線)

認証、許可、およびアカウントिंग (AAA) サービスをイネーブルにするには、**accounting** コマンドを使用します。AAA アカウント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

<b>commands</b>	選択した回線で、すべての XR EXEC モードシェル コマンドのアカウントングをイネーブルにします。
<b>exec</b>	XR EXEC モードセッションをイネーブルにします。
<b>default</b>	<b>aaa accounting</b> コマンドを使用して作成したデフォルトのメソッドリストの名前。
<i>list-name</i>	使用するアカウントング メソッドリストの名前を指定します。このリストは <b>aaa accounting</b> コマンドを使用して作成されます。

### コマンド デフォルト

アカウント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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**aaa accounting** コマンドをイネーブルにし、特定のタイプのアカウントングに名前付きのアカウントングメソッドリストを定義 (またはデフォルトのリストを使用) した後に、定義したリストを実行するアカウントング サービスの適切な回線に適用する必要があります。**accounting** コマンドを使用して、指定したメソッドリストを選択した回線または回線のグループに適用します。このようにメソッド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トングが適用されません。

## タスク ID

## タスク ID

## 動作

aaa

読み取り、書き込み

## 例

次に、*configure* という回線テンプレートの *listname2* というアカウントングメソッドリストを使用してコマンドアカウントングサービスをイネーブルにする例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template configure
RP/0/RP0/CPU0:router(config-line)# accounting commands listname2
```

## authorization (回線)

特定の回線または回線のグループに認証、認可、およびアカウントング (AAA) 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**| **eventmanager**} {**default**| *list-name*}

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

### 構文の説明

<b>commands</b>	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。
<b>exec</b>	インタラクティブ XR EXEC モードセッションの許可をイネーブルにします。
<b>default</b>	<b>aaa authorization</b> コマンドを使用して作成したデフォルトのメソッドリストを適用します。
<b>eventmanager</b>	eventmanager 許可方式を設定します。この方式は Embedded Event Manager に使用されます。
<i>list-name</i>	使用する許可メソッド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。このリストは <b>aaa authorization</b> コマンドを使用して作成されます。

### 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**aaa authorization** コマンドを使用して、特定のタイプの許可に名前付きの許可メソッドリストを定義 (またはデフォルトのメソッドリストを使用) した後に、許可を実行する適切な回線に定義



した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、指定したメソッドリスト（または、指定しなかった場合はデフォルトのメソッドリスト）を選択した回線または回線のグループに適用します。

---

**タスク ID**

タスク ID	動作
aaa	読み取り、書き込み

---

---

**例**

次に、*configure* という回線テンプレートの *listname4* というメソッドリストを使用してコマンド許可をイネーブルにする例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template configure
RP/0/RP0/CPU0:router(config-line)# authorization commands listname4
```

## description (AAA)

タスクグループまたはユーザグループの説明を設定時に作成するには、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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

タスクグループまたはユーザグループのコンフィギュレーションサブモード内で **description** を使用し、タスクグループ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	動作
aaa	読み取り、書き込み

## 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/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# taskgroup alpha  
RP/0/RP0/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/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# usergroup alpha  
RP/0/RP0/CPU0:router(config-ug)# description this is a sample user group
```

## 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。ユーザを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。

```
group {cisco-support| maintenance| netadmin| operator| provisioning| retrieve| root-lr| serviceadmin|
sysadmin| group-name}
```

```
no group {cisco-support| maintenance| netadmin| operator| provisioning| retrieve| root-lr| serviceadmin|
sysadmin| group-name}
```

### 構文の説明

<b>cisco-support</b>	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。 (注) IOS XR 6.0 リリース以降、シスコ サポート グループはルートシステム グループと統合されています。これにより、ルートシステム グループに属していたユーザは、シスコ サポート グループに含まれているコマンドにもアクセスできます。
<b>maintenance</b>	事前に定義された SCAPA メンテナンス グループにユーザを追加します。
<b>netadmin</b>	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。
<b>operator</b>	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。
<b>provisioning</b>	事前に定義された SCAPA プロビジョニング グループにユーザを追加します。
<b>retrieve</b>	事前に定義された SCAPA 取得グループにユーザを追加します。
<b>root-lr</b>	事前定義された root-lr グループにユーザを追加します。root-lr 権限を持つユーザのみがこのオプションを使用できます。
<b>serviceadmin</b>	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。
<b>sysadmin</b>	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。
<i>group-name</i>	<b>usergroup</b> コマンドですでに定義されている名前付きのユーザ 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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

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、XR コンフィギュレーションモードで **username**, (115 ページ) コマンドを使用します。

システム管理コンフィギュレーションモードで **group** コマンドを使用した場合は、シスコサポートのキーワードだけを指定できます。

シスコサポートグループに関連付けられた特権はルートシステムグループにも含まれています。シスコサポートグループを設定に使用する必要はなくなりました。

## タスク ID

タスク ID	動作
aaa	読み取り、書き込み

## 例

次に、ユーザグループのオペレータを user1 というユーザに割り当てる例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# group operator
```

# inherit taskgroup

タスク グループが別のタスク グループから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**| **serviceadmin**}

## 構文の説明

<i>taskgroup-name</i>	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。
<b>netadmin</b>	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。
<b>operator</b>	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。
<b>sysadmin</b>	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。
<b>cisco-support</b>	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。
<b>root-lr</b>	root-lr タスク グループからアクセス許可を継承します。
<b>serviceadmin</b>	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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**inherit taskgroup** コマンドを使用して、1つのタスク 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	動作
	aaa	読み取り、書き込み

