Red Hat Hybrid Cloud Console 2022

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

ガイド

Last Updated: 2022-06-22

Red Hat Hybrid Cloud Console 2022 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

ガイド

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

本書は、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。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティー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。これは大規模な取り組みであるため、これらの変更は今後の複数のリリースで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。

RED HAT HYBRID CLOUD CONSOLE ドキュメントへのフィードバック

弊社のドキュメントについてのご意見をお聞かせください。ドキュメントの改善点はございませんか。これを行うには、Bugzilla のチケットを作成します。

1. Bugzilla の Web サイトに移動します。
2. 「Component (コンポーネント)」として **Documentation** を使用します。
3. **Description** フィールドに、ドキュメントの改善に向けたご提案を記入してください。ドキュメントの該当部分へのリンクも追加してください。
4. **Submit Bug** をクリックします。

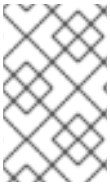
第1章 ロールベースアクセス制御 (RBAC) のユーザーアクセス設定ガイド

1.1. ユーザーアクセスとは

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。

1.1.1. 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、組織管理者および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。

1.1.2. 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。

1.1.3. 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パーミッション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。また、**Default access** グループには、組織内の認証済みユーザーがすべて含まれます。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。

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。

1.1.3.1. 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。

Default admin access グループに含まれているロールについては 「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。

1.1.3.2. 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。**Default access** グループの利点の 1 つは、Red Hat Hybrid Cloud Console で **Default access** グループのロールが追加されたときに自動的に更新されることです。

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。「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。

組織管理者は、**Default access** グループにロールを追加したり、**Default access** グループからロールを削除したりできます。**Default access** 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。

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。

注記

Default access グループを変更して保存すると、その名前が **Custom default access**になります。この名前変更を元に戻したり、取り消すことはできません。これ以降、組織管理者がグループへの更新および変更をすべて行います。**Custom default access**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。

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。事前定義されたロール、カスタムロール、またはその両方の組み合わせを使用する新規アクセスグループを作成できます。

1.1.3.3. 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、サービスの **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、そのサービスに対する読み取りと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ースは **Members** タブにユーザーを一覧表示します。

1.1.3.4. 追加アクセス

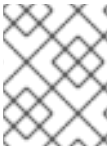
Red Hat Hybrid Cloud Console のユーザーアクセスは追加モデルを使用します。つまり、**deny** ロールはありません。つまり、アクションが許可されるだけです。アクセスは、必要なパーミッションを持つ適切なロールをグループに割り当てることで制御し、ユーザーをそれらのグループに追加することによって制御できます。個別のユーザーに許可されるアクセスは、そのユーザーが属するすべてのグループに割り当てられたすべてのロールの合計です。

1.1.3.5. 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

2.1. ユーザーアクセス設定の手順

組織管理者または User Access administrator として  (**設定**) をクリックして、ユーザーアクセスグループ、ロール、およびパーミッションを表示、設定、および変更できます。

2.1.1. 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。

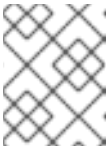
User Access administrator を持つと、組織管理者ではないユーザーは、ユーザーアクセス機能を管理するための数多くの組織管理機能を実行できます。**User Access administrator** のロールは、**Default admin access** グループのロールを継承しません。そのグループのロールは、組織管理者に制限されています。

前提条件

- 組織管理者である。
- **Create role** ウィザードを起動していること。
- ウィザードの **Add permissions** ステップを使用している。

手順

1. Red Hat Hybrid Cloud Console で Red Hat 組織のアカウントにログインします。
2. Settings アイコン (歯車) をクリックして Settings ページを開きます。
3. Settings ページで User access タブをクリックして展開します。
4. Groups タブをクリックして Groups ページを表示します。
5. Create group をクリックします。
6. 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。
    a. 認識可能な名前 (**User Access Admin**) でグループに名前を付けます。
    b. 意味のある説明 (**User Access Organization Administrator permissions**) を記入します。
    c. **Next** ボタンをクリックしてロールを追加します。
    d. **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。
    e. **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。

7. **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。

2.1.2. 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済みのロールの一覧は、*4章 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。

