ユーザープロファイルの作成および権限の割り当て

ルータ上の XR およびシステム管理設定へのアクセス権を管理するには、権限を割り当てたユーザープロファイルを作成します。権限はコマンド ルールとデータ ルールを使用して指定します。

ユーザー、グループ、コマンドルール、およびデータルールを作成するには、認証、許可、およびアカウンティング（AAA）コマンドを使用します。aaa コマンドはディザスタ リカバリ パスワードを変更する際にも使用します。

（注） 外部 AAA サーバーおよびサービスは、システム管理 VM からは設定できず、XR VM からのみ設定できます。

制御されていないアクセスをユーザーが行わないよう制限するために、AAA 認証を設定します。AAA 認証が設定されていない場合、ユーザーに割り当てられたグループに関連付けられたコマンドおよびデータルールはバイパスされます。IOS-XR ユーザーは、ネットワーク設定プロトコル（NETCONF）、Google 定義のリモート プロシージャ コール（gRPC）または任意の YANG ベースのエージェントを介して、IOS-XR 設定への完全な読み取り/書き込みアクセス権を持つことができます。制御されていないアクセスを許可しないようにするには、いずれかの設定を行う前に AAA 認証を有効にします。

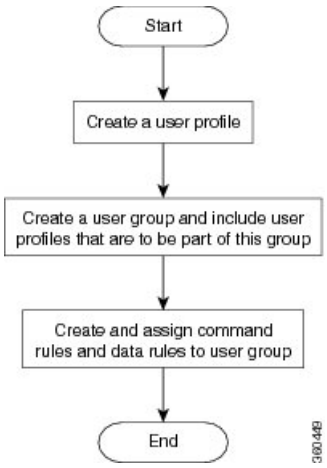
（注） XR 上のいずれかのユーザーが削除されている場合、ローカル データベースは、システム管理 VM に最初のユーザーが存在するかどうかを確認します。

- 最初のユーザーが存在する場合、同期は実行されません。
- 最初のユーザーが存在しない場合は、XR の最初のユーザー（作成順序に基づく）がシステム管理 VM に同期されます。
- ユーザーが XR に追加され、システム管理モードにユーザーが存在しない場合、そのユーザーは sysadmin-vm に同期されます。同期後、XR VM のユーザーに対する変更は、システム管理 VM では同期されません。
- システム管理 VM に追加されたユーザーが XR VM と同期しない。
- システム管理 VM で作成された最初のユーザーまたはディザスタリカバリユーザーのみがホスト VM と同期します。
- システム管理 VM の最初のユーザーまたはディザスタリカバリユーザーのログイン情報の変更は、ホスト VM と同期されます。
- システム管理 VM で削除された最初のユーザーまたはディザスタリカバリユーザーは、ホスト VM と同期されません。ホスト VM でユーザーが保持されます。

ユーザーの認証にはユーザー名とパスワードが使用されます。認証されたユーザーは、ユーザー グループに対して作成および適用されているコマンド ルールとデータ ルールに基づいて、コマンドを実行しデータ要素にアクセスする権利が与えられます。ユーザー グループに属するすべてのユーザーには、そのユーザー グループのコマンド ルールおよびデータ ルールで定義されているシステムへのアクセス権があります。

ユーザー プロファイルを作成するためのワークフローを次のフローチャートに示します。

図 *1*: ユーザー プロファイル作成のワークフロー



（注） ルータの初回起動時に作成された XR VM の root-lr ユーザーは、システム管理 VM の root-system ユーザーにマッピングされます。root-system ユーザーにはシステム管理 VM のスーパーユーザー権限があるため、アクセスは制限されません。

既存の AAA 設定を表示するには、コンフィギュレーション モードで **show run aaa** コマンドを使用します。

この章で説明する内容は次のとおりです。

ユーザーグループの作成

新しいユーザーグループを作成してコマンドルールとデータルールを関連付けます。コマンドルールおよびデータルールは、ユーザーグループに属するすべてのユーザーに適用されます。