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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup tg1
RP/0/RP0/CPU0:router(config-tg)# inherit taskgroup tg2
RP/0/RP0/CPU0:router(config-tg)# end
```

# inherit usergroup

ユーザグループが別のユーザグループから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

<i>usergroup-name</i>	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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

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、1つの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 のタスクマップの集合になります。ユーザグループは事前に設定された `root-system users`、`root-sdr users`、`netadmin users` などのグループからプロパティは継承できません。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

## 動作

aaa

読み取り、書き込み

## 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/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# usergroup purchasing  
RP/0/RP0/CPU0:router(config-ug)# inherit usergroup sales
```

## 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化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

<i>0clear-text-key</i>	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。
<i>7encrypted-key</i>	暗号化共有キーを指定します。
<i>auth-key</i>	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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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+ デーモンで使用す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、このサーバに対して **tacacs-server key** コマンドで設定されたキーのみが上書きされます。

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

## 動作

aaa

読み取り、書き込み

## 例

次に、暗号キーを **anykey** に設定する例を示します。

```
RP/0/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226  
RP/0/RP0/CPU0:router(config-tacacs-host)# key anykey
```

# login authentication

ログインに対する認証、認可、およびアカウントिंग（AAA）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

<b>default</b>	<b>aaa authentication login</b> コマンドによって設定した AAA 認証方式のデフォルトリスト。
<i>list-name</i>	認証に使用するメソッドリストの名前です。 <b>aaa authentication login</b> コマンドを使用してこのリストを指定します。

## コマンド デフォルト

このコマンドでは、**aaa authentication login** コマンドで設定し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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**login authentication** コマンドは、AAA で使用する回線単位のコマンドであり、ログインを試行する AAA 認証方式のリストの名前を指定します。



### 注意

**aaa authentication login** コマンドで設定していない *list-name* 値を使用した場合は、設定が拒否されます。

**login authentication** コマンドの **no** 形式を入力すると、**default** キーワードを使用したコマンドの入力と同じ効果があります。

このコマンドを実行する前に、**aaa authentication login** 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	動作
aaa	読み取り、書き込み
tty-access	読み取り、書き込み

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template template1
RP/0/RP0/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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# line template template2
RP/0/RP0/CPU0:router(config-line)# login authentication list1
```

## 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

<b>0</b>	(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。
<b>7</b>	暗号化パスワードが続くことを指定します。
<i>password</i>	「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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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。

パスワードが保護されている回線で XR EXEC モード プロセスが開始されると、そのプロセスによってパスワードの入力が求められます。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** コマンドは、**0** オプションが使用されている場合は常に、クリアテキストのログインパスワードを暗号化された形式で表示します。

#### タスク ID

タスク ID	動作
aaa	読み取り、書き込み

#### 例

次に、暗号化されていないパスワード *pwd1* をユーザに確立する例を示します。**show** コマンドによる出力には、暗号化された形式でパスワードが表示されます。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/CPU0:router(config-un)# password 0 pwd1
RP/0/RP0/CPU0:router(config-un)# commit
RP/0/RP0/CPU0:router(config-un)# show running-config
Building configuration...
username user1
password 7 141B1309
```

## radius-server dead-criteria time

RADIUS サーバからの有効なパケットをルータが最後に受信してから、そのサーバを **dead** とマーキングするまでに経過させる必要がある最小時間を秒単位で指定するには、XR 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。設定されてい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

<i>seconds</i>	秒単位の時間です。範囲は、1～120 秒です。 <i>seconds</i> 引数を設定しない場合、この秒数はサーバのトランザクション レートに応じて 10～60 になります。  (注) 時間基準は、 <b>dead</b> 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

このコマンドを使用しない場合、この秒数はサーバのトランザクション レートに応じて 10～60 になります。

### コマンド モード

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドラ

(注) **radius-server deadtime** コマンドよりも前に **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。



## タスク ID

## タスク ID

## 動作

aaa

読み取り、書き込み

## 例

次に、**radius-server dead-criteria time** コマンドに対して RADIUS サーバが dead とマーキングされる **dead-criteria** 条件となる時間を設定する例を示します。

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# radius-server dead-criteria time 5
```

## radius-server dead-criteria tries

RADIUS サーバが **dead** とマーキングされるまでにルータで発生する連続タイムアウトの回数を指定するには、XR 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。設定されてい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

<i>tries</i>	1～100 のタイムアウト回数。 <i>tries</i> 引数を設定しない場合、連続タイムアウトの回数は、サーバのトランザクション レートと設定した再送信回数に応じて 10～100 になります。
(注)	試行基準は、 <b>dead</b> 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

このコマンドを使用しない場合、サーバのトランザクション レートと設定した再送信回数に応じて、連続タイムアウトの回数は 10～100 になります。

### コマンド モード

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

サーバが認証とアカウント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** コマンドよりも前に **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。

## タスク ID

## タスク ID

## 動作

aaa

読み取り、書き込み

## 例

次に、RADIUS サーバが **radius-server dead-criteria tries** コマンドに対して **dead** とマーキングされる **dead-criteria** 条件となる再試行回数を設定する例を示します。

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# radius-server dead-criteria tries 4
```

## radius-server deadtime (BNG)

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、XR 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。deadtime 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

<i>value</i>	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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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	動作
aaa	読み取り、書き込み

## 例

次に、**radius-server deadtime** コマンドで、認証要求に回答しない RADIUS サーバの deadtime を 5 分に設定する例を示します。

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# radius-server deadtime 5
```

## radius-server key (BNG)

ルータと RADIUS デーモン間のすべての RADIUS 通信に認証および暗号キーを設定するには、XR 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

<b>0</b> <i>clear-text-key</i>	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。
<b>7</b> <i>encrypted-key</i>	暗号化共有キーを指定します。
<i>clear-text-key</i>	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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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	動作
aaa	読み取り、書き込み

---

例

次に、クリアテキストキーを「samplekey」に設定する例を示します。

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# radius-server key 0 samplekey
```