注記

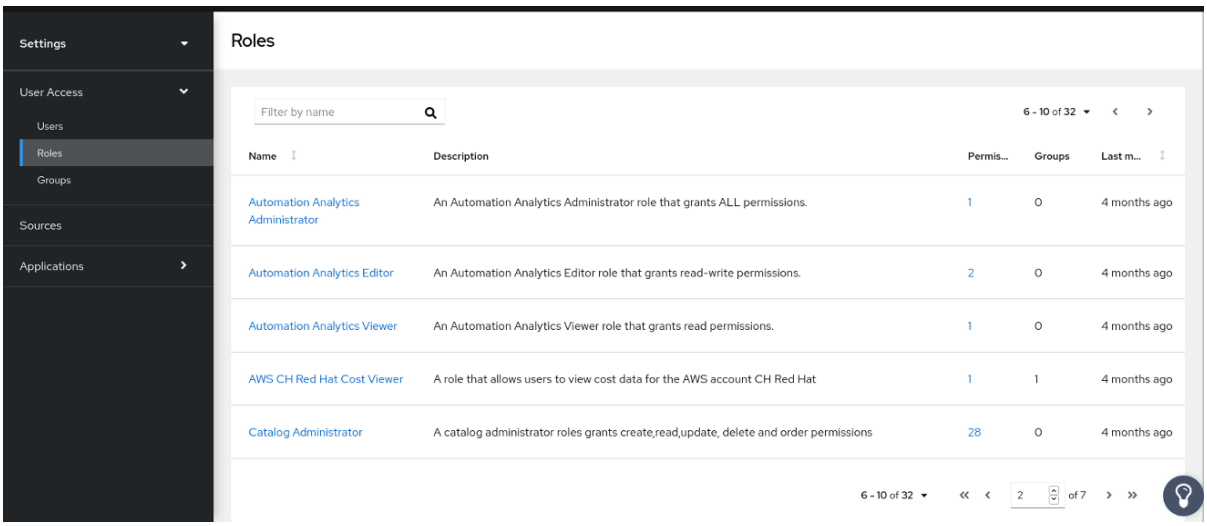
事前定義されたロールを変更することはできません。

前提条件

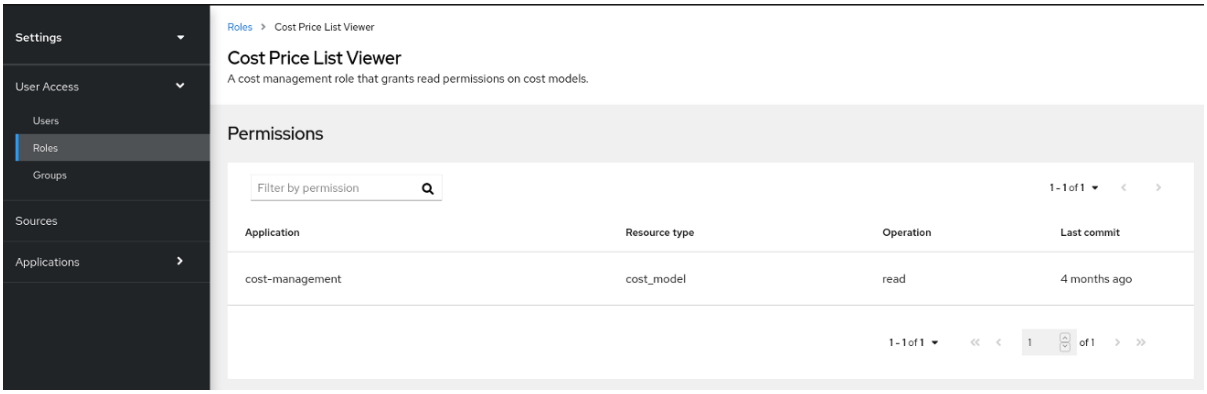
- 組織管理者である。
- 組織管理者でない場合は、**User Access administrator** のロールが割り当てられているグループのメンバーである。

手順

1. Red Hat Hybrid Cloud Console で、Red Hat の組織のアカウントにログインします。
2. Settings アイコン (歯車) をクリックして **Settings** ページを開きます。
3. **Settings** ページで **User access** タブをクリックして展開します。
4. **Role** タブをクリックして、ユーザーアクセスロールを表示します。全ロールのリストをスクロールできます。



5. 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。



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付与し、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。