ユーザーグループ、タスクグループ、RADIUS および TACACS 設定の作成の詳細については、*System Security Configuration Guide for Cisco ASR 9000 Series Routers*の「*AAA* サービスの設定」の章を参照してください。コマンド、構文、および構文の説明の詳細については、*System Security Command Reference for Cisco ASR 9000 Series Routers*の「認証、許可、およびアカウンティング コマンド」の章を参照してください。

XR VM でのユーザーグループの設定

ユーザー グループは、タスク グループなど一連のユーザー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、ユーザー 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、特定のユーザー 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ー 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ーだけ、ユーザー グループを設定できます。ユーザー 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。

ステップ 1 **configure**

例：

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

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **usergroup** *usergroup-name*

例：

```
RP/0/RSP0/cpu 0: router(config)# usergroup beta
```

特定のユーザー グループの名前を作成し、ユーザー 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、特定のユーザー 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/RSP0/cpu 0: router(config-ug)#
description this is a sample user group description
```

（任意）ステップ 2 で指定したユーザー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/RSP0/cpu 0: router(config-ug)#
inherit usergroup sales
```

- ユーザー 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/RSP0/cpu 0: router(config-ug)# taskgroup beta
```

ステップ 2 で指定したユーザー 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。

- ユーザー 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 で指定したユーザー 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** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。

- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

システム管理 VM でのユーザーグループの作成

システム管理 VM のユーザーグループを作成します。

ルータでは、最大 32 のユーザー グループがサポートされます。

始める前に

ユーザー プロファイルを作成します。「ユーザーの作成」の項を参照してください。

ステップ 1 **admin**

例：

```
RP/0/RSP0/cpu 0: router# admin
```

管理 EXEC モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

モードを開始します。

ステップ 3 **aaa authentication groups group** *group_name*

例：

```
sysadmin-vm:0_RP0(config)#aaa authentication groups group gr1
```

新しいユーザー グループ（まだ存在していない場合）を作成して、グループ コンフィギュレーション モードを開始します。この例では、ユーザー グループ「gr1」が作成されます。

（注） デフォルトで、root ユーザーの作成時にユーザー グループ「root-system」がシステムによって作成されます。root ユーザーはこのユーザー グループのメンバです。このグループに追加されたユーザーは root ユーザー権限を取得します。

ステップ 4 **users** *user_name*

例：

```
sysadmin-vm:0_RP0(config-group-gr1)#users us1
```

ユーザーグループに含めるユーザーの名前を指定します。

複数のユーザー名を二重引用符で囲んで指定することができますたとえば、**users** "*user1 user2 ...* "となります。

ステップ 5 **gid** *group_id_value*

例：