次に、暗号化共有キーを「anykey」に設定する例を示します。

```
RP/0/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# radius-server key 7 anykey
```

## radius-server retransmit (BNG)

Cisco IOS XR ソフトウェアがサーバへのパケットの送信を中止する前に再送信する回数を指定するには、XR 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。このコマンドの **no** 形式を使用すると、デフォルト値の 3 に設定されます。

**radius-server retransmit** {*retries* **disable**}

**no radius-server retransmit** {*retries* **disable**}

### 構文の説明

<b>retries</b>	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。
<b>disable</b>	radius-server transmit コマンドをディセーブルにします。

### 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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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	動作
aaa	読み取り、書き込み



## 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/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# radius-server retransmit 5
```

## radius-server timeout (BNG)

サーバホストがタイムアウトする前に応答するまでルータが待機するインターバルを設定するには、XR 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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

**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

デフォルトの radius-server timeout 値は 5 秒です。

### コマンド モード

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**radius-server timeout** コマンドを使用して、タイムアウトする前にサーバホストが応答するまでルータが待機する秒数を設定します。

### タスク ID

タスク ID	動作
aaa	読み取り、書き込み

### 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# radius-server timeout 10
```

## radius source-interface (BNG)

RADIUS が、すべての発信 RADIUS パケットに対して指定し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には、XR 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。指定したインターフェイス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

<i>interface-name</i>	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。
<i>vrfvrf-id</i>	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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**radius source-interface** コマンドを使用して、指定したインターフェイスまたはサブインターフェイスの IP アドレスをすべての発信 RADIUS パケットに設定します。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。これを防ぐには、IPアドレスをインターフェイスまたはサブインターフェイスに追加するか、あるいはインターフェイスを起動状態にします。

**radius source-interface** コマンドは、ルータに多く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アドレスが含まれている場合は特に便利です。

---

**タスク ID**

タスク ID	動作
aaa	読み取り、書き込み

---

**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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# radius source-interface loopback 10 vrf vrf1
```

## 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

<b>0</b>	(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。
<b>5</b>	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。
<i>secret-login</i>	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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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イク認証プロトコル) 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。

パスワードが保護されている回線ではXR EXECモードプロセスが開始されると、そのプロセスによってシークレットの入力が求められます。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方向に暗号化されているため、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パスワード暗号化がイネーブルになってい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) **show running-config** コマンドは、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しているときは、ログインパスワードをクリアテキストで表示しません。「例」の項を参照してください。

## タスク ID

タスク ID	動作
aaa	読み取り、書き込み

## 例

次に、ユーザ *user2* にクリアテキストのシークレット「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/RSP00/CPU0:router(config-un)# show running-config
Building configuration...
username user2
  secret 5 $1$DTmd$q7C6fhzje7Cc7Xzmu2FrX1
  !
end
```

## server (RADIUS)

特定の RADIUS サーバと定義済みのサーバグループを関連付けるには、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 ip-address [auth-port port-number] [acct-port port-number]
```

```
no server ip-address [auth-port port-number] [acct-port port-number]
```

### 構文の説明

<i>ip-address</i>	RADIUS サーバホストの IP アドレスです。
<b>auth-port</b> <i>port-number</i>	(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。 <i>port-number</i> 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。
<b>acct-port</b> <i>port-number</i>	(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。 <i>port-number</i> 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**server** コマンドを使用して、特定の RADIUS サーバと定義済みのサーバグループを関連付けます。

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。サーバを IP アドレスを使用して識別できます。また、任意で **auth-port** キーワードと **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できます。

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（アカウントリングなど）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トリング 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トリング サービス用に設定されている 2 番目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	動作
aaa	読み取り、書き込み

---



---

**例**

次に、同一のサービス、つまり認証とアカウントリ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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server 1.1.1.1 auth-port 1645 acct-port 1646
RP/0/RP0/CPU0:router(config-sg-radius)# server 2.2.2.2 auth-port 2000 acct-port 2001
```



## server (TACACS+)

特定の TACACS+ サーバと定義済みのサーバグループを関連付けるには、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

<i>hostname</i>	サーバホスト名の指定に使用する文字列です。
<i>ip-address</i>	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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**server** コマンドを使用して、特定の TACACS+ サーバと定義済みのサーバグループを関連付けます。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、アカウントिंग (AAA) の設定に使用されるメソッドリストから、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	動作
aaa	読み取り、書き込み

## 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/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ tac1  
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server 192.168.60.15
```

## server-private (RADIUS)

プライベート RADIUS サーバの IP アドレスをグループ サーバに設定するには、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** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

**no server-private** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

### 構文の説明

<i>ip-address</i>	RADIUS サーバ ホストの IP アドレスです。
<b>auth-port</b> <i>port-number</i>	(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。 <i>port-number</i> 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。
<b>acct-port</b> <i>port-number</i>	(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。 <i>port-number</i> 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。
<b>timeout</b> <i>seconds</i>	(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。この設定は <b>radius-server timeout</b> コマンドのグローバル値を上書きします。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。  <i>seconds</i> 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。
<b>retransmit</b> <i>retries</i>	(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。この設定は <b>radius-server transmit</b> コマンドのグローバル設定を上書きします。  <i>retries</i> 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。
<b>key</b> <i>string</i>	(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。このキーは <b>radius-server key</b> コマンドのグローバル設定を上書きします。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
- アカウントング 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 6.0	このコマンドが導入されました。

**使用上のガイドライン** **server-private** コマンドを使用して、特定のプライベート サーバと定義済みのサーバグループを関連付けます。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。したがって、サーバグループ内のサーバのリストには、プライベートサーバの設定内や定義内にあるホストへの参照が含まれています。

**auth-port** キーワードと **acct-port** キーワードは両方とも、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 モードを開始します。

タスク ID	タスク ID	動作
	aaa	読み取り、書き込み

**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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 timeout 5
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 retransmit 3
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 key coke
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
```

```
RP/0/RP0/CPU0:router(config-sg-radius-private)# exit
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 timeout 5
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 retransmit 3
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 key coke
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)#

RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server radius group1
RP/0/RP0/CPU0:router(config-sg-radius)# server-private 10.1.1.1 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)# exit
(config-sg-radius)# server-private 10.2.2.2 auth-port 300
RP/0/RP0/CPU0:router(config-sg-radius-private)#
```