2.1.3. 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。

Member 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

- 組織管理者である。
- 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

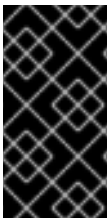
1. Red Hat Hybrid Cloud Console で、Red Hat の組織のアカウントにログインします。
2. Settings アイコン (歯車) をクリックして **Settings** ページを開きます。
3. **Settings** ページで **User access** タブをクリックして展開します。
4. **Groups** タブをクリックして **Groups** ページを表示します。
5. **Create group** をクリックします。
6. ウィザードが提供するガイド付きのアクションに従い、ユーザーとロールを追加します。
7. 追加のグループアクセスを付与するには、グループを編集し、追加のロールを追加します。

2.1.4. 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。

グループに追加したロールは、User Access で提供される事前定義済みのロール一覧、組織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。

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、属するその他の全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が既存のパーミッションに追加されます。



重要

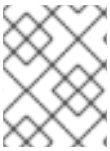
この手順では、**Default access** グループを変更します。変更したら、**デフォルトのアクセス** グループを復元できません。**Default access** グループを修正すると、その名前が **Custom default access** になります。**Custom default access** グループは、Red Hat によって Red Hat Hybrid Cloud Console から変更をプッシュしても更新されません。

前提条件

- 組織管理者である。
- 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 で、Red Hat の組織のアカウントにログインします。
2. Settings アイコン (歯車) をクリックして **Settings** ページを開きます。
3. **Settings** ページで **User access** タブをクリックして展開します。
4. **Groups** タブをクリックして **Groups** ページを表示します。
5. **Default access** グループからすべてのロールを削除します。
   組織の全ユーザーは **Default access** グループに属するため **Default access** で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して、ユーザーは **Default access** からロールパーミッションを継承しません。
6. **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。
7. 許可されたアクセスパーミッションのユーザーと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す。

2.1.5. 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

- 組織管理者である。
- 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。
  「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」

手順

1. Red Hat Hybrid Cloud Console で、Red Hat の組織のアカウントにログインします。
2. Settings アイコン (歯車) をクリックして **Settings** ページを開きます。
3. **Settings** ページで **User access** タブをクリックして展開します。
4. **Groups** タブをクリックして **Groups** ページを表示します。
5. 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。
6. 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一覧を表示します。
7. **Add member** タブをクリックします。
8. **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。
9. 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。

2.1.6. 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

- 組織管理者である。
- 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 で、Red Hat の組織のアカウントにログインします。
2.  (設定) アイコンをクリックして、**Settings** ページを開きます。
3. **Settings** ページで **User access** タブをクリックして展開します。
4. **Groups** タブをクリックして **Groups** ページを表示します。
5. 変更するグループ **Name** をクリックします。
6. **Role** タブをクリックします。
7. 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。
8. **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  をクリックして、**Remove from group** をクリックします。
9. 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。

2.1.7. ユーザーアクセスのための詳細なパーミッション

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が可能なスーパーユーザーロールと同等です。

詳細な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 (読み取り専用や読み取り/更新など) を作成 (または変更) できます。ただし、削除はできません。

たとえば、OCI Administrator および Cost Price List Viewer 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
コスト管理者	コスト管理	* (all)	* (all)

ロール	アプリケーション	リソース	操作
コスト価格リストビューアー	コスト管理	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。

2.1.7.1. 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済みのロールの一覧は、*4章 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。

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

- 組織管理者である。
- 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従って、ロールの追加手順を進めます。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. 組織管理者権限を持つユーザーとして Red Hat Hybrid Cloud Console にログインします。
2. ログイン後にホームページから  (**Settings**) をクリックし、設定ウィンドウを開きます。
3. **User Access** タブをクリックし、ドロップダウンの選択を展開します。
4. **Role** タブをクリックします。**Roles** ウインドウが表示されます。
5. **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。

2.1.7.2. ゼロからのロールの作成

特定の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

- 組織管理者である。
- 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こと。

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一覧表示されます。
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一覧を使用して、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。

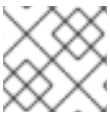
7. **Next** ボタンをクリックして詳細を確認します。**Submit** ボタンをクリックし、ロールの送信、**Back** ボタンを押して変更を行い、**Cancel** ボタンを押してアクションを取り消します。

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る。

2.1.7.3. 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済みのロールの一覧は、*4章 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。



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

- 組織管理者である。
- 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こと。

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一覧表示されます。

   ヒント

   カスタムロールは、詳細な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 でフィルターを行います。

   ヒント

   ウィザードページの上部にある一覧を使用して、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る。

2.1.7.4. 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の許可される **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

