AAA サービスの設定

このモジュールでは、ソフトウェア システムでユーザ アクセスの制御に使用されるタスクベース認可の管理モデルの実装について説明します。タスクベース認可の実装では、主にユーザ グループおよびタスク グループを設定する必要があります。

ユーザ グループとタスク グループは、認証サービス、認可サービス、アカウンティング（AAA）サービスで使用されるソフトウェア コマンドセットを介して設定されます。認証コマンドは、ユーザまたはプリンシパルの ID の検証に使用されます。認可コマンドは、認証済みユーザ（またはプリンシパル）に特定のタスクを実行するための権限が付与されていることを確認するために使用します。アカウンティング コマンドは、セッションのログイン、および特定のユーザまたはシステムにより生成されるアクションを記録することで監査証跡を作成するときに使用されます。

AAA はソフトウェア ベース パッケージの一部であり、デフォルトで使用可能です。

AAA サービスの設定の機能履歴

AAA サービスの設定

このモジュールでは、ソフトウェア システムでユーザ アクセスの制御に使用されるタスクベース認可の管理モデルの実装について説明します。タスクベース認可の実装では、主にユーザ グループおよびタスク グループを設定する必要があります。

ユーザ グループとタスク グループは、認証サービス、認可サービス、アカウンティング（AAA）サービスで使用されるソフトウェア コマンドセットを介して設定されます。認証コマンドは、ユーザまたはプリンシパルの ID の検証に使用されます。認可コマンドは、認証済みユーザ（またはプリンシパル）に特定のタスクを実行するための権限が付与されていることを確認するために使用します。アカウンティング コマンドは、セッションのログイン、および特定のユーザまたはシステムにより生成されるアクションを記録することで監査証跡を作成するときに使用されます。

AAA はソフトウェア ベース パッケージの一部であり、デフォルトで使用可能です。

AAA サービスの設定の機能履歴

AAA サービスの設定に関する前提条件

次に、AAA サービスの設定に関する前提条件を示します。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。
- 初期設定ダイアログを使用してルート システム ユーザを確立します。管理者は、特定の AAA 設定なしでいくつかのローカル ユーザを設定できます。外部セキュリティ サーバは、ユーザアカウントが管理ドメイン内の複数のルータで共有される場合に必要になります。一般的な設定では、外部サーバが到達不能になった場合のバックアップとしてローカルデータベース オプションを使用して、外部AAAセキュリティ サーバおよびデータベースを使用します。

AAA サービスの設定に関する制約事項

ここでは、AAA サービスを設定する場合の制限を示します。

互換性

互換性は Cisco のフリーウェア TACACS+ サーバおよび FreeRADIUS だけで検証されます。

相互運用性

ルータの管理者は、ルータと現在 Cisco ソフトウェアを実行していない他のシスコ製機器に対して、同じ AAA サーバのソフトウェアとデータベース（CiscoSecure ACS など）を使用できます。タスク ID をサポートしない外部 TACACS+ サーバとルータとの間の相互運用性をサポートするには、「TACACS+ および RADIUS 認証ユーザのタスク ID （42 ページ）」の項を参照してください。

タスク グループの設定

タスクベースの認可では、その基本要素としてタスク *ID* の概念が使用されます。タスク ID は、ユーザの操作実行許可を定義します。各ユーザは、タスク ID で識別される許可されたルータ操作タスクのセットが関連付けられます。ユーザは、ユーザ グループに関連付けられることで許可が付与されます。ユーザ グループには、タスク グループが関連付けられます。各タスク グループは 1 つ以上のタスク ID に関連付けられます。認可スキームを設定する場合、最初にタスク グループを設定します。次に、タスク グループ、個々のユーザの順に設定します。

no プレフィックスを指定して **task** コマンドを使用すると、特定のタスク ID をタスク グループから削除できます。

タスク グループ自体は削除できます。ドキュメント名のあるタスク グループを削除すると、エラーが発生します。

始める前に

タスク グループを作成して、タスク ID を関連付ける前に、タスク ID のルータ リストおよび各タスク ID の目的について理解しておく必要があります。タスク ID の完全なリストを表示するには、**show aaa task supported** コマンドを使用します。

（注） AAA タスク ID の write 許可を持っているユーザだけタスク グループを設定できます。

手順

ステップ 1 **configure**

ステップ 2 **taskgroup** *taskgroup-name*

例：

```
RP/0/RP0/cpu 0: router(config)# taskgroup beta
```

特定のタスク グループの名前を作成し、タスク グループ コンフィギュレーション サブモードを開始します。

- **taskgroup** コマンドの **no** 形式を指定すると、特定のタスク グループをシステムから削除できます。

ステップ 3 **description** *string*

例：

```
RP/0/RP0/cpu 0: router(config-tg)# description this is a sample task group description
```

（任意）ステップ 2 で指定したタスク グループの説明を作成します。

ステップ 4 **task** {**read** | **write** | **execute** | **debug**} *taskid-name*

例：

```
RP/0/RP0/cpu 0: router(config-tg)# task read bgp
```

ステップ 2 で指定したタスク グループに関連付けるタスク ID を指定します。

- そのタスク ID が関連付けられ、タスク グループのメンバにより実行される任意の CLI または API 呼び出しに **read** 許可を割り当てます。
- **no** プレフィックスを指定して **task** コマンドを使用すると、特定のタスク ID をタスク グループから削除できます。

ステップ 5 ステップ 2 で指定したタスク グループに関連付ける各タスク ID に対して手順を繰り返します。

—

ステップ 6 **commit**

次のタスク

タスク グループのすべてのセットの設定が完了したら、ユーザ グループのフル セットを設定します（「ユーザ グループの設定」の項を参照）。

ユーザ グループの設定

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。 **usergroup** コマンドを入力すると、ユーザ グループ コンフィギュレーション サブモードが開始されます。 **usergroup** コマンドの **no** 形式を使用すると、特定のユーザ グループを削除できます。システムで参照されているユーザ グループを削除すると、警告が表示されます。

始める前に

（注） WRITE:AAA タスク ID が関連付けられているユーザだけ、ユーザ グループを設定できます。ユーザ グループは、事前定義されたグループのプロパティ（owner-sdr など）を継承できません。

手順

ステップ 1 **configure**

ステップ 2 **usergroup** *usergroup-name*

例：

```
RP/0/RP0/cpu 0: router(config)# usergroup beta
```

特定のユーザ グループの名前を作成し、ユーザ グループ コンフィギュレーション サブモードを開始します。

- **usergroup** コマンドの **no** 形式を指定すると、特定のユーザ グループをシステムから削除できます。

ステップ 3 **description** *string*

例：

```
RP/0/RP0/cpu 0: router(config-ug)#
description this is a sample user group description
```

（任意）ステップ 2 で指定したユーザ グループの説明を作成します。

ステップ 4 **inherit usergroup** *usergroup-name*

例：

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

- ユーザ グループの権限を明示的に定義します。

ステップ 5 **taskgroup** *taskgroup-name*

例：

```
 RP/0/RP0/cpu 0: router(config-ug)# taskgroup beta
```

ステップ 2 で指定したユーザ グループをこのステップで指定したタスク グループに関連付けます。

- ユーザ グループは、入力したタスク グループに対してすでに定義されている設定属性（タスク ID リストと権限）を取ります。

ステップ 6 ステップ 2 で指定したユーザ グループを関連付ける各タスク グループに対して手順を繰り返します。

—

ステップ 7 **commit**

ユーザの設定

ユーザを設定するには、次のタスクを実行します。

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。

手順

ステップ 1 **configure**

ステップ 2 **username** *user-name*

例：

```
 RP/0/RP0/cpu 0: router(config)# username user1
```

新しいユーザの名前を作成（または現在のユーザを識別）して、ユーザ名コンフィギュレーション サブモードを開始します。

- *user-name* 引数には 1 つの単語だけ使用できます。スペースと引用符は使用できません。

ステップ 3 次のいずれかを実行します。

- **password** {**0** | **7**} *password*
- **secret** {**0** | **5**} *secret*

例：

```
RP/0/RP0/cpu 0: router(config-un)# password 0 pwd1
```

または

```
RP/0/RP0/cpu 0: router(config-un)# secret 0 sec1
```

ステップ 2 で指定したユーザのパスワードを指定します。

- **secret** コマンドを使用して、ステップ 2 で指定したユーザ名用の安全なログイン パスワードを作成します。
- **password** コマンドの後に **0** を入力すると、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が指定されます。 **password** コマンドの後に **7, 8, 9, 10** を入力すると、暗号化されたパスワードが続くことが指定されます。
- **secret** コマンドの後に **0** を入力すると、セキュアな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が指定されます。 **secret** コマンドの後に **5** を入力すると、セキュアな暗号化されたパスワードが続くことが指定されます。
- タイプ **0** が、 **password** コマンドおよび **secret** コマンドのデフォルトです。

ステップ 4 **group** *group-name*

例：

```
RP/0/RP0/cpu 0: router(config-un)# group sysadmin
```

ステップ 2 で指定したユーザを **usergroup** コマンドで定義したユーザ グループに割り当てます。

- ユーザは、ユーザ グループのさまざまなタスク グループへの割り当てによって定義された内容に従って、ユーザ グループのすべての属性を受け取ります。
- 各ユーザは、少なくとも 1 つのユーザ グループに割り当てる必要があります。ユーザは複数のユーザ グループに属することがあります。

ステップ 5 ステップ 2 で指定したユーザに関連付けるユーザ グループごとに、ステップ 4 を繰り返します。

—

ステップ 6 **commit**

タイプ 8 とタイプ 9 のパスワードの設定

パスワードを設定する場合、ユーザには次の 2 つのオプションがあります。

- ユーザはすでに暗号化された値を提供できます。この値はさらに暗号化されずにシステムに直接保存されます。
- ユーザは内部で暗号化され、システムに保存されているクリアテキストのパスワードを提供できます。

タイプ 5、タイプ 8、およびタイプ 9 の暗号化方式では、ユーザがパスワードを設定するために前述のオプションを使用できます。

タイプ 8 およびタイプ 9 の暗号化方式の設定の詳細については、ユーザの設定 （5 ページ）の項を参照してください。

設定例

タイプ 8 の暗号化パスワードを直接設定するには、次のコマンドを実行します。

```
Router(config)# username demo8
Router(config-un)#secret 8 $8$dsYGNam3K1SIJO$7nv/35M/qr6t.dVc7UY9zrJDWRVqncHub1PE9UlMQFs
```