## server-private (TACACS+)

プライベート TACACS+ サーバの IP アドレスをグループ サーバに設定するには、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

<i>hostname</i>	サーバ ホスト名の指定に使用する文字列です。
<i>ip-address</i>	TACACS+ サーバ ホストの IP アドレスです。IPv4 アドレスおよび IPv6 アドレスのどちらもサポートされています。
<b>port</b> <i>port-number</i>	(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。
<b>timeout</b> <i>seconds</i>	(任意) 認証、許可、アカウントング (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。このオプションは、このサーバのみに対して <b>tacacs-server timeout</b> コマンドで設定されたグローバル タイムアウト値を上書きします。範囲は 1 ~ 1000 です。デフォルトは 5 分です。
<b>keystring</b>	(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 <b>tacacs-server key</b> コマンドのグローバル設定を上書きします。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* 引数を指定しない場合は、デフォルトで標準ポート 49 が設定されます。

*seconds* 引数を指定しない場合は、デフォルトで 5 秒に設定されます。

### 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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**server-private** コマンドを使用して、特定のプライベートサーバと定義済みのサーバグループを関連付けます。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	動作
aaa	読み取り、書き込み

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa group server tacacs+ myserver
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 timeout 5
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 key a secret
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.1.1.1 port 51
RP/0/RP0/CPU0:router(config-sg-tacacs-private)# exit
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 timeout 5
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 key coke
RP/0/RP0/CPU0:router(config-sg-tacacs+)# server-private 10.2.2.2 port 300
RP/0/RP0/CPU0:router(config-sg-tacacs-private)#
```

## show aaa (XR-VM)

インターネット キー エクスチェンジ (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、または タスク グループ に関する情報を表示する、または、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 に関連付けられたすべての タスク ID のリストを表示する、あるいは、指定した 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 のすべての タスク ID のリストを表示するには、XR EXEC モードで **show aaa** コマンドを使用します。

**show aaa** {**ikegroup** *ikegroup-name*| **loginsync**| **usergroup** [*usergroup-name* ]| **trace**| **userdb** [*username* ]| **task**| **taskgroup** }

### 構文の説明

<b>ikegroup</b>	ローカル IKE グループの詳細情報を表示します。
<i>ikegroup-name</i>	(任意) 詳細が表示される IKE グループです。
<b>login</b>	ログイン サブシステムのデータを表示します。
<b>sync</b>	データをサブシステムと同期します。
<b>usergroup</b>	すべてのユーザ グループの詳細を表示します。
<i>usergroup-name</i>	(任意) ユーザグループ名です。
<b>trace</b>	AAA サブシステムに関するトレース データを表示します。
<b>userdb</b>	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。
<i>username</i>	(任意) 詳細を表示する対象のユーザです。
<b>task</b>	タスクの情報を表示します。
<b>taskgroup</b>	すべてのタスク グループの詳細を表示します。 (注) <b>taskgroup</b> のキーワードについては、オプションの <b>usergroup name</b> キーワードリストを参照してください。

### 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

XR EXEC モード



コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

使用上のガイドライン

**show aaa** コマンドを使用して、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、AAA タスク ID、またはタスクグループのリストを表示します。任意で *ikegroup-name* 引数、*usergroup-name* 引数、*username* 引数引数を使用して、指定した 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情報をそれぞれ表示します。

タスク ID

タスク ID	動作
aaa	読み取り

例

次に、**ikegroup** キーワードを使用した **show aaa** コマンドによる出力の例を示します。

```
RP/0/RP0/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** コマンドによる出力の例を示します。

```
RP/0/RP0/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、**netadmin** というタスクグループに対して **taskgroup** キーワードを使用した **show aaa** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# show aaa taskgroup netadmin
Task group 'netadmin'
Task group 'netadmin' has the following combined set
of task IDs (including all inherited groups):
```

show aaa (XR-VM)

```

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:          bcddl    : 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、operator に対して **taskgroup** キーワードを使用した **show aaa** コマンドによる出力の例を示します。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、root system に対して **taskgroup** キーワードを使用した **show aaa** コマンドによる出力の例を示します。タスクグループのルートシステムには、継承したすべてのグループが含まれている次のタスク ID の組み合わせがあります。

```
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
```

## show aaa (XR-VM)

```

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、**task supported** キーワードを使用した **show aaa** コマンドによる出力の例を示します。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-systemlrlr
root-system
route-map
route-policy
sbc
snmp

```

```
sonet-sdh
static
sysmgr
system
transport
tty-access
tunnel
universal
vlan
vrrp
```

# show aaa accounting

AAA サブシステムのコマンド履歴を日時とともに表示するには、システム管理 EXEC モードで **show aaa accounting** コマンドを使用します。システム管理 VM に `group aaa-r` または `root-system` が必要です。

## show aaa accounting

### 構文の説明

このコマンドにはキーワードまたは引数はありません。

### コマンド デフォルト

なし

### コマンド モード

システム管理 EXEC モード

### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

### タスク ID

タスク ID	動作
aaa	読み取り

### 例

次に、**show aaa accounting** コマンドによる出力例を示します。