```
sysadmin-vm:0_RP0(config-group-gr1)#gid 50
```

数値を指定します。32 ビットの整数を入力できます。

ステップ 6 **commit** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。
- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

次のタスク

- コマンド ルールを作成します。
- データ ルールを作成します。

ユーザーの作成

新しいユーザーを作成し、特定の権限を持つユーザーグループにそのユーザーを含めることができます。ルータでは、最大で 1024 個のユーザープロファイルがサポートされます。

（注） システム管理 VM で作成したユーザーは、XR VM で作成したユーザーとは異なるため、システム管理 VM ユーザーのユーザー名とパスワードを使用して XR VM にアクセスすることはできません。逆も同様です。

XR VM およびシステム管理 VM ユーザー プロファイルの同期

ユーザープロファイルの初期同期：ユーザープロファイルを XR VM で初めて作成した場合、そのユーザーがシステム管理VMに存在しない場合のみ、ユーザー名とパスワードがシステム管理 VM に同期されます。この初期同期により、2 つの VM 間でのユーザー情報の一貫性が確保されます。

後続の変更の制限：ただし、システム管理 VM では、XR VM 内で行われた後続のパスワード変更やユーザーの削除は同期されないことに注意することが重要です。その結果、XR VM とシステム管理 VM のパスワードが異なり、XR VM 内での削除を反映するためにユーザープロファイルがリアルタイムで更新されない場合があります。

ユーザーの削除処理：さらに、XR VM 内でユーザーが削除されても、システム管理 VM 内の対応するユーザープロファイルは影響を受けません。つまり、XR VM でユーザーを削除しても、システム管理 VM のユーザープロファイルは自動的に削除されません。

ユーザーグループ、タスクグループ、RADIUS および TACACS 設定の作成の詳細については、*System Security Configuration Guide for Cisco ASR 9000 Series Routers*の「*AAA* サービスの設定」の章を参照してください。コマンド、構文、および構文の説明の詳細については、*System Security Command Reference for Cisco ASR 9000 Series Routers*の「認証、許可、およびアカウンティングコマンド」の章を参照してください。

XR VM でのユーザープロファイルの作成

表 *1*：機能の履歴（表）

機能名	リリース情報	機能説明
拡張ログインバナーの標準規格	リリース 7.3.1	US DoD に準拠するために、ログインバナーの表示を有効にするオプションが導入されました。ログインバナーは、成功したログイン試行回数と失敗したログイン試行回数、タイムスタンプ、ログイン方法などの情報を提供します。 login-history コマンドが導入されました。

各ユーザーは、管理ドメイン内で一意のユーザー名によって識別されます。各ユーザーは、少なくとも 1 つのユーザーグループのメンバーである必要があります。ユーザー 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ーが孤立する場合があります。AAA サーバーでは孤立したユーザーも認証されますが、ほとんどのコマンドは許可されません。

AAA の詳細については、*System Security Configuration Guide for Cisco ASR 9000 Series Routers*の「*AAA* サービスの設定」の章を参照してください。関連コマンド、構文、および構文の説明の詳細については、*System Security Command Reference for Cisco ASR 9000 Series Routers*の「認証、許可、およびアカウンティングコマンド」の章を参照してください。

ステップ 1 **configure**

例：

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

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **username** *user-name*

例：

```
RP/0/RSP0/cpu 0: router(config)# username user1
```

新しいユーザーの名前を作成（または現在のユーザーを識別）して、ユーザー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** | **8** | **9** | **10**} *secret*

例：

```
Router(config-un)# password 0 pwd1
```

または

```
Router(config-un)# secret 0 sec1
```

ステップ 2 で指定したユーザー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 で指定したユーザー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** 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** コマンドでは、次の値を入力できます。
  - **0** ：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を指定します。
  - **5** ：MD5 ハッシュアルゴリズムを使用するセキュアな暗号化パスワードが続くことを指定します。
  - **8** ：SHA256 ハッシュアルゴリズムを使用するタイプ 8 シークレットが続くことを指定します。
  - **9** ：scrypt ハッシュアルゴリズムを使用するタイプ 9 シークレットが続くことを指定します。

    （注） タイプ 8 およびタイプ 9 のシークレットは、Cisco IOS XR ソフトウェアリリース 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。リリース 7.0.1 より前は、IOS XR 32 ビット オペレーティング システムでのみサポートされていました。

  - **10** ：SHA512 ハッシュアルゴリズムを使用するタイプ 10 シークレットを指定します。

（注）
- タイプ 10 シークレットは、Cisco IOS XR 64 ビットプラットフォームでのみサポートされています。
- まだ **MD5** または **SHA256** 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、設定の損失、認証の失敗など、後方互換性の問題が発生することが予想されます。タイプ 10 シークレットがある場合、システムをバージョン 7.0.1 以降からバージョン 6.5.3 以降にダウングレードする場合は、**シークレット** をタイプ 5 に変換します。システムをバージョン 7.0.1 以降から 6.5.3 未満のバージョンにダウングレードする場合は、install activate を実行する前に、XR-vm および sysadmin-vm からすべてのユーザーの設定を解除します。Cisco IOS XR 32 ビットソフトウェアを実行している Cisco ASR 9000 シリーズ ルータには、タイプ 10 シークレットが適用されないため、後方互換性の問題は発生しません。
- 最初のユーザー設定シナリオの場合やユーザーを再設定する場合は、タイプ 5 およびタイプ 10 シークレットのみが XR VM からシステム管理 VM とホスト VM に同期されます。このようなシナリオでは、タイプ 8 およびタイプ 9 シークレットは同期されません。

- 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。
- Cisco IOS XR ソフトウェアリリース 7.0.1 以降では、設定でタイプを選択せずにクリアテキストシークレットが設定されている場合、デフォルトのハッシュタイプは 10（SHA512）です。

ステップ 4 **group** *group-name*

例：