タイプ 8 暗号化方式を使用して暗号化されたクリアテキストのパスワードを設定するには、次のコマンドを実行します。

```
Router(config)# username demo8
Router(config-un)#secret 0 enc-type 8 PASSWORD
```

タイプ 9 の暗号化パスワードを直接設定するには、次のコマンドを実行します。

```
Router(config)# username demo9
Router(config-un)# secret 9 $9$nhEmQVczB7dqsO$X.HsgL6x1il0RxkOSSvyQYwucySCt7qFm4v7pqCxkKM
```

タイプ 9 暗号化方式を使用して暗号化されたクリアテキストのパスワードを設定するには、次のコマンドを実行します。

```
Router(config)# username demo9
Router(config-un)#secret 0 enc-type 9 PASSWORD
```

関連項目

- タイプ 8 とタイプ 9 のパスワード （39 ページ）
- タイプ 10 パスワード （40 ページ）

関連コマンド

- secret
- username

タイプ 10 パスワードの設定

次のオプションを使用して、タイプ 10 パスワード（**SHA512** ハッシュアルゴリズムを使用）をユーザに設定します。

設定例

Release 7.0.1 以降では、クリアテキストのパスワードを使用してユーザを作成した場合のパスワードのデフォルトでタイプ 10 が適用されます。

```
Router#configure
Router(config)#username user10 secret testpassword
Router(config-un)#commit
```

また、明示的にタイプ 10 パスワードを設定するために **username** コマンドの **secret** オプションとして新しいパラメータの「10」を使用できます。

```
Router#configure
Router(config)#username root secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
Router(config-un)#commit
```

クリアテキストのパスワードを入力する必要があるシナリオでは、次に示すように、**enc-type** キーワードとクリアテキストのパスワードを使用することで、使用する暗号化アルゴリズムを指定できます。

```
Router#configure
Router(config)#username user10 secret 0 enc-type 10 testpassword
Router(config-un)#commit
```

前述の設定では、タイプ 10 パスワードを使用してユーザを設定します。

システム管理 VM では、次に示すように、タイプ 10 暗号化パスワードを指定できます。

```
Router#admin
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authentication users user user10 password testpassword
sysadmin-vm:0_RP0(config)# commit
Commit complete.
sysadmin-vm:0_RP0(config)# end
sysadmin-vm:0_RP0# exit
Router#
```

実行コンフィギュレーション

```
Router#show running-configuration username user10
!
username user10
secret 10
$6$9UvJidvsTEqgkAPU$3CL1Ei/F.E4v/Hi.UaqLwX8UsSEr9ApG6c5pzhMJmZtgW4jObAQ7meAwyhu5VM/aRFJqe/jxZG17h6xPrvJWf1
!
```

システム管理 VM で、次の手順を実行します。

```
sysadmin-vm:0_RP0#show running-configuration aaa authentication users user user10
Tue Jan 14 07:32:44.363 UTC+00:00
aaa authentication users user user10
password
$6$MMvhlj1CzSd2nJfB$BbzvxzriwxiLFg75w4zj15YK3yeoq5UoRyc1evtSX0c4EuaMlqK.v7E3zbY1yKKxkN6rXpQuhMJOuyRHItDc1
!
sysadmin-vm:0_RP0#
```

同様に、XR VM に **admin show running-configuration aaa authentication users user user10** コマンドを使用して、ユーザに設定されたパスワードの詳細を表示できます。

関連項目

- タイプ 10 パスワード （40 ページ）
- パスワードタイプの下位互換性 （9 ページ）

関連コマンド

- secret
- username

パスワードタイプの下位互換性

Cisco IOS XR ソフトウェア Release 7.0.1 から下位のバージョンにダウングレードすると、設定の損失、認証の失敗、ダウングレードの中止、または XR VM のダウンなどの問題が発生することがあります。タイプ 5（MD5）は古いリリースのデフォルトの暗号化であるため、これらの問題が発生します。

ダウングレード時にこのような下位互換性の問題が発生しないようにするには、次のステップに従うことをお勧めします。

- **install activate** のステップを除き、ダウングレードのすべてのインストール操作を実行します。
- この **install activate** のステップを実行する前に、両方の VM でユーザ設定のバックアップを作成します。**show running-configuration username | file harddisk:***filename* コマンドを同様に使用できます。
- 両方の VM のすべてのユーザを削除し、**install activate** のステップを開始します。
- ルータが下位のバージョンで起動すると、最初のルートシステムユーザの作成を要求するプロンプトが表示されます。
- 最初のユーザのクレデンシャルを使用してログインした後、以前に保存した設定を両方の VM に適用します。

たとえば、ダウングレード後の認証失敗のシナリオを考えてみましょう。ダウングレードプロセスは、タイプ 5 の秘密を持つ既存のユーザ名設定には影響しません。このようなユーザは、クリアテキストのパスワードを使用して問題なくログインできます。しかし、タイプ 10 設定を持つユーザでは認証が失敗し、ログインできない場合があります。このような場合は、文字列「10<space><sha512-hashed-text>」全体がクリアテキストのパスワードとして処理されてタイプ 5（MD5）パスワードに暗号化されます。この「10<space><sha512-hashed-text>」文字列をそのタイプ 10 ユーザのパスワードとしてログインに使用します。前述のステップを使用してログインした後、「設定例」の項で説明されているように、XR VM および システム管理 VM でクリアテキストのパスワードを明示的に設定します。

RADIUS サーバ通信用のルータの設定

ルータと RADIUS サーバの通信を設定します。通常、RADIUS ホストは、シスコ（CiscoSecure ACS）、Livingston、Merit、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。RADIUS サーバとの通信のためにルータを設定するには、次のような要素があります。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- 再送信回数
- タイムアウト時間
- キー文字列

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定のユーザ データグラム プロトコル（UDP）ポート番号、または IP アドレスおよび特定の UDP ポート番号により識別されます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。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。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリの自動スイッチオーバー バックアップとして動作します。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）。

RADIUS サーバと Cisco ルータは、共有秘密テキスト ストリングを使用してパスワードを暗号化し、応答を交換します。RADIUS を設定して AAA セキュリティ コマンドを使用するには、RADIUS サーバデーモンを実行するホストと、ルータと共有する秘密テキスト（キー）ストリングを指定する必要があります。

タイムアウト値、再送信値、および暗号キー値には、すべての RADIUS サーバを対象にしたグローバル設定、サーバ別設定、またはグローバル設定とサーバ別設定の組み合わせを使用できます。すべての RADIUS サーバとルータとの通信にこのようなグローバル設定を適用するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** という 3 つの固有なグローバル コンフィギュレーション コマンドを使用します。特定の RADIUS サーバにこれらの値を適用するには、**radius-server host** コマンドをグローバル コンフィギュレーション モードで使用します。

（注） 同じシスコ製ネットワーク アクセス サーバで、タイムアウト、再送信、およびキー値のコマンドを同時に設定（グローバル設定およびサーバ別設定）できます。ルータにグローバル機能とサーバ別機能の両方を設定する場合、サーバ別のタイマー、再送信、およびキー値のコマンドの方が、グローバルのタイマー、再送信、およびキー値のコマンドよりも優先されます。

手順

ステップ 1 **configure**

ステップ 2 **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

例：

```
RP/0//CPU0:router(config)# radius-server host host1
```

リモート RADIUS サーバ ホストのホスト名または IP アドレスを指定します。

- **auth-port** *port-number* オプションを使用して、認証専用の RADIUS サーバに固有の UDP ポートを設定します。
- **acct-port** *port-number* オプションを使用して、アカウンティング専用の RADIUS サーバに固有の UDP ポートを設定します。
- ネットワーク アクセス サーバが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な回数だけ繰り返します。その際、各 UDP ポート番号が異なっていることを確認してください。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
- タイムアウトを設定しない場合、グローバル値が使用されます。設定する場合、値の範囲は 1 ～ 1000 です。再送信値を設定しない場合、グローバル値が使用されます。設定する場合、値の範囲は 1 ～ 100 です。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。

（注） キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーの先頭にあるスペースは無視されますが、キー内のスペースとキー末尾のスペースは使用されるため、キーは常に **radius-server host** コマンド構文の最後のアイテムとして設定してください。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。

ステップ 3 **radius-server retransmit** *retries*

例：

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

ソフトウェアが RADIUS サーバ ホストのリストを検索する回数の最大値を指定します。

- この例では、再送信の試行回数は 5 に設定されます。

ステップ 4 **radius-server timeout** *seconds*

例：

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

タイムアウトになるまでルータがサーバ ホストの応答を待機する秒数を設定します。

- 次に、インターバル タイマーが 10 秒に設定されている例を示します。

ステップ 5 **radius-server key** {**0** *clear-text-key* | **7** *encrypted-key* | *clear-text-key*}

例：

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

ルータおよび RADIUS デーモン間のすべての RADIUS コミュニケーションの認証キーおよび暗号キーを指定します。

ステップ 6 **radius source-interface** *type instance* [**vrf** *vrf-id*]

例：

```
RP/0/RP0/cpu 0: router(config)# radius source-interface 0/3/0/1
```

（任意）RADIUS で、すべての発信 RADIUS パケットに指定のインターフェイスまたはサブインターフェイスの IP アドレスが使用されるようにします。

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

vrf キーワードは、VRF 単位で仕様を有効にします。

ステップ 7 設定する各外部サーバに対して ステップ 2 ～ 6 を繰り返します。

—

ステップ 8 **commit**

ステップ 9 show radius

例：

```
RP/0/RP0/cpu 0: router# show radius
```

（任意）システムに設定されている RADIUS サーバの情報を表示します。

Radius の要約の例

```
radius source-interface Mgm0/rp0/cpu0/0 vrf default
radius-server timeout 10
radius-server retransmit 2
!
```

```
! OOB RADIUS
radius-server host 123.100.100.186 auth-port 1812 acct-port 1813
key cisco123
timeout 10
retransmit 2
!
radius-server host 123.100.100.187 auth-port 1812 acct-port 1813
key cisco123
timeout 10
retransmit 2
!
aaa group server radius radgrp
server 123.100.100.186 auth-port 1812 acct-port 1813
server 123.100.100.187 auth-port 1812 acct-port 1813
!
aaa authorization exec radauthen group radgrp local
aaa authentication login radlogin group radgrp local
!
line template vty
authorization exec radauthen
login authentication radlogin
timestamp disable
exec-timeout 0 0
!
vty-pool default 0 99 line-template vty
```

