Cisco NCS 5000 シリーズ ルータ向けシステム セキュリティ コマンド リファレンス

初版：2015 年 12 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

目 次

はじめに

「はじめに」の内容は次のとおりです。

マニュアルの変更履歴

表 1 に、初版後、このマニュアルに加えられた技術的な変更の履歴を示します。

表 *1*：マニュアルの変更履歴

日付	Summary
2015 年 12 月	このマニュアルの初版

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

認証、許可、アカウンティング コマンド

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

AAA の概念、設定作業、および例の詳細については、『*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

アカウンティ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

commands	XR EXEC シェル コマンドのアカウンティングをイネーブルにします。
exec	XR EXEC セッションのアカウンティングをイネーブルにします。
mobile	モバイル IP 関連のアカウンティング イベントをイネーブルにします。
network	Internet Key Exchange（IKE; インターネットキー交換）や Point-to-Point Protocol（PPP; ポイントツーポイントプロトコル）など、すべてのネットワーク関連サービス要求に対するアカウンティングをイネーブルにします。
system	すべてのシステム関連イベントをイネーブルにします。
event manager	XR EXEC 用の許可リストを設定します。
default	このキーワードに続くアカウンティング メソッドのリストをアカウンティング 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。
list-name	アカウンティング メソッド リストの名前の指定に使用する文字列です。
start-stop	プロセスの開始時に「start accounting」通知を送信し、プロセスの終了時に「stop accounting」通知を送信します。要求されたユーザ プロセスは、「start accounting」通知がアカウンティング サーバで受信されたかどうかに関係なく開始されます。
stop-only	要求されたユーザ プロセスの終了時に「stop accounting」通知を送信します。 注：これはシステム アカウンティングではサポートされていません。
none	アカウンティングを使用しません。

method	AAA システム アカウンティングのイネーブル化に使用する方式です。値は、次のいずれかになります。 • **group tacacs+**：すべての TACACS+ サーバのリストをアカウンティングに使用します。 • **group radius**：すべての RADIUS サーバのリストをアカウンティングに使用します。 • **group***named-group*：**aaa group server tacacs+** コマンド、または **aaa group server radius** コマンドで定義されたアカウンティング用の 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。

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

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ティング 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ティングをイネーブルにします。

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

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

最小アカウンティングでは、**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ティングでは、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。アカウンティング 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」通知がアカウンティング サーバで受信されたかどうかに関係なく開始されます。

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

タスク ID

タスク ID	動作
aaa	読み取り、書き込み

例

次に、デフォルトの commands アカウンティング 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ティング 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、およびアカウンティング（AAA）システム アカウンティングをイネーブルにするには、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 アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

no aaa accounting system default

構文の説明

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

コマンド デフォルト

AAA アカウンティングはディセーブルです。

コマンド モード

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

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

デフォルトのメソッド 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す。デフォルトのメソッド リストが定義されていない場合、アカウンティ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

中間アカウンティング レコードがアカウンティング サーバに定期的に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。中間アカウンティ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

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

コマンド デフォルト

AAA のアカウンティングのアップデートはディセーブルになります。

コマンド モード

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

periodic キーワードと一緒に使用した場合、中間アカウンティング レコードは*minutes* 引数で定義したとおりに定期的に送信されます。中間アカウンティング レコードには、アカウンティング レコードが送信される時点までにそのユーザに関して記録されたすべてのアカウンティング情報が含まれます。

newinfo キーワードと **periodic** キーワードを一緒に使用すると、中間アカウンティング レコードは、レポートする新しいアカウンティング情報が発生するたびにアカウンティング 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ティング レコードがアカウンティング サーバに定期的に送信されます。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ティング 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ティング 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ティング レコードを 30 分間隔で RADIUS サーバに送信する例を示します。

```
RP/0/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ティング情報があるときに、中間アカウンティング レコードを RADIUS サーバに送信する例を示します。

```
RP/0/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

login	ログインの認証を設定します。
ppp	ポイントツーポイント プロトコルの認証を設定します。
default	このキーワードに続く認証方式のリストを認証のデフォルト メソッド リストとして使用します。
list-name	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。
method-list	AAA システム アカウンティングのイネーブル化に使用する方式です。値は、次のいずれかになります。 • **group tacacs+**：設定されたすべての TACACS+ サーバのリストを認証に使用するメソッド リストを指定します。 • **group radius**：設定されたすべての RADIUS サーバのリストを認証に使用するメソッド リストを指定します。 • **group***named-group*：**aaa group server tacacs+** コマンド、または **aaa group server radius** コマンドで定義された認証用の 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。 • **local**：ローカル ユーザ名データベース方式を認証に使用するメソッド 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。 • **line**：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。

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

commands	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。
eventmanager	イベント マネージャ（障害マネージャ）を許可するための許可方式を適用します。
exec	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。
network	PPP やインターネットキー交換（IKE）などのネットワーク サービスに対する許可を設定します。
default	このキーワードに続く許可方式のリストを許可のデフォルト メソッド リストとして使用します。
list-name	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。
none	許可を使用しません。**none** 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。
local	ローカルの許可を使用します。この許可方式は、コマンドの許可には使用できません。
group tacacs+	設定されているすべての TACACS+ サーバのリストを許可に使用します。
group radius	設定されているすべての RADIUS サーバのリストを許可に使用します。この許可方式は、コマンドの許可には使用できません。
group*group-name*	**aaa group server tacacs+** コマンド、または **aaa group server radius** コマンドで定義された許可用の 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 デフォルト

XR すべてのアクション（**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、各エントリが一意の ID を持っていれば、同一サーバに複数のホスト エントリを組み込むことができます。IP アドレスと 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、およびアカウンティング（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ティング サービスを提供できなかった場合、ネットワーク ア

クセス サーバは同じデバイス上の 2 つ目のホスト エントリでアカウンティング サービスを試行します。RADIUS ホスト エントリは、サーバ グループに設定された順序で試行されます。

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

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

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

タスク ID

タスク ID	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。

aaa group server tacacs+

異なるTACACS+サーバホストを重複し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 tacacs+** コマンドを使用します。サーバ グループ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 tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

構文の説明

group-name	サーバ グループの名前の指定に使用する文字列です。

コマンド デフォルト

このコマンドはディセーブルになります。

コマンド モード

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

aaa group server tacacs+ コマンドにより、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** コマンドは特定の TACACS+ サーバを定義済みのサーバ グループに関連付けます。

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

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

（注） グループ名方式では、定義済みの一連の TACACS+ サーバを参照します。**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、およびアカウンティング（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 アカウンティング サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

commands	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ティングをイネーブルにします。
exec	XR EXEC モード セッションをイネーブルにします。
default	**aaa accounting** 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。
list-name	使用するアカウンティング メソッド リストの名前を指定します。このリストは **aaa accounting** コマンドを使用して作成されます。

