ユーザ プロファイルの作成および権限の割り当て

ルータ上の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 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、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、認可、およびアカウンティング（AAA）コマンドをシステム管理コンフィギュレーション モードで使用します。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） システム管理 VM から外部 AAA サーバおよびサービスを設定することはできません。その設定は XR VM からのみ実行できます。

ユーザが制御されていないアクセスを行うのを制限するために 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 に最初のユーザが存在するかどうかを確認します。

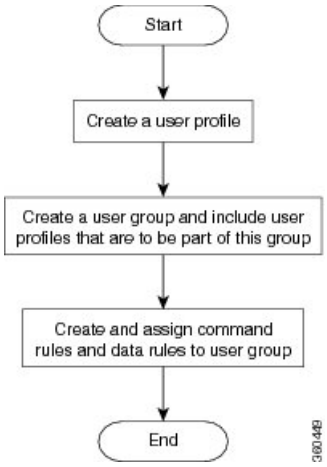
- 最初のユーザが存在する場合、同期は実行されません。
- 最初のユーザが存在しない場合は、XR の最初のユーザ（作成順序に基づく）がシステム管理 VM に同期されます。

ユーザの認証にはユーザ名とパスワードが使用されます。認証されたユーザは、ユーザ 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 グループに属するすべての

ユーザには、そのユーザ 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 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 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 ユーザは、システム管理 VM の root-system ユーザにマッピングされます。root-system ユーザにはシステム管理 VM のスーパーユーザ権限があるため、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、システム管理コンフィギュレーションconfig 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 プロファイルの作成 （2 ページ）
- ユーザ グループの作成 （4 ページ）
- コマンド ルールの作成 （6 ページ）
- データ ルールの作成 （8 ページ）
- ディザスタ リカバリのユーザ名とパスワードの変更 （10 ページ）

ユーザ プロファイルの作成

システム管理 VM の新しいユーザを作成します。ユーザはユーザ 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を持ちます。

ルータでは、最大で 1024 個のユーザ プロファイルがサポートされます。

（注） システム管理 VM で作成したユーザは、XR VM で作成したユーザとは異なります。したがって、システム管理 VM ユーザのユーザ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 プロファイルの同期

ユーザ プロファイルを XR VM で初めて作成するとき、システム管理 VM にユーザが存在しない場合、ユーザ名とパスワードはシステム管理 VM に同期されます。

ただし、同期されたユーザの XR VM での後続のパスワード変更またはユーザ削除は、システム管理 VM と同期されません。

そのため、XR VM およびシステム管理 VM のパスワードが同じでない可能性があります。また、ユーザが XR VM で削除されても、システム管理 VM と同期されたユーザは削除されません。

XR VM の root-lr ユーザがシステム管理 VM にアクセスするには、XR EXEC モードXR EXEC モードで **Admin** コマンドを入力します。ルータではユーザ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 ユーザには、システム管理 VM へのフル アクセス権が提供されます。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/cpu 0: router# admin
```

モードを開始します。

ステップ 2 **config**

例：

```
sysadmin-vm:0_RP0sysadmin-vm:0_RP0#config
```

システム管理コンフィギュレーション System Admin 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
```

新しいユーザを作成し、ユーザ 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「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**

次のタスク

- このタスクで作成したユーザを含めるユーザ グループを作成します。ユーザ グループの作成 （4 ページ）を参照してください。
- ユーザ グループに適用するコマンド ルールを作成します。コマンド ルールの作成 （6 ページ）を参照してください。
- ユーザ グループに適用するデータ ルールを作成します。「データ ルールの作成 （8 ページ）」を参照してください。

ユーザ グループの作成

新しいユーザ 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 グループに属するすべてのユーザに適用されます。

ルータでは、最大 32 のユーザ グループがサポートされます。

始める前に

ユーザ プロファイルを作成します。ユーザ プロファイルの作成および権限の割り当て （1 ページ）を参照してください。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/cpu 0: router# admin
```

モードを開始します。

ステップ 2 **config**

例：

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

システム管理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 **aaa authentication groups group** *group_name*

例：

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

新しいユーザ 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 グループ「gr1」が作成されます。

（注） デフォルトで、root ユーザの作成時にユーザ グループ「root-system」がシステムによって作成されます。rootユーザはこのユーザ 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は root ユーザ権限を取得します。

ステップ 4 **users** *user_name*

例：

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

ユーザ グループに含めるユーザの名前を指定します。

複数のユーザ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**

次のタスク

- コマンド ルールを作成します。コマンド ルールの作成 （6 ページ）を参照してください。
- データ ルールを作成します。「データ ルールの作成 （8 ページ）」を参照してください。

コマンド ルールの作成

コマンド ルールとは、ユーザ グループ内のどのユーザ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 グループに関連付けられ、そのユーザ グループに属するすべてのユーザに適用されます。

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 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 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 グループを作成します。ユーザ グループの作成 （4 ページ）を参照してください。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/cpu 0: router# admin
```

モードを開始します。

ステップ 2 **config**

例：

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

システム管理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 **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** ：ユーザはその動作の実行を許可されます。
- **accept_log**：ユーザ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 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**

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 （8 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 グループ内のどのユーザ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 グループに関連付けられます。データ ルールは、ユーザ グループに属するすべてのユーザに適用されます。

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 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 グループを作成します。ユーザ グループの作成 （4 ページ）を参照してください。

手順

ステップ 1 **admin**

例：

```
RP/0/RP0/cpu 0: router# admin
```

モードを開始します。

ステップ 2 **config**

例：

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

システム管理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 **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** ：ユーザはその動作の実行を許可されます。
- **accept_log**：ユーザ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 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**

ディザスタ リカバリのユーザ名とパスワードの変更

ルータの起動後、最初にroot-systemユーザ名とパスワードを定義すると、同じユーザ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、新しいユーザを作成する。

（注） ルータでは、ディザスタ リカバリ ユーザ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

ステップ 1 **admin**

例：

```
RP/0/RP0/cpu 0: router# admin
```

モードを開始します。

ステップ 2 **config**

例：

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

システム管理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 **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 ユーザ名とパスワードを指定します。既存のユーザをディザスタ リカバリ ユーザ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**