RADIUS Dead サーバ検出の設定

RADIUS Dead-Server Detection 機能を使用すると、RADIUS サーバをデッド状態と指定するために使用する条件を設定および決定できます。条件が明示的に設定されていない場合は、条件は未処理のトランザクションの数に基づいて動的に計算されます。RADIUS Dead-Server Detection を設定すると、応答を停止しているRADIUSサーバが即時検出されます。この未応答RADIUSサーバの即時検出、動きが鈍いサーバの誤検出の回避、デッド状態とライブ状態を繰り返す現象の回避が有効になると、デッドタイムが短くなり、パケット処理が高速になります。

ルータが RADIUS サーバから有効なパケットを最後に受け取ってから RADIUS サーバがデッド状態と指定されるまでに経過する必要がある最低時間を秒単位で設定することができます。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。

さらに、RADIUSサーバがデッド状態と指定されるまでにルータで発生する必要がある連続タイムアウト回数を設定することもできます。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、両方の種類のパケットがこの回数に含まれます。正しく作成されていないパケットは、タイムアウトになっているものとしてカウントされます。カウントされるのは再転送だけで、最初の転送はカウントされません。たとえば、各タイムアウトで1回の再送信が送信されます。

（注） 時間の条件と試行回数の条件の両方を満たしていないと、サーバはデッド状態と指定されません。

radius-server deadtime コマンドは、サーバがデッド状態とマークされて、デッド状態に留まる時間を分単位で指定します。この時間が経過すると、サーバからの応答が受信されない場合

でも、サーバは稼働中とマークされます。デッド条件を設定しても、**radius-server deadtime** コマンドを設定しない限り、サーバはモニタされません。

手順

ステップ 1 **configure**

ステップ 2 **radius-server deadtime** *minutes*

例：

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

いくつかのサーバが使用不能になったときのRADIUSサーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。

ステップ 3 **radius-server dead-criteria time** *seconds*

例：

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

RADIUS サーバがデッド状態として指定されるデッド条件の時間を確立します。

ステップ 4 **radius-server dead-criteria tries** *tries*

例：

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

RADIUS サーバがデッド状態として指定されるデッド条件の試行回数を確立します。

ステップ 5 **commit**

ステップ 6 **show radius dead-criteria host** *ip-addr* [**auth-port** *auth-port*] [**acct-port** *acct-port*]

例：

```
RP/0/RP0/cpu 0: router# show radius dead-criteria host 172.19.192.80
```

（任意）指定 IP アドレスで RADIUS サーバに要求された dead-server-detection 情報を表示します。

TACACS+ サーバの設定

TACACS+ サーバを設定します。

ポートが指定されていない場合、標準ポート番号49がデフォルトで使用されます。**timeout** および **key** パラメータは、すべてのTACACS+サーバに対してグローバルで指定できます。**timeout** パラメータは、AAAサーバがTACACS+サーバから応答を受信するまでの時間を指定します。**key** パラメータは、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。

手順

ステップ 1 **configure**

ステップ 2 **tacacs-server host** *host-name* **port** *port-number*

例：

```
RP/0/RP0/cpu 0: router(config)# tacacs-server host 209.165.200.226 port 51
RP/0/RP0/cpu 0: router(config-tacacs-host)#
```

TACACS+ ホスト サーバを指定し、オプションでサーバ ポート番号を指定します。

- このオプションによって、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。

ステップ 3 **tacacs-server host** *host-name* **timeout** *seconds*

例：

```
RP/0/RP0/cpu 0: router(config-tacacs-host)# tacacs-server host 209.165.200.226 timeout
30
RP/0/RP0/cpu 0: router(config)#
```

TACACS+ ホスト サーバを指定し、オプションで、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。

- このオプションを指定すると、このサーバに限り、 **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が上書きされます。タイムアウト値は、タイムアウト間隔を指定する整数として表されます。範囲は 1 ～ 1000 です。

ステップ 4 **tacacs-server host** *host-name* **key** [**0** | **7**] *auth-key*

例：

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

TACACS+ ホスト サーバを指定し、オプションで、AAA サーバと TACACS+ サーバ間で共有される認証および暗号キーを指定します。

- TACACS+ パケットは、このキーを使って暗号化されます。このキーは TACACS+ デーモンで使用されるキーと一致する必要があります。このキーを指定すると、このサーバに限り、 **tacacs-server key** コマンドで設定されたグローバル キーが上書きされます。
- （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（クリアテキスト）キーが続くことを指定します。
- *auth-key* 引数は、AAA サーバと TACACS+ サーバ間で共有される暗号化されたまたは暗号化されていないキーを指定します。

ステップ 5 **tacacs-server host** *host-name* **single-connection**

例：

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

単一 TCP 接続を介してすべての TACACS+ 要求をこのサーバに多重化するようにルータを設定します。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。

ステップ 6 **tacacs source-interface** *type instance*

例：

```
RP/0/RP0/cpu 0: router(config)# tacacs source-interface 0/4/0/0
```

（任意）すべての発信 TACACS+ パケットに対して、選択したインターフェイスの発信元 IP アドレスを指定します。

- 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、TACACS+ はデフォルトインターフェイスに戻ります。これを回避するには、インターフェイスまたはサブインターフェイスに IP アドレスを追加するか、そのインターフェイスをアップ状態にします。
- **vrf** オプションは、AAA TACACS+ サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照を指定します。

ステップ 7 設定する各外部サーバに対して ステップ 2 ～ 5 を繰り返します。

—

ステップ 8 **commit**

ステップ 9 **show tacacs**

例：

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

（任意）システムに設定されている TACACS+ サーバの情報を表示します。

Tacacs の要約の例：

```
! OOB TAC
tacacs-server host 123.100.100.186 port 49
key lm51
!
tacacs-server host 123.100.100.187 port 49
key lm51
!
aaa group server tacacs+ tacgrp
server 123.100.100.186
server 123.100.100.187
!
aaa group server tacacs+ eem
server 123.100.100.186
```

```
server 123.100.100.187
!
aaa authorization exec tacauthen group tacgrp local
aaa authentication login taclogin group tacgrp local
!
line console
authorization exec tacauthen
login authentication taclogin
timeout login response 30
timestamp
exec-timeout 0 0
session-timeout 15
!
vty-pool default 0 99 line-template console
```

RADIUS サーバ グループの設定

この作業では、RADIUS サーバ グループを設定します。

1 つ以上の **server** コマンドを入力できます。 **server** コマンドは、外部 RADIUS サーバのホスト名または IP アドレスをポート番号とともに指定します。設定されている場合、このサーバ グループは、AAA 方式リスト（認証、認可またはアカウンティングの設定に使用されます）から参照できます。

始める前に

正常に設定を行うため、外部サーバが設定時にアクセスできる必要があります。

手順

ステップ 1 **configure**

ステップ 2 **aaa group server radius** *group-name*

例：

```
RP/0/RP0/cpu 0: router(config)# aaa group server radius radgroup1
```

各種サーバ ホストを別個のリストにグループ化し、サーバ グループ コンフィギュレーション モードを開始します。

ステップ 3 **server** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]

例：

```
RP/0/RP0/cpu 0: router(config-sg-radius)# server 192.168.20.0
```

外部 RADIUS サーバのホスト名または IP アドレスを指定します。

- サーバ グループは、設定されると、AAA 方式リスト（認証、認可またはアカウンティングの設定に使用されます）から参照できます。

ステップ 4 ステップ 3 で指定したサーバ グループに追加する各外部サーバに対し、ステップ 4 を繰り返します。

—

ステップ 5 **deadtime** *minutes*

例：

```
RP/0/RP0/cpu 0: router(config-sg-radius)# deadtime 1
```

RADIUS サーバ グループ レベルでデッドタイム値を設定します。

- *minutes* 引数には、トランザクション要求によって RADIUS サーバをスキップする時間を分単位で指定します。最長 1440 分（24 時間）まで指定できます。指定できる範囲は 1 ～ 1440 です。

RADIUS サーバ グループ radgroup1 が認証要求への応答に失敗したときの **deadtime** コマンドに対して、1 分のデッドタイムを指定する例を示します。

（注） グループの作成後にグループ レベルのデッド タイムを設定できます。

ステップ 6 **commit**

ステップ 7 **show radius server-groups** [*group-name* [**detail**]]

例：

```
RP/0/RP0/cpu 0: router# show radius server-groups
```

（任意）システムで設定されている各 RADIUS サーバ グループの情報を表示します。

次のタスク

RADIUS サーバ グループを設定したら、認証、認可およびアカウンティングを設定して方式リストを定義します

TACACS+ サーバ グループの設定

TACACS+ サーバ グループを設定します。

1 つ以上の **server** コマンドを入力できます。 **server** コマンドは、外部 TACACS+ サーバのホスト名または IP アドレスを指定します。設定後は、このサーバ グループは、AAA 方式リスト（認証、認可またはアカウンティングの設定に使用されます）から参照できます

始める前に

正常に設定を行うため、外部サーバが設定時にアクセスできる必要があります。グローバルおよび VRF 設定の両方に同じ IP アドレスを設定するときは、server-private パラメータが必要です（「*VRF TACACS+* サーバグループごとの設定」の項を参照）。

手順

ステップ 1 **configure**

ステップ 2 **aaa group server tacacs+** *group-name*

例：

```
RP/0/RP0/cpu 0: router(config)# aaa group server tacacs+ tacgroup1
```

各種サーバ ホストを別個のリストにグループ化し、サーバ グループ コンフィギュレーション モードを開始します。

ステップ 3 **server** {*hostname* | *ip-address*}

例：

```
RP/0/RP0/cpu 0: router(config-sg-tacacs+)# server 192.168.100.0
```

外部 TACACS+ サーバのホスト名または IP アドレスを指定します。

- 設定されている場合、このグループは、AAA方式リスト（認証、認可またはアカウンティングの設定に使用されます）から参照できます

ステップ 4 ステップ 2 で指定したサーバ グループに追加する各外部サーバに対し、ステップ 3 を繰り返します。

—

ステップ 5 **server-private** {*hostname* | *ip-address in IPv4 or IPv6 format*} [**port** *port-number*] [**timeout** *seconds*] [**key** *string*]