```
RP/0/RSP0/cpu 0: router(config-un)# group sysadmin
```

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

- ユーザーは、ユーザー 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、ユーザー グループのすべての属性を受け取ります。
- 各ユーザーは、少なくとも 1 つのユーザー グループに割り当てる必要があります。ユーザーは複数のユーザー 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 で指定したユーザーに関連付けるユーザー グループごとに、ステップ 4 を繰り返します。

ステップ 6 （任意）米国国防総省（DoD）承認済みログインバナーの表示を有効にできます。バナーは、デバイスへのアクセスを許可する前に表示されます。バナーにより、適用される連邦法に準拠したプライバシーとセキュリティの確保も行われます。さらに、システムは、システムブートから、またはユーザープロファイルが作成された直後から、ログインの追跡を行います。

（注） ルータをリロードすると、ログイン通知がリセットされます。

次のコマンドを使用して、ログインバナーを有効または無効にします。

例：

```
Router(config-un)#login-history enable
Router(config-un)#login-history disable
```

`show running-config username user1` コマンドを実行して、ログインバナーの状態を確認します。

```
Router(config-un)# show running-config username NAME1
Fri Jan 29 13:55:28.261 UTC
username NAME1
 group UG1
 secret * **********
 password * ******
 login-history enable
```

ステップ 7 **commit** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。
- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

システム管理 VM でのユーザープロファイルの作成

システム管理 VM の新しいユーザーを作成します。ユーザーはユーザー グループに含まれ、特定の権限が割り当てられます。ユーザーには、割り当てられた権限に基づいて、システム管理 VM コンソールのコマンドと設定への制限付きアクセス権が付与されます。

ルータでは、最大で 1024 個のユーザープロファイルがサポートされます。

XR VM の root-lr ユーザーは、EXEC モードで **Admin** コマンドを入力することで、システム管理 VM にアクセスできます。ルータではユーザー名とパスワードの入力を求めるプロンプトは表示されません。XR VM の root-lr ユーザーには、システム管理 VM へのフルアクセス権が付与されます。

ステップ 1 **admin**

例：

```
RP/0/RSP0/cpu 0: router# admin
```

管理 EXEC モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

モードを開始します。

ステップ 3 **aaa authentication users user** *user_name*

例：

```
sysadmin-vm:0_RP0(config)#aaa authentication users user us1
```

新しいユーザーを作成し、ユーザー コンフィギュレーション モードを開始します。例では、ユーザー「us1」が作成されます。

ステップ 4 **password** *password*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#password pwd1
```

システム管理 VM へのログイン時にユーザー認証に使用するパスワードを入力します。

ステップ 5 **uid** *user_id_value*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#uid 100
```

数値を指定します。32 ビットの整数を入力できます。

ステップ 6 **gid** *group_id_value*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#gid 50
```

数値を指定します。32 ビットの整数を入力できます。

ステップ 7 **ssh_keydir** *ssh_keydir*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#ssh_keydir dir1
```

英数字の値を指定します。

ステップ 8 **homedir** *homedir*

例：