```
sysadmin-vm:0_RP0#show aaa accounting
Mon Nov  3 13:37:21.573 UTC

Detail audit log information
-----
Time                Username           Session-ID         Node-Information   Command
-----
2014-11-03.13:14:27 UTC    root              17                System             logged in from
the CLI with aaa disabled
..
..
..
```

```

2014-11-03.13:37:01 UTC      cisco      57      0/RP0      assigned to
groups: root-system
2014-11-03.13:37:03 UTC      cisco      57      0/RP0      CLI 'config
terminal'
2014-11-03.13:37:03 UTC      cisco      57      0/RP0      CLI done
2014-11-03.13:37:09 UTC      cisco      57      0/RP0      CLI 'aaa
authentication users user temp'
2014-11-03.13:37:09 UTC      cisco      57      0/RP0      CLI done
2014-11-03.13:37:11 UTC      cisco      57      0/RP0      CLI 'password
****
2014-11-03.13:37:11 UTC      cisco      57      0/RP0      CLI done
2014-11-03.13:37:12 UTC      cisco      57      0/RP0      CLI 'commit'
2014-11-03.13:37:14 UTC      cisco      57      0/RP0      CLI done
2014-11-03.13:37:16 UTC      cisco      57      0/RP0      CLI 'exit'
2014-11-03.13:37:16 UTC      cisco      57      0/RP0      CLI done
2014-11-03.13:37:18 UTC      cisco      57      0/RP0      CLI 'exit'
2014-11-03.13:37:18 UTC      cisco      57      0/RP0      CLI done
2014-11-03.13:37:21 UTC      cisco      57      0/RP0      CLI 'show aaa
accounting'

```

## show radius

システムに設定されている RADIUS サーバに関する情報を表示するには、XR 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または引数はありません。

#### 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

XR EXEC モード

#### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

#### 使用上のガイドライン

**show radius** コマンドを使用して、設定済みの各 RADIUS サーバに関する統計情報を表示します。

#### タスク ID

タスク ID	動作
aaa	読み取り

#### 例

次に、**show radius** コマンドによる出力の例を示します。

```
RP/0/RP0/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
Quarantined: No
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

```

次の表で、この出力に表示される重要なフィールドを説明します。

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/アカウントング要求の 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。

# show radius accounting

RADIUS アカウントング サーバおよびポートの情報および詳細統計情報を取得するには、XR 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または引数はありません。

### 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

XR EXEC モード

### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

### タスク ID

タスク ID	動作
aaa	読み取り

### 例

次に、**show radius accounting** コマンドよりサーバ単位で表示された出力の例を示します。

```
RP/0/RP0/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
```

次の表で、この出力に表示される重要なフィールドを説明します。

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、アカウントティング要求の UDP 宛先ポートです。

# show radius authentication

RADIUS 認証サーバおよびポートの情報と詳細統計情報を取得するには、XR 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または引数はありません。

### 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

XR EXEC モード

### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

### タスク ID

タスク ID	動作
aaa	読み取り

### 例

次に、**show radius authentication** コマンドによる出力の例を示します。

```
RP/0/RP0/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
```

次の表で、この出力に表示される重要なフィールドを説明します。

**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、アカウントティング要求の UDP 宛先ポートです。

## 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、XREXEC 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

<b>hostip-addr</b>	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。
<b>auth-portauth-port</b>	(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。
<b>acct-portacct-port</b>	(任意) RADIUS サーバに対するアカウント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

時間および試行回数のデフォルト値は 1 つの値に固定されていません。これらの値は計算され、時間の場合は 10 ~ 60 秒、再試行回数の場合は 10 ~ 100 の範囲になります。

### コマンド モード

XR EXEC モード

### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

### タスク ID

タスク ID	動作
aaa	読み取り

## 例

次に、**show radius dead-criteria** コマンドによる出力の例を示します。

```
RP/0/RP0/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)
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 4 : **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/アカウントング要求の 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。

# show radius server-groups

システムに設定されている RADIUS サーバグループに関する情報を表示するには、XREXEC 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

<i>group-name</i>	(任意) サーバグループの名前。プロパティが表示されます。
<b>detail</b>	(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

XREXEC モード

## コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**show radius server-groups** コマンドを使用して、設定されている各 RADIUS サーバグループに関する情報を表示します。表示される情報には、グループ名、グループ内のサーバの数、名前付きサーバグループ内のサーバのリストが含まれます。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ト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	動作
aaa	読み取り

## 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** コマンドによる出力の例を示します。

```
RP/0/RP0/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/RP0/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「radgrp-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/RP0/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:
```

## show radius server-groups

```

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

```

次の表で、この出力に表示される重要なフィールドを説明します。

表 5 : *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/アカウントリング要求の UDP 宛先ポートです。

## show tacacs

システムに設定されている TACACS+ サーバに関する情報を表示するには、XR 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または引数はありません。

#### コマンド デフォルト

なし

#### コマンド モード

XR EXEC モード

#### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

#### 使用上のガイドライン

**show tacacs** コマンドを使用して、設定済みの各 TACACS+ サーバに関する統計情報を表示します。

#### タスク ID

タスク ID	動作
aaa	読み取り

#### 例

次に、**show tacacs** コマンドによる出力例を示します。

```
RP/0/RP0/CPU0:router# show tacacs

For IPv4 IP addresses:
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
```

```

For IPv6 IP addresses:
Server: 1.2.3.5/49 family = AF_INET opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0
        status=up single-connect=false

```

次の表で、この出力に表示される重要なフィールドを説明します。

表 6 : *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+ サーバグループに関する情報を表示するには、XR 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または引数はありません。