コマンド デフォルト

アカウンティングはディセーブルです。

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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ティングに名前付きのアカウンティング 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ティング 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ティ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* というアカウンティング メソッド リストを使用してコマンド アカウンティング サービスをイネーブルにする例を示します。

```
RP/0/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、およびアカウンティング（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

commands	選択した回線におけるすべてのコマンドの許可をイネーブルにします。
exec	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。
default	**aaa authorization** 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。
eventmanager	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。
list-name	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 **aaa authorization** 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

cisco-support	事前定義されたシスコ サポート担当者グループにユーザを追加します。 （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。
maintenance	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。
netadmin	事前定義されたネットワーク管理者グループにユーザを追加します。
operator	事前定義されたオペレータ グループにユーザを追加します。
provisioning	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。
retrieve	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。
root-lr	事前定義された root-lr グループにユーザを追加します。root-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。
serviceadmin	事前定義されたサービス管理者グループにユーザを追加します。
sysadmin	事前定義されたシステム管理者グループにユーザを追加します。
group-name	**usergroup** 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

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

コマンド デフォルト

なし

コマンド モード

タスク グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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

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

コマンド デフォルト

なし

コマンド モード

ユーザ グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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

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

コマンド デフォルト

なし

コマンド モード

TACACS ホスト コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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 **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、およびアカウンティング（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

default	**aaa authentication login** 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。
list-name	認証に使用するメソッド リストの名前です。**aaa authentication login** 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

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

コマンド デフォルト

パスワードは暗号化されていないクリア テキストです。

コマンド モード

ユーザ名コンフィギュレーション

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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

seconds	秒単位の時間です。範囲は、1 ～ 120 秒です。*seconds* 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、dead マークを付けるサーバについて満たす必要があります。

コマンド デフォルト

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。

使用上のガイドライン

（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

tries	1 ～ 100 のタイムアウト回数。*tries* 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、dead マークを付けるサーバについて満たす必要があります。

コマンド デフォルト

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

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

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

コマンド デフォルト

デッド タイムは 0 に設定されます。

コマンド モード

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、認証要求に応答しない 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

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

コマンド デフォルト

認証および暗号キーはディセーブルになります。

コマンド モード

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

retries	再送信の最大試行回数です。範囲は 1 ～ 100 です。デフォルトは 3 です。
disable	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ようにするには、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

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

コマンド デフォルト

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

コマンド モード

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

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

コマンド デフォルト

パスワードは指定されません。

コマンド モード

ユーザ名コンフィギュレーション

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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

る一方向ハッシュ関数であり、強力な暗号化保護を可能にします。MD5暗号化を使用すると、クリアテキスト パスワードを取得できません。したがって、MD5 で暗号化されたパスワードは、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）など、クリアテキスト パスワードの取得を必要とするプロトコルと一緒には使用できません。

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

パスワード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

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

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

RADIUS サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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（アカウンティングなど）に対して設定すると、2 番目に設定したホスト エントリは最初のホスト エントリをバックアップする自動スイッチオーバーとして機能します。この場合、最初のホスト エントリがアカウンティング サービスを提供できなかった場合、ネットワーク アクセス サーバは同じ装置上でアカウンティング サービス用に設定されている 2 番めのホスト エントリを試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

タスク ID

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

```
RP/0/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

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

コマンド デフォルト

なし

コマンド モード

TACACS+ サーバグループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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、アカウンティング（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

ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port*port-number*	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポートを指定します。*port-number* 引数は、認証要求に対するポート番号を指定します。この値が 0 に設定されている場合、そのホストは認証に使用されません。デフォルト値は 1645 です。
acct-port*port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。*port-number* 引数は、アカウンティング要求に対するポート番号を指定します。この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。デフォルト値は 1646 です。
timeout*seconds*	（任意）再送信するまでにルータが RADIUS サーバの応答を待機する秒数を指定します。この設定は **radius-server timeout** 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。 *seconds* 引数はタイムアウト値を秒単位で指定します。範囲は 1 ～ 1000 です。タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit*retries*	（任意）サーバが応答しない、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。この設定は **radius-server transmit** コマンドのグローバル設定を上書きします。 *retries* 引数は再送信値を指定します。範囲は 1 ～ 100 です。再送信値が指定されていない場合は、グローバル値が使用されます。
key*string*	（任意）ルータと RADIUS サーバ上で稼働する RADIUS デーモン間で使用される認証および暗号キーを指定します。このキーは **radius-server key** 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-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

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

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

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):
```

```
Task:                 aaa  : READ
Task:                 acl  : READ    WRITE    EXECUTE    DEBUG
Task:               admin  : READ
Task:                ancp  : READ    WRITE    EXECUTE    DEBUG
Task:                 atm  : READ    WRITE    EXECUTE    DEBUG
Task:       basic-services  : READ    WRITE    EXECUTE    DEBUG
Task:                bcdl  : READ
Task:                 bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                 bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                boot  : READ    WRITE    EXECUTE    DEBUG
Task:              bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                 cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                 cef  : READ    WRITE    EXECUTE    DEBUG
Task:                 cgn  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:              crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                diag  : READ    WRITE    EXECUTE    DEBUG
Task:             drivers  : READ
Task:                dwdm  : READ    WRITE    EXECUTE    DEBUG
Task:                 eem  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:    ethernet-services  : READ
Task:          ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:              fabric  : READ    WRITE    EXECUTE    DEBUG
Task:           fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:          filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:            firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                  fr  : READ    WRITE    EXECUTE    DEBUG
Task:                hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:       host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:           interface  : READ    WRITE    EXECUTE    DEBUG
Task:           inventory  : READ
Task:         ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                isis  : READ    WRITE    EXECUTE    DEBUG
Task:               l2vpn  : READ    WRITE    EXECUTE    DEBUG
Task:                  li  : READ    WRITE    EXECUTE    DEBUG
Task:             logging  : READ    WRITE    EXECUTE    DEBUG
Task:                lpts  : READ    WRITE    EXECUTE    DEBUG
Task:             monitor  : READ
Task:            mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:         mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:           multicast  : READ    WRITE    EXECUTE    DEBUG
Task:             netflow  : READ    WRITE    EXECUTE    DEBUG
Task:             network  : READ    WRITE    EXECUTE    DEBUG
Task:                ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                ouni  : READ    WRITE    EXECUTE    DEBUG
Task:             pkg-mgmt  : READ
Task:             pos-dpt  : READ    WRITE    EXECUTE    DEBUG
Task:                 ppp  : READ    WRITE    EXECUTE    DEBUG
Task:                 qos  : READ    WRITE    EXECUTE    DEBUG
Task:                 rib  : READ    WRITE    EXECUTE    DEBUG
Task:                 rip  : READ    WRITE    EXECUTE    DEBUG
Task:             root-lr  : READ                                (reserved)
Task:           route-map  : READ    WRITE    EXECUTE    DEBUG
Task:        route-policy  : READ    WRITE    EXECUTE    DEBUG
Task:                 sbc  : READ    WRITE    EXECUTE    DEBUG
Task:                snmp  : READ    WRITE    EXECUTE    DEBUG
Task:           sonet-sdh  : READ    WRITE    EXECUTE    DEBUG
Task:              static  : READ    WRITE    EXECUTE    DEBUG
Task:              sysmgr  : READ
Task:              system  : READ    WRITE    EXECUTE    DEBUG
Task:           transport  : READ    WRITE    EXECUTE    DEBUG
Task:          tty-access  : READ    WRITE    EXECUTE    DEBUG
Task:              tunnel  : READ    WRITE    EXECUTE    DEBUG
Task:           universal  : READ                                (reserved)
Task:                vlan  : READ    WRITE    EXECUTE    DEBUG
Task:                vrrp  : READ    WRITE    EXECUTE    DEBUG
```

次に、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
```

```
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 *2*：*show radius* フィールドの説明

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

show radius accounting

RADIUS アカウンティング 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 *3*：*show radius accounting* フィールドの説明

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

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

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

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、XR EXEC モードで **show radius dead-criteria** コマンドを使用します。

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

構文の説明

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

コマンド デフォルト

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

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

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、XR EXECモードで **show radius server-groups** コマンドを使用します。

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

構文の説明

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

コマンド デフォルト

なし

コマンド モード

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 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ティングのポート番号と一緒に表示されます。

タスク ID

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

```
RP/0/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:
```

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

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

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 *7*：*show tacacs* フィールドの説明

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

show tacacs server-groups

システムに設定されている TACACS+ サーバ グループ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
```

