



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、およびアカウントिंग (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 LXC 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 LXC からのみ実行できます。

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。



(注) ルータの初回起動時に作成された XR LXC の root-lr ユーザは、システム管理 LXC 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 LXC 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, 5 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 LXC 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 LXC 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 LXC で作成したユーザは、XR LXC 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 LXC ユーザのユーザ名とパスワードを使用して XR LXC にアクセスすることはできません。逆も同様です。

XR LXC の root-lr ユーザがシステム管理 LXC にアクセスするには、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 LXC の root-lr ユーザには、システム管理 LXC へのフルアクセス権が提供されます。

手順の概要

1. **admin**
2. **config**
3. **aaaauthenticationusersuseruser_name**
4. **passwordpassword**
5. **uiduser_id_value**
6. **gidgroup_id_value**
7. **ssh_keydirssh_keydir**
8. **homedirhomedir**
9. **commit**

手順の詳細

ステップ 1 admin

例 :

```
RP/0/RP0/CPU0: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 **aaaauthenticationusersuseruser_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 **passwordpassword**

例：

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

システム管理 LXC 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 **uiduser_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 **gidgroup_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_keydirssh_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 **homedirhomedir**

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**

次の作業

- 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](#)、(5 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。

はじめる前に

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](#)、(2 ページ) を参照してください。

手順の概要

1. **admin**
2. **config**
3. **aaaauthenticationgroupsgroupgroup_name**
4. **usersuser_name**
5. **gidgroup_id_value**
6. **commit**

手順の詳細

ステップ 1 admin

例 :

```
RP/0/RP0/CPU0: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 aaaauthenticationgroupsgroupgroup_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（例：**users "user1user2..."**）。

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

次の作業

- コマンドルールを作成します。 [コマンドルールの作成, \(5 ページ\)](#) 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**拒否**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。

はじめる前に

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。

手順の概要

1. **admin**
2. **config**
3. **aaaauthorizationcmdrulescmdrulecommand_rule_number**
4. **commandcommand_name**
5. **ops{r|x|rx}**
6. **action {accept|accept_log|reject}**
7. **groupuser_group_name**
8. **contextconnection_type**
9. **commit**

手順の詳細

ステップ 1 admin

例：

```
RP/0/RP0/CPU0: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 aaaauthorizationcmdrulescmdrulecommand_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。

コマンドにアスタリスク「*」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

次の作業

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。

はじめる前に

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。

手順の概要

1. **admin**
2. **config**
3. **aaaauthorizationdatarulesdataruledata_rule_number**
4. **keypathkeypath**
5. **opsoperation**
6. **action {accept|accept_log|reject}**
7. **groupuser_group_name**
8. **contextconnection type**
9. **namespacenamespace**
10. **commit**

手順の詳細

ステップ 1 admin

例：

```
RP/0/RP0/CPU0: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。キーパスにアスタリスク「*」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 `groupuser_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 `contextconnection 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 `namespacenamespace`

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 LXC 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 LXC 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 LXC 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 LXC 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。

はじめる前に

ユーザを作成します。詳細については、[ユーザプロファイルの作成](#)、(2 ページ) を参照してください。

手順の概要

1. **admin**
2. **config**
3. **aaadisaster-recoveryusernameusernamepasswordpassword**
4. **commit**

手順の詳細

ステップ 1 admin

例：

```
RP/0/RP0/CPU0: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 aaadisaster-recoveryusernameusernamepasswordpassword

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