例：

```
Router(config-sg-tacacs+)# server-private 10.1.1.1 key a_secret
```

グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。

（注） プライベート サーバ パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。

ステップ 6 （任意）**vrf** *vrf-id*

例：

```
Router(config-sg-tacacs+)# vrf test-vrf
```

vrf オプションは、AAA TACACS+ サーバ グループのバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）参照を指定します。

ステップ 7 **commit**

ステップ 8 **show tacacs server-groups**

例：

```
RP/0/RP0/cpu 0: router# show tacacs server-groups
```

（任意）システムで設定されている各 TACACS+ サーバ グループの情報を表示します。

一連の認証方式の作成

認証は、ユーザ（またはプリンシパル）が検証されるプロセスです。認証設定は、方式リストを使用して、さまざまなデータ ソースに保存されている、AAA データ ソースの優先順位を定義します。認証を設定して、複数の方式リストを定義できます。アプリケーションは（ログインなど）、これらのいずれかを選択できます。たとえば、コンソール ポートと VTY ポートとで異なる方式リストを使用できます。方式リストが指定されていない場合、アプリケーションは、デフォルトの方式リストを使用します。

（注） 方式リストが有効になるようにするには、アプリケーションは明示的に定義済みの方式リストを示す必要があります。

認証は、**login authentication** ライン コンフィギュレーション サブモード コマンドを使用して、TTY 回線に適用できます。方式が、サーバ グループではなく、RADIUS または TACACS+ サーバの場合、RADIUS または TACACS+ サーバは、設定されている RADIUS および TACACS+ サーバのグローバル プールから、設定順に選択されます。このグローバル プールから選択されるサーバは、サーバ グループに追加できるサーバです。

後続の認証方式は、初期方式がエラーを返すか、要求が拒否された場合だけ使用されます。

始める前に

（注） デフォルトの方式リストは、デフォルト以外の名前付き方式リストが明示的に設定されている場合（この場合は名前付き方式リストが適用される）を除き、認証のすべてのインターフェイスに適用されます。

aaa authentication コマンドの **group radius, group tacacs+** および **group** *group-name* 形式は、以前に定義した一連の RADIUS サーバまたは TACACS+ サーバを参照します。ホスト サーバを設定するには、**radius server-host or tacacs-server host** コマンドを使用します。特定のサーバ グループを作成するには、**aaa group server radius or aaa group server tacacs+** コマンドを使用します。

手順

ステップ 1 **configure**

ステップ 2 **aaa authentication** {**login**} {**default** | *list-name*} *method-list*

例：

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

一連の認証方式、つまり方式リストを作成します。

- **login** キーワードを使用すると、ログインの認証が設定されます。**ppp** キーワードを使用すると、ポイントツーポイント プロトコルの認証が設定されます。
- **default**キーワードを入力すると、このキーワードの後ろにリストされている認証方式が、認証のデフォルトの方式リストになります。
- *list-name* 文字列を入力すると、認証方式リストが識別されます。
- 方式リストのタイプの後ろに*method-list*引数を入力します。方式リスト タイプは、目的の順序で入力します。リストされる方式タイプは、次のいずれかのオプションです。
  - **group tacacs+**：サーバ グループまたは TACACS+ サーバを認証に使用します
  - **group radius**：サーバ グループまたは RADIUS サーバを認証に使用します
  - **group***named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットを認証に使用します。
  - **local**：ユーザ名またはパスワードのローカル データベースを認証に使用します
  - **line**：回線パスワードまたはユーザ グループを認証に使用します
- この例では、**default**方式リストが認証に使用されます。

ステップ 3 **commit**

ステップ 4 設定されるすべての認証方式リストに対して、ステップ 1 ～ 3 を繰り返します。

—

一連の許可方式の作成

許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、シーケンスで照会される認可方式（TACACS+ など）を説明する単なる名前付きリストです。方式リストを使用すると、認可に使用するセキュリティ プロトコルを1つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。ソフトウェアは方式リストの最初の方式を使用して、特定のネットワーク サービスに対してユーザを許可します。その方式が応答に失敗すると、方式リスト内の次の方式が選択されます。このプロセスは、リスト内の許可方式との通信に成功するまで、または定義されている方式を使い果たすまで続行されます。

（注） ソフトウェアは、前の方式から応答がない場合またはエラー（障害ではない）応答が返された場合にのみ、次に指定されている方式を使って許可を試みます。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。

名前付き方式リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。方式リストを定義した場合、定義した方式のいずれかを実行するには、まず特定の回線またはインターフェイスに方式リストを適用する必要があります。新しいメソッドリストを作成するときに、TACACS+ などの方式名を使用しないでください。

ラインテンプレートにコマンド認可方式リストを適用した結果の「コマンド」の許可とは別個であり、ルータで自動的に実行される「タスクベース」の許可に加えて実行される方式です。コマンドの許可のデフォルト動作はnoneです。デフォルトの方式リストが設定されていても、その方式リストは、使用するためのライン テンプレートに追加する必要があります。

aaa authorization commands コマンドにより、許可プロセスの一環として、一連の属性値（AV）ペアを含む要求パケットがTACACS+デーモンに送信されます。デーモンは、次のいずれかのアクションを実行できます。

- 要求をそのまま受け入れます。
- 許可を拒否します。

aaa authorization コマンドを使用して、認可パラメータを設定し、各回線またはインターフェイスで使用できる特定の許可方式を定義する名前付き方式リストを作成します。

手順

ステップ 1 **configure**

ステップ 2 **aaa authorization** {**commands** | **eventmanager** | **exec** | **network**} {**default** | *list-name*} {**none** | **local** | **group** {**tacacs+** | **radius** | *group-name*}}

例：

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

一連の認可方式、つまり方式リストを作成します。

- **commands** キーワードは、すべての XR EXEC モード シェル コマンドに対して許可を設定します。コマンドの認可は、ユーザにより発行される EXEC モード コマンドに適用されます。コマンドの認可では、すべての XR EXEC モード コマンドに対して許可が試行されます。
- **eventmanager** キーワードは、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** キーワードは、インタラクティブ セッション（XR EXEC モード）に対する許可を設定します。
- **network** キーワードは、PPP または 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** キーワードを指定すると、このキーワードの後ろにリストされている許可方式が、許可のデフォルトの方式リストになります。

- *list-name* 文字列は、許可方式リストを識別します。方式リスト自体は、方式リスト名に続きます。方式リスト タイプは、目的の順序で入力します。リストされる方式リスト タイプは、次のいずれかにできます。
  - **none**：ネットワーク アクセス サーバ（NAS）は、許可情報を要求しません。認可は常に成功します。以降の認可方式は試行されません。ただし、タスク ID の許可は常に必要であり、ディセーブルにはできません。
  - **local**：ローカル データベースを認可に使用します。
- **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。NAS は、認可情報を TACACS+ セキュリティ デーモンと交換します。TACACS+ 認可は、AV ペアを関連付けることでユーザに特定の権限を定義します。AV は適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。
- **group radius**：設定されているすべての RADIUS サーバのリストを許可に使用します。
- **group** *group-name*：**aaa group server tacacs+** または **aaa group server radius** コマンドによって定義されている名前付きサーバ グループ、TACACS+ または RADIUS サーバのサブセットを許可に使用します。

ステップ 3 **commit**

一連のアカウンティング方式の作成

aaa accounting コマンドを使用して、デフォルトまたは名前付き方式リストを作成し、各回線またはインターフェイスに使用可能な特定のアカウンティング方式を定義します。

現時点では、アカウンティングに対して TACACS+ および RADIUS の両方の方式がサポートされています。ルータは、アカウンティング レコードの形式で TACACS+ または RADIUS セキュリティ サーバにユーザ アクティビティを報告します。各アカウンティング レコードは、アカウンティング AV ペアが含まれ、セキュリティ サーバ上で保管されます。

アカウンティング方式リストには、アカウンティングの実行方法が定義されます。このリストを使用して、特定のタイプのアカウンティング サービスに固有の回線またはインターフェイスに使用する特定のセキュリティ プロトコルを指定できます。方式リストの名前を付ける場合、TACACS+ などの方式の名前を使用しないでください。

最低限のアカウンティングを行う場合は、**stop-only** キーワードを指定して、要求されたユーザ プロセスの終了時に「stop accounting」通知を送信するようにします。詳細なアカウンティングを行う場合は、**start-stop** キーワードを使用できます。このキーワードを指定すると、外部 AAA サーバは要求されたプロセスの開始時に「start accounting」通知を送信し、プロセスの終了時に「stop accounting」通知を送信します。また、 **aaa accounting update** コマンドを使用して、累積情報を含む更新レコードを定期的に送信できます。アカウンティング レコードは、TACACS+ または RADIUS サーバだけに格納されます。

AAA アカウンティングをアクティブにすると、ルータは、これらの属性をアカウンティング レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

手順

ステップ 1 **configure**

ステップ 2 次のいずれかを実行します。

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

例：

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

（注） コマンド アカウンティングは RADIUS ではサポートされいませんが、TACACS ではサポートされます。

一連のアカウンティング方式、つまり方式リストを作成します。

- **commands** キーワードは、XR EXEC モード シェル コマンドでアカウンティングを有効にします。
- **exec** キーワードは、インタラクティブ（XR EXEC モード）セッションに対するアカウンティングを有効にします。
- **network** キーワードは、ポイントツーポイント プロトコル（PPP）など、ネットワーク関連のすべてのサービス要求に対してアカウンティングを有効にします。
- **default** キーワードを指定すると、このキーワードの後ろにリストされているアカウンティング方式が、アカウンティングのデフォルトの方式リストになります。
- *list-name* 文字列は、アカウンティング方式リストを識別します。
- **start-stop** キーワードは、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** キーワードは、要求されたユーザ プロセスの終了時に「stop accounting」通知を送信します。
- **none** キーワードは、アカウンティングを行わないことを指定します。
- 方式リスト自体は、**start-stop** キーワードの後ろに続きます。方式リスト タイプは、目的の順序で入力します。method 引数には次のタイプがあります。
  - **group tacacs+**：アカウンティングにすべての設定済み TACACS+ サーバのリストを使用します。

- **group radius—**アカウンティングにすべての設定済み RADIUS サーバのリストを使用します。
- **group** *group-name*：**aaa group server tacacs+** または **aaa group server radius** コマンドによって定義されている名前付きサーバ グループ、TACACS+ または RADIUS サーバのサブセットをアカウンティングに使用します。