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

フィールド	説明
Server	サーバの IP アドレス。

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

all	（任意）現在ログインしているユーザに関するすべてのユーザ グループとタスク ID を表示します。
authentication	（任意）現在ログインしているユーザの認証方式パラメータを表示します。
group	（任意）現在ログインしているユーザに関連付けられているユーザ グループを表示します。
tasks	（任意）現在ログインしているユーザに関連付けられているタスク ID を表示します。**tasks** キーワードは、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:                 bcdl  : READ    WRITE    EXECUTE    DEBUG
Task:                  bfd  : READ    WRITE    EXECUTE    DEBUG
Task:                  bgp  : READ    WRITE    EXECUTE    DEBUG
Task:                 boot  : READ    WRITE    EXECUTE    DEBUG
Task:               bundle  : READ    WRITE    EXECUTE    DEBUG
Task:                  cdp  : READ    WRITE    EXECUTE    DEBUG
Task:                  cef  : READ    WRITE    EXECUTE    DEBUG
Task:          config-mgmt  : READ    WRITE    EXECUTE    DEBUG
Task:      config-services  : READ    WRITE    EXECUTE    DEBUG
Task:               crypto  : READ    WRITE    EXECUTE    DEBUG
Task:                 diag  : READ    WRITE    EXECUTE    DEBUG
Task:              drivers  : READ    WRITE    EXECUTE    DEBUG
Task:               eigrp  : READ    WRITE    EXECUTE    DEBUG
Task:           ext-access  : READ    WRITE    EXECUTE    DEBUG
Task:               fabric  : READ    WRITE    EXECUTE    DEBUG
Task:           fault-mgr  : READ    WRITE    EXECUTE    DEBUG
Task:          filesystem  : READ    WRITE    EXECUTE    DEBUG
Task:            firewall  : READ    WRITE    EXECUTE    DEBUG
Task:                  fr  : READ    WRITE    EXECUTE    DEBUG
Task:                hdlc  : READ    WRITE    EXECUTE    DEBUG
Task:        host-services  : READ    WRITE    EXECUTE    DEBUG
Task:                hsrp  : READ    WRITE    EXECUTE    DEBUG
Task:           interface  : READ    WRITE    EXECUTE    DEBUG
Task:           inventory  : READ    WRITE    EXECUTE    DEBUG
Task:          ip-services  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv4  : READ    WRITE    EXECUTE    DEBUG
Task:                ipv6  : READ    WRITE    EXECUTE    DEBUG
Task:                isis  : READ    WRITE    EXECUTE    DEBUG
Task:             logging  : READ    WRITE    EXECUTE    DEBUG
Task:                lpts  : READ    WRITE    EXECUTE    DEBUG
Task:             monitor  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-ldp  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-static  : READ    WRITE    EXECUTE    DEBUG
Task:             mpls-te  : READ    WRITE    EXECUTE    DEBUG
Task:             multicast  : READ    WRITE    EXECUTE    DEBUG
Task:             netflow  : READ    WRITE    EXECUTE    DEBUG
Task:             network  : READ    WRITE    EXECUTE    DEBUG
Task:                ospf  : READ    WRITE    EXECUTE    DEBUG
Task:                ouni  : READ    WRITE    EXECUTE    DEBUG
```

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

次に、**show user** コマンドによる、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:                 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
```

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、アカウンティング要求でこの TCP 接続が使用されるようにする例を示します。この

設定は、TACACS+ サーバも単一接続モードで設定されている場合に限り機能します。TACACS+ サーバを単一接続モードで設定する方法については、各サーバのマニュアルを参照してください。

```
RP/0/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

host-name	TACACS+ サーバのホスト名またはドメイン名または IP アドレス。
port*port-number*	（任意）サーバのポート番号を指定します。この設定によって、デフォルトのポート 49 は上書きされます。有効なポート番号の範囲は 1 ～ 65535 です。
timeout*seconds*	（任意）認証、許可、アカウンティング（AAA）サーバが TACACS+ サーバからの応答を待機する時間の長さを設定するタイムアウト値を指定します。このオプションは、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。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 config-tacacs-host サブモードでのみ使用できます。
key[**0** | **7**] *auth-key*	（任意）AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。TACACS+ パケットは、このキーを使って暗号化されます。このキーは TACACS+ デーモンで使用されるキーと一致する必要があります。このキーを指定すると、このサーバに対して **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。 （任意）**0** 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）**7** 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。 *auth-key* 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 config-tacacs-host サブモードでのみ使用できます。
single-connection	（任意）単一の TCP 接続を介してこのサーバにすべての TACACS+ 要求を多重送信します。デフォルトでは、セッションごとに別個の接続が使用されます。 注：このパラメータは config-tacacs-host 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

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

コマンド デフォルト

なし

コマンド モード

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す。

- <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

type	インターフェイス タイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
path-id	物理インターフェイスまたは仮想インターフェイス。 （注） 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 **showinterfaces** 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。
vrf*vrf-id*	割り当てられている VRF の名前を指定します。

コマンド デフォルト

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

コマンド モード

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

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

コマンド デフォルト

新しく作成したタスク グループには、タスク ID は割り当てられません。

コマンド モード

タスク グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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

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

コマンド デフォルト

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

コマンド モード

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、およびアカウンティング（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

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

user-name	ユーザ名。*user-name* 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。
password	（任意）名前付きユーザにパスワードを作成できます。
0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。シスコ独自の暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。
7	（任意）暗号化パスワードが続くことを指定します。
password	（任意）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。
secret	（任意）名前付きユーザに対して、MD5 で保護されたパスワードを作成できます。
0	（任意）暗号化されていない（クリアテキスト）パスワードが続くことを指定します。MD5 暗号化アルゴリズムを使用した設定では、パスワードは保存用に暗号化されます。
5	（任意）暗号化パスワードが続くことを指定します。
group	（任意）名前付きユーザをユーザ グループに関連付けることができます。
usergroup-name	（任意）**usergroup** コマンドで定義したユーザ グループの名前。

コマンド デフォルト

システムにユーザ名は定義されません。

コマンド モード

XR コンフィギュレーション モード

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

（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/RSP0/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 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

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

コマンド デフォルト

なし

コマンド モード

回線テンプレート コンフィギュレーション

コマンド履歴

リリース	変更内容
リリース 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
```

キーチェーン管理コマンド

ここでは、キーチェーン管理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。

キーチェーン管理の概念、設定作業、および例については、『*System Security Configuration Guide for Cisco NCS 5000 Series Routers*』の「Implementing Keychain Management」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。

accept-lifetime

キーチェーン上の認証キーが有効であるとして受信される時間を設定するには、キー コンフィギュレーション モードで **accept-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

accept-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

no accept-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

構文の説明

start-time	キーが有効になる開始時間を *hh:mm:ss* 日月年の形式で指定します。範囲は 0:0:0 ～ 23:59:59 です。 日付の範囲は 1 ～ 31 です。 年の範囲は 1993 ～ 2035 です。
duration*duration value*	（任意）キーのライフタイムを秒で指定します。範囲は、1～2147483646 です。
infinite	（任意）有効になった後、そのキーが期限切れにならないことを示します。
end-time	（任意）キーが期限切れとなる時刻を *hh:mm:ss* 日月年の形式で指定します。範囲は 0:0:0 ～ 23:59:59 です。

コマンド デフォルト

なし

コマンド モード

キー 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

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
system	読み取り、書き込み

例

次に、**accept-lifetime** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# accept-lifetime 1:00:00 June 29 2006 infinite
```

accept-tolerance

ピアが使用する accept キーに許容度または制限値を秒単位で指定するには、キーチェーン コンフィギュレーション モードで **accept-tolerance** 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。

accept-tolerance [*value*| **infinite**]

no accept-tolerance [*value*| **infinite**]

構文の説明

value	（任意）秒で示される許容値の範囲。範囲は、1 ～ 8640000 です。
infinite	（任意）指定された許容値が無限であることを示します。この受け入れキーは期限切れになりません。無限の許容限度は、受け入れキーが常に受け入れ可能であり、ピアが使用する際に検証されることを意味します。

コマンド デフォルト

デフォルト値は、許容しないことを意味する 0 です。

コマンド モード

キーチェーン 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

command コマンドを設定しない場合は、許容度値はゼロに設定されます。

キーが有効なライフタイムの範囲外にある場合でも、許容限度内にあればそのキーは受け入れ可能と判断されます（たとえば、ライフタイムの開始前やライフタイムの終了後など）。

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**accept-tolerance** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# accept-tolerance infinite
```

cryptographic-algorithm

キーIDに設定したキー文字列を使用してパケットに適用する暗号化アルゴリズムの選択を指定するには、キーチェーン キー コンフィギュレーション モードで **cryptographic-algorithm** 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。

cryptographic-algorithm [**HMAC-MD5**| **HMAC-SHA1-12**| **HMAC-SHA1-20**| **MD5**| **SHA-1**]

no cryptographic-algorithm [**HMAC-MD5**| **HMAC-SHA1-12**| **HMAC-SHA1-20**| **MD5**| **SHA-1**]

