



Red Hat Hybrid Cloud Console 1-latest

FedRAMP を使用したロールベースのアクセス制御 (RBAC) でのユーザーアクセス設定ガイド

ユーザーアクセス機能を使用して、Red Hat Hybrid Cloud Console でホストされているサービスの RBAC を設定する方法

Red Hat Hybrid Cloud Console 1-latest FedRAMP を使用したロールベースのアクセス制御 (RBAC) でのユーザーアクセス設定ガイド

ユーザーアクセス機能を使用して、Red Hat Hybrid Cloud Console でホストされているサービスの RBAC を設定する方法

法律上の通知

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

本書は、ユーザーアクセス機能を使用して、FedRAMP[®] を備えた Red Hat Hybrid Cloud Console でホストされるサービスのロールベースアクセス制御 (RBAC) を設定する Red Hat アカウントユーザーを対象にしています。Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、用語の置き換えは、今後の複数のリリースにわたって段階的に実施されます。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

目次

第1章 ロールベースアクセス制御 (RBAC) のユーザーアクセス設定ガイド	3
1.1. ユーザーアクセスと SOFTWARE AS A SERVICE (SAAS) アクセスモデル	3
1.2. USER ACCESS を使用できるユーザー	3
1.3. USER ACCESS の使用方法	3
第2章 ユーザーアクセス設定の手順	7
2.1. ユーザーアクセス管理者の作成	7
2.2. ロールおよびパーミッションの表示	8
2.3. ユーザーのパーミッションの確認	9
2.4. ロールおよびメンバーを使用したグループアクセスの管理	9
2.5. 単一ユーザーへのサービスアクセスの制限	11
2.6. グループに組織管理者を含める	13
2.7. グループアクセスの無効化	13
2.8. ユーザーアクセスのための粒度の細かいパーミッション	14
第3章 事前定義された USER ACCESS ロール	22
RED HAT ドキュメントへのフィードバック (英語のみ)	25

第1章 ロールベースアクセス制御 (RBAC) のユーザーアクセス設定ガイド

ユーザーアクセス機能は、[Red Hat Hybrid Cloud Console](#) でホストされるさまざまなサービスへのユーザーアクセスを制御するロールベースのアクセス制御 (RBAC) の実装です。Hybrid Cloud Console でホストされるサービスへのユーザーアクセスを許可するようにユーザーアクセス機能を設定します。

1.1. ユーザーアクセスと SOFTWARE AS A SERVICE (SAAS) アクセスモデル

Red Hat のカスタマーアカウントには、数百もの認証ユーザーがある場合もありますが、すべてのユーザーが [Red Hat Hybrid Cloud Console](#) で利用可能な SaaS サービスに同じレベルのアクセスを必要とするわけではありません。ユーザーアクセス機能により、組織管理者は [Red Hat Hybrid Cloud Console](#) でホストされるサービスへのユーザーアクセスを管理できます。



注記

ユーザーアクセスは OpenShift Cluster Manager パーミッションを管理しません。OpenShift Cluster Manager では、組織のすべてのユーザーが情報を表示できますが、組織の管理者とクラスターの所有者のみがクラスターでアクションを実行できます。詳細は、OpenShift Cluster Manager ドキュメントの [OpenShift Cluster Manager でのクラスターへのアクセスの設定](#) を参照してください。

1.2. USER ACCESS を使用できるユーザー

[Red Hat Hybrid Cloud Console](#) でユーザーアクセスを最初に表示および管理するには、組織管理者である必要があります。これは、ユーザーアクセスには、[Red Hat カスタマーポータル](#) から指定されたユーザー管理機能が必要なためです。これらの機能は、組織管理者のみに帰属します。

ユーザーアクセス管理者 ロールは、組織管理者が割り当てることができる特別なロールです。このロールにより、組織管理者ユーザー以外のユーザーが [Red Hat Hybrid Cloud Console](#) でユーザーアクセスを管理できるようになります。

1.3. USER ACCESS の使用方法

ユーザーアクセス機能は、特定のユーザーに個別に権限を割り当てるのではなく、ロールの管理に基づいています。ユーザーアクセスでは、各ロールに特定のパーミッションセットがあります。たとえば、ロールはアプリケーションの読み取りパーミッションを許可する場合があります。別のロールによって、アプリケーションの書き込みパーミッションが許可される可能性があります。

ロールを含むグループを作成し、拡張で各ロールに割り当てられたパーミッションを作成します。グループにユーザーを割り当てます。つまり、グループ内の各ユーザーには、そのグループ内のロールのパーミッションが付与されます。

異なるグループを作成し、そのグループのロールを追加または削除することで、そのグループに許可されるパーミッションを制御できます。グループにユーザーを追加すると、1人以上のユーザーはそのグループに許可されたすべてのアクションを実行できます。

Red Hat は、ユーザーアクセス用に 2 つのデフォルトアクセスグループを提供します。

- **Default admin access** グループ。Default admin access グループは、組織内の組織管理者ユーザーに制限されています。Default admin access グループのロールを変更または修正することはできません。