- 組織管理者である。
- 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こと。
- 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。

2.1.7.5. 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、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

- コスト管理 Operator がインストールされ、設定されている。
- 組織管理者である。
- 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。
- コスト管理用に少なくともソースが 1 つ設定されている。
- **Create role** ウィザードを起動していること。

手順

この手順では、費用管理のパーミッションを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** ウイ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のチェックボックスをそれぞれクリックします。
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。

2.1.7.5.1. 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

- 組織管理者である。
- 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。
- コスト管理用に少なくともソースが 1 つ設定されている。
- Create role ウィザードを起動していること。

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. **ロール名** 用の **AWS Org Unit Cost Viewer** を入力し、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 一覧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。

2.1.7.6. 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

- 組織管理者である。
- 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. ログイン後にホームページから  (Settings) をクリックし、設定ウィンドウを開きます。
2. User Access タブをクリックし、ドロップダウンの選択を展開します。

3. **Role** タブをクリックします。**Roles** ウインドウが表示されます。**Roles**ウィンドウで、カスタムロールはその名の右側に (**more options**) を持ちます。
4. (**more options**) をクリックします。
5. **Edit** をクリックしてロール名または説明を変更します。
6. **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。

7. 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。

2.1.7.7. 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

- 組織管理者である。
- 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. ログイン後にホームページから (**Settings**) をクリックし、設定ウィンドウを開きます。
2. **User Access** タブをクリックし、ドロップダウンの選択を展開します。
3. **Role** タブをクリックします。**Roles** ウインドウが表示されます。**Roles**ウィンドウで、カスタムロールはその名の右側に (**more options**) を持ちます。
4. 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。
5. **Permissions** 一覧で、アプリケーションパーミッション名の右側にある (**more options**) をクリックし、**Remove** をクリックします。
6. 確認ウィンドウが表示されます。**Remove permission** をクリックします。

第3章 カスタマーアカウントに一時的にアクセスする手順

3.1. アクセス要求機能の使用のタイミング

お客様に Red Hat Hybrid Cloud Console のアカウントに関する質問がある場合には、Red Hat スタッフ（通常は Red Hat テクニカルアカウントマネージャー(TAM)または Red Hat Customer Experience and Engagement サポートエンジニア）に一時的にアカウントへのアクセス権限を付与することができます。顧客がアカウントへのアクセス権限を付与すると、Red Hat TAM またはサポートエンジニアはお客様のアカウントのメンバーであるかのように Red Hat Hybrid Cloud Console のアカウント情報にアクセスできます。

Red Hat サポートサービスの詳細は、「Red Hat Service offerings」を参照してください。

Red Hat Technical Account Manager (TAM)または Red Hat Customer Experience and Engagement サポートエンジニアがカスタマーアカウントへのアクセスを要求した場合、表示/操作可能な内容は、アクセスリクエストにどのユーザーアクセスロールが割り当てられているかにより制限され、また Red Hat Hybrid Cloud Console で利用可能なカスタマーアカウント情報に限定されます。

デフォルトのユーザーアクセスロールの詳細は、「事前定義されたユーザーアクセスロール」を参照してください。

3.2. アクセスリクエスト機能を使用してカスタマーアカウントへのアクセスを提供する

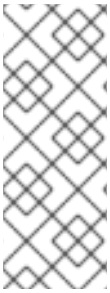
顧客アカウントへの直接アクセスは、スクリーンショットやリモート表示セッションが成功しない場合に問題の解決に役立ちます。アクセスリクエスト機能を使用することで、Red Hat サポートチームはアクセスレベルとアクセス期間に同意したお客様と連携します。

一般的な状況では、お客様が Red Hat サポートチームとサポートケースを作成します。Red Hat サポートチームは、顧客と連携してお客様のアカウントへのアクセスを準備し、Red Hat Hybrid Cloud Console にログインします。

アクセスリクエストのアクションを開始する前に、以下の情報を確認してください。

- カスタマーアカウント番号。
- 最大 12 カ月までの最長期間を含むアクセス期間。
- お客様が Red Hat サポートチームに付与するデフォルトのユーザーアクセスロール。