構文の説明

HMAC-MD5	HMAC-MD5 をダイジェスト サイズ 16 バイトの暗号化アルゴリズムとして設定します。
HMAC-SHA1-12	HMAC-SHA1-12 をダイジェスト サイズ 12 バイトの暗号化アルゴリズムとして設定します。
HMAC-SHA1-20	HMAC-SHA1-20 をダイジェスト サイズ 20 バイトの暗号化アルゴリズムとして設定します。
MD5	MD5 をダイジェスト サイズ 16 バイトの暗号化アルゴリズムとして設定します。
SHA-1	SHA-1-20 をダイジェスト サイズ 20 バイトの暗号化アルゴリズムとして設定します。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

キーチェーンのキー 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

暗号化アルゴリズムを設定しない場合、MAC 計算と API 検証は無効になります。

各プロトコルがサポートする暗号化アルゴリズムは次のとおりです。

- ボーダー ゲートウェイ プロトコル（BGP）は HMAC-MD5 と HMAC-SHA1-12 だけをサポート
- Intermediate System-to-Intermediate System（IS-IS）は HMAC-MD5 だけをサポート
- Open Shortest Path First（OSPF）は MD5 だけをサポート

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**ryptographic-algorithm** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# cryptographic-algorithm HMAC-MD5
```

key（キーチェーン）

キーチェーン キーを作成または変更するには、キーチェーン キー コンフィギュレーション モードで **key** 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 *key-id*

no key *key-id*

構文の説明

key-id	48 ビット整数型のキー ID。範囲は 0 ～ 281474976710655 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

キーチェーンのキー 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

Border Gateway Protocol（BGP）のキーチェーン設定では、*key-id* 引数の範囲は 0 ~ 53 である必要があります。この範囲が 63 の値を超えると、BGP キーチェーンの操作は拒否されます。

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**key** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
```

```
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)#
```

key chain（キーチェーン）

キーチェーンを作成または変更するには、**key chain** 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 chain *key-chain-name*

no key chain *key-chain-name*

構文の説明

key-chain-name	キーチェーンの名前を指定します。最大文字数は 48 です。

コマンド デフォルト

デフォルトの動作または値はありません。

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

ボーダー ゲートウェイ プロトコル（BGP）のキーチェーンは、ネイバー、セッション グループ、またはネイバー グループとして設定できます。BGP はこのキーチェーンを使用して、ヒットしないキー更新を認証にインプリメントできます。

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、キーチェーンの isis キーの名前が **key chain** コマンド用である例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
```

```
RP/0/RP0/CPU0:router(config-isis-keys)#
```

key-string（キーチェーン）

キーにテキスト文字列を指定するには、キーチェーン キー コンフィギュレーション モードで **key-string** 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-string [**clear**| **password**] *key-string-text*

no key-string [**clear**| **password**] *key-string-text*

構文の説明

clear	キー文字列をクリアテキスト形式で指定します。
password	キーを暗号化形式で指定します。
key-string-text	キーのテキスト文字列。パーサー プロセスによって暗号化されてから、設定に保存されます。テキスト文字列には、次の文字制限があります。 • プレーン テキストのキー文字列：最小 1 文字、最大 32 文字。 • 暗号化されたキー文字列：最小 4 文字、上限はなし。

コマンド デフォルト

デフォルト値は clear です。

コマンド モード

キーチェーンのキー 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

暗号化パスワードが有効であるためには、次の条件を満たしている必要があります。

- 文字列に 4 文字以上の偶数個の文字が含まれている。
- パスワード文字列の最初の 2 文字は 10 進数、残りの文字は 16 進数である。
- 最初の 2 桁は 53 以下である。

次の例は、どちらも有効な暗号化パスワードです。

1234abcd

または

50aefd

タスク ID

タスク ID	動作
system	読み取り、書き込み

例

次に、**keystring** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router:# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# key-string password 850aefd
```

send-lifetime

有効なキーを送信し、ローカル ホストからピアへの情報を認証するには、キーチェーン キー コンフィギュレーション モードで **send-lifetime** 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。

send-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

no send-lifetime *start-time* [**duration** *duration value*| **infinite**| *end-time*]

構文の説明

start-time	キーが有効になる開始時間を *hh:mm:ss* 日月年の形式で指定します。範囲は 0:0:0 ～ 23:59:59 です。 日付の範囲は 1 ～ 31 です。 年の範囲は 1993 ～ 2035 です。
duration*duration value*	（任意）キーのライフタイムを秒で指定します。
infinite	（任意）一旦有効になると、そのキーは期限切れにならないことを示します。
end-time	（任意）キーが期限切れとなる時刻を *hh:mm:ss* 日月年の形式で指定します。範囲は 0:0:0 ～ 23:59:59 です。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

キーチェーンのキー 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

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
system	読み取り、書き込み

例

次に、**send-lifetime** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# key chain isis-keys
RP/0/RP0/CPU0:router(config-isis-keys)# key 8
RP/0/RP0/CPU0:router(config-isis-keys-0x8)# send-lifetime 1:00:00 June 29 2006 infinite
```

show key chain

キーチェーンを表示するには、**show key chain** コマンドを使用します。

show key chain *key-chain-name*

構文の説明

key-chain-name	指定したキーチェーンのキーの名前です。最大文字数は32です。

コマンド デフォルト

パラメータを指定せずにコマンドを使用すると、すべてのキー チェーンのリストを表示します。

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

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
system	読み取り

例

セキュアなキーストレージが使用可能になった場合は、ユーザにマスターパスワードの入力を要求し、暗号化してからキー ラベルを表示するのが、キーチェーン管理にとっては望ましい方法です。次に、**show key chain** コマンドで暗号化されたキー ラベルのみを表示する例を示します。

```
RP/0/RP0/CPU0:router# show key chain isis-keys

Key-chain: isis-keys/ -

accept-tolerance -- infinite
Key 8 -- text "8"
  cryptographic-algorithm -- MD5
```

```
Send lifetime:   01:00:00, 29 Jun 2006 - Always valid  [Valid now]
Accept lifetime: 01:00:00, 29 Jun 2006 - Always valid [Valid now]
```

セキュア シェル コマンド

ここでは、セキュア シェル（SSH）を設定するために使用される Cisco IOS XR ソフトウェア コマンドについて説明します。

SSH 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「Implementing Secure Shell」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。

clear ssh

着信または発信セキュア シェル（SSH）接続を終了するには、**clear ssh** コマンドを使用します。

clear ssh {*session-id*| **outgoing** *session-id*}

構文の説明

session-id	**show ssh** コマンドの出力で表示される着信接続のセッション ID 番号。範囲は 0 ～ 1024 です。
outgoing*session-id*	**show ssh** コマンドの出力での表示のとおりに、発信接続のセッション ID 番号を指定します。指定できる範囲は 1 ～ 10 です。

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

clear ssh コマンドを使用して着信 SSH 接続または発信 SSH 接続を切断します。着信接続は、ローカル ネットワーキング デバイス上で実行している SSH サーバによって管理されます。発信接続は、ローカル ネットワーキング デバイスから開始されます。

接続のセッション ID を表示するには、**show ssh** コマンドを使用します。

タスク ID

タスク ID	動作
crypto	実行

例

次に、**show ssh** コマンドを使用して、ルータに対するすべての着信接続および発信接続を表示します。その後で、**clear ssh** コマンドを使用し、ID 番号 0 で着信セッションを終了します。

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

SSH version: Cisco-2.0
session     pty  location   state       userid     host        ver
--------------------------------------------------------------------
Incoming sessions
0           vty0 0/33/1  SESSION_OPEN   cisco   172.19.72.182   v2
1           vty1 0/33/1  SESSION_OPEN   cisco   172.18.0.5      v2
2           vty2 0/33/1  SESSION_OPEN   cisco   172.20.10.3     v1
3           vty3 0/33/1  SESSION_OPEN   cisco   3333::50        v2

Outgoing sessions
1               0/33/1  SESSION_OPEN    cisco   172.19.72.182   v2
2               0/33/1  SESSION_OPEN    cisco   3333::50        v2

RP/0/RP0/CPU0:router# clear ssh 0
```