- この例は、**default** コマンドによるアカウンティング方式リストの定義を示しています。アカウンティング サービスは TACACS+ セキュリティ サーバによって提供され、stop-only 制限が設定されています。

ステップ 3 **commit**

中間アカウンティング レコードの生成

アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。**aaa accounting update** コマンドをアクティブにすると、システム上のすべてのユーザの中間アカウンティング レコードが発行されます。

（注） 中間アカウンティング レコードは、インターネット キー交換（IKE）アカウンティングなど、ネットワーク セッションに対してのみ生成されます。これは、**network** キーワードを指定した **aaa accounting** コマンドで制御されます。システム、コマンドまたは EXEC アカウンティング セッションでは、中間レコードは生成されません。

手順

ステップ 1 **configure**

ステップ 2 **aaa accounting update** {**newinfo** | **periodic** *minutes*}

例：

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

アカウンティング サーバに送信される定期的中間アカウンティング レコードをイネーブルにします。

- **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、IPCP がリモート ピアとの間で IP アドレスのネゴシエーションを完了したときなどです。中間アカウンティング レコードには、リモート ピアに使用されるネゴシエート済み IP アドレスが含まれます。
- **periodic** キーワードを使用すると、中間アカウンティング レコードは引数の数字で定義されたとおり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、中間アカウン

ティング レコードが送信される時間までに、そのユーザについ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。

注意 **periodic** キーワードを使用すると、多数のユーザがネットワークにログインしているときに、大きな輻輳が生じる場合があります。

ステップ 3 **commit**

方式リストの適用

aaa authorization コマンドを使用して、特定のタイプの許可に対して名前付き許可方式リストを定義（またはデフォルトの方式リストを使用）した後、許可を実行する該当の回線に、定義済みのリストを適用する必要があります。**authorization** コマンドを使用し、選択した回線または回線グループに指定の方式リスト（または、方式リストを指定していない場合はデフォルトの方式リスト）を適用します。

手順

ステップ 1 **configure**

ステップ 2 **line** { **console** | **default** | **template** *template-name*}

例：

```
RP/0//CPU0:router(config)# line console
```

回線テンプレート コンフィギュレーション モードを開始します。

ステップ 3 **authorization** {**commands** | **exec**} {**default** | *list-name*}

例：

```
RP/0//CPU0:router(config-line)# authorization commands listname5
```

AAA 認可を特定の回線または回線のグループに対してイネーブルにします。

- **commands** キーワードは、すべてのコマンドに対して、選択した回線における許可を有効にします。
- **exec** キーワードは、インタラクティブ（XR EXEC モード）セッションに対する許可を有効にします。
- **default** キーワードを入力し、**aaa authorization** コマンドで定義されているように、デフォルトの方式リストの名前を適用します。
- 使用する認可方式リストの名前を入力します。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。
- 次に、方式リスト listname5 を使用したコマンド認可の例を示します。

ステップ 4 **commit**

次のタスク

AAA 認可をイネーブルにして認可方式リストを適用したら、AAA アカウンティングをイネーブルにしてアカウンティング方式リストを適用します

アカウンティング サービスのイネーブル化

アカウンティング サービスを特定の回線または回線のグループに対してイネーブルにします。

手順

ステップ 1 **configure**

ステップ 2 **line { console | default | template template-name}**

例：

```
RP/0//CPU0:router(config)# line console
```

回線テンプレート コンフィギュレーション モードを開始します。

ステップ 3 **accounting** {**commands** | **exec**} {**default** | *list-name*}

例：

```
RP/0//CPU0:router(config-line)# accounting commands listname7
```

AAA アカウンティングを特定の回線または回線のグループに対してイネーブルにします。

- **commands** キーワードは、すべての XR EXEC モード シェル コマンドに対して、選択した回線におけるアカウンティングを有効にします。
- **exec** キーワードは、インタラクティブ（XR EXEC モード）セッションに対するアカウンティングを有効にします。
- **default** キーワードを入力し、**aaa accounting** コマンドで定義されているように、デフォルトの方式リストの名前を適用します。
- 使用するアカウンティング方式リストの名前を指定します。リスト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 accounting** コマンドを使用して作成されます。
- 次に、方式リスト listname7 を使用したコマンド アカウンティングの例を示します。

ステップ 4 **commit**

次のタスク

AAA アカウンティング サービスをイネーブルにしてアカウンティング方式リストを適用したら、ログイン パラメータを設定します

ログイン パラメータの設定

サーバがログインの応答を待機する間隔を設定します。

手順

ステップ 1 **configure**

ステップ 2 **line template** *template-name*

例：

```
RP/0//CPU0:router(config)# line template alpha
```

設定する回線を指定して、回線テンプレート コンフィギュレーション モードを開始します。

ステップ 3 **timeout login response** *seconds*

例：

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

サーバがログインの応答を待つ時間を設定します。

- *seconds* 引数には、タイムアウト間隔（秒単位）を 0 ～ 300 の範囲で指定します。デフォルトは 30 秒です。
- この例では、インターバル タイマーを 20 秒に変更します。

ステップ 4 **commit**

タスク マップ

外部 TACACS+ サーバおよび RADIUS サーバを使用して認証されるユーザに対して、Cisco IOS XR ソフトウェア AAA は、タスク ID をリモートで定義する方式をサポートします。

タスク ストリングの形式

TACACS+ サーバのコンフィギュレーション ファイルのタスク文字列は、カンマ（,）で区切られたトークンで構成されます。各トークンは、タスク ID 名およびその許可、またはこの特定のユーザを含むユーザ グループのいずれかで構成されます（次の例を参照）。

task = “ *permissions* : *taskid name* , # *usergroup name* , ...”

（注） Cisco IOS XR ソフトウェアでは、タスク ID を外部 RADIUS または TACACS+ サーバの属性として指定できます。サーバが非 Cisco IOS XR ソフトウェア システムと共有される場合、これらの属性には、サーバ マニュアルで示されているように、オプション マークが付けられます。たとえば、CiscoSecure ACS および Cisco のフリーウェア TACACS+ サーバでは、オプション属性の属性値の前に等号記号（=）ではなく、アスタリスク（*）が必要です。属性をオプションとして設定する場合、TACACS+ サーバのマニュアルを参照してください。

たとえば、user1 BGP という名前のユーザに、read、write および execute 許可を付与し、user1 を operator という名前のユーザ グループに含める場合、外部サーバの TACACS+ コンフィギュレーション ファイルのユーザ名エントリは次のようになります。

```
user = user1{
member = some-tac-server-group
opap = cleartext "lab"
service = exec {
task = "rwx:bgp,#operator"
}
}
```

r、w、x、d はそれぞれ read、write、execute、debug に対応し、ポンド記号（#）はユーザ グループが続くことを示します。

（注） Cisco IOS ソフトウェアに基づいたシステムとの相互運用性をイネーブルにするには、「task」の前にオプション キーワードを追加する必要があります。

CiscoSecure ACS が使用される場合、次の手順を実行して、タスク ID とユーザ グループを指定します。

手順

ステップ 1 ユーザ名とパスワードを入力します。

ステップ 2 [**Group Setup**] ボタンをクリックすると、[**Group Setup**] ウィンドウが表示されます。

ステップ 3 [Group] ドロップダウン リストから、更新するグループを選択します。

ステップ 4 [**Edit Settings**] ボタンをクリックします。

ステップ 5 スクロール矢印を使用して、[Shell (exec)] チェックボックスを探します。

ステップ 6 [**Shell (exec)**] チェックボックスをオンにして、カスタム属性設定を有効にします。

ステップ 7 [**Custom attributes**] チェックボックスをオンにします。

ステップ 8 フィールドに空白や引用符を含めずに次のタスク文字列を入力します。

例：

```
task=rwx:bgp,#netadmin
```

ステップ 9 [**Submit + Restart**] ボタンをクリックしてサーバを再起動します。

次の RADIUS ベンダー固有属性（VSA）の例では、ユーザは、sysadmin 事前定義タスク グループに含まれ、BGP を設定でき、OSPF の設定を表示できます。

例：

```
user Auth-Type := Local, User-Password == lab
        Service-Type = NAS-Prompt-User,
        Reply-Message = "Hello, %u",
        Login-Service = Telnet,
        Cisco-AVPair = "shell:tasks=#sysadmin,rwx:bgp,r:ospf"
```

user1 がユーザ名 user1 と適切なパスワードを使用して、正常に外部 TACACS+ サーバに接続してログインすると、XR EXEC モードで **show user tasks** コマンドを使用して、user1 が実行可能なタスクをすべて表示できます。次に例を示します。

例：

```
Username:user1
Password:
RP/0/RP0/cpu 0: router# show user tasks

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

タスク文字列が指定されていない user2 という名前のユーザが外部サーバにログインすると、次の情報が表示されます。

例：