- **Default access グループ。** **Default access** グループには、組織内の認証されたすべてのユーザーが含まれます。これらのユーザーは、事前定義されたロールの選択を自動的に継承します。



注記

Default access グループに変更を加えることができます。ただし、これを行うと、その名前が **Custom default access** グループに変更されます。

Red Hat は、事前に定義されたロールのセットを提供します。アプリケーションによっては、対応のアプリケーションごとに事前定義されたロールでは、アプリケーションに対してカスタマイズされるパーミッション異なる場合があります。

1.3.1. Default admin access グループ

Default admin access グループは、Red Hat によって [Red Hat Hybrid Cloud Console](#) で提供されます。これには、システムで組織管理者のロールを持つすべてのユーザーに割り当てられる一連のロールが含まれています。このグループのロールは、[Red Hat Hybrid Cloud Console](#) で事前定義されています。

Default admin access グループのロールは、追加または変更できません。このグループは Red Hat によって提供されるため、Red Hat が **Default admin access** グループにロールを割り当てると自動的に更新されます。

Default admin access グループの利点は、組織管理者にロールを自動的に割り当てることができることです。

デフォルトの管理者アクセス グループに含まれるロールは、[事前定義されたユーザーアクセスロール](#) を参照してください。

1.3.2. Default access グループ

Default access グループは、Red Hat によって [Red Hat Hybrid Cloud Console](#) で提供されます。これには、[Red Hat Hybrid Cloud Console](#) で事前定義されたロールのセットが含まれます。**Default access** グループには、組織内の認証されたすべてのユーザーも含まれます。**デフォルトのアクセス** グループが [Red Hat Hybrid Cloud Console](#) に追加されると、**デフォルトのアクセス** グループは自動的に更新されます。



注記

Default access グループには、事前定義されたすべてのロールのサブセットが含まれます。詳細は、[デフォルトの管理者アクセス](#) グループに含まれるロールについて [定義済みユーザーアクセスロール](#) セクションを参照してください。

組織管理者は、**Default access** グループに対するロールの追加/削除が可能です。これを行うと、その名前が **Custom default access** グループに変更されます。このグループに加える変更は、組織内のすべての認証ユーザーに影響します。

1.3.3. Custom default access グループ

Default access グループを手動で変更すると、その名前が **Custom default access** になり、内容が変更されたことを示します。さらに、[Red Hat Hybrid Cloud Console](#) から自動的に更新されなくなります。

この以降、組織管理者は、**Custom default access** グループへの更新および変更をすべて行います。このグループは、[Red Hat Hybrid Cloud Console](#) で管理または更新されなくなりました。



重要

Default access グループまたは **Custom default access** グループを削除することはできません。

Default access グループを復元でき、**Custom default access** グループと変更を加えたすべての変更が削除されます。[デフォルトアクセスグループの復元](#) を参照してください。

1.3.4. ユーザーアクセスグループ、ロール、パーミッション

ユーザーアクセスは以下のカテゴリーを使用して、組織管理者がサポートされる [Red Hat Hybrid Cloud Console](#) サービスに付与できるユーザーアクセスのレベルを決定します。許可されたユーザーに提供されるアクセスは、そのユーザーが属するグループと、そのグループに割り当てられたロールによって異なります。

- **Group:** ロールをユーザーにマッピングするアカウントに属するユーザーのコレクション。組織管理者は、グループを使用してグループにロールを割り当て、グループにユーザーを追加することができます。ロールがなく、ユーザーがないグループも作成できます。
- **Role:** Insights などの特定サービスへのアクセスを提供するパーミッションのセット。特定の操作を実行するパーミッションは特定のロールに割り当てられます。ロールはグループに割り当てられます。たとえば、サービスに **read** ロールと **write** ロールがあるとします。両方のロールをグループに追加すると、そのグループのすべてのメンバーに、そのサービスの読み取りおよび書き込みパーミッションが付与されます。
- **Permissions:** サービスの要求可能な個別のアクション。パーミッションはロールに割り当てられます。

組織管理者は、ロールとユーザーをグループに追加するか、削除します。グループは、組織管理者によって作成された新規グループにすることも、グループを既存グループにすることもできます。特定のロールを持つグループを作成し、そのグループにユーザーを追加することにより、そのグループとそのメンバーが [Red Hat Hybrid Cloud Console](#) サービスと対話する方法を制御できます。

グループにユーザーを追加すると、そのグループのメンバーになります。グループメンバーは、所属する他のすべてのグループのロールを継承します。ユーザーインターフェイスは **Members** タブにユーザーをリスト表示します。

1.3.5. 追加アクセス

[Red Hat Hybrid Cloud Console](#) のユーザーアクセスは追加モデルを使用します。つまり、**deny** ロールはありません。つまり、アクションが許可されるだけです。アクセスを制御するには、必要な権限を持つ適切なロールをグループに割り当て、ユーザーをそのグループに追加します。個別のユーザーに許可されるアクセスは、そのユーザーが属するすべてのグループに割り当てられたすべてのロールになります。