次に、リリース 6.0 以降に適用される **clear ssh** の出力を示します。

```
RP/0/RP0/CPU0:router# show ssh
SSH version : Cisco-2.0


id  chan pty     location        state           userid    host                  ver
authentication connection type
-----------------------------------------------------------------------------------------------
Incoming sessions
0   1    vty0    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   2    vty1    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   3            0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.57.75           v2
rsa-pubkey     Sftp-Subsystem
1       vty7    0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.22.57          v1  password
       Command-Line-Interface
3   1           0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2  password
       Netconf-Subsystem
4   1    vty3    0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.55          v2  password
       Command-Line-Interface

Outgoing sessions
1               0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.51          v2  password

RP/0/RP0/CPU0:router# clear ssh 0
```

clear netconf-yang agent session

指定した netconf エージェント セッションをクリアするには、EXEC モードで **clear netconf-yang agent session** を使用します。

clear netconf-yang agent session *session-id*

構文の説明

session-id	クリアする必要があるセッション ID。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更内容
リリース 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。

show netconf-yang clients コマンドを使用して必要なセッション ID を取得できます。

タスク ID

タスク ID	動作
config-services	読み取り、書き込み

例

次に、**clear netconf-yang agent session** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  clear netconf-yang agent session 32125
```

netconf-yang agent ssh

SSH（セキュア シェル）で netconf エージェントをイネーブルにするには、グローバル コンフィギュレーション モードで **netconf-yang agent ssh** コマンドを使用します。netconf 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。

netconf-yang agent ssh

nonetconf-yang agent ssh

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

グローバル設定

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

現在、SSH は Netcof でサポートされている転送方式です。

タスク ID

タスク ID	動作
config-services	読み取り、書き込み

例

次に、**netconf-yang agent ssh** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  netconf-yang agent ssh
```

sftp

セキュア FTP（SFTP）クライアントを起動するには、**sftp** コマンドを使用します。

sftp [*username* **@** *host* : *remote-filenam* **e**] *source-filename dest-filename* [**source-interface** *type interface-path-id*] [**vrf** *vrf-name*]

構文の説明

username	（任意）ファイル転送を実行するユーザの名前。ユーザ名のあとにアットマーク（@）が必要です。
*hostname:remote-filenam*e	（任意）Secure Shell File Transfer Protocol（SFTP; セキュア シェル ファイル転送プロトコル）サーバの名前。ホスト名のあとにコロン（:）が必要です。
source-filename	SFTP の発信元（パスを含む）
dest-filename	SFTP の宛先（パスを含む）
source-interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。詳細については、疑問符（**?**）オンラインヘルプ機能を使用してください。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） 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 EXEC モードで **showinterfaces** 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。
vrf*vrf-name*	発信元インターフェイスに対応づける VRF の名前を指定します。

コマンド デフォルト

username 引数を指定しない場合は、ルータのログイン名が使用されます。*hostname* 引数を指定しない場合は、ファイルがローカルと見なされます。

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

SFTP では、ルータとリモート ホストの間でファイルの安全な（および認証された）コピーを行うことができます。**copy** コマンドと同様に、**sftp** コマンドは XR EXEC モードでのみ呼び出すことができます。

ユーザ名を省略すると、ルータのログイン名がデフォルトとして使用されます。ホスト名を省略すると、ファイルはローカルにあると見なされます。

送信元インターフェイスが **sftp** コマンド内に指定されている場合、**sftp** インターフェイスは **ssh client source-interface** コマンド内に指定されているインターフェイスよりも優先されます。

ファイルの宛先がローカルパスの場合、すべての発信元ファイルがリモートホスト上になければなりません。その逆の場合も同様です。

複数の発信元ファイルが存在する場合、宛先は、すでに存在するディレクトリでなければなりません。それ以外の場合、宛先には、ディレクトリ名または宛先ファイル名のいずれかを指定できます。ファイルの発信元をディレクトリ名にはできません。

ファイルを複数のリモート ホストからダウンロードする場合、つまり、発信元に複数のリモートホストを指定すると、SFTP クライアントによって SSH インスタンスがホストごとに生成されます。そのため、ユーザ認証を複数回要求されることがあります。

タスク ID

タスク ID	動作
crypto	実行
basic-services	実行

例

次の例では、ユーザ *abc* がファイル *ssh.diff* を SFTP サーバの *ena-view1* から *disk0* にダウンロードします。

```
RP/0/RP0/CPU0:router#sftp abc@ena-view1:ssh.diff disk0
```

次の例では、ユーザ *abc* が disk 0:/sam_* から ena-view1 というリモート SFTP サーバ上の /users/abc/ に複数のファイルをアップロードします。

```
RP/0/RP0/CPU0:router# sftp disk0:/sam_* abc@ena-view1:/users/abc/
```

次の例では、ユーザ *admin* が IPv6 アドレスを使用してファイル *run* を *disk0a:* からローカル SFTP サーバ上の *disk0:/v6copy* にダウンロードします。

```
RP/0/RP0/CPU0:router#sftp admin@[2:2:2::2]:disk0a:/run disk0:/V6copy
Connecting to 2:2:2::2...
Password:

disk0a:/run
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (338172)bytes/sec

RP/0/RP0/CPU0:router#dir disk0:/V6copy

Directory of disk0:

70144       -rwx  308413      Sun Oct 16 23:06:52 2011  V6copy

2102657024 bytes total (1537638400 bytes free)
```

次の例では、ユーザ *admin* が IPv6 アドレスを使用してファイル *v6copy* を *disk0:* からローカル SFTP サーバ上の *disk0a:/v6back* にアップロードします。

```
RP/0/RP0/CPU0:router#sftp disk0:/V6copy admin@[2:2:2::2]:disk0a:/v6back
Connecting to 2:2:2::2...
Password:

/disk0:/V6copy
  Transferred 308413 Bytes
  308413 bytes copied in 0 sec (421329)bytes/sec

RP/0/RP0/CPU0:router#dir disk0a:/v6back

Directory of disk0a:

66016       -rwx  308413      Sun Oct 16 23:07:28 2011  v6back

2102788096 bytes total (2098987008 bytes free)
```

次の例では、ユーザ *admin* が IPv4 アドレスを使用してファイル *sampfile* を *disk0:* からローカル SFTP サーバ上の *disk0a:/sampfile_v4* にダウンロードします。

```
RP/0/RP0/CPU0:router#sftp admin@2.2.2.2:disk0:/sampfile disk0a:/sampfile_v4
Connecting to 2.2.2.2...
Password:

disk0:/sampfile
  Transferred 986 Bytes
  986 bytes copied in 0 sec (493000)bytes/sec

RP/0/RP0/CPU0:router#dir disk0a:/sampfile_v4

Directory of disk0a:

131520      -rwx  986         Tue Oct 18 05:37:00 2011  sampfile_v4

502710272 bytes total (502001664 bytes free)
```

次の例では、ユーザ *admin* が IPv4 アドレスを使用してファイル *sampfile_v4* を *disk0a:* からローカル SFTP サーバ上の *disk0:/sampfile_back* にアップロードします。

```
RP/0/RP0/CPU0:router#sftp disk0a:/sampfile_v4 admin@2.2.2.2:disk0:/sampfile_back
Connecting to 2.2.2.2...
Password:

disk0a:/sampfile_v4
```

```
  Transferred 986 Bytes
  986 bytes copied in 0 sec (564000)bytes/sec

RP/0/RP0/CPU0:router#dir disk0:/sampfile_back

Directory of disk0:

121765      -rwx  986         Tue Oct 18 05:39:00 2011  sampfile_back

524501272 bytes total (512507614 bytes free)
```

sftp（インタラクティブ モード）

ユーザをイネーブルにして、セキュア FTP（SFTP）クライアントを起動するには、**sftp** コマンドを使用します。

sftp [*username* **@** *host* : *remote-filenam* **e**] [**source-interface** *type interface-path-id*]