```
Username:user2
Password:
RP/0/RP0/cpu 0: router# show user tasks
No task ids available
```

AAA サービスに関する情報

この項には、AAA でユーザ グループやタスク グループを設定したり、リモート認証ダイヤルインユーザ サービス（RADIUS）サーバまたは TACACS+ サーバを設定したりする前に、ソフトウェア ユーザが理解しておく必要があるすべての概念情報が記載されています。概念情報では、AAA について、およびなぜ重要なのかについても説明します。

ユーザ、ユーザグループおよびタスクグループ

ユーザ属性は、この Cisco ソフトウェアの管理モデルの基礎となるものです。各ルータ ユーザには、次の属性が関連付けられます。

- 管理ドメイン内でユーザを一意に特定するユーザ ID（ASCII 文字列）

- 253 文字以下のパスワードおよび一方向の暗号化シークレット
- ユーザがメンバである（タスク ID などの属性をイネーブルにした）ユーザ グループ（1 つ以上）のリスト

ユーザ カテゴリ

ルータ ユーザは、次のカテゴリに分類されます。

- ルート セキュア ドメイン ルータ（SDR）ユーザ（特定の SDR 管理権限）
- SDR ユーザ（特定の SDR ユーザ アクセス）

ルート システム ユーザ

ルート システム ユーザは、ルータ シャーシ全体の「所有」が許可されたエンティティです。ルート システム ユーザは、すべてのルータ コンポーネントに対して最も高い特権を持って操作し、システム内のすべてのセキュア ドメイン ルータをモニタできます。ルータの設定時に、少なくとも 1 つのルート システム ユーザ アカウントを作成する必要があります。ルート システム ユーザは複数作成できます。

ルート システム ユーザは次を含む設定またはモニタ タスクを実行できます。

- セキュア ドメイン ルータを設定します。
- ルート SDR ユーザを作成、削除、変更します（ルート システムとしてセキュア ドメイン ルータにログイン後）。
- セキュア ドメイン ルータ ユーザを作成、削除、変更し、ユーザ タスクの権限を設定します（ルート システムとしてセキュア ドメイン ルータにログイン後）。
- セキュア ドメイン ルータに割り当てられていないファブリック ラックまたはルータ リソースにアクセスし、セキュア ドメイン ルータの設定に関係なく、ルート システム ユーザが任意のルータ ノードに認証されるようにします。

ルート SDR ユーザ

ルート SDR ユーザは、特定の SDR の設定およびモニタリングを制御します。ルート SDR ユーザは、ユーザを作成し、SDR 内での権限を設定できます。複数のルート SDR ユーザが独立して作業できます。1 つの SDR に、複数の SDR ユーザを作成できます。

ルート SDR ユーザは、特定の SDR に対して次の管理タスクを実行できます。

- SDR のセキュア ドメイン ルータ ユーザおよび権限を作成、削除、変更します。
- SDR にアクセスできるユーザ グループを作成、削除、変更します。
- SDR のほぼすべてを管理します。

ルート SDR ユーザは、ルート システム ユーザへのアクセスを拒否できません

セキュア ドメイン ルータ（SDR）ユーザ

SDR ユーザには、ルート SDR ユーザによって定義された SDR への制限付きアクセス権があります。SDR ユーザは、日常のシステムおよびネットワーク管理アクティビティを行います。セキュア ドメイン ルータ ユーザが実行できるタスクは、そのユーザが属するユーザ グループに関連付けられているタスク ID によって決まりますシャーシ内での複数の SDR はサポートされません。

ユーザ グループ

ユーザ グループは、アクセス権限など、属性のセットを共有するユーザの集まりです。Cisco ソフトウェアでは、システム管理者は、ユーザのグループ、およびユーザのグループに共通するジョブ特性を設定できます。ユーザはデフォルトでグループに割り当てられないので、明示的に割り当てる必要があります。ユーザは、複数のグループに割り当てることができます。

各ユーザは、1 つ以上のユーザ グループに関連付けることができます。ユーザ グループは、次の属性を持ちます。

- ユーザ グループは、ユーザの認証を定義するタスク グループのリストから構成されます。cisco-support 以外のすべてのタスクは、デフォルトで、ルート システム ユーザに許可されています
- 各ユーザ タスクには、読み取り、書き込み、実行またはデバッグ権限を割り当てることができます。

事前定義ユーザ グループ

この Cisco ソフトウェアには、属性が定義済みの一連のユーザ グループが用意されています。事前定義されているグループは次のとおりです。

- **cisco-support**：このグループは、Cisco サポート チームが使用します。
- **netadmin**：すべてのシステムおよびネットワーク パラメータを制御およびモニタできます。
- **operator**：基本権限を持つデモンストレーション グループ。
- **root-lr**：特定のセキュア ドメイン ルータを制御およびモニタできます。
- **sysadmin**：すべてのシステム パラメータを制御およびモニタできますが、ネットワーク プロトコルを設定できません。
- **serviceadmin**：セッション ボーダー コントローラ（SBC）などのサービス管理タスク。

ユーザ定義ユーザ グループ

管理者は、特定のニーズを満たすために自分のユーザ グループを設定できます。

ユーザ グループの継承

ユーザ グループは、別のユーザ グループから属性を継承できます。（同様に、タスク グループは、別のタスク グループから属性を継承できます）。たとえば、ユーザ グループ A がユーザ グループ B から属性を継承すると、ユーザ グループ A の新しいタスク属性セットは、A と B との集合になります。グループ A がグループ B から属性を継承する場合は、グループ B を

明示的に再継承しなくても、グループ B での変更がグループ A に反映されます。この点で、ユーザ グループ間の継承関係は動的です。

タスク グループ

タスク グループは、アクションのタイプ（read、write など）に対応した許容タスク ID のリストによって定義します。タスク ID は、ルータ システムで基本的に定義されます。外部ソフトウェアのタスク グループを設定するには、タスク ID 定義が事前にサポートされている必要があります。

タスク ID は、外部 TACACS+ サーバまたは RADIUS サーバで設定できます。

事前定義タスク グループ

次に、管理者が通常の初期設定で使用できる事前定義タスク グループを示します。

- **cisco-support**：Cisco サポート担当タスク
- **netadmin**：ネットワーク管理者タスク
- **operator**：オペレータの日常業務（デモンストレーション目的）
- **root-lr**：セキュア ドメイン ルータ管理者タスク
- **sysadmin**：システム管理者タスク
- **serviceadmin**：SBC などのサービス管理タスク

ユーザ定義タスク グループ

ユーザは、特定のニーズを満たすために独自のタスク グループを設定できます。

グループ継承

タスク グループは、他のタスク グループからの継承をサポートします（同様に、ユーザ グループは、別のユーザ グループから属性を継承できます。たとえば、タスク グループ A がタスク グループ B から継承する場合、タスク グループ A の新しい属性セットは A と B の集合となります。

XR モードおよび管理モードでのコマンド アクセス

admin コマンドを使用して XR モードからシステム管理モードにアクセスすると、XR ユーザ グループとタスクが システム管理 VM グループにマッピングされます。ユーザは システム管理 VM で対応するアクセス権限を使用できます。現時点では、AAA グループ、管理タスク グループ、root lr グループのみが システム管理 VM グループまたはタスクにマッピングされます。プロトコルなどの他のタスクはマッピングされません。システム管理 VM ではこれらのサービスがサポートされていないからです。システム管理 VM のディザスタ リカバリ ユーザは、ホスト VM と同期されます。

XR のタスクまたはグループ	Sysadmin VM グループ	アクセス	例
root-lr	ルートシステム グループ	システム設定へのフルアクセス	RP/0/RP0/CPU0:ios#show user group Mon Nov 3 13:48:54.536 UTC root-lr, cisco-support RP/0/RP0/CPU0:ios#show user tasks | inc root-lr Mon Nov 3 13:49:06.495 UTC Task: root-lr : READ WRITE EXECUTE DEBUG (reserved) RP/0/RP0/CPU0:ios#admin sysadmin-vm:0_RP0# show aaa user-group Mon Nov 3 13:48:00.790 UTC User group : root-system
Admin-r/w/x/d	Admin-r	Sysadmin VM で読み取り専用コマンド	taskgroup tg-admin-write task write admin task execute admin ! usergroup ug-admin-write taskgroup tg-admin-write ! username admin-write group ug-admin-write password admin-write ! RP/0/RP0/CPU0:ios#show user group Mon Nov 3 14:09:29.676 UTC ug-admin-write RP/0/RP0/CPU0:ios#show user tasks Mon Nov 3 14:09:35.244 UTC Task: admin : READ WRITE EXECUTE RP/0/RP0/CPU0:ios#admin Mon Nov 3 14:09:40.401 UTC admin-write connected from 127.0.0.1 using console on xr-vm_node0_RP0_CPU0 sysadmin-vm:0_RP0# show aaa user-group Mon Nov 3 13:53:00.790 UTC User group : admin-r

XR のタスクまたはグループ	Sysadmin VM グループ	アクセス	例
Netadmin または sysadmin グループ Admin-r/ wx /d, aaa -r/w/x/d	Aaa -r および admin -r	Sysadmin VM で読み取り専用コマンド	RP/0/RP0/CPU0:ios#show user group Mon Nov 3 13:44:39.176 UTC netadmin RP/0/RP0/CPU0:ios#show user tasks | inc aaa Mon Nov 3 13:45:00.999 UTC Task: aaa : READ RP/0/RP0/CPU0:ios#show user tasks | inc admin Mon Nov 3 13:45:09.567 UTC Task: admin : READ RP/0/RP0/CPU0:ios#admin Mon Nov 3 13:46:21.183 UTC netadmin connected from 127.0.0.1 using console on xr-vm_node0_RP0_CPU0 sysadmin-vm:0_RP0# show aaa user-group Mon Nov 3 13:44:23.939 UTC User group : admin-r,aaa-r sysadmin-vm:0_RP0#

管理モデル

ルータは、管理（admin）プレーンとセキュア ドメイン ルータ（SDR）プレーンの 2 つのプレーンで機能します。admin（共有）プレーンは、すべての SDR で共有されるリソースで構成され、SDR プレーンは、特定の SDR に固有なリソースで構成されます。

各 SDR には、ローカル ユーザ、グループ、TACACS+ および RADIUS 設定など、独自の AAA 設定があります。1 つの SDR で作成されたユーザは、これらのユーザが他の SDR で設定されない限り、他の SDR にアクセスできません。

管理アクセス

システムへの管理アクセスは、次の操作を十分理解していない場合、または注意して計画していない場合、失われる可能性があります。

- 使用できないリモート AAA サーバを使用する認証（特にコンソールの認証）を設定する。

（注） 他の方式リストを指定せずに **none** オプションを使用することはサポートされていません。

- コンソールでコマンド認可または XR EXEC モード認可を設定する場合は十分に注意してください。これは、この設定により TACACS+ サーバが使用できなくなる、またはすべてのコマンドが拒否され、ユーザがロックアウトされる場合があるためです。このロックアウトは、特に、TACACS+ サーバで認識されていないユーザで認証が行われる場合、あるいは TACACS+ ユーザで何らかの理由によりほとんど、またはすべてのコマンドが拒否される場合に発生します。

ロックアウトを回避するには、次のいずれか、または両方を推奨します。

- コンソールで TACACS+ コマンド認可または XR EXEC モード認可を設定する前に、認可を設定するユーザが、TACACS+ プロファイルの適切なユーザ権限を使用してログインしていることを確認してください。
- サイトのセキュリティ ポリシーで許可されている場合は、コマンド認可や XR EXEC モード認可に **none** オプションを使用します。これにより、TACACS+ サーバに到達できない場合に、AAA が **none** 方式にロールオーバーするので、ユーザはコマンドを実行することができます。

AAA データベース

AAA データベースは、ユーザ、グループ、およびシステムへのアクセスを制御するタスクの情報を保存します。AAA データベースはローカルまたはリモートにできます。特定の状況で使用されるデータベースは、AAA 設定により異なります。

ローカル データベース

ユーザ、ユーザ グループ、タスク グループなどの AAA データは、セキュア ドメイン ルータ内でローカルに保存できます。このデータは、メモリ内データベースに保存され、コンフィギュレーション ファイルに保存されます。保存されたパスワードは暗号化されます。

（注） データベースは、保存されている特定のセキュア ドメイン ルータ（SDR）に対してローカルで、定義されているユーザまたはグループは、同じシステムの他の SDR に表示されません。

残りすべてのユーザをローカル データベースから削除できます。すべてのユーザを削除すると、ユーザが次にログインするときに、設定ダイアログが表示され、新しいユーザ名およびパスワードを入力するよう求められます。

（注） 設定ダイアログは、ユーザがコンソールにログインするときだけ表示されます。

リモート データベース

AAA データは、CiscoSecure ACS などの外部セキュリティ サーバに保存することができます。サーバに保存されているデータは、クライアントがサーバの IP アドレスと共有秘密がわかっていれば、任意のクライアント（ネットワーク アクセス サーバ [NAS] など）が使用できます。

リモート *AAA* 設定

CiscoSecure ACS のような製品は、共有または外部 AAA データベースを管理するために使用できます。ルータは、標準的な IP ベースのセキュリティ プロトコル（TACACS+ または RADIUS など）を使用してリモート AAA サーバと通信します。

クライアント設定

セキュリティ サーバは、ルータと共有するシークレット キーおよびクライアントの IP アドレスで設定する必要があります。

ユーザ グループ

外部サーバで作成されるユーザ グループは、ルータのローカル AAA データベース設定のユーザ グループとは関係がありません。外部 TACACS+ サーバまたは RADIUS サーバ ユーザ グループの管理は別であるため、ルータはユーザ グループ構造を認識しません。リモート ユーザまたはグループ プロファイルには、ユーザが属するグループ（ルータで定義）、および個々のタスク ID を指定する属性を含めることができます。

外部サーバのユーザ グループの設定は、個々のサーバ製品の設計により異なります。該当するサーバ製品のマニュアルを参照してください。

タスク グループ

タスク グループは、アクションのタイプ（read、write など）に対応した許容タスク ID のリストによって定義します。タスク ID は、ルータ システムで基本的に定義されます。外部ソフトウェアのタスク グループを設定するには、タスク ID 定義が事前にサポートされている必要があります。

タスク ID は、外部 TACACS+ サーバまたは RADIUS サーバで設定できます。

AAA 設定

ここでは、AAA 設定についての情報を提供します。

方式リスト

AAA データは、さまざまなデータ ソースに保存できます。AAA 設定は、方式リストを使用して、AAA データのソースの優先順位を定義します。AAA は、複数の方式リストを定義でき、アプリケーション（ログインなど）は、これらのいずれかを選択できます。たとえば、コンソール ポートと VTY ポートとで異なる方式リストを使用できます。方式リストが指定されていない場合、アプリケーションは、デフォルトの方式リストを使用します。デフォルトの方式リストが存在しない場合、AAA は、ローカル データベースとしてソースを使用します。

ロールオーバー メカニズム

AAA は、データベース オプションの優先順位リストを使用するよう設定できます。システムがデータベースを使用できない場合、リストの次のデータベースに自動的にロールオーバーします。認証、認可またはアカウンティング要件がデータベースで拒否されると、ロールオーバーは発生せず、要求が拒否されます。

次の方法が選択可能です。

- Local：ローカルで設定されるデータベースを使用します（アカウンティングや一部の認可には適していません）。
- TACACS+：TACACS+ サーバ（CiscoSecure ACS など）を使用します。
- RADIUS：RADIUS サーバを使用します。
- Line：回線パスワードおよびユーザ グループを使用します（認証のみに適しています）。

• None：要求を許可します（認証には適していません）。

サーバのグループ化

サーバの1つのグローバル リストを保持する代わりに、さまざまなAAAプロトコル（RADIUS や TACACS+ など）用のサーバ グループを作成し、AAA アプリケーション（PPP や XR EXEC モードなど）に関連付けることができます。

認証

認証は、プリンシパル（ユーザまたはアプリケーション）がシステムへのアクセスを取得する最も重要なセキュリティ プロセスです。プリンシパルは、管理ドメインで一意であるユーザ名（またはユーザ ID）により定義されます。ユーザにサービスを提供するアプリケーション（または管理エージェントなど）は、ユーザからユーザ名およびクレデンシャルを取得します。AAA は、アプリケーションにより渡されたユーザ名およびクレデンシャルに基づいて認証を実行します。認証ユーザのロールは、ユーザが属する 1 つ以上のグループにより決まります（ユーザは、1 つ以上のユーザ グループのメンバにすることができます）。

所有者以外のセキュア ドメイン ルータ ユーザの認証

所有者以外のセキュア ドメイン ルータにログインする場合、ルート システム ユーザは、「@admin」サフィクスをユーザ名に追加する必要があります。「@admin」サフィクスを使用すると、認証要求が所有者のセキュア ドメイン ルータに送信され、確認されます。所有者のセキュア ドメイン ルータは、認証方式の選択にリスト名 **remote** を使用します。**remote** 方式リストは、**aaa authentication login remote** *method1 method2 ...* コマンドを使用して設定されます。

所有者のセキュア ドメイン ルータ ユーザの認証

所有者のセキュア ドメイン ルータ ユーザは、所有者のセキュア ドメイン ルータ ユーザに関連付けられている特定のセキュア ドメイン ルータに属するノードだけにログインできます。ユーザが root-sdr グループのメンバである場合、ユーザは、所有者のセキュア ドメイン ルータ ユーザとして認証されます。

セキュア ドメイン ルータ ユーザの認証

セキュア ドメイン ルータ ユーザの認証は、所有者のセキュア ドメイン ルータ ユーザの認証と似ています。あるユーザが、指定された所有者のセキュア ドメイン ルータ ユーザ グループのメンバーであると判明しなかった場合、そのユーザはセキュア ドメイン ルータ ユーザとして認証されます。

認証フロー制御

AAA は、次のプロセスに従い認証を実行します。

1. ユーザが、ユーザ名およびパスワード（またはシークレット）を提供して認証を要求します。
2. AAAが、ユーザのパスワードを検証して、パスワードがデータベースのものと一致しない場合ユーザを拒否します。
3. AAA が、ユーザのロールを決定します（ルート SDR ユーザまたは SDR ユーザ）。

- ユーザが所有者のセキュア ドメイン ルータ ユーザ グループのメンバとして設定されている場合、AAA は、そのユーザを所有者のセキュア ドメイン ルータ ユーザとして認証します。
- ユーザがある所有者のセキュア ドメイン ルータ ユーザ グループのメンバーとして設定されていない場合、AAA は、そのユーザを所有者のセキュア ドメイン ルータ ユーザとして認証します。

クライアントは、ユーザの許可されているタスク ID を認証中に取得できます。この情報は、ユーザが属するユーザ グループで指定されているすべてのタスク グループ定義の集合を形成することで取得されます。このような情報を使用するクライアントは、通常、タスク ID セットが静的であるユーザのセッション（API セッションなど）を作成します。XR EXEC モードおよび外部 API クライアントは、どちらもこの機能を使用して操作を最適化できます。XR EXEC モードは該当しないコマンドを非表示にでき、EMS アプリケーションは、たとえば、該当しないグラフィカル ユーザ インターフェイス（GUI）メニューを無効にできます。

ユーザ グループ メンバーシップなどのユーザの属性やタスク権限が変更されると、これらの変更された属性は、ユーザの現在アクティブなセッションでは反映されません。これらは、ユーザの次のセッションで有効になります。

パスワード タイプ

ユーザおよびそのユーザのグループ メンバーシップを設定する場合、暗号化またはクリア テキストの 2 つのパスワードを指定できます。

ルータは、二方向および一方向（シークレット）の両方の暗号化ユーザ パスワードをサポートします。オリジナルの暗号化されていないパスワード文字列が暗号化シークレットからは推測できないため、シークレット パスワードはユーザ ログイン アカウントに適しています。アプリケーションによっては（PPP など）、パケットでのパスワードの送信など、独自の機能のための保存パスワードを復号化する必要があるので、二方向のみのパスワードが必要です。ログイン ユーザでは、両方のタイプのパスワードを設定できますが、一方のパスワードがすでに設定されている状態でもう一方のパスワードを設定すると、警告メッセージが表示されます。

シークレットとパスワードの両方をユーザに設定すると、ログインなど、復号化できるパスワードを必要としないすべての操作で、シークレットが優先されます。PPP などのアプリケーションでは、シークレットが存在する場合でも、二方向の暗号化パスワードが使用されます。

タイプ 8 とタイプ 9 のパスワード

この機能は、AAA セキュリティ サービスでタイプ 8 およびタイプ 9 のパスワードのオプションを提供します。タイプ 8 およびタイプ 9 のパスワードは、パスワードを各ユーザ名に保存するためのよりセキュアで堅牢なサポートを提供します。したがって、多くの機密データを維持する必要があるシナリオでは、これらの暗号化方式によって管理者や他のユーザ パスワードが強力に保護されます。

タイプ 8 パスワードの実装では SHA256 ハッシュ アルゴリズムが使用され、タイプ 9 パスワードは scrypt ハッシュ アルゴリズムを使用します。

（注） タイプ 8 およびタイプ 9 のパスワードは、Cisco IOS XR ソフトウェア Release 7.0.1 以降の IOS XR 64 ビットオペレーティングシステムでサポートされています。

タイプ *10* パスワード

Cisco IOS XR 64 ビットソフトウェアには、**SHA512** 暗号化アルゴリズムを使用するタイプ 10 パスワードのサポートが導入されています。**SHA512** 暗号化アルゴリズムは、**MD5** や **SHA256** などの古いアルゴリズムと比較して、ユーザパスワードのセキュリティを向上させます。この機能を使用すると、**SHA512** は、最初のユーザ作成シナリオであっても、ユーザ名設定のパスワードのデフォルトの暗号化アルゴリズムになります。タイプ 10 パスワードが導入されるまでは、デフォルトのアルゴリズムとして **MD5** が使用されていました。

タイプ 10 パスワードを設定するには、タイプ 10 パスワードの設定 （7 ページ）を参照してください。

タイプ 10 パスワードの使用に関する制約事項

この制約事項は、タイプ 10 パスワードの使用に適用されます。

- まだ **MD5** または **SHA256** の暗号化アルゴリズムを使用している下位バージョンにダウングレードする場合に設定の損失、認証の失敗などの下位互換性の問題が予期されます。このような問題の影響を最小限に抑えるには、このようなダウングレードの前にパスワードをタイプ 10 に変換します。詳細については、パスワードタイプの下位互換性 （9 ページ）を参照してください。
- 最初のユーザ設定シナリオの場合やユーザを再設定する場合、システムは XR VM からシステム管理 VM のタイプ 5 とタイプ 10 のパスワードとホスト VM のみを同期します。このようなシナリオでは、タイプ 8 とタイプ 9 のパスワードは同期されません。

タスクベースの認可

AAA は、CLI または API を介した操作の任意の制御、設定またはモニタに「タスク許可」を使用します。特権レベルに関する Cisco IOS ソフトウェアの概念は、ソフトウェアではタスクベースの認可システムに置き換えられています。

タスク *ID*

ユーザによる Cisco ソフトウェアの制御、設定、モニタを可能にする操作タスクは、タスク ID 別に示されます。タスク ID は、コマンドで操作をする許可を定義します。ユーザには、ルータに許可されているアクセスの範囲を定義するタスク ID のセットが関連付けられます。

タスク ID は、次のようにしてユーザに割り当てられます。

各ユーザは、1 つの以上のユーザ グループに関連付けられます。各ユーザ グループは 1 つ以上のタスク グループに関連付けられます。次に、各タスク グループは、一連のタスク ID によって定義されます。つまり、ユーザと特定のユーザ グループを関連付けることで、そのユーザと

タスク ID の特定のセットが関連付けられます。タスク ID に関連付けられたユーザは、そのタスク ID に関連する処理を実行できます。

タスク *ID* に関する一般的な使用上のガイドライン

大部分のルータ制御、設定、モニタリング操作（CLI、Netconf、Restconf、XML API）には、特定の タスク ID セットが関連付けられています。通常、特定の CLI コマンドまたは API イノベーションは、1 つ以上のタスク ID が関連付けられます。config および commit コマンドでは、特定のタスク ID 許可は必要ありません。設定およびコミット操作では、特定のタスク ID 許可は必要ありませんエイリアスでもタスク ID 許可は必要ありません。コンフィギュレーション交換は、root-lr 許可が割り当てられるまで実行できません。コンフィギュレーションモードを開始しない場合、TACACS+ コマンド認可を使用して、config コマンドを拒否できます。これらの関連付けは、ルータ内でハードコード化されていて、変更できません。タスク ID は、特定のタスクを実行する許可を付与します。タスク ID では、タスクを実行する許可は拒否されません。タスク ID 操作は、次の表にリストされているクラスの 1 つ、すべて、または任意の組み合わせにすることができます。

（注） Restconf は今後のリリースでサポートされる予定です。

表 *1:* タスク *ID* クラス

動作	説明
Read	読み取り専用操作を許可します。
Write	変更操作を許可、および読み取り操作を暗黙的に許可します。
Execute	ping や Telnet などのアクセス操作を許可します。
Debug	デバッグ操作を許可します。

システムは、各 CLI コマンドおよび API イノベーションがユーザのタスク ID 許可リストと一致しているか検証します。CLI コマンドの使用時に問題が発生した場合、システム管理者に連絡してください。

スラッシュで区切られた複数のタスク ID 操作（read/write など）は、両方の操作が指定のタスク ID に適用されることを示します。

カンマで区切られた複数のタスク ID 操作（read/write, execute など）は、両方の操作が個々のタスク ID に適用されることを示します。たとえば、**copy ipv4 access-list** コマンドを使用すると、読み取りおよび書き込み操作を acl タスク ID に適用し、実行操作を filesystem タスク ID に適用できます。

タスク ID と操作の列に値が指定されていない場合は、このコマンドの使用に際して、タスク ID および操作との以前の関連付けは考慮されません。また、ROM モニタ コマンドを使用するために、ユーザにタスク ID を関連付ける必要はありません。

コマンドが特定のコンフィギュレーションサブモードで使用される場合、そのコマンドを使用するための追加タスク ID をユーザに関連付ける必要があります。たとえば、**show redundancy** コマンドを実行するには、システム（read）タスク ID と操作をユーザに関連付ける必要があります（次の例を参照）。