```
sysadmin-vm:0_RP0(config-user-us1)#homedir dir2
```

英数字の値を指定します。

ステップ 9 **commit** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。
- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

コマンド ルールの作成

コマンド ルールとは、ユーザー グループ内のどのユーザーが特定のコマンドの使用を許可または拒否されるかに基づいたルールです。コマンド ルールはユーザー グループに関連付けられ、そのユーザー グループに属するすべてのユーザーに適用されます。

コマンドでの動作を許可するか拒否するかを指定することで、コマンドルールを作成します。次の表に、有効な動作と権限の組み合わせを示します。

動作	承認権限	拒否権限
読み取り（R）	「?」を使用した場合にCLIにコマンドが表示されます。	「?」を使用した場合にCLIにコマンドが表示されません。
実行（X）	CLI からコマンドを実行できます。	CLI からコマンドを実行できません。
読み取りおよび実行（RX）	コマンドが CLI に表示され、実行可能です。	コマンドは CLI に表示されず、実行することもできません。

デフォルトでは、すべての権限が **Reject** に設定されています。

各コマンド ルールは、関連付けられている番号によって識別されます。ユーザー グループに複数のコマンド ルールを適用すると、より小さい番号のコマンド ルールが優先されます。たとえば cmdrule 5 は読み取りアクセスを許可しますが、cmdrule 10 は読み取りアクセスを拒否するとします。これら両方のコマンド ルールを同じユーザー グループに適用すると、cmdrule 5 が優先されるため、このグループのユーザーは読み取りアクセス権を持ちます。

このタスクの例として、「show platform」コマンドの読み取りおよび実行権限を拒否するルールを作成します。

始める前に

ユーザー グループを作成します。システム管理 VM でのユーザーグループの作成 （5 ページ）を参照してください。

手順の概要

1. **admin**
2. **config**
3. **aaa authorization cmdrules cmdrule** *command_rule_number*
4. **command** *command_name*
5. **ops {r | x | rx}**
6. **action** {**accept** | **accept_log** | **reject**}
7. **group** *user_group_name*
8. **context** *connection_type*
9. **commit** または **end** コマンドを使用します。

手順の詳細

ステップ 1 **admin**

例：

```
RP/0/RSP0/cpu 0: router# admin
```

管理 EXEC モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

モードを開始します。

ステップ 3 **aaa authorization cmdrules cmdrule** *command_rule_number*

例：

```
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 1100
```

コマンド ルール番号として数値を指定します。32 ビットの整数を入力できます。

重要　1 ～ 1000 の数字はシスコで予約済みのため使用しないでください。

このコマンドによって、新しいコマンドルール（まだ存在していない場合）が作成され、コマンドルール コンフィギュレーション モードが開始されます。例では、コマンド ルール「1100」が作成されます。

（注）　デフォルトでは、root-system ユーザーの作成時に「cmdrule 1」がシステムによって作成されます。このコマンド ルールは、すべてのコマンドの「読み取り」および「実行」動作に対する「承認」権限を提供します。したがって「cmdrule 1」が変更されない限り、root ユーザーに課せられる制限はありません。

ステップ 4 **command** *command_name*

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#command "show platform"
```

権限を制御するコマンドを指定します。

commandにアスタリスク「*」を入力した場合、そのコマンド ルールがすべてのコマンドに適用されることを意味します。

ステップ 5 **ops {r | x | rx}**

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#ops rx
```

権限を指定する必要がある動作を指定します。

- **r** ：読み取り
- **x** ：実行

- **rx** ：読み取りおよび実行

ステップ 6 **action** {**accept** | **accept_log** | **reject**}

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#action reject
```