構文の説明

username	（任意）ファイル転送を実行するユーザの名前。ユーザ名のあとにアットマーク（@）が必要です。
hostname:remote-filename	（任意）Secure Shell File Transfer Protocol（SFTP; セキュア シェル ファイル転送プロトコル）サーバの名前。ホスト名のあとにコロン（:）が必要です。
source-interface	（任意）すべての発信 SSH 接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。詳細については、疑問符（**?**）オンライン ヘルプ機能を使用してください。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） 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 EXEC モードで **showinterfaces** 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。

コマンド デフォルト

username 引数を指定しない場合は、ルータのログイン名が使用されます。*hostname* 引数を指定しない場合は、ファイルがローカルと見なされます。

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

SFTP クライアントは、インタラクティブ モードで、ユーザがサポートされているコマンドを入力できるセキュアな SSH チャネルを作成します。ユーザがインタラクティブ モードで SFTP クライアントを起動すると、SFTP クライアント プロセスによってセキュアな SSH チャネルが作成され、ユーザがサポートされているコマンドを入力できるエディタが開きます。

複数の要求を SFTP サーバに送信してコマンドを実行することができます。サーバに対する「未確認」または未処理の要求に数の制限はありませんが、サーバは便宜上これらの要求をバッファリングするか、またはキューに入れる場合があります。このため、要求の順番に論理的な順序があることがあります。

インタラクティブ モードでサポートされる UNIX ベース コマンドは次のとおりです。

- bye
- **cd**<*path*>
- **chmod**<*mode*> <*path*>
- exit
- **get**<*remote-path*> *[local-path]*
- help
- **ls***[-alt] [path]*
- **mkdir<path>**
- **put**<*local-path*> *[remote-path]*
- pwd
- quit
- **rename<old-path> <new-path>**
- **rmdir<path>**
- **rm<path>**

次のコマンドはサポートされません。

- lcd、lls、lpwd、lumask、lmkdir
- ln、symlink
- chgrp、chown
- !、！コマンド
- ?
- mget、mput

タスク ID

タスク ID	動作
crypto	実行
basic-services	実行

例

次の例では、ユーザ *admin* が IPv6 アドレスを使用して外部 SFTP サーバに対してファイルをダウンロードおよびアップロードします。

```
RP/0/RP0/CPU0:router#sftp admin@[2:2:2::2]

Connecting to 2:2:2::2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/admin
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/admin/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

次の例では、ユーザ *abc* が IPv4 アドレスを使用して外部 SFTP サーバに対してファイルをダウンロードおよびアップロードします。

```
RP/0/RP0/CPU0:router#sftp abc@2.2.2.2
Connecting to 2.2.2.2...
Password:
sftp> pwd
Remote working directory: /
sftp> cd /auto/tftp-server1-users5/abc
sftp> get frmRouter /disk0:/frmRouterdownoad

/auto/tftp-server1-users5/abc/frmRouter
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (27684)bytes/sec
sftp> put /disk0:/frmRouterdownoad againtoServer

/disk0:/frmRouterdownoad
  Transferred 1578 Bytes
  1578 bytes copied in 0 sec (14747)bytes/sec
sftp>
```

show netconf-yang clients

netconf-yangに関するクライアントの詳細情報を表示するには、XR EXECモードで**show netconf-yang clients** コマンドを使用します。

show netconf-yang clients

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

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
config-services	読み取り

例

次に、**show netconf-yang clients** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  sh netconf-yang clients
Netconf clients
client session ID|   NC version|    client connect time|        last OP time|        last
OP type|    <lock>|
 22969|                     1.1|          0d  0h  0m  2s|            11:11:24|
close-session|        No|
 15389|                     1.1|          0d  0h  0m  1s|            11:11:25|
get-config|        No|
```

表 *9*：フィールド説明

フィールド名	説明
Client session ID	割り当てられたセッション ID
NC version	hello メッセージでアドバタイズされる Netconf クライアントのバージョン
Client connection time	クライアントが接続されてからの経過時間
Last OP time	最終操作時刻
Last OP type	最終操作タイプ
Lock（yes または no）	設定データストアにセッションのロックが保持されているかどうかを確認します。

show netconf-yang statistics

netconf-yangに関する統計詳細情報を表示するには、システム管理EXECモードで**show netconf-yang statistics** コマンドを使用します。

show netconf-yang statistics

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

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
config-services	読み取り

例

次に、**show netconf-yang statistics** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  sh netconf-yang statistics
Summary statistics
                          # requests|             total time|   min time per request|   max
 time per request|   avg time per request|
other                              0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
close-session                      4|       0h  0m  0s   3ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
kill-session                       0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get-schema                         0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get                                0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
```

```
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
get-config                          1|       0h  0m  0s   1ms|       0h  0m  0s   1ms|
 0h  0m  0s   1ms|       0h  0m  0s   1ms|
edit-config                         3|       0h  0m  0s   2ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
commit                              0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
cancel-commit                       0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
lock                                0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
unlock                              0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
discard-changes                     0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
validate                            0|       0h  0m  0s   0ms|       0h  0m  0s   0ms|
 0h  0m  0s   0ms|       0h  0m  0s   0ms|
xml parse                           8|       0h  0m  0s   4ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
netconf processor                   8|       0h  0m  0s   6ms|       0h  0m  0s   0ms|
 0h  0m  0s   1ms|       0h  0m  0s   0ms|
```

表 *10*：フィールド説明

フィールド名	説明
Requests	特定のタイプの処理済みの要求の総数
Total time	特定のタイプのすべての要求の合計処理時間
Min time per request	特定のタイプの要求の最小処理時間
Max time per request	特定のタイプの要求の最大処理時間
Avg time per request	要求タイプの平均処理時間

show ssh

ルータに対するすべての発着信接続を表示するには、**show ssh** コマンドを使用します。

show ssh

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 ssh コマンドを使用して、セキュア シェル（SSH）バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）のすべての発着信接続を表示します。

タスク ID

タスク ID	動作
crypto	読み取り

例

次に、SSH がイネーブルになっている場合の **show ssh** コマンドによる出力の例を示します。

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

SSH version : Cisco-2.0

id  pty   location    state         userid    host          ver       authentication
-----------------------------------------------------------------------------------------------------------------
Incoming sessions

Outgoing sessions
1         0/3/CPU0    SESSION_OPEN    lab     12.22.57.     v2        password
```

```
2          0/3/CPU0     SESSION_OPEN    lab     12.22.57.75   v2         keyboard-interactive
```

次に、IOS-XR 6.0 リリース以降に適用される **show ssh** コマンドの出力を示します。

```
RP/0/RP0/CPU0:router# show ssh
SSH version : Cisco-2.0

id  chan pty     location        state           userid    host                  ver
authentication connection type
-----------------------------------------------------------------------------------------------------------------
Incoming sessions
0   1    vty0    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   2    vty1    0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2
rsa-pubkey     Command-Line-Interface
0   3            0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.57.75           v2
rsa-pubkey     Sftp-Subsystem
1       vty7    0/RSP0/CPU0     SESSION_OPEN    cisco     12.22.22.57          v1  password
       Command-Line-Interface
3   1           0/RSP0/CPU0     SESSION_OPEN    lab       12.22.57.75           v2  password
       Netconf-Subsystem
4   1    vty3    0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.55          v2  password
       Command-Line-Interface

Outgoing sessions
1              0/RSP0/CPU0     SESSION_OPEN    lab       192.168.1.51          v2  password
```