#### コマンド デフォルト

なし

#### コマンド モード

XR EXEC モード

#### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

#### 使用上のガイドライン

**show tacacs server-groups** コマンドを使用して、設定されている各 TACACS+ サーバグループに関する情報を表示します。表示される情報には、グループ名、グループ内のサーバの数、名前付きサーバグループ内のサーバのリストが含まれます。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	動作
aaa	読み取り

#### 例

次に、**show tacacs server-groups** コマンドによる出力例を示します。

```
RP/0/RP0/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
```

## show tacacs server-groups

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

次の表で、この出力に表示される重要なフィールドを説明します。

表 7: *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。

## 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、XR 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

<b>all</b>	(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。
<b>authentication</b>	(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。
<b>group</b>	(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。
<b>tasks</b>	(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。 <b>tasks</b> キーワードは、出力例で予約されているタスクを示します。

### コマンド デフォルト

オプションを指定せずに **show user** コマンドを使用すると、現在ログインしているユーザの ID を表示します。

### コマンド モード

XR EXEC モード

### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**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たすべてのユーザグループおよびタスク ID を表示します。

### タスク ID

タスク ID	動作
none	—

例

次に、**show user** コマンドによる、認証方式パラメータを表示する出力の例を示します。

```
RP/0/RP0/CPU0:router# show user authentication method
```

```
local
```

次に、**show user** コマンドによる、グループを表示する出力の例を示します。

```
RP/0/RP0/CPU0:router# show user group
```

```
root-system
```

次に、**show user** コマンドによる、グループとタスクに関するすべての情報を表示する出力の例を示します。

```
RP/0/RP0/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:          bccl : 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** コマンドによる、タスクを表示し、予約されるタスクを示した出力の例を示します。

RP/0/RP0/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:          hrsrp    : 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
    
```

## show user

```
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
```

## show aaa user-group

AAAサブシステムのユーザグループ情報を表示するには、システム管理EXECモードで **show aaa user-group** コマンドを使用します。システム管理 VM に `group aaa-r` または `root-system` が必要です。

### show aaa user-group

#### 構文の説明

このコマンドにはキーワードまたは引数はありません。

#### コマンド デフォルト

なし

#### コマンド モード

システム管理 EXEC モード

#### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

#### 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

#### タスク ID

タスク ID	動作
aaa	読み取り

#### 例

次に、**show aaa user-group** コマンドによる出力例を示します。

```
sysadmin-vm:0_RP0#show aaa user-group
Mon Nov  3 13:39:33.380 UTC

User group : root-system
sysadmin-vm:0_RP0#
```

## show tech-support aaa

AAA のデバッグ ファイルおよびトレース ファイルを システム管理 VM から取得するには、システム管理 EXEC モードで **show tech-support aaa** コマンドを使用します。

### show tech-support aaa

#### 構文の説明

このコマンドにはキーワードまたは引数はありません。

#### コマンド デフォルト

なし

#### コマンド モード

システム管理 EXEC モード

#### コマンド履歴

リリース	変更内容
リリース 6.0	このコマンドが導入されました。

#### 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

#### タスク ID

タスク ID	動作
aaa	読み取り

#### 例

次に、**show tech-support aaa** コマンドによる出力の例を示します。

```
sysadmin-vm:0_RP0#show tech-support aaa
Mon Nov  3 13:39:33.380 UTC

Fri Oct 24 07:22:15.740 UTC ++ Show tech start time: 2014-Oct-24.072216.UTC ++
Waiting for gathering to complete /opt/cisco/calvados/script/show_tech_aaa: line 27: rse:
command not found .
Compressing show tech output
Show tech output available at /misc/disk1//showtech-aaa-admin-2014-Nov-04.082457.UTC.tgz
Please collect show tech-support ctrace in addition to any sysadmin show-tech-support
collection
++ Show tech end time: 2014-Nov-04.UTC ++
sysadmin-vm:0_RP0#
```

## single-connection

単一の TCP 接続を介したこのサーバへのすべての TACACS+ 要求を多重化するには、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。個別の接続を使用する新たなセッションすべてに対して単一の TCP 接続をディセーブルにするには、このコマンドの **no** 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または引数はありません。

### 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**single-connection** では、サーバへの要求の送信に複数の TCP 接続を使用し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	動作
aaa	読み取り、書き込み

### 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、アカウントング要求でこの 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/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226  
RP/0/RP0/CPU0:router(config-tacacs-host)# single-connection
```

## tacacs-server host

TACACS+ ホストサーバを指定するには、XR 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。指定し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

<i>host-name</i>	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。
<i>port</i> <i>port-number</i>	(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。
<i>timeout</i> <i>seconds</i>	(任意) 認証、許可、アカウントング (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。このオプションは、このサーバのみに対して <b>tacacs-server timeout</b> コマンドで設定されたグローバルタイムアウト値を上書きします。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。 注：このパラメータは <b>config-tacacs-host</b> サブモードでのみ使用できます。
<i>key</i> [0   7] <i>auth-key</i>	(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、このサーバに対して <b>tacacs-server key</b> コマンドで設定されたキーのみが上書きされます。  (任意) <b>0</b> を入力することにより、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) <b>7</b> を入力することにより、暗号化されたキーが続くことを指定します。  <i>auth-key</i> 引数は、AAA サーバと TACACS+ サーバ間に暗号化されていないキーを指定します。  注：このパラメータは <b>config-tacacs-host</b> サブモードでのみ使用できます。
<i>single-connection</i>	(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。 注：このパラメータは <b>config-tacacs-host</b> サブモードでのみ使用できます。

### コマンド デフォルト

TACACS+ ホストは指定されません。

*port-name* 引数を指定しない場合は、デフォルトで標準ポート 49 が設定されます。

*seconds* 引数を指定しない場合は、デフォルトで 5 秒に設定されます。

コマンドモード XR 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 6.0	このコマンドが導入されました。

使用上のガイドライン

複数の **tacacs-server host** コマンドを使用して、追加する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	動作
aaa	読み取り、書き込み

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/RP0/CPU0:router(config)# tacacs-server host 209.165.200.226
RP/0/RP0/CPU0:router(config-tacacs-host)#
```