1.3.6. アクセス構造

以下は、ユーザーアクセスのユーザーアクセス構造の概要です。

- **Group:** ユーザーは1つまたは複数のグループのメンバーになります。
- **Role:** 1つまたは複数のグループにロールを追加できます。

- **Permission:** 1つまたは複数のパーミッションをロールに割り当てることができます。

初期のデフォルト設定では、すべてのユーザーアクセスアカウントユーザーが **Default access** グループで提供されるロールを継承します。



注記

グループに追加するユーザーは、[Red Hat Hybrid Cloud Console](#) の組織アカウントの認証ユーザーである必要があります。

第2章 ユーザーアクセス設定の手順

組織管理者またはユーザーアクセス管理者は  > **Identity & Access Management** をクリックして、ユーザーアクセスグループ、ロール、および権限を表示、設定、および変更できます。

2.1. ユーザーアクセス管理者の作成

User Access administrator は、組織管理者がグループに割り当てる特別なロールです。このグループの全ユーザーは、グループおよびロールの追加、変更、削除などのユーザーアクセス管理ロールを実行できます。**User Access administrator** のロールは、**Default Admin Access** グループで定義されたロールを継承しません。

User Access administrator ロールは、ユーザーアクセス管理者グループを作成または変更できません。組織管理者のみが、**User Access administrator** のロールが割り当てられているグループを作成、変更、または削除できます。



注記

User Access administrator ロールでは、顧客のアクセス要求を表示および承認する権限は付与されません。

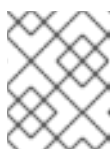
User Access administrator を持つと、組織管理者ではないユーザーは、ユーザーアクセス機能を管理するための数多くの組織管理機能を実行できます。**User Access administrator** のロールは、**Default admin access** グループのロールを継承しません。そのグループのロールは、組織管理者に制限されています。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。

手順

- [Red Hat Hybrid Cloud Console](#) > [Settings](#) > [Identity & Access Management](#) > [User Access](#) > [Groups](#) に移動します。
- Create group** をクリックします。
- ウィザードが提供するガイド付きのアクションに従い、ユーザーとロールを追加します。
 - 認識可能な名前 (**User Access Admin**) でグループに名前を付けます。
 - 意味のある説明 (**User Access Organization Administrator permissions**) を記入します。
 - Next** ボタンをクリックしてロールを追加します。
 - User Access administrator** ロールを検索し、選択ボックスをクリックしてこのロールをグループに追加します。必要に応じて、追加のロールを選択します。
 - Next** ボタンをクリックして、グループにメンバーを追加します。



注記

追加するメンバーは、組織アカウントのアクティブなメンバーである必要があります。

- f. グループのメンバーを選択したら、**Next** ボタンをクリックして詳細を確認します。
 - g. **Back** ボタンをクリックして戻り変更するか、**Cancel** ボタンをクリックしてアクションを取り消します。
4. **Submit** ボタンをクリックして、**Create group** ウィザードを完了します。新規グループが **Groups** タブに表示されます。

2.2. ロールおよびパーミッションの表示

[Red Hat Hybrid Cloud Console](#) コンソールでユーザーアクセスのロールおよびパーミッションを表示できます。Red Hat が提供する事前定義されたロールのリストは、[事前定義されたユーザーアクセスロール](#) セクションを参照してください。



注記

事前定義されたロールを変更することはできません。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#) に移動します。ユーザーアクセスロールが表示されます。全ロールのリストをスクロールできます。
2. 表で、ロールの **Name** またはロール **Permissions** のいずれかをクリックし、ロールに割り当てられたパーミッションの詳細を表示します。たとえば、**Cost Price List Viewer** ロールをクリックすると、以下の情報が表示されます。

[Roles](#) > [Cost Price List Viewer](#)

Cost Price List Viewer

A cost management role that grants read permissions on cost models.

Application	Resource type	Operation	Resource definitions ⓘ	Last commit
cost-management	cost_model	read	N/A	19 May 2021



注記

アスタリスク * はワイルドカードパーミッションを示します。ワイルドカードパーミッションはすべてのリソースタイプへのアクセスを許可し、ロール内のアプリケーションに対するすべての操作を許可します。

2.3. ユーザーのパーミッションの確認

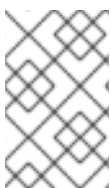
ユーザーの詳細ページから、ユーザーのパーミッションおよびその他のアクセス関連情報を表示できます。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users](#) に移動して、組織内のユーザーのリストを表示します。
2. **Username** をクリックして、そのユーザーに関する詳細情報を表示します。
3. ユーザーの詳細ページで、以下を表示できます。
 - ユーザーが組織内の組織管理者である場合
 - ユーザーのメールアドレス
 - Hybrid Cloud Console 上のユーザーのユーザー名 (Red Hat ログインとも呼ばれます)
 - ユーザーに関連付けられたロールのリスト。各ロールの詳細を表示するには、以下を行います。
 - **Groups** 列の数をクリックすると、このロールが割り当てられているグループが表示されます。
 - **Permissions** 列の数をクリックすると、ロールが提供するパーミッションが表示されます。