アクセス要求機能を使用する場合、システムへのアクセスは常にお客様によって制御されます。お客様はアクセス権限をいつでも拒否できます。



注記

アクセス要求のアクションは、リクエストを行ったサポートチーム上の Red Hat スタッフの一意のユーザー名に関連付けられます。つまり、各 Red Hat アクセス要求は、リクエストを作成した Red Hat スタッフにしか表示されず、このスタッフだけがお客様のシステムにアクセスできます。別の Red Hat サポートエンジニアがサポートケースに関与し、アクセスする必要がある場合は、その一意の Red Hat ユーザー名に対する新しいアクセスリクエストアクションが必要になります。

3.2.1. アカウントへのアクセスの承認

お客様および組織管理者は、Red Hat アクセスリクエストを承認することで、アカウントへのアクセス権限を付与します。組織管理者がログインし、リクエストを受信すると、アクセス要求の通知ポップアップが Red Hat Hybrid Cloud Console に一時的に表示されます。

Red Hat Hybrid Cloud Console の  （**Settings**）で、システムのすべてのアカウントアクセス要求およびそれらのステータスを表示できます。

注記

組織管理者のみがアクセス要求を承認または拒否できます。User Access administrator ロールは、アクセス要求を承認または拒否するパーミッションを提供しません。

前提条件

Red Hat サポートエンジニアと連携し、サポートエンジニアがアクセス要求を作成して承認を得られるように、以下の情報を提供している。

- Red Hat カスタマーアカウント番号。
- システムアクセスの開始日。
- システムアクセスの終了日。
- アクセス要求が Red Hat サポートエンジニアに付与するユーザーアクセスロールを理解している。

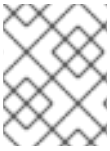
手順

1. Red Hat Hybrid Cloud Console にログインします。
2.  （**Settings**）をクリックします。
3. **User Access > Red Hat Access Requests**ウィンドウに移動します。
すべてのアクセス要求の一覧が表示されます。
4. 推奨される方法は、Request ID 番号（16 進数の文字列）をクリックすることです。
5. 要求の詳細と要求されたロールを慎重に確認します。
6. **Approve** をクリックし、要求を承認します。アクションが確認され、ステータスが Approved に変わります。
7. 編集機能を使用して応答を変更します。

3.2.2. アカウントへのアクセスの拒否

お客様および組織管理者は、Red Hat アクセスリクエストを拒否することで、アカウントへのアクセス権限を拒否します。

Red Hat Hybrid Cloud Console の  （**Settings**）で、すべてのアカウントアクセス要求およびそれらのステータスを表示できます。



注記

組織管理者のみがアクセス要求を承認または拒否できます。User Access administrator ロールは、アクセス要求を承認または拒否するパーミッションを提供しません。

前提条件

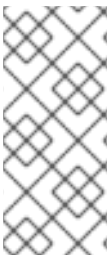
- Red Hat サポートエンジニアがアクセスリクエストを作成している。
- アクセスリクエストが **Red Hat Account Requests**一覧に表示されている。

手順

1. Red Hat Hybrid Cloud Console にログインします。
2.  （**Settings**）をクリックします。
3. **User Access > Red Hat Access Requests**ウィンドウに移動します。
すべてのアクセス要求の一覧が表示されます。
4. 推奨される方法は、Request ID 番号（16 進数の文字列）をクリックすることです。
5. 要求の詳細と要求されたロールを慎重に確認します。
6. **Deny** をクリックして、要求を拒否します。アクションが確認され、ステータスが Denied に変わります。
7. 編集機能を使用して応答を変更します。

3.2.3. カスタマーアカウントへのアクセスの要求（Red Hat サポートチーム）

Red Hat サポートチームのメンバーは、アクセスリクエスト機能を使用して、Red Hat Hybrid Cloud Console のお客様のアカウントへのアクセスを取得します。アクセスリクエストを受信すると、お客様はリクエストを承認または拒否できます。



注記

アクセス要求機能は、検証済みの Red Hat スタッフユーザーアカウントを持つ Red Hat スタッフだけが利用可能です。アクセス要求機能は、スタッフ以外には表示されません。この情報は、Red Hat Technical Account Manager (TAM)または Red Hat Customer Experience and Engagement サポートエンジニアを支援し、顧客と Red Hat サポートチームメンバー間の要件の通信を強化するために提供されます。

前提条件

アクセスリクエストのアクションを開始する前に、以下の情報を確認している。

- カスタマーアカウント番号またはお客様の組織 ID。
- 最大 12 カ月までの最長期間を含むアクセス期間。
- お客様が Red Hat サポートチームに付与するユーザーアクセスロール。