次の表に、この出力で表示される重要フィールドの説明を示します。

表 *11*：*show ssh* フィールドの説明

フィールド	説明
session	着信および発信 SSH 接続のセッション ID。
chan	着信（v2）SSH接続のチャネルID。SSH v1 セッションについては NULL。
pty	着信セッションに割り当てられた仮想端末ID。発信 SSH 接続の場合は Null になります。
location	着信接続用のSSHサーバの場所を指定します。発信接続の場合、location は、SSH セッションがどのルートプロセッサから開始されるかを示します。
state	接続の現在の SSH 状態。
userid	ルータへ、またはルータからの接続に使用される認証、許可、アカウンティング（AAA）ユーザ名
host	リモート ピアの IP アドレス

フィールド	説明
ver	接続タイプが SSHv1 と SSHv2 のいずれであるかを示します。
authentication	ユーザが選択した認証方式のタイプを指定します。
connection type	この接続で実行されるアプリケーション（コマンドライン インターフェイス、リモート コマンド、SCP、SFTP サブシステム、または Netconf サブシステム）を指定します。

show ssh session details

セキュア シェル バージョン2（SSHv2）のすべての発着信接続に関する詳細情報を表示するには、**show ssh session details** コマンドを使用します。

show ssh session details

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 ssh session details コマンドを使用して、ルータに対する SSHv2 接続に関する特定のセッションに選択した暗号を含む詳細レポートを表示します。

タスク ID

タスク ID	動作
crypto	読み取り

例

次に、SSHv2 のすべての発着信接続に関する詳細を表示する **show ssh session details** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# show ssh session details

SSH version: Cisco-2.0
session     key-exchange   pubkey   incipher   outcipher    inmac     outmac
---------------------------------------------------------------------------
Incoming Session

0           diffie-hellman ssh-dss  3des-cbc   3des-cbc     hmac-md5  hmac-md5
```

```
Outgoing connection

1           diffie-hellman ssh-dss  3des-cbc   3des-cbc     hmac-md5  hmac-md5
```

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 *12*：*show ssh session details* フィールドの説明

フィールド	説明
session	着信および発信 SSH 接続のセッション ID。
key-exchange	相互に認証するために両方のピアによって選択されたキー交換アルゴリズム。
pubkey	キー交換用に選択された公開キー アルゴリズム。
incipher	Rx トラフィック用に選択された暗号化。
outcipher	Tx トラフィック用に選択された暗号化。
inmac	Rx トラフィック用に選択された認証（メッセージ ダイジェスト）アルゴリズム。
outmac	Tx トラフィック用に選択された認証（メッセージ ダイジェスト）アルゴリズム。

ssh

セキュア シェル（SSH）クライアント接続を開始し、SSHサーバへのアウトバウンド接続をイネーブルにするには、**ssh** コマンドを使用します。

ssh {**ipv4-address**| **ipv6-address**| **hostname**} [**username** *user-id*] [**cipher aes** {**128-cbc**| **192-cbc**| **256-cbc**}][**source-interface** *type interface-path-id*][**command***command-name*]

構文の説明

ipv4-address	A:B:C:D 形式の IPv4 アドレス。
ipv6-address	X:X::X 形式の IPv6 アドレス。
hostname	リモート ノードのホスト名。このホスト名に IPv4 アドレスと IPv6 アドレスの両方が設定されている場合、IPv6 アドレスが使用されます。
username*user-id*	（任意）SSH サーバを実行しているリモート ネットワーキング デバイスにログインするときに使用するユーザ名を指定します。ユーザ ID を省略すると、デフォルトとして現在のユーザ ID が使用されます。
cipheraes	（任意）SSH クライアント接続の暗号化として Advanced Encryption Standard（AES）を指定します。 （注） 管理者によって特定の暗号化が指定されていない場合、クライアントは互換性を確保するためにデフォルトとしてトリプルDESを提案します。
128-CBC	CBC モードの 128 ビット キー。
192-CBC	CBC モードの 192 ビット キー。
256-CBC	CBC モードの 256 ビット キー。
source interface	（任意）すべての発信SSH接続に対して、選択したインターフェイスの発信元 IP アドレスを指定します。
type	インターフェイス タイプ。詳細については、疑問符（**?**）オンライン ヘルプ機能を使用してください。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） 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 EXEC モードで **showinterfaces** 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。

command	（任意）リモート コマンドを指定します。このキーワードを追加すると、インタラクティブ セッションを開始するのではなく、非インタラクティブ モードで **ssh** コマンドを解析し、実行するように SSHv2 に要求します。

コマンド デフォルト

3DES cipher

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

ssh コマンドを使用して、アウトバウンド クライアント接続を行います。SSH クライアントにより、リモート ピアへの SSHv2 接続が試みられます。リモート ピアで SSHv1 サーバしかサポートされていない場合、リモート サーバへの SSHv1 接続が内部生成されます。リモート ピアのバージョンの検出と適切なクライアント接続の生成のプロセスは、ユーザからは見えません。

VRF が **ssh** コマンドに指定されている場合は、**ssh** インターフェイスが ssh client source-interface, （166 ページ）コマンドで指定されたインターフェイスよりも優先されます。

cipher aes を設定した場合は、指定した 1 つ以上のキーサイズを含めて、SSH サーバへの要求の一部として SSH クライアントが提案を行います。SSH サーバは、サーバがサポートする暗号化およびクライアントの提案に基づいて最適な暗号化を選択します。

（注） AES 暗号化アルゴリズムは、SSHv1 サーバおよびクライアントではサポートされていません。SSHv2 クライアントから SSHv1 サーバに送信された AES 暗号の要求はすべて無視されます。代わりにサーバではトリプル DES を使用します。

SSH を実行するには VRF が必要ですが、これはデフォルト VRF またはユーザによって指定された VRF のいずれかです。ssh client source-interface, （166 ページ）または ssh client knownhost, （164 ページ）コマンドの設定時に VRF を指定しなかった場合は、デフォルトの VRF が使用されます。

command キーワードを使用して、SSHv2 サーバをイネーブルにし、インタラクティブ セッションを開始するのではなく、非インタラクティブ モードで **ssh** コマンドを解析し、実行します。

タスク ID

タスク ID	動作
crypto	実行
basic-services	実行

例

次に、アウトバウンド SSH クライアント接続をイネーブルにする **ssh** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# ssh vrf green  username userabc

Password:
Remote-host>
```

ssh client knownhost

サーバ パブリック キー（pubkey）を認証するには、**ssh client knownhost** コマンドを使用します。サーバ pubkey の認証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。

ssh client knownhost device:/**filename**

no ssh client knownhost device:/**filename**

構文の説明

device:/*filename*	ファイル名の完全なパス（たとえば、slot0:/server_pubkey）。コロン（:）とスラッシュ（/）が必要です。

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

サーバ *pubkey* は、クライアント側で全員が知る公開キーとキーのオーナーしか知らない秘密キーの 2 つのキーを使用する暗号化システムです。証明書がない場合、サーバ pubkey は、アウトオブバンドセキュア チャネルを介してクライアントに転送されます。クライアントでは、この pubkey がローカルデータベースに保存され、セッション構築ハンドシェイクのキーネゴシエーションの初期段階にサーバから提供されたキーと比較されます。キーが一致しない、またはクライアントのローカル データベースにキーが見つからない場合、セッションを許可するか拒否するかを確認するプロンプトが表示されます。