```
RP/0/RP0/cpu 0: router# show redundancy
```

TACACS+ および RADIUS 認証ユーザのタスク ID

Cisco ソフトウェアの AAA では、TACACS+ および RADIUS 方式で認証されるユーザに次の方法でタスク許可を割り当てることができます。

- タスク マップのテキスト バージョンを、外部 TACACS+ および RADIUS サーバのコンフィギュレーション ファイルに直接指定します。
- 外部 TACACS+ および RADIUS サーバのコンフィギュレーション ファイルで特権レベルを指定します。
- TACACS+ および RADIUS 方式で認証するユーザと同じユーザ名でローカル ユーザを作成します。
- 許可が TACACS+ および RADIUS 方式で認証する任意のユーザに適用されるデフォルト タスク グループを設定別に指定します。

特権レベル マッピング

タスク ID の概念をサポートしない TACACS+ デーモンとの互換性のため、AAA は外部 TACACS+ サーバ設定ファイル内でユーザに定義されている特権レベルとローカル ユーザ グループとの間のマッピングをサポートします。TACACS+ 認証後、外部 TACACS+ サーバから返される権限レベルからマッピングされたユーザ グループのタスク マップがユーザに割り当てられます。たとえば、特権レベル 5 が外部 TACACS サーバから返された場合、AAA はローカル ユーザ グループ priv5 のタスク マップを取得することを試みます。このマッピング プロセスは、1 ～ 13 の他の特権レベルでも同様です。特権レベル 14 は、ユーザ グループ オーナー SDR にマッピングされます。

たとえば、Cisco のフリーウェア TACACS+ サーバでは、コンフィギュレーション ファイルは、次の例に示すようにコンフィギュレーション ファイルで *priv_lvl* を指定する必要があります。