ユーザーがその動作の使用を許可されるか拒否されるかを指定します。

- **accept** ：ユーザーはその動作の実行を許可されます。
- **accept_log**：ユーザーはその動作の実行を許可され、アクセスの試行がすべて記録されます。
- **reject**：ユーザーはその動作の実行を制限されます。

ステップ 7 **group** *user_group_name*

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#group gr1
```

コマンド ルールを適用するユーザーグループを指定します。

ステップ 8 **context** *connection_type*

例：

```
sysadmin-vm:0_RP0(config-cmdrule-1100)#context *
```

このルールを適用する接続タイプを指定します。接続タイプは *netconf*（ネットワーク設定プロトコル）、*cli*（コマンドライン インターフェイス）、または *xml*（Extensible Markup Language）です。アスタリスク「*」の入力が推奨されます。これは、そのコマンド ルールがすべての接続タイプに適用されることを示します。

ステップ 9 **commit** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。
- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

次のタスク

データ ルールを作成します。データ ルールの作成 （15 ページ）を参照してください。

データ ルールの作成

データ ルールとは、ユーザーグループ内のどのユーザーが設定データ要素へのアクセスとその変更を許可または拒否されるかに基づいたルールです。データ ルールはユーザー グループに関連付けられます。データ ルールは、ユーザー グループに属するすべてのユーザーに適用されます。

各データ ルールは、関連付けられている番号によって識別されます。ユーザー グループに複数のデータ ルールを適用すると、より小さい番号のデータ ルールが優先されます。

始める前に

ユーザー グループを作成します。システム管理 VM でのユーザーグループの作成 （5 ページ）を参照してください。

手順の概要

1. **admin**
2. **config**
3. **aaa authorization datarules datarule** *data_rule_number*
4. **keypath** *keypath*
5. **ops** *operation*
6. **action** {**accept** | **accept_log** | **reject**}
7. **group** *user_group_name*
8. **context** *connection type*
9. **namespace** *namespace*
10. **commit** または **end** コマンドを使用します。

手順の詳細

ステップ 1 **admin**

例：

```
RP/0/RSP0/cpu 0: router# admin
```

管理 EXEC モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

モードを開始します。

ステップ 3 **aaa authorization datarules datarule** *data_rule_number*

例：

```
sysadmin-vm:0_RP0(config)#aaa authorization datarules datarule 1100
```

データ ルール番号として数値を指定します。32 ビットの整数を入力できます。

重要　1 ～ 1000 の数字はシスコで予約済みのため使用しないでください。

このコマンドによって、新しいデータ ルール（まだ存在していない場合）が作成され、データ ルール コンフィギュレーション モードが開始されます。例では、データ ルール「1100」が作成されます。

（注）　デフォルトで、root-system ユーザーの作成時に「datarule 1」がシステムによって作成されます。このデータ ルールは、すべての設定データの「読み取り」、「書き込み」、および「実行」動作に対する「承認」権限を提供します。したがって「datarule 1」が変更されない限り、root ユーザーに課せられる制限はありません。

ステップ 4　**keypath** *keypath*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#keypath  /aaa/disaster-recovery
```

データ要素のキーパスを指定します。キーパスはデータ要素の場所を定義する式です。**keypath** にアスタリスク「*」を入力した場合、そのコマンドルールがすべての設定データに適用されることを意味します。

ステップ 5　**ops** *operation*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#ops rw
```

権限を指定する必要がある動作を指定します。各動作は次の文字で識別されます。

- c：作成
- d：削除
- u：更新
- w：書き込み（作成、更新、および削除の組み合わせ）
- r：読み込み
- x：実行

ステップ 6　**action** {**accept** | **accept_log** | **reject**}

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#action reject
```

ユーザーがその動作を許可されるか拒否されるかを指定します。

- **accept** ：ユーザーはその動作の実行を許可されます。
- **accept_log**：ユーザーはその動作の実行を許可され、アクセスの試行がすべて記録されます。
- **reject**：ユーザーはその動作の実行を制限されます。