サーバ pubkey が、アウトオブバンド セキュア チャネルを介して最初に取得されたときに、ローカル データベースに保存されることが動作の前提条件になっています。このプロセスは、UNIX 環境でセキュア シェル（SSH）の実装に採用されている現行のモデルと同じです。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次に、**ssh client knownhost** コマンドによる出力の例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh client knownhost disk0:/ssh.knownhost
RP/0/RP0/CPU0:router(config)# commit
RP/0/RP0/CPU0:router# ssh host1 username user1234
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Password:
RP/0/RP0/CPU0:host1# exit
RP/0/RP0/CPU0:router# ssh host1 username user1234
```

ssh client source-interface

すべての発信セキュア シェル（SSH）接続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、**ssh client 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。

ssh client source-interface *type interface-path-id*

no ssh client source-interface *type interface-path-id*

構文の説明

type	インターフェイスタイプ。詳細については、疑問符（?）オンライン ヘルプ機能を使用します。
interface-path-id	物理インターフェイスまたは仮想インターフェイス。 （注） 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、**showinterfaces** 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。

コマンド デフォルト

発信元インターフェイスは使用されません。

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

ssh client source-interface コマンドを使用して、すべての発信 SSH 接続に指定したインターフェイスの IP アドレスを設定します。このコマンドを設定しなければ、ソケットが接続されるときの TCP の発信元 IP アドレスは、使用される発信インターフェイスに基づいて選択されます。つまり、サーバに到達するために必要なルートに基づきます。このコマンドは、SSH セッションだけでなく、セキュア シェル ファイル転送プロトコル（SFTP）セッション上でも発信シェルに適用されます。これらのセッションでは、転送に ssh クライアントが使用されます。

source-interface の設定は、同じアドレス ファミリ内のリモート ホストへの接続にしか影響しません。システム データベース（Sysdb）により、コマンドで指定されたインターフェイスに、対応する（同じファミリ内の）IP アドレスが設定されているかどうか検証されます。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次に、すべての発信 SSH 接続に対して管理イーサネット 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)# ssh client source-interface MgmtEth 0/RP0/CPU0/0
```

ssh server

セキュア セル（SSH）サーバを起動状態にし、1 つ以上の VRF を使用できるようにするには、**ssh server** コマンドを使用します。SSH サーバが指定された VRF の接続をこれ以上受信し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。

ssh server [**vrf vrf-name**| **v2**]

no ssh server [**vrf vrf-name**| **v2**]

構文の説明

vrf*vrf-name*	SSH サーバが使用する VRF の名前を指定します。VRF の最大長は 32 文字です。 （注） VRF が指定されていない場合、デフォルトの VRF が使用されます。
v2	SSH サーバ バージョンを強制的に 2 だけにします。

コマンド デフォルト

デフォルトの SSH サーバ バージョンは 2（SSHv2）です。着信 SSH クライアント接続が SSHv1 に設定されると、1（SSHv1）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

SSH サーバは少なくとも 1 つの VRF に対して設定する必要があります。デフォルトを含め、設定済みのすべての VRF を削除すると、SSH サーバのプロセスは停止します。**ssh client knownhost** や **ssh client source-interface** などの他のコマンドを適用する際に SSH クライアントに対して特定の VRF を設定しない場合は、デフォルトの VRF が使用されます。

SSH サーバは、ポート 22 で着信クライアント接続を待ち受けます。このサーバでは、IPv4 と IPv6 の両方のアドレス ファミリに対してセキュア シェル バージョン 1（SSHv1）と SSHv2 の両方の着信クライアント接続が処理されます。セキュア シェル バージョン 2 の接続だけを許可するには、ssh server v2, （175 ページ）コマンドを使用します。

SSH サーバが起動し、実行していることを確認するには、**show process sshd** コマンドを使用します。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次の例では、SSH サーバが起動され、VRF「green」の接続を受信します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh serverserver vrf green
```

ssh server logging

SSH サーバのロギングをイネーブルにするには、**ssh server logging** コマンドを使用します。SSH サーバのロギングを停止するには、このコマンドの **no** 形式を使用します。

ssh server logging

no ssh server logging

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 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

SSHv2 クライアント接続だけが許可されます。

ロギングを設定すると、次のメッセージが表示されます。

- Warning: The requested term-type is not supported
- SSH v2 connection from %s succeeded (*user:%s, cipher:%s, mac:%s, pty:%s*)

警告メッセージは、サポートされていない端末タイプを使用して接続しようとした場合に表示されます。Cisco IOS XR ソフトウェアを実行しているルータがサポートするのは vt100 端末タイプだけです。

2 番めのメッセージでログインに成功したことを確認します。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次に、SSH サーバのロギングの開始例を示します。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server logging
```

ssh server rate-limit

1 分間に許可する着信セキュア シェル（SSH）接続要求の数を制限するには、**ssh server rate-limit** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ssh server rate-limit *rate-limit*

no ssh server rate-limit

構文の説明

rate-limit	1 分間あたりに許可される着信 SSH 接続要求の数。範囲は 1 ～ 120 です。 1 分間あたりの再試行回数を 60 に設定すると、基本的に 1 秒間に 1 回が許可されることになります。2 つの異なるコンソールから同時に 2 つのセッションをセットアップする場合、そのうちの 1 つのレートは制限されます。これは、SSH サーバへの接続試行であり、インターフェイス/ユーザ名などのバインドはベースになりません。したがって、30 という値は 2 秒ごとに 1 セッションということになります。

コマンド デフォルト

rate-limit：1 分間あたり 60 個の接続要求

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

ssh server rate-limit コマンドを使用して、着信 SSH 接続要求を設定済みのレートに制限します。このレート制限を超える接続要求は、SSH サーバから拒否されます。レート制限の変更は、確立している SSH セッションには影響しません。

たとえば、*rate-limit* 引数を 30 に設定すると、1 分間に 30 の要求が許可されます。また、より厳密には、接続間に 2 秒のインターバルが適用されることになります。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次の例は、着信 SSH 接続要求の制限を 1 分あたり 20 に設定する方法です。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server rate-limit 20
```

ssh server session-limit

許容可能な同時着信セキュア シェル（SSH）セッションの数を設定するには、**ssh server session-limit** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ssh server session-limit *sessions*

no ssh server session-limit

構文の説明

sessions	ルータで許可される着信 SSH セッションの数。有効な範囲は 1 ～ 1024 です。

コマンド デフォルト

sessions：ルータあたり 64

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

ssh server session-limit コマンドを使用して、許容可能な同時着信 SSH 接続を設定します。発信接続はこの制限に含まれません。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次の例は、着信 SSH 接続の制限を 50 に設定する方法です。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh server session-limit 50
```

ssh server v2

SSH サーバのバージョンを 2（SSHv2）に限定するには、**ssh server v2** コマンドを使用します。SSHv2 の SSH サーバを停止するには、このコマンドの **no** 形式を使用します。

ssh server v2

no ssh server v2

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 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

SSHv2 クライアント接続だけが許可されます。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次の例は、SSH サーバ バージョンを SSHv2 に限定して開始する方法です。

```
 RP/0/RP0/CPU0:router#configure
RP/0/RP0/CPU0:router(config)# ssh server v2
```

ssh server netconf

netconf SSH サーバにポートを設定するには、XR コンフィギュレーション モードで **ssh server netconf port** を使用します。設定済みのポートの netconf 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。

ssh server netconf[**port***port-number*]

nossh server netconf[**port***port-number*]

構文の説明

port-number	netconf SSH サーバのポート番号（デフォルトのポート番号は 830）。

コマンド デフォルト

デフォルトのポート番号は 830 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

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
crypto	読み取り、書き込み

例

次に、**ssh server netconf port** コマンドを使用する例を示します。

```
RP/0/RP0/CPU0:router (config) #  ssh server netconf port 830
```

ssh timeout

認証、認可、およびアカウンティング（AAA）にユーザ認証のタイムアウト値を設定するには、**ssh timeout** コマンドを使用します。タイムアウト値をデフォルトの時間に設定するには、このコマンドの **no** 形式を使用します。

ssh timeout *seconds*

no ssh timeout *seconds*

構文の説明

seconds	ユーザ認証の時間（秒単位）。範囲は 5 ～ 120 です。

コマンド デフォルト

seconds：30

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

ssh timeout コマンドを使用して、AAA に対してユーザ認証のタイムアウト値を設定します。設定された時間内にユーザ自身の認証が AAA に対してできないと、接続は中断されます。値を設定しなければ、30 秒のデフォルト値が使用されます。

タスク ID

タスク ID	動作
crypto	読み取り、書き込み

例

次の例では、AAA ユーザ認証のタイムアウト値が 60 秒に設定されます。

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# ssh timeout 60
```