次に、**tacacs-server host** によるデフォルト値が **show run** コマンドによって表示される例を示します。

```
RP/0/RP0/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/RP0/CPU0:router(config)# tacacs-server host host1 port 51
RP/0/RP0/CPU0:router(config-tacacs-host)# timeout 30
RP/0/RP0/CPU0:router(config-tacacs-host)# key a_secret
```



## tacacs-server key

ルータとTACACS+ デーモン間のすべての TACACS+ 通信に使用する認証暗号キーを設定するには、XR 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

<b>0</b> <i>clear-text-key</i>	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。
<b>7</b> <i>encrypted-key</i>	暗号化共有キーを指定します。
<i>auth-key</i>	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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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**

---

**動作**

---

aaa

---

読み取り、書き込み

---

**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/RP0/CPU0:router(config)# tacacs-server key key1
```

## tacacs-server timeout

サーバホストの応答をサーバが待機するインターバルを設定するには、XR 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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

**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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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	動作
aaa	読み取り、書き込み

### 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/RP0/CPU0:router(config)# tacacs-server timeout 10
```

## tacacs-server ipv4

IP ヘッダーのタイプ オブ サービス (ToS) バイトの最初の 6 ビットで表される DiffServ コード ポイント (DSCP) を設定するには、XR コンフィギュレーションモードで **tacacs-server ipv4** コマンドを使用します。

**tacacs-server ipv4 dscp** *dscp-value*

### 構文の説明

---

**ipv4** IPv4 パケットに dscp ビットを指定します。

---

**dscp** IP ヘッダーに DSCP を設定します。

---

---

*dscp-value* DSCP の値を設定するためのオプションを指定します。次のオプションを使用できません。

- <0-63> Differentiated services codepoint value
- af11 Match packets with AF11 dscp (001010)
- af12 Match packets with AF12 dscp (001100)
- af13 Match packets with AF13 dscp (001110)
- af21 Match packets with AF21 dscp (010010)
- af22 Match packets with AF22 dscp (010100)
- af23 Match packets with AF23 dscp (010110)
- af31 Match packets with AF31 dscp (011010)
- af32 Match packets with AF32 dscp (011100)
- af33 Match packets with AF33 dscp (011110)
- af41 Match packets with AF41 dscp (100010)
- af42 Match packets with AF42 dscp (100100)
- af43 Match packets with AF43 dscp (100110)
- cs1 Match packets with CS1(precedence 1) dscp (001000)
- cs2 Match packets with CS2(precedence 2) dscp (010000)
- cs3 Match packets with CS3(precedence 3) dscp (011000)
- cs4 Match packets with CS4(precedence 4) dscp (100000)
- cs5 Match packets with CS5(precedence 5) dscp (101000)
- cs6 Match packets with CS6(precedence 6) dscp (110000)
- cs7 Match packets with CS7(precedence 7) dscp (111000)
- default Match packets with default dscp (000000)
- ef Match packets with EF dscp (101110)

---

コマンド デフォルト    なし

---

コマンド モード        XR 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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドの使用に影響する特定のガイドラインはありません。

## タスク ID

タスク ID	動作
aaa	読み取り、書き込み

## 例

次に、DSCP 値を相対的優先転送 (AF) 11 に設定する例を示します。

```
RP/0/RSP0/CPU0:router(config)# tacacs-server ipv4 dscp af11
```

## tacacs source-interface

すべての発信 TACACS+ パケットに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、XR 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の 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

<i>type</i>	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。
<i>path-id</i>	物理インターフェイスまたは仮想インターフェイス。 (注) ルータ上に現在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するには、XR コンフィギュレーションモードで <b>showinterfaces</b> コマンドを使用します。 ルータの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。
<i>vrfvrf-id</i>	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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**tacacs source-interface** コマンドを使用して、指定したインターフェイスの IP アドレスをすべての発信 TACACS+ パケットに設定します。インターフェイスが起動状態にある間は、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 アドレスがない、または指定したインターフェイスがダウン状態のときは、TACACS+ は送信元インターフェイスの設定が使用されていない場合と同様に動作します。

---

#### タスク ID

タスク ID	動作
aaa	読み取り、書き込み

---

#### 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# tacacs source-interface TenGigabitEthernet 0/0/0/29 vrf abc
```



# 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 ID をタスク 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。

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

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

## 構文の説明

<b>read</b>	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。
<b>write</b>	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。
<b>execute</b>	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。
<b>debug</b>	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。
<i>taskid-name</i>	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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

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 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	動作
	aaa	読み取り、書き込み

**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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup taskgroup1
RP/0/RP0/CPU0:router(config-tg)# task execute config-services
```

# taskgroup

タスク グループを一連のタスク ID と関連付けてタスク グループ コンフィギュレーション モードを開始するように設定するには、XR 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

<i>taskgroup-name</i>	特定のタスク グループの名前です。
<b>description</b>	(任意) 名前付きタスク グループの説明を作成できます。
<i>string</i>	(任意) タスク グループの説明に使用する文字列です。
<b>task</b>	(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。
<b>read</b>	(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。
<b>write</b>	(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。
<b>execute</b>	(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。
<b>debug</b>	(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。
<i>taskid-name</i>	(任意) タスクの名前: タスク ID です。
<b>inherit taskgroup</b>	(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。
<i>taskgroup-name</i>	(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