手順

1. Red Hat Hybrid Cloud Console にログインします。
2. Red Hat Hybrid Cloud Console ウィンドウの右上にあるユーザーアバターをクリックします。ドロップダウンリストが表示されます。
3. ドロップダウンリストで **Internal** をクリックします。
4. **Internal** ウィンドウが表示されたら、**Access Requests** をクリックします。
5. **Create request** をクリックします。ウィザードが、ステップを順を追ってガイドします。
6. アクセスリクエストを作成し、お客様がリクエストを承認または拒否する前に、リクエストを編集するか、またはキャンセルすることができます。

検証

アクセス可能なアカウントの一覧が、Red Hat Hybrid Cloud Console アカウントのマストヘッドのコンテキストスイッチに表示されます。このリストには、個人アカウントが含まれます。

コンテキストスイッチャーから別のアカウントを選択すると、バナーが Red Hat Hybrid Cloud Console ウィンドウに表示されます（例：「Viewing as account 654321」）。

ヒント

Access Requests ウィンドウには、送信したすべてのアクセス要求のステータスが表示されます。アカウント要求はユーザー名にリンクされ、ユーザーに固有のものです。作成したリクエストに対して他の Red Hat スタッフが表示したり、処理したりすることはできません。

第4章 事前定義されたユーザーアクセスロール

4.1. 事前定義されたユーザーアクセスロール

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一覧です。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4.1 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	Default admin access グループ
Approval Administrator	ワークフロー、要求、アクション、テンプレートを管理するパーミッションを付与する承認管理者ロール。		
Approval User	リクエストの作成/読み取り/句へのパーミッションとワークフローの読み取り/読み取りの権限を付与する承認ユーザーロール。	x	
Approval Approver	要求の読み取りおよび承認のパーミッションを付与する承認承認者ロール。		
Automation Analytics Administrator	All パーミッションを付与する Automation Analytics の管理者ロール。		
Automation Analytics Editor	読み取り/書き込みパーミッションを付与する自動化分析編集者ロール。	x	

ロール名	説明	デフォルトのアクセスグループ	Default admin access グループ
Automation Analytics Viewer	読み取りパーミッションを付与する Automation Analytics Viewer ロール		
Catalog Administrator	カタログ管理者のロールは、createreadupdate の削除権限および発注権限を付与します		
Catalog User	カタログユーザーロールは読み取りおよび順序のパーミッションを付与します。	x	
Compliance administrator	コンプライアンスリソースに対して利用可能な操作を実行します。	x	
RHC Administrator	サービス有効化ダッシュボードでの操作を実行します。		
RHC Viewer	サービス有効化ダッシュボードを表示できます。	x	
Cost Administrator	読み取りおよび書き込みパーミッションを付与するコスト管理の管理者ロール。		x
Cost Price List Administrator	コストモデルに読み書きパーミッションを付与するコスト管理ロール。		
Cost Price List Viewer	コストモデルに読み取りパーミッションを付与するコスト管理ロール。		
Cost Cloud Viewer	クラウドソースに関連するコストレポートの読み取りパーミッションを付与するコスト管理ロール。		

ロール名	説明	デフォルトのアクセスグループ	Default admin access グループ
Cost OpenShift Viewer	OpenShift ソースに関連するコストレポートの読み取りパーミッションを付与するコスト管理ロール。		
Drift analysis administrator	Drift analyze リソースに対して利用可能な操作を実行します。	x	
Insights 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 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。	x	
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。		
Malware detection viewer	マルウェア検出リソースを読み取ります。		
Migration Analytics administrator	任意の Migration Analytics リソースに対して利用可能な操作を実行します。	x	
Notifications administrator	通知および統合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	通知および統合アプリケーションへの読み取り専用アクセス。		
OCP Advisor administrator	OCP 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	
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	

ロール名	説明	デフォルトのアクセスグループ	Default admin access グループ
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	
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。		
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 create、view、update、delete 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	
Sources administrator	任意のソースに対して利用可能な操作を実行します。		
Subscription Watch administrator	サブスクリプションリソースに対して利用可能な操作を実行します。		
Subscriptions user	サブスクリプションリソースを表示します。	x	

ロール名	説明	デフォルトのアクセスグループ	Default admin access グループ
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	x
Vulnerability viewer	脆弱性リソースを読みます。		