注記

組織管理者でない場合は、[Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > My User Access](#) に移動して、さまざまなサービスに対するご自身のパーミッションを表示できます。

2.4. ロールおよびメンバーを使用したグループアクセスの管理

グループアクセスを管理するには、グループを作成し、ロールとユーザーをグループに追加します。ロールとそのパーミッションは、グループのすべてのメンバーに付与されるアクセスのタイプを決定します。

Members タブには、グループに追加できるすべてのユーザーが表示されます。グループにユーザーを追加すると、そのグループのメンバーになります。グループメンバーは、所属する他のすべてのグループのロールを継承します。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。

- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。



注記

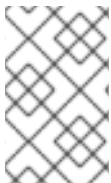
組織管理者のみが、**User Access administrator** のロールをグループに割り当てることができます。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#) に移動して、**Groups** ページを開きます。
2. **Create group** をクリックします。
3. ウィザードが提供するガイド付きのアクションに従い、ユーザーとロールを追加します。
4. 追加のグループアクセスを付与するには、グループを編集し、追加のロールを追加します。

2.4.1. グループへのロールの追加

既存のグループにロールを追加して、そのグループのすべてのメンバーに追加の権限を付与します。ユーザーの詳細を表示して、ユーザーが属するグループにロールを追加できます。



注記

Users ページからグループにロールを追加するか、**Groups** ページからグループを編集できます。これらの手順では、ユーザーの詳細ページからグループを編集する方法を示します。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users](#) に移動して、**Users** リストを開きます。
2. ユーザーの **Username** をクリックして、ユーザーの詳細ページを開きます。
3. ロールの **Groups** 列の数をクリックします。これは、ユーザーがこのロールが割り当てられているメンバーであるグループを示します。



注記

Permissions 列の数をクリックすると、ロールが提供する権限を表示できます。

4. グループ名の横にある **Add role to this group** をクリックして、グループにロールを追加します。これにより、**Add roles** ダイアログが開きます。

5. グループに追加する各ロールのチェックボックスを選択します。(グループにまだ関連付けられていないロールのみがリストされます。) **Add to group** をクリックします。
6. ユーザー詳細ページをリロードして、グループに追加したロールを確認します。

これで、グループにはコンソールでこれらの追加の権限が与えられました。

2.4.2. グループへのユーザーの追加

ユーザーを既存のグループに追加すると、そのグループに割り当てられたロールによって付与される権限がそのユーザーに付与されます。

これは、新しいチームメンバーが組織に参加し、そのメンバーの作業に必要なすべての権限を付与したい場合に便利です。



注記

Users ページからユーザーをグループに追加するか、**Groups** ページからグループを編集することができます。これらの手順では、ユーザーの詳細ページからユーザーをグループに追加する方法を示します。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. [Red Hat Hybrid Cloud Console](#) > [Settings](#) > [Identity & Access Management](#) > [User Access](#) > [Users](#) に移動して、**Users** リストを開きます。
2. 編集するユーザーのユーザー名をクリックします。
3. ユーザーの詳細ページで、**Add user to a group** をクリックします。ダイアログが開き、ユーザーがメンバーではないグループのリストが表示されます。
4. ユーザーを追加する1つ以上のグループのチェックボックスを選択し、**Add to group** をクリックします。
5. ユーザーの詳細ページをリロードして、追加したロールを確認します。

ユーザーは、追加されたグループによって付与された権限を持ちます。

2.5. 単一ユーザーへのサービスアクセスの制限

単一ユーザーを含む新しいグループを作成し、そのグループにロールを追加できます。追加するロールは、単一ユーザーに許可するサービスアクセスパーミッションを提供します。他のユーザーをグループに追加すると、追加したユーザーは同じグループパーミッションを持ちます。

グループに追加するロールは、ユーザーアクセスで提供される事前定義済みロールリスト、組織の管理者によって作成されたカスタムロール、またはその両方の組み合わせから取得されます。

事前定義されたロールの詳細は、[事前定義されたユーザーアクセスロール](#) セクションを参照してください。

ユーザーを新規グループに追加すると、ユーザーは新しいグループの権限を取得し、所属する他のすべてのグループのパーミッションも継承します。新規グループのパーミッションは、既存のパーミッションに追加されます。



重要

この手順では、**Default access** グループを変更します。変更されると、**Default access** グループ名が **Custom default access** に変わります。**Custom default access** グループは、Red Hat によって [Red Hat Hybrid Cloud Console](#) から変更をプッシュしても更新されません。