XR 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 6.0	このコマンドが導入されました。

**使用上のガイドライン** 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。

キーワードまたは引数を指定せずに **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** コマンド、**inherit** コマンド、**show** コマンド、および **task** コマンドを使用できます。

タスク ID	タスク ID	動作
	aaa	読み取り、書き込み

**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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# taskgroup alpha
RP/0/RP0/CPU0:router(config-tg)# task read bgp
```

## timeout (TACACS+)

認証、認可、およびアカウントング (AAA) サーバが TACACS+ サーバからの応答の受信を待機する時間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、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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

**timeout (TACACS+)** コマンドは、このサーバのみに対して **tacacs-server timeout** コマンドで設定されたグローバルタイムアウト値を上書きします。

### タスク ID

タスク ID	動作
aaa	読み取り、書き込み

## 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/RP0/CPU0:router (config) # tacacs-server host 209.165.200.226  
RP/0/RP0/CPU0:router (config-tacacs-host) # timeout 500
```

## timeout login response

ログインへの応答をサーバが待機するインターバルを設定するには、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。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

**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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

ライン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	動作
aaa	読み取り、書き込み

---

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/RP0/CPU0:router# configure  
RP/0/RP0/CPU0:router(config)# line template alpha  
RP/0/RP0/CPU0:router(config-line)# timeout login response 20
```



## usergroup

ユーザグループを一連のタスクグループと関連付けて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ように設定するには、XR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、または指定したユーザグループとのタスクグループ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

<i>usergroup-name</i>	ユーザグループの名前です。 <i>usergroup-name</i> 引数には1つの単語だけが使用できます。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

XR 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 6.0	このコマンドが導入されました。

### 使用上のガイドライン

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**, (32 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。ユーザグループは事前に設定された **root-system** や **owner-sdr** などのグループから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**

---

**動作**

---

aaa

---

読み取り、書き込み

---

**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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router (config)# usergroup alpha
RP/0/RP0/CPU0:router (config-ug)# inherit usergroup beta
```

## username

ユーザ名を使用して新しいユーザを設定し、パスワードを設定し、ユーザにアクセス許可を付与し、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、XR コンフィギュレーション モードまたは システム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。ユーザをデータベースから削除するには、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

<i>user-name</i>	ユーザ名。 <i>user-name</i> 引数には1つの単語のみを使用できます。スペースと引用符は使用できません。
<b>password</b>	(任意) 名前付きユーザにパスワードを作成できます。
<b>0</b>	(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。
<b>7</b>	(任意) 暗号化パスワードが続くことを指定します。
<i>password</i>	(任意) ユーザがログインするために入力する、暗号化されていないパスワードテキスト (たとえば、「lab」) 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。
<b>secret</b>	(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。
<b>0</b>	(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。
<b>5</b>	(任意) 暗号化パスワードが続くことを指定します。
<b>group</b>	(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。
<i>usergroup-name</i>	(任意) <b>usergroup</b> コマンドで定義したユーザ グループの名前。


### コマンド モデル

システムにユーザ名は定義されません。  
XR コンフィギュレーションモード

システム管理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 6.0	このコマンドが導入されました。

使用上のガイドラ 

(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。パスワードとグループの割り当てはXR コンフィギュレーションモードまたは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より行えます。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。

XR 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。

**username** コマンドは、デフォルトでローカルログイン認証用の特定のユーザに関連付けられています。または、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できます。詳細については、[aaa authentication \(XR-VM\)](#)、(11 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クデバイスをイネーブルにし、リモートの **Challenge Handshake Authentication Protocol (CHAP)** のチャレンジに応答するには、**username** コマンドの1つのエントリが、他のネットワーク デバイスにすでに関連付けられているホスト名エントリと同じである必要があります。

タスク ID

タスク ID	動作
aaa	読み取り、書き込み

例 次に、**username** コマンドの実行後に使用できるコマンドの例を示します。

```
RP/0/RP0/CPU0:router# config
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/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
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	XR 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/RP0/CPU0:router(config-un)#
```

次に、クリアテキストのパスワード *password1* をユーザ名 *user1* に対して設定する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# username user1
RP/0/RP0/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 セキュア シークレットを設定する例を示します。

```
RP/0/RP0/CPU0:P1(admin-config)# username user1
RP/0/RP0/CPU0:P1(admin-config-un)# secret 0 lab
RP/0/RP0/CPU0:P1(admin-config-un)# commit
RP/0/RP0/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/RP0/CPU0:P1(admin-config-un)# exit
RP/0/RP0/CPU0:P1(admin-config)# show run username
```

**username**

```
username user1 secret 5 $1$QB03$3H29k3ZT.0PMQ8GQQKXCF0  
!
```

## users group

ユーザグループとその特権を回線と関連付けるには、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。

```
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| serviceadmin| sysadmin}
```

### 構文の説明

<i>usergroup-name</i>	ユーザグループの名前です。 <i>usergroup-name</i> 引数には1つの単語だけを使用できます。スペースと引用符は使用できません。
<b>cisco-support</b>	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。
<b>netadmin</b>	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。
<b>operator</b>	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。
<b>root-lr</b>	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。
<b>root-system</b>	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。
<b>serviceadmin</b>	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。
<b>sysadmin</b>	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 6.0	このコマンドが導入されました。

## 使用上のガイドライン

**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と関連付けできるようにします。つまり、回線を通じてログインするユーザには特定のユーザグループの特権が付与されます。

## タスク ID

タスク ID	動作
aaa	読み取り、書き込み

## 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/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# aaa authen login vty-authen line
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router(config)# line template vty
RP/0/RP0/CPU0:router(config-line)# users group operator
RP/0/RP0/CPU0:router(config-line)# login authentication
```