ステップ 7 **group** *user_group_name*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#group gr1
```

データ ルールを適用するユーザー グループを指定します。複数のグループ名を指定することもできます。

ステップ 8 **context** *connection type*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#context *
```

このルールを適用する接続タイプを指定します。接続タイプは*netconf*（ネットワーク設定プロトコル）、*cli*（コマンドライン インターフェイス）、または *xml*（Extensible Markup Language）です。アスタリスク「*」の入力が推奨されます。これは、そのコマンドがすべての接続タイプに適用されることを示します。

ステップ 9 **namespace** *namespace*

例：

```
sysadmin-vm:0_RP0(config-datarule-1100)#namespace *
```

アスタリスク「*」を入力して、データ ルールが名前空間の値すべてに適用されることを示します。

ステップ 10 **commit** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。
- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

ディザスタ リカバリのユーザー名とパスワードの変更

ルータの起動後、最初にroot-systemユーザー名とパスワードを定義すると、同じユーザー名とパスワードがシステム管理コンソールのディザスタ リカバリ ユーザー名およびパスワードとしてマッピングされます。ただし、これらは変更可能です。

ディザスタ リカバリ ユーザー名およびパスワードは、次の状況で役立ちます。

- システム管理コンソールでの認証のデフォルト ソースである AAA データベースが破損した場合にシステムへアクセスする。
- 何らかの理由でシステム管理コンソールが機能しない場合に、管理ポートを通じてシステムにアクセスする。

- 通常のユーザー名およびパスワードを忘れた場合に、ディザスタ リカバリ ユーザー名とパスワードを使用してシステム管理コンソールにアクセスし、新しいユーザーを作成する。

（注） ルータでは、ディザスタ リカバリ ユーザー名およびパスワードを一度に 1 つのみ設定できます。

手順の概要

1. **admin**
2. **config**
3. **aaa disaster-recovery username** *username* **password** *password*
4. **commit** または **end** コマンドを使用します。

手順の詳細

ステップ 1 **admin**

例：

```
RP/0/RSP0/cpu 0: router# admin
```

管理 EXEC モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0#config
```

モードを開始します。

ステップ 3 **aaa disaster-recovery username** *username* **password** *password*

例：

```
sysadmin-vm:0_RP0(config)#aaa disaster-recovery username us1 password pwd1
```

ディザスタ リカバリ ユーザー名とパスワードを指定します。既存のユーザーをディザスタ リカバリ ユーザーとして選択する必要があります。この例では、ディザスタ リカバリ ユーザーとして「us1」が選択され、パスワード「pwd1」が割り当てられます。パスワードは、プレーン テキストまたは MD5 ダイジェスト文字列として入力することができます。

ディザスタ リカバリ ユーザー名を使用する場合は、*username***@localhost** の形式で入力してください。

ステップ 4 **commit** または **end** コマンドを使用します。

commit ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

end ：次のいずれかのアクションの実行をユーザーに要求します。

- **Yes** ：設定の変更を保存し、コンフィギュレーション セッションを終了します。
- **No** ：設定の変更をコミットせずに、コンフィギュレーション セッションを終了します。
- **Cancel** ：設定の変更をコミットせずに、コンフィギュレーション セッションに留まります。

PXE ブートを使用したパスワードの回復

ログインできない場合、またはXRおよびシステム管理パスワードを紛失した場合は、次の手順を使用して新しいパスワードを作成します。紛失したパスワードは回復できません。代わりに、新しいユーザー名とパスワードを非グレースフルPXEブートで作成する必要があります。

ステップ 1 PXE を使用してルータを起動します。

（注） PXEブートは完全に侵入型なので、ルータの状態、設定、およびイメージがリセットされます。

ルータを PXE ブートするには、iPXE を使用したルータの起動を参照してください。

ステップ 2 パスワードのリセット。

翻訳について
このドキュメントは、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。