ヒント

Default access グループを復元でき、**Custom default access** グループと変更を加えたすべての変更が削除されます。[デフォルトアクセスグループの復元](#) を参照してください。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#) に移動します。**Groups** ページが表示されます。
2. **Default access** グループからすべてのロールを削除します。
Default access グループには組織の全ユーザーが属するため、**Default access** に単一のユーザーを追加または削除してアクセス制御を作成することはできません。すべてのロールを削除すると、ユーザーは **Default access** からロールパーミッションを継承しなくなります。
 - a. グループ内のすべてのロールを選択するには、ロールリストの上にあるチェックボックスを選択します。
 - b. その他のオプションアイコン (:) > **Remove** をクリックします。
 - c. **Remove roles** をクリックして確認します。
3. **Default access** グループに対する変更を保存します。名前が **Custom default access** に変わります。
4. 許可されたアクセスパーミッションのユーザーおよびロールが含まれる新しいグループを作成します。
たとえば、Vulnerability サービスに完全アクセスできるユーザーが含まれるグループ **Security Admin** を作成します。
 - a. グループ **Security Admin** を作成します。
 - b. **Members** リストからグループにユーザーを追加します。
 - c. **Vulnerability administrator** ロールを追加します。

このグループに追加する各ユーザーは、Vulnerability サービスに完全アクセスできます。



注記

組織管理者にアクセス権を付与する場合は、組織管理者ユーザーをグループに追加しません。

2.6. グループに組織管理者を含める

グループに組織管理者を含めることができます。そのグループに割り当てられたロールを組織管理者に持たせたい場合は、組織管理者ユーザーをグループに追加します。組織管理者は、すべての [Red Hat Hybrid Cloud Console](#) アプリケーションで利用可能なロールをすべて継承しません。Default access グループまたは Default admin access グループで継承されていないロールは、グループメンバーシップを介して割り当てる必要があります。



注記

この手順では、既存のグループを変更し、組織管理者をグループに追加することを仮定します。または、新しいグループの作成時に組織管理者をグループに追加できます。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、User Access administrator のロールが割り当てられているグループのメンバーである。
- グループが存在しない場合は作成する。詳細は、[ロールとメンバーによるグループアクセスの管理](#) を参照してください。
- 動作グループの通知を設定する方法は、[通知動作グループを設定する](#) を参照してください。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#) に移動します。Groups ページが表示されます。
2. グループ Name をクリックして、グループの詳細を表示します。
3. グループの詳細ページで Member タブをクリックして、グループのメンバーである許可されたユーザーのリストを表示します。
4. Add member タブをクリックします。
5. Add members to the group ページで組織管理者ユーザー名を見つけ、名前の横にあるチェックボックスをクリックします。
たとえば、組織管理者ユーザー名が smith-jones の場合は、その名前を見つけ、smith-jones の横にあるチェックボックスをクリックします。名前を追加できます。
6. 名前リストが完了したことを確認し、Add to group アクションをクリックします。

アクションが正常に終了すると、通知ポップアップが表示されます。


2.7. グループアクセスの無効化

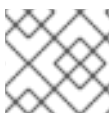
グループからロールを削除して、グループアクセスを無効にできます。ロールとそのパーミッションはグループに付与されるアクセスのタイプを決定するため、ロールを削除するとそのロールのグループアクセスが無効になります。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#) に移動します。 **Groups** ページが表示されます。
2. 変更するグループ **Name** をクリックします。
3. **Role** タブをクリックします。
4. 削除するロール **Name** の横にあるチェックボックスをクリックします。
Name 列の上部にあるチェックボックスをクリックして、全ロールを選択できます。
5. **Add role** タブの横にあるその他のオプションメニューアイコン  をクリックし、**Remove from group** をクリックします。
6. 表示される確認ウィンドウで、**Remove role** または **Cancel** のいずれかをクリックし、アクションを完了します。



注記

グループにはロールがなく、メンバーも含まれず、有効なグループになります。

2.8. ユーザーアクセスのための粒度の細かいパーミッション

粒度の細かいパーミッションにより、組織管理者は1つ以上のアプリケーションのロールパーミッションを定義できます。事前定義されたロールの多くはワイルドカードパーミッションを提供します。これは、すべてのアクションへのフルアクセスを持つスーパーユーザーロールと同等です。

粒度の細かいパーミッションを定義することで、パーミッションが制限されたロール (読み取り専用または読み取り/更新など) を作成 (または変更) できますが、削除することができません。

たとえば、コスト管理者とコスト価格リストビューアーの事前定義されたロールを比較します。

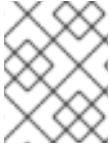
ロール	アプリケーション	リソース	操作
Cost Administrator	cost-management	* (すべて)	* (すべて)
Cost Price List Viewer	cost-management	cost_model	読み込み

新規ロールを作成すると、そのロールに固有のアプリケーション、リソース、および操作を定義できます。

2.8.1. カスタムユーザーアクセスロールの追加

ユーザーアクセスは、グループに追加できる事前定義済みのロールを多数提供します。事前定義されたロールを使用するほか、1つ以上のアプリケーションに対する粒度の細かいパーミッションでユーザーアクセスロールを作成および管理できます。

Red Hat が提供する事前定義されたロールのリストは、[事前定義されたユーザーアクセスロール](#) セクションを参照してください。



注記

Default access グループには、事前定義されたすべてのロールのサブセットが含まれます。詳細は、

[事前定義された User Access ロール](#) を参照してください。



注記

事前定義されたロールを変更することはできません。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

ガイド付きウィザードにより、ロールの追加手順が実施されます。

以下の手順では、**Create role** ウィザードを使用する方法を説明します。

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#) に移動します。**Roles** ウィンドウが表示されます。
2. **Create role** ボタンをクリックします。これにより、**Create role** ウィザードが起動します。

ウィザードのこの時点で、ゼロからロールを作成するか、既存のロールをコピーすることができます。

2.8.2. ゼロからのロールの作成

特定の粒度の細かいパーミッションを持つロールを作成する場合は、ゼロからロールを作成します。たとえば、組織に単一のロールを作成して、すべての利用可能なアプリケーションのリソースに対して読み取り専用のパーミッションを提供することができます。デフォルトのアクセスグループにこのロールを追加および管理することで、デフォルトのアクセス権限を読み取り専用に変更することができます。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- **Create role** ウィザードを起動している。

手順

1. **Create role** ウィザードで **Create a role from scratch** ボタンをクリックします。
2. 必須の **Role name** を入力します。
3. 任意で、**Role description** を入力します。
4. **Next** ボタンをクリックします。ロール名がすでに存在する場合は、続行する前に別の名前を指定する必要があります。
5. **Add permissions** ウィンドウで、ロールに追加するアプリケーションパーミッションを選択します。デフォルトでは、パーミッションはアプリケーションごとにリスト表示されます。
6. オプションでフィルタードロップダウンを使用して、Applications、Resources、または Operations でフィルターを行います。

ヒント

ウィザードページの上部にあるリストを使用して、ロールに追加したすべてのパーミッションを表示します。パーミッションをクリックして削除することができます。

7. **Next** ボタンをクリックして詳細を確認します。**Submit** ボタンをクリックし、ロールの送信、**Back** ボタンを押して変更を行い、**Cancel** ボタンを押してアクションを取り消します。

作成したロールを User Access グループに追加するのに利用できます。

2.8.3. 既存ロールのコピー

そのロールに、使用するパーミッションの多くがすでに含まれており、一部のパーミッションを変更、追加、または削除する必要がある場合には、既存のロールをコピーします。

既存のロールは、Red Hat が提供する事前定義済みロールの1つであることも、以前に作成したカスタムロールにすることができます。

Red Hat が提供する事前定義されたロールのリストは、[事前定義されたユーザーアクセスロール](#) セクションを参照してください。



注記

事前定義されたロールを変更することはできません。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- **Create role** ウィザードを起動している。

手順

1. **Create role** ウィザードで **Copy an existing role** ボタンをクリックします。

2. コピーするロールの横にあるボタンをクリックします。
3. **Next** ボタンをクリックします。
4. **Name and description** ウィンドウには、**Role name** のコピーと、記入されている既存の **Role description** が表示されます。必要に応じて変更します。
5. **Next** ボタンをクリックします。ロール名がすでに存在する場合は、続行する前に別の名前を指定する必要があります。
6. **Add permissions** ウィンドウで、ロールに追加するアプリケーションパーミッションを選択します。デフォルトでは、パーミッションはアプリケーションごとにリスト表示されます。

ヒント

カスタムロールは、粒度の細かいパーミッションのみをサポートします。**approval:*:*** などのワイルドカードパーミッションはカスタムロールにコピーされません。

7. オプションでフィルタードロップダウンを使用して、Applications、Resources、または Operations でフィルタを行います。

ヒント

ウィザードページの上部にあるリストを使用して、ロールに追加したすべてのパーミッションを表示します。パーミッションをクリックして削除することができます。

8. **Next** ボタンをクリックして詳細を確認します。**Submit** ボタンをクリックし、ロールの送信、**Back** ボタンを押して変更を行い、**Cancel** ボタンを押してアクションを取り消します。

作成したロールを User Access グループに追加するのに利用できます。

2.8.4. アプリケーション固有のロールの作成

Create role ウィザードによって提供されるフィルターを使用して、特定のアプリケーションのロールを作成します。特定のアプリケーションのロールを作成すると、フィルターには選択したアプリケーションで許可される **Resource type** および **Operation** が表示されます。

複数のアプリケーションを含むアプリケーション固有のロールを作成できます。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- **Create role** ウィザードを起動している。
- ウィザードの **Add permissions** ステップを使用している。

手順

1. **Add permissions** ウィンドウで、**Filter by application** フィールドをクリックします。

2. アプリケーション名の最初の数文字を入力してアプリケーションを選択します。ウィザードには、そのアプリケーションの一致するパーミッションが表示されます。
3. 必要に応じて、ナビゲーションツールを使用して、利用可能なアプリケーションおよびパーミッションのリストをスクロールします。
4. アプリケーション固有のロールで、必要なパーミッションの横にあるチェックボックスをクリックします。
5. **Next** ボタンをクリックして詳細を確認します。**Submit** ボタンをクリックし、ロールの送信、**Back** ボタンを押して変更を行い、**Cancel** ボタンを押してアクションを取り消します。

2.8.5. コスト管理アプリケーションロールの作成

コスト管理アプリケーションに固有のロールを作成できます。コスト管理ロールを作成する場合は、そのロールのコスト管理リソース定義を定義します。他のアプリケーションロールでは、その選択肢が提供されません。

前提条件

- Cost management Operator がインストールされ、設定されている。
- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- Cost Management 用に少なくとも1つのクラウド統合が設定されている。
- **Create role** ウィザードを起動している。

手順

この手順では、コスト管理のパーミッションでゼロからロールを作成する方法を説明します。

1. **Create role** ウィンドウでラジオボタンをクリックし、**Create a role from scratch** をクリックします。
2. **Role name** (必須) および **Role description** (任意) を入力します。
3. **Next** ボタンをクリックして **Add permissions** ウィンドウを表示します。
4. **Filter by application** フィールドに **cost** を入力してコスト管理アプリケーションを表示し、**cost-management** チェックボックスをクリックします。
5. **Add permissions** ウィンドウが表示されたら、このロールに含めるコスト管理パーミッションごとにチェックボックスをクリックします。
6. **Next** ボタンをクリックして、**Define Cost Management resources** ウィンドウを表示します。
7. ロールに追加したアプリケーションパーミッションごとに、利用可能な **Resource definitions** のドロップダウンリストが表示されます。各コスト管理パーミッションで、1つ以上のリソースのチェックボックスをクリックする必要があります。
8. **Next** ボタンをクリックして詳細を確認します。**Submit** ボタンをクリックし、ロールの送信、**Back** ボタンを押して変更を行い、**Cancel** ボタンを押してアクションを取り消します。

2.8.5.1. ロールをゼロから作成するためのコスト管理の例

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- Cost Management 用に少なくとも1つのクラウド統合が設定されている。
- **Create role** ウィザードを起動している。

手順

1. **Create role** ウィザードを起動し、**Create a role from scratch** をクリックします。
2. **Role name** の **AWS Org Unit Cost Viewer** を入力してから、**Submit** ボタンをクリックします。説明は必要ありません。
3. **Filter by application** フィールドに **cost** を入力してコスト管理アプリケーションを表示し、**cost-management** チェックボックスをクリックします。
4. **aws.organizational_unit** が含まれる行のチェックボックスをクリックし、**Next** ボタンをクリックしてパーミッションで利用可能な **Resource definitions** のドロップダウンリストを表示します。
5. **Resource definitions** リストに表示されているリソースのチェックボックスをクリックし、**Next** ボタンをクリックして詳細を確認します。
6. **Permissions** と **Resource definitions** を表示するこのロールの詳細を確認した後に、**Submit** ボタンをクリックしてロールを送信します。



2.8.6. カスタムロール名の編集

カスタムロールの名前は、メインのロールページまたは **Permissions** ページから変更できます。

前提条件


- * 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- カスタムロールが1つ以上存在している。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#) に移動します。**Roles** ウィンドウが表示されます。**Roles** ウィンドウには、カスタムロールの名前の右側に  (**more options**) があります。
2.  (**more options**) をクリックします。

3. **Edit** をクリックしてロール名または説明を変更します。
4. **Delete** をクリックしてカスタムロールを削除します。

ヒント

ロール名をクリックして、**Permissions** ウィンドウを開き、ロール名の右側にある  (**more options**) をクリックして、**Edit** および **Delete** アクションにアクセスすることもできます。

5. 確認ウィンドウが表示されます。このアクションを元に戻すことができないことが確認されると、カスタムロールが削除されます。



2.8.7. カスタムロールからのパーミッションの削除

カスタムロールからパーミッションを削除できます。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- カスタムロールが1つ以上存在している。

手順

1. [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#) に移動します。**Roles** ウィンドウが表示されます。**Roles** ウィンドウには、カスタムロールの名前の右側に  (**more options**) があります。
2. カスタムロール名をクリックして、**Permissions** ウィンドウを開きます。
3. **Permissions** リストでアプリケーション権限名の右側にある  (**more options**) をクリックし、**Remove** をクリックします。
4. 確認ウィンドウが表示されます。**Remove permission** をクリックします。

2.8.8. デフォルトアクセスグループの復元

Default access グループは、Red Hat サービスが提供する状態に復元できます。これを実行すると、**Custom default access** グループは、そのグループに加えられた変更と共に削除されます。

Default access グループを復元する場合には、**Custom default access** グループを復元する方法はありません。

Default access グループを復元する理由:

- 意図されていない **Default access** グループに変更を加えた場合
- **Default access** グループを作り直す場合

- Custom default access グループを削除する場合。
- Red Hat サービスによってプッシュされた Default access グループへの変更を取得して、Custom default access グループを破棄する場合。



注記

Default access グループまたは Custom default access グループのいずれかである default グループの1つがシステム上に常に存在します。

前提条件

- 組織管理者権限を持つユーザーとして [Red Hat Hybrid Cloud Console](#) にログインしている。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。
- Custom default access グループが存在する。

手順

1. [Red Hat Hybrid Cloud Console](#) > [Settings](#) > [Identity & Access Management](#) > [User Access](#) > [Groups](#) に移動します。Groups ページが表示されます。
2. Groups ページで Custom default access をクリックします。
3. Restore to default をクリックし、警告メッセージを受け入れます。Default access は Groups ページに表示されます。

第3章 事前定義された USER ACCESS ロール

以下の表は、ユーザーアクセスで提供される事前定義済みロールのリストです。事前定義されたロールの一部は **Default access** グループに含まれます。これには、組織内の認証されたすべてのユーザーが含まれます。

組織内の組織管理者ユーザーのみが、**Default admin access** グループのロールを継承します。このグループは Red Hat によって提供されるため、Red Hat が **Default admin access** グループにロールを割り当てると自動的に更新されます。

事前定義されたロールを表示する方法は、[2章 ユーザーアクセス設定の手順](#) を参照してください。

注記

事前定義されたロールは Red Hat によって更新および変更されますが、変更することはできません。この表には、現在利用可能なすべての事前定義済みロールが含まれているとは限りません。

表3.1 ユーザーアクセスで提供される事前定義されたロール

ロール名	説明	デフォルトのアクセスグループ	デフォルトの管理者アクセスグループ
Compliance administrator	コンプライアンスリソースへの完全アクセスを付与するコンプライアンスロール。		X
Compliance viewer	コンプライアンスリソースへのアクセス権限を付与するコンプライアンスロール。	X	
Drift analysis administrator	Drift Analysis リソースに対して利用可能な操作を実行します。		X
Drift viewer	Drift Analysis リソースに対して読み取り専用操作を実行します。	X	
RHEL Advisor administrator	RHEL アドバイザーリソースに対して利用可能な操作を実行します。	X	
Inventory Groups Administrator	インベントリーグループデータの読み取りと編集ができるようになります。		X
Inventory Groups Viewer	インベントリーグループデータを読み取ることができます。		

ロール名	説明	デフォルトのアクセスグループ	デフォルトの管理者アクセスグループ
Inventory Hosts Administrator	インベントリーホストデータの読み取りと編集ができるようになります。	X	X
Inventory Hosts Viewer	インベントリーホストデータを読み取ることができます。		
Inventory administrator	任意の Inventory リソースに対して利用可能な操作を実行します。		
Malware detection administrator	マルウェア検出リソースに対して利用可能な操作を実行します。		X
Malware detection viewer	マルウェア検出リソースを読み取ります。		
Notifications administrator	通知およびインテグレーションアプリケーションに対して使用可能な操作を実行します。		X
Notifications viewer	通知およびインテグレーションアプリケーションへの読み取り専用アクセス。		
Patch administrator	Patch リソースに対して利用可能な操作を実行します。		X
Patch viewer	パッチリソースを読み取ります。	X	
Policies administrator	任意の Policies リソースに対して利用可能な操作を実行します。		X
Policies viewer	ポリシーリソースに対して読み取り専用操作を実行します。	X	

ロール名	説明	デフォルトのアクセスグループ	デフォルトの管理者アクセスグループ
Remediations administrator	Remediations リソースに対して利用可能な操作を実行します。		
Remediations user	Remediations リソースに対して作成、表示、更新、削除の操作を実行します。	X	
Resource Optimization administrator	リソース最適化リソースに対して使用可能な操作を実行します。		X
Resource Optimization user	読み取り専用権限を付与するリソース最適化ユーザーロール。	X	
Tasks administrator	タスクリソースに対して利用可能な操作を実行します。		X
User Access administrator	console.redhat.com でホストされるサービスへのユーザーアクセスを設定および管理するために、組織以外の管理者フルアクセスを付与します。このロールは、組織の管理者だけが表示および割り当てることができます。		
User Access principal viewer	非組織管理者に、ユーザーアクセス内のプリンシパルへの読み取りアクセスを許可します。		
Vulnerability administrator	Vulnerability リソースに対して利用可能な操作を実行します。		X
Vulnerability viewer	脆弱性リソースを読みます。	X	

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。ご要望に対応できるよう、できるだけ詳細にご記入ください。

前提条件

- Red Hat アカウントを持っている。Red Hat アカウントをお持ちでない場合は、[Red Hat カスタマーポータル](#) ホームページで **登録** をクリックしてアカウントを作成できます。
- Red Hat アカウントにログインしている。

手順

1. フィードバックを提供するには、[Create Issue](#) のリンクをクリックします。
2. **Summary** テキストボックスに、問題または機能拡張に関する説明を入力します。
3. **Description** テキストボックスに、問題または機能拡張の詳細を入力します。
4. Red Hat ユーザー名が **Reporter** テキストボックスに自動的に表示されない場合は、入力します。
5. ページの一番下までスクロールし、**Create** ボタンをクリックします。ドキュメントの問題に関するチケットが作成され、適切なドキュメントチームに転送されます。

フィードバックの提供にご協力いただきありがとうございました。