```
user = sampleuser1{
    member = bar
    service = exec-ext {
        priv_lvl = 5
    }
}
```

この例の 5 という数値は、ユーザの *sampleuser* に割り当てる必要がある任意の特権レベルに置き換えることができます。

AAA サービスの XML スキーマ

Extensible Markup Language（XML）インターフェイスは、XML ドキュメント形式で要求と応答を使用して、AAA を設定およびモニタします。AAA コンポーネントは、設定およびモニタリングに使用されるデータの内容と構造に対応するXMLスキーマを発行します。XMLツールおよびアプリケーションは、このスキーマを使用して、XML エージェントと通信して設定を実行します。

次のスキーマは、AAA を使用して発行されます。

- 認証、認可、アカウンティング設定
- ユーザ、ユーザ グループおよびタスク グループ設定
- TACACS+ サーバおよびサーバ グループ設定
- RADIUS サーバおよびサーバ グループ設定

AAA サービスの *Netconf* および *Restconf*

XML スキーマと同様、NetconfおよびRestconfでは、ユーザ名とパスワードはローカル サービスまたはトリプル A（AAA）サービスによって制御されます。

（注） Restconf は今後のリリースでサポートされる予定です。

RADIUS について

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では、RADIUS クライアントはCisco ルータ上で稼働します。認証要求とアカウンティング要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

RADIUSは完全にオープンなプロトコルであり、ソース コード形式で配布されているため、現在使用できる任意のセキュリティ システムと連携するように変更できます。

シスコは、AAA セキュリティ パラダイムの下で RADIUS をサポートしています。RADIUS は、TACACS+、Kerberos、ローカル ユーザ名の検索など、他の AAA セキュリティ プロトコルと併用できます。

（注） RADIUS はすべての Cisco プラットフォームでサポートされますが、RADIUS でサポートされる一部の機能は、指定されたプラットフォームだけで実行されます。

RADIUS は、リモート ユーザのネットワーク アクセスを維持すると同時に高度なレベルのセキュリティを必要とするさまざまなネットワーク環境に実装されています。

RADIUS は、アクセスのセキュリティが必要な次のネットワーク環境で使用できます。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数ベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティ システムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、「スマート カード」アクセス コントロール システムを使用するアクセス環境。ある事例では、RADIUS と Enigma のセキュリティ カードを併用してユーザを検証し、ネットワーク リソースに対するアクセス権を付与しています。
- すでに RADIUS を使用中のネットワーク。RADIUS 機能を持つ Cisco ルータをネットワークに追加できます。Terminal Access Controller Access Control System Plus（TACACS+）サーバに移行する場合、これが最初の手順となります。
- ユーザが単一のサービスにだけアクセスする必要があるネットワーク。RADIUS を使用すると、単一ホスト、単一ユーティリティ（Telnet など）、または単一プロトコル（ポイントツーポイント プロトコル（PPP））に対するユーザ アクセスを制御できます。たとえば、ユーザがログインすると、RADIUS は、IP アドレス 10.2.3.4 を使用してそのユーザが PPP を実行する権限を持っていることを識別し、定義済みのアクセス リストが開始されます。
- リソース アカウンティングが必要なネットワーク。RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、セキュリティおよび課金の独自ニーズを満たすこともできます。
- 事前認証をサポートしているネットワーク。ネットワークに RADIUS サーバを導入すると、AAA 事前認証を設定し、事前認証のプロファイルを設定できます。サービス プロバイダーが事前認証を使用すると、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービス レベル契約を提供できるようになります。

RADIUS が適さないネットワーク セキュリティ状況

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は次のプロトコルをサポートしていません。
  - NetBIOS Frame Control Protocol（NBFCP）
  - NetWare Asynchronous Services Interface（NASI）
  - X.25 PAD 接続
- ルータ間で接続している環境。RADIUS は、双方向認証を行いません。RADIUS は、ルータと RADIUS 認証を必要とするシスコ製以外のルータとの認証に使用できます。

- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS の動作

ユーザがログインを試行し、RADIUS を使用してアクセス サーバから認証を受ける場合、次の手順が発生します。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
    1. ACCEPT：ユーザが認証されたことを表します。
    1. REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
    1. CHALLENGE：RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。
    1. CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

    ACCEPT または REJECT 応答には、XR EXEC モードまたはネットワーク認可に使用される追加データが含まれています。RADIUS 認可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

    - ユーザがアクセスできるサービス。これには、Telnet、rlogin、ローカルエリア トランスポート（LAT）の各接続、および PPP、Serial Line Internet Protocol（SLIP）、XR EXEC モードの各サービスなどが該当します。
    - ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ。