Red Hat Hybrid Cloud Console 2023

基于角色的访问控制(RBAC)的用户访问权限配置指南

如何使用 User Access 功能为 Red Hat Hybrid Cloud Console 上托管的服务配置 RBAC

Last Updated: 2023-05-26

Red Hat Hybrid Cloud Console 2023 基于角色的访问控制(RBAC)的用户访问权限配置指南

如何使用 User Access 功能为 Red Hat Hybrid Cloud Console 上托管的服务配置 RBAC

法律通告

摘要

本指南适用于希望使用 User Access 功能为托管在 Red Hat Hybrid Cloud Console 上的服务配置基于角色的访问控制(RBAC)的红帽帐户用户。 红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 信息。

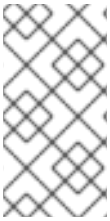
目录

第 1 章 基于角色的访问控制(RBAC)的用户访问权限配置指南

User Access 功能是基于角色的访问控制(RBAC)的实施，用于控制用户访问 Red Hat Hybrid Cloud Console 上托管的各种服务。您可以配置 User Access 功能，以授予用户对混合云控制台上托管的服务的访问权限。

1.1. 用户访问和软件作为服务(SAAS)访问模型

红帽客户帐户可能具有数百个经过身份验证的用户，但所有用户都需要相同级别访问 Red Hat Hybrid Cloud Console 上的 SaaS 服务。通过 User Access 功能，机构管理员可以管理用户对 Red Hat Hybrid Cloud Console 上托管的服务的访问权限。



注意

用户访问不管理 OpenShift Cluster Manager 权限。对于 OpenShift Cluster Manager，机构管理员和集群所有者都可以查看信息，但只有机构管理员和集群所有者对集群执行操作。详情请参阅 Openshift Cluster Manager 文档中的在 OpenShift Cluster Manager 中配置对集群的访问。

1.2. 谁可以使用用户访问权限

要初始查看和管理 Red Hat Hybrid Cloud Console 上的用户访问权限，您必须是一个机构管理员。这是因为用户访问权限需要从 红帽客户门户网站 处指定的用户管理功能。这些功能仅属于机构管理员。

User Access administrator 角色是机构管理员可以分配的特殊角色。此角色允许不是机构管理员的用户在 Red Hat Hybrid Cloud Console 上管理用户访问权限。

1.3. 如何使用用户访问

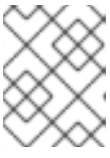
User Access 功能基于管理角色，而不是单独为特定用户分配权限。在 User Access 中，每个角色都有一组特定的权限。例如，角色可能允许应用程序的读取权限。另一个角色可能允许应用程序的写入权限。

您可以创建包含角色和扩展名的组，以为每个角色分配权限。您可以将用户分配给组。这意味着，为组中的每个用户分配该组中角色的权限。

通过创建不同的组并为该组添加或删除角色，您可以控制该组允许的权限。将一个或多个用户添加到组中时，这些用户可以执行该组允许的所有操作。

红帽为用户访问提供了两个默认访问组：

- **默认 admin 访问** 组。**Default admin 访问权限** 组仅限于您所在机构的机构管理员用户。您不能更改或修改 **Default admin 访问** 组中的角色。
- **默认访问**组。**Default 访问** 组包含您的机构中的所有经过身份验证的用户。这些用户会自动继承预定义角色的选择。



注意

您可以对 **Default 访问** 组进行更改。但是，当您这样做时，其名称会更改为 **Custom default access** group。

红帽提供了一组预定义的角色。根据应用程序，每个支持的应用程序的预定义角色可能会有针对应用程序量身定制的不同权限。

1.3.1. 默认管理员访问 组

默认管理员访问 组由红帽在 Red Hat Hybrid Cloud Console 上提供。它包含一组分配给系统上具有机构管理员角色的用户的角色。此组中的角色在 Red Hat Hybrid Cloud Console 中预定义。

Default admin 访问 组中的角色不能添加到或修改中。由于此组由红帽提供，因此当红帽为 **Default admin 访问权限** 组分配角色时，它会自动更新。

Default admin 访问权限 组的好处是它允许自动为机构管理员分配角色。

有关角色，请参阅 预定义的 User Access 角色，以了解 **默认 admin 访问** 组中。

1.3.2. Default 访问 组

默认访问组 由红帽在 Red Hat Hybrid Cloud Console 上提供。它包含 Red Hat Hybrid Cloud Console 中预定义的一组角色。**Default 访问** 组包含您机构中的所有经过身份验证的用户。当在 Red Hat Hybrid Cloud Console 中添加 **Default access** 组角色时，**Default access** 组会自动更新。

注意

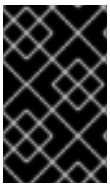
Default 访问 组包含所有预定义的角色的子集。如需更多信息，请参阅预定义的用户访问角色。

作为机构管理员，您可以将角色添加到 **默认访问组中，并从 Default 访问** 组中删除角色。当您这样做时，其名称会更改为 **Custom default access**group。您对此组所做的更改会影响您机构中的所有经过身份验证的用户。

1.3.3. 自定义默认访问组

手动修改 **Default 访问组时**，其名称会更改为 **Custom default access**，这表示它已被修改。此外，它不再从 Red Hat Hybrid Cloud Console 自动更新。

从现在起，机构管理员负责所有更新和对 **自定义默认访问组** 的更改。Red Hat Hybrid Cloud Console 不再管理或更新该组。



重要

您不能删除 **Default access** group 或 **Custom default access**组。
您可以恢复 **Default 访问** 组，这将删除 **自定义默认** 访问组以及您所做的任何更改。请参阅恢复默认访问组。

1.3.4. User Access groups、role 和 permissions

用户访问使用以下类别来确定机构管理员可授予受支持的 Red Hat Hybrid Cloud Console 服务的用户访问权限级别。提供给任何授权用户的访问权限取决于用户所属的组以及分配给该组的角色。

- 组 ：属于帐户的用户集合，它提供角色映射到用户的映射。机构管理员可以使用组来为组分配一个或多个角色，并在组中包含一个或多个用户。您可以创建没有角色的组，且没有用户。
- **角色** ：一组提供对给定服务的访问权限的权限，如 Insights。执行某些操作的权限被分配给特定的角色。角色分配到组。例如，您可能具有服务的 **read** 角色和 **write** 角色。将这两个角色添加到组会授予该组的所有成员对该服务进行读写权限。
- **权限** ：可以请求的离散操作。权限分配给角色。

机构管理员向组添加或删除角色和用户。组可以是由机构管理员创建的新组，也可以是组可以是现有的组。通过创建包含一个或多个特定角色的组，然后将用户添加到该组中，您可以控制该组及其成员如何与 Red Hat Hybrid Cloud Console 服务交互。

当您将用户添加到组中时，他们将成为该组的成员。组成员继承其所属的所有其他组的角色。用户界面在 **Members** 选项卡中列出用户。

1.3.5. 添加访问

Red Hat Hybrid Cloud Console 的用户访问使用附加模型，这意味着没有 **拒绝** 角色。换句话说，仅允许操作。若要控制访问权限，请为组分配具有所需权限的适当角色，然后将用户添加到这些组中。允许任何单个用户的访问权限是分配给该用户所属的所有组的所有角色的总和。

1.3.6. 访问结构

以下是用户访问的用户访问结构的概述：

- **组** ：用户可以是一个或多个组的成员。
- **角色** ：可以将角色添加到一个或多个组中。
- **权限** ：可以为角色分配一个或多个权限。

在初始默认配置中，所有 User Access 帐户用户都会继承 **Default 访问组中提供的角色**。

注意

添加到组的任何用户都必须是 Red Hat Hybrid Cloud Console 上机构帐户的经过身份验证的用户。

第 2 章 配置用户访问的步骤

作为机构管理员或用户访问权限 **管理员**，您可以点击  > **Identity & Access Management**查看、配置和修改 User Access groups、角色和权限。

2.1. 创建用户访问权限管理员

User Access 管理员 是一个特殊的角色，机构管理员分配给组。此组中的所有用户可以执行 User Access 管理角色，如添加、修改或删除组和角色。**User Access 管理员角色** 不会继承 **Default Admin Access** 组中定义的角色。

User Access administrator 角色无法创建或修改 User Access 管理员组。只有机构管理员可以创建、修改或删除分配了 **User Access 管理员角色** 的组。

通过具有 **User Access administrator** 角色，不是机构管理员的用户可以执行许多机构管理员功能来管理用户访问权限。**User Access 管理员角色** 不会继承 **Default admin 访问** 组的角色。该组中的角色仅限于机构管理员。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Groups。
2. 点 **Create group**。
3. 按照向导提供的指导操作来创建组并添加用户和角色。
   a. 使用可识别名称命名组： **User Access Admin**。
   b. 提供一个有意义的描述：**User Access Organization Administrator permissions**
   c. 点 **Next** 按钮来添加角色。
   d. 搜索 **User Access administrator** 角色，再点选择框将此角色添加到组中。（可选）选择其他角色。
   e. 单击 **Next** 按钮，将成员添加到组中。

      注意

      您添加的任何成员都必须是机构帐户的活跃成员。

   f. 为组选择了成员后，点 **Next** 按钮来查看详情。
   g. 您可以点击 **Back** 按钮返回并进行更改，**或者取消** 该操作。
4. 点 **Submit** 按钮完成 **Create group** 向导。新组将显示在 **Groups** 选项卡中。

2.2. 查看角色和权限

您可以在 Red Hat Hybrid Cloud Console 查看用户访问的角色和权限。有关红帽提供的预定义角色列表，请参阅 预定义的用户访问角色 部分。

注意

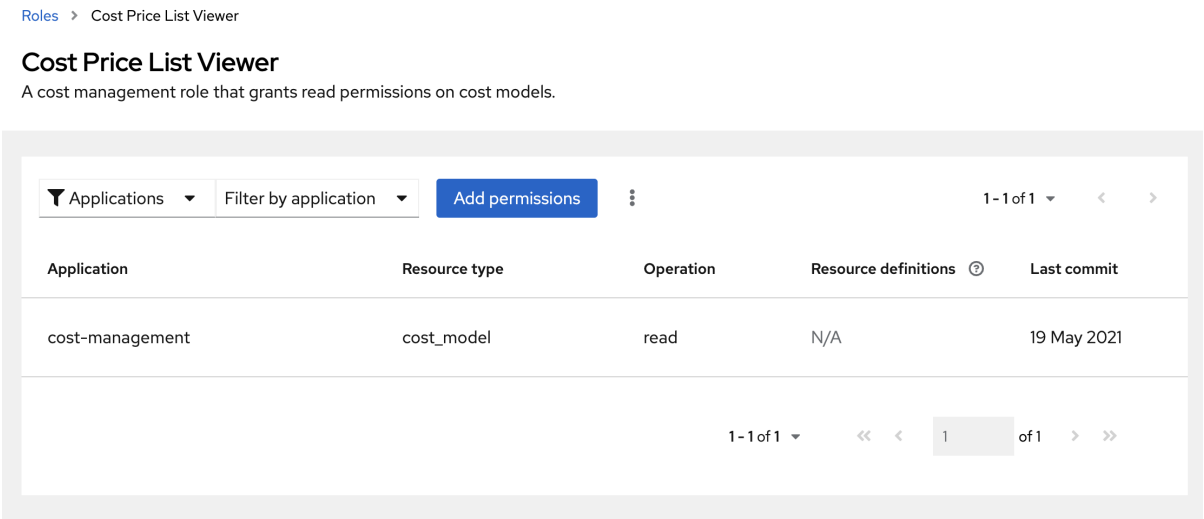
您无法修改预定义的角色。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Roles。此时会显示 User Access 角色。您可以滚动所有角色的列表。
2. 在表中，点角色**名称**或角色**权限**来查看分配给该角色的权限的详细信息。例如，如果您单击 **Cost the List Viewer** 角色，您会看到以下信息：



注意

星号 **指示** 通配符权限。通配符权限授予对所有资源类型的访问权限，并允许角色中的所有应用程序操作。

2.3. 查看用户权限

您可以在用户详情页面中查看用户的权限和其他与访问相关的信息。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。

流程

1. 导航到 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Users 来查看您的机构中的用户列表。
2. 点 **用户名** 查看该用户的更多详情。
3. 在用户详情页面中，您可以查看：
   - 如果用户是您所在机构的机构管理员
   - 用户的电子邮件地址
   - 混合云控制台上的用户用户名（也称为红帽登录）
   - 与用户关联的角色列表。查看每个角色的更多详情：
     - 单击 **Groups** 列中的数量，以显示分配了此角色的组。
     - 单击 **Permissions** 列中的数量，以显示角色提供的权限。

注意

如果您不是机构管理员，您可以通过导航到 Red Hat Hybrid Cloud Console > Settings 菜单(gear 图标) > Identity & Access Management > My User Access 来查看您自己的服务权限。

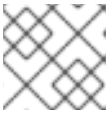
2.4. 使用角色和成员管理组访问权限

您可以通过创建组并将角色和用户添加到组中来管理组访问。角色及其权限决定了授予组所有成员的访问权限类型。

Members 选项卡显示您可以添加到组中的所有用户。当您将用户添加到组中时，他们将成为该组的成员。组成员继承其所属的所有其他组的角色。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。



注意

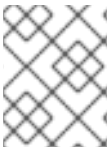
只有机构管理员才能将 **User Access administrator** 角色分配给组。

流程

1. 导航到 Red Hat Hybrid Cloud Console > Settings 菜单(gear icon)> Identity & Access Management > User Access > Groups 以打开 **Groups** 页面。
2. 点 **Create group**。
3. 按照向导提供的指导操作来添加用户和角色。
4. 要授予其他组访问权限，请编辑组并添加额外的角色。

2.4.1. 将角色添加到组中

向现有组添加角色，为该组的所有成员提供额外的权限。您可以查看用户详情，将角色添加到用户所属的组中。



注意

您可以从 **Users** 页面或通过从 **Groups** 页面编辑组，将角色添加到组中。这些步骤演示了如何从用户详情页面编辑组。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。

流程

1. 导航到 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Users 以打开 **Users** 列表。
2. 单击用户的 **Username**，以打开用户详情页面。
3. 点角色的 **Groups** 列中的 count。这表明用户是分配了此角色的成员。

注意

您可以点击 **Permissions** 列中的计数来查看角色提供的权限。

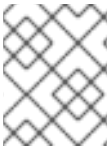
4. 单击 **组名称旁边的 Add role**，将额外角色添加到组中。这将打开 **Add roles** 对话框。
5. 选择您要添加到组的每个角色的复选框。（仅列出未与组关联的角色。） 点 **Add to group**。
6. 重新加载用户详情页面，以查看您添加到组中的角色。

组现在在控制台中有这些额外权限。

2.4.2. 将用户添加到组中

将用户添加到现有组中，为该用户提供分配给该组的角色授予权限。

当新团队成员加入您的机构并且您想要为其提供工作所需的所有权限时，这非常有用。



注意

您可以从 **Users** 页面将用户添加到组中，或者从 **Groups** 页面编辑组。这些步骤演示了如何从用户详情页面将用户添加到组中。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。

流程

1. 导航到 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Users 以打开 **Users** 列表。
2. 点您要编辑的用户的用户名。
3. 在用户详情页面上，单击 **Add user to a group**。此时会打开一个对话框，显示用户不是用户所属的组列表。
4. 选中一个或多个组的复选框，将用户添加到组中，然后单击 **Add to group**。
5. 重新加载用户详情页面，以查看您添加的角色。

用户现在具有他们添加到的组授予权限。

2.5. 限制对单个用户的服务访问

您可以创建一个包含单个用户的新组，并将角色添加到该组。您添加的角色为您提供了您希望单个用户具有的服务访问权限。如果您将其他用户添加到组中，则添加的用户将具有相同的组权限。

您添加到组的角色可以从 User Access 提供的预定义角色列表中，来自机构管理员创建的自定义角色，或两者的组合。

如需有关预定义角色的更多信息，请参阅 预定义的用户访问角色 部分。

当您将用户添加到新组时，用户获取新组的权限，并继承他们所属的所有其他组的权限。新组的权限添加到现有权限中。

重要

在此过程中，您可以修改 **Default 访问** 组。修改后，**默认访问** 组名称将更改为 **自定义默认访问**。通过 Red Hat Hybrid Cloud Console 推送的更改，不再更新 **自定义默认访问组**。

提示

您可以恢复 **Default 访问** 组，这将删除 **自定义默认** 访问组以及您所做的任何更改。请参阅恢复默认访问组。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Groups。此时会显示 **Groups** 页面。
2. 从 **Default 访问组中删除** 所有角色。
   由于机构中的所有用户都属于 **Default 访问** 组，所以您无法在 **Default 访问权限** 中添加或删除单个用户，以创建访问控制。通过删除所有角色，用户不会继承 **默认访问的角色权限**。
   a. 选中 roles 列表上方的复选框，以选择组中的所有角色。
   b. 点击更多选项图标，即 **删除**。

c. 单击 **Remove roles** 进行确认。

3. 保存对 **Default 访问** 组的更改。名称更改为 **Custom default access**。

4. 创建一个包含允许访问权限的用户和角色的新组。
例如，创建一个组 **Security Admin**，其中包含有权访问安全漏洞服务的用户。

a. 创建组 **Security Admin**。

b. 从 **Members** 列表中向组添加一个或多个用户。

c. 添加 **Vulnerability 管理员**角色。
您添加到此组的每个用户对漏洞服务具有完全访问权限。

注意

如果您希望机构管理员具有访问权限，请将机构管理员用户添加到组中。

2.6. 在组中包含机构管理员

您可以在组中包含机构管理员。如果您希望机构管理员将角色分配给该组，您可以将机构管理员用户添加到组中。机构管理员不会继承所有 Red Hat Hybrid Cloud Console 应用程序的所有可用角色。没有通过 **Default access** 组或 **Default admin access** 组继承的任何角色，都必须通过组成员资格分配。

注意

此流程假设您想修改现有组，并将机构管理员添加到组中。或者，您可以在创建新组时将机构管理员添加到组中。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 如果组不存在，请创建一个组。如需更多信息，请参阅使用角色和成员管理组访问。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Groups。此时会显示 **Groups** 页面。

2. 单击组名称， 以显示组的详细信息。

3. 在组详细信息页面上，单击 **Members** 选项卡，以显示属于组成员的授权用户列表。

4. 点 **Add member** 选项卡。

5. 在显示的组页面上的 **Add members to the group** 页面中，找到机构管理员用户名，然后点击名称旁边的复选框。
例如，如果机构管理员用户名是 **smith-jones**，找到该名称并点击 **smith-jones** 旁边的复选框。
您可以添加其他名称。

6. 验证名称列表已完成，然后单击 **Add to group** 操作。

当操作成功完成时，会出现通知弹出窗口。

2.7. 禁用组访问

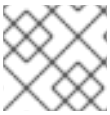
您可以通过从组中删除角色来禁用组访问。由于角色及其权限决定了授予组的访问权限的类型，因此删除角色会禁用该角色的组访问。

前提条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。

流程

1. 导航到 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Groups，并在需要时登录。此时会显示 **Groups** 页面。
2. 点击您要修改的 Group **Name**。
3. 点 **Roles** 选项卡。
4. 单击您要删除的 **角色** 名称旁边的复选框。
   您可以点击 **Name** 列顶部的复选框来选择所有角色。
5. 点击 **Add role** 选项卡旁的 More options 菜单图标 ⋮ ，然后点 **Remove from group**。
6. 在出现的确认窗口中，单击 **Remove role** 或 **Cancel** 以完成该操作。



注意

组不包含角色，没有成员，并且仍然是有效的组。

2.8. 用户访问的粒度权限

粒度权限允许机构管理员为一个或多个应用程序定义角色权限。许多预定义的角色提供通配符权限，这等同于一个超级用户角色，并完全访问所有操作。

通过定义粒度权限，您可以创建（或修改）具有有限权限（如只读）或读和更新的角色，但不能删除。

例如，比较成本管理员和成本分析器的预定义角色。

角色	Application（应用程序）	资源	操作
Cost Administrator	Cost-management	过程（全部）	过程（全部）
成本增强列表查看器	Cost-management	cost_model	读取

通过创建新角色，您可以定义特定于该角色的应用程序、资源和操作。

2.8.1. 添加自定义用户访问角色

User Access 提供了多个可添加到组中的预定义角色。除了使用预定义的角色外，您还可以为一个或多个应用程序创建和管理具有粒度权限的自定义用户访问角色。

有关红帽提供的预定义角色列表，请参阅 预定义的用户访问角色 部分。

注意

您无法修改预定义的角色。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
    1. 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。

流程

使用指导向导可帮助您完成添加角色的步骤。

以下步骤描述了如何使用 **Create role** 向导。

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Roles。此时会出现 **Roles** 窗口。
2. 点 **Create role** 按钮。这将启动 **Create role** 向导。

此时，您可以从头开始创建角色或复制现有角色。

2.8.2. 从头开始创建角色

当您想创建具有特定粒度权限的角色时，从头开始创建角色。例如，您可以为您的机构创建一个角色，为所有可用应用程序提供所有资源的只读权限。通过在默认访问组中添加和管理此角色，您可以将默认访问权限更改为只读。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 您已启动了 **Create role** 向导。

流程

1. 在 **Create role** 向导中，点 **Create a role from scratch**按钮。
2. 输入 **角色名称**，这是必需的。
3. （可选）输入 **角色描述**。
4. 点 **Next** 按钮。如果角色名称已存在，则必须在继续操作前提供不同的名称。

5. 使用 **Add permissions** 窗口选择要包含在角色中的应用程序权限。默认情况下，权限由应用程序列出。

6. （可选）使用 filter 下拉菜单根据 Applications、Resources 或 Operations 过滤。

   提示

   使用向导页面顶部的列表查看添加到角色的所有权限。您可以点击权限来删除它。

7. 点 **Next** 按钮查看详情。您可以点击 **Submit** 按钮来提交角色，**返回** 以返回并进行更改，或者取消该操作的 **Cancel** 按钮。

您创建的角色可用于添加到 User Access 组中。

2.8.3. 复制现有角色

当该角色已包含您要使用的许多权限且需要更改、添加或删除某些权限时，复制现有角色。

现有角色可以是红帽提供的预定义角色之一，也可以是之前创建的自定义角色。有关红帽提供的预定义角色列表，请参阅 预定义的用户访问角色 部分。

注意

您无法修改预定义的角色。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 您已启动了 **Create role** 向导。

流程

1. 在 **Create role** 向导中，点 **Copy an existing role** 按钮。
2. 点击您要复制的角色旁的按钮。
3. 点 **Next** 按钮。
4. **Name and description** 窗口显示 **Role name** 的副本，并填写了现有**角色描述**。根据需要进行更改。
5. 点 **Next** 按钮。如果角色名称已存在，则必须在继续操作前提供不同的名称。
6. 使用 **Add permissions** 窗口选择要包含在角色中的应用程序权限。默认情况下，权限由应用程序列出。

   提示

   自定义角色仅支持粒度权限。通配符权限，如 **approval:*:***，不会复制到一个自定义角色中。

7. （可选）使用 filter 下拉菜单根据 Applications、Resources 或 Operations 过滤。

提示

使用向导页面顶部的列表查看添加到角色的所有权限。您可以点击权限来删除它。

8. 点 **Next** 按钮查看详情。您可以点击 **Submit** 按钮来提交角色，**返回** 以返回并进行更改，或者取消该操作的 **Cancel** 按钮。

您创建的角色可用于添加到 User Access 组中。

2.8.4. 创建特定于应用程序的角色

使用 **Create role** 向导提供的过滤器为特定应用程序创建角色。当您为特定应用程序创建角色时，过滤器会为所选的应用程序显示允许的**资源**类**型**和**操作**。

您可以创建包含多个应用程序的应用程序特定角色。

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 您已启动了 **Create role** 向导。
- 您位于向导中的 **Add permissions** 步骤。

流程

1. 在 **Add permissions** 窗口中，点 **Filter by application** 字段。
2. 输入应用程序名称的第一个几个字母来选择应用程序。向导显示该应用的匹配权限。
3. （可选）使用导航工具滚动可用应用程序和权限列表。
4. 点击特定于应用程序的角色的权限旁边的复选框。
5. 点 **Next** 按钮查看详情。您可以点击 **Submit** 按钮来提交角色，**返回** 以返回并进行更改，或者取消该操作的 **Cancel** 按钮。

2.8.5. 创建成本管理应用程序角色

您可以创建一个特定于成本管理应用程序的角色。当您创建成本管理角色时，您可以为该角色定义成本管理资源定义。其他应用程序角色不提供该选择。

先决条件

- 已安装并配置成本管理 Operator。
- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 至少配置一个源以成本管理。
- 您已启动了 **Create role** 向导。

流程

这个步骤描述了如何从头开始创建带有成本管理权限的角色。

1. 在 Create role 窗口中，单击单选按钮 **从头创建角色**。
2. 输入 **角色名称** （必需）和角色 **描述** （可选）。
3. 点 Next 按钮显示 Add permissions 窗口。
4. 在 Filter by application 字段中输入 **cost**，以显示成本管理应用程序并点击 Cost -management 复选框。
5. 出现 Add permissions 窗口时，点角色中包含的每个成本管理权限的复选框。
6. 单击 Next 按钮，以显示 **定义成本管理资源** 窗口。
7. 您将看到添加到角色的每个应用程序权限的可用资源 **定义** 下拉列表。您必须点每个成本管理权限中至少有一个资源的复选框。
8. 点 Next 按钮查看详情。您可以点击 Submit 按钮来提交角色，**返回** 以返回并进行更改，或者取消该操作的 Cancel 按钮。

2.8.5.1. 从头开始创建角色的成本管理示例

先决条件

- 您必须是一个机构管理员。
- 如果您不是机构管理员，则必须是分配了 User Access administrator 角色的用户的成员。
- 至少配置一个源以成本管理。
- 您已启动了 Create role 向导。

流程

1. 启动 Create role 向导，再点 Create a role from scratch。
2. 输入 **AWS Org Unit Cost Viewer** 作为 **角色名称**，然后点 Submit 按钮。不需要描述。
3. 在 Filter by application 字段中输入 **cost**，以显示成本管理应用程序并点击 Cost -management 复选框。
4. 点包含 **aws.organizational_unit** 的行的复选框，然后点 Next 按钮显示权限可用资源 **定义** 的下拉列表。
5. 点 **资源定义** 列表中列出的至少一个资源的复选框，然后点 Next 按钮来查看详情。
6. 在检查了此角色的详细信息（显示**权限**和**资源定义**）后，点 Submit 按钮以提交角色。

2.8.6. 编辑自定义角色名称

您可以从主角色页面或从 Permissions 页面更改自定义角色的名称。

先决条件

- 一种具有机构管理员权限的用户，您已登陆到 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 一个或多个自定义角色必须存在。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Roles。此时会出现 **Roles** 窗口。在 **Roles** 窗口中，自定义角色具有其名称右侧的 ⋮ (**更多选项**)。
2. 点击 ⋮ (**更多选项**)。
3. 点 **Edit** 以更改角色名称或描述。
4. 点 **Delete** 以删除自定义角色。

   提示

   您还可以点角色名称打开 **Permissions** 窗口，然后点击角色名称右侧的 ⋮ (**更多选项**)来访问 Edit 和 Delete 操作。

5. 此时会出现确认窗口。确认无法撤销此操作后，会删除自定义角色。

2.8.7. 从自定义角色中删除权限

您可以从自定义角色中删除权限。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- 一个或多个自定义角色必须存在。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Roles。此时会出现 **Roles** 窗口。在 **Roles** 窗口中，自定义角色具有其名称右侧的 ⋮ (**更多选项**)。
2. 点自定义角色名称打开 **Permissions** 窗口。
3. 在 **Permissions** 列表中，点应用程序权限名称右侧的 ⋮ (**更多选项**)并点 **Remove**。
4. 此时会出现确认窗口。单击 **Remove permissions**。

2.8.8. 恢复默认访问组

您可以根据红帽提供的，将 **Default 访问** 组恢复到其状态。当您这样做时，**自定义默认访问组** 也会与该组所做的任何更改一起删除。

当恢复 **Default access** 组时，无法恢复 **Custom default access**组。

恢复默认访问组 的原因：

- 您对未预期的 **Default 访问** 组进行了更改。
- 您希望从 **Default access group** 开始。
- 您要删除 **Custom default access**组。
- 您需要获取红帽服务推送的 **Default 访问** 组的更改，并取消 **自定义默认访问组**。

注意

系统中的一个默认组(**默认访问组** **或自定义默认访问组**)始终存在。

先决条件

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 如果您不是机构管理员，则必须是分配了 **User Access administrator** 角色的用户的成员。
- **自定义默认访问** 组必须存在。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Groups。此时会显示 **Groups** 页面。
2. 在 **Groups** 页面中点 **Custom default access**。
3. 点 **Restore to default** 并接受小心的信息。
Default access appears on the **Groups** 页面中。

第 3 章 临时访问客户帐户的流程

当客户在 Red Hat Hybrid Cloud Console 上有疑问时，他们可以向红帽关联授予其帐户的临时访问权限，通常是红帽大客户经理(TAM)，或红帽客户体验与参与支持。客户授予帐户访问权限后，Red Hat 人员或支持工程师可以登录客户帐户并访问 Red Hat Hybrid Cloud Console 上的帐户信息，就像他们是客户帐户的成员一样。

有关红帽支持服务的更多信息，请参阅 Red Hat Service 产品。

当红帽大客户经理(TAM)或红帽客户体验与参与支持工程师访问客户帐户时，他们可以看到和认为哪些用户访问角色被分配给访问请求，并仅限于 红帽混合云控制台 上可用的客户帐户信息。

有关默认用户访问角色的更多信息，请参阅参考部分，请参阅 *预定义的用户访问角色*。

3.1. 使用访问请求功能提供对客户帐户的访问权限

直接访问客户帐户有助于在屏幕屏屏和远程查看会话不成功时解决问题。通过使用访问请求功能，红帽支持团队与同意访问级别和访问时间的客户进行合作。

在典型的情况下，客户向红帽支持团队创建一个支持问题单。红帽支持团队与客户合作，安排客户的帐户，并登录其 Red Hat Hybrid Cloud Console。

在开始任何访问请求操作前，请确定验证以下信息：

- 客户帐户号。
- 访问的持续时间，其中包括最长持续时间，最多 12 个月。
- 客户希望获得红帽支持团队的默认用户访问角色。

使用访问请求功能时，系统访问始终由客户控制。客户可以随时拒绝访问权限。

注意

任何访问请求操作都与红帽与发出请求的支持团队关联的唯一用户名相关联。这意味着，每个红帽访问请求都只对发出请求的关联可见，只有关联才能访问客户系统。如果其他红帽支持工程师带到支持问题单中，则需要一个新的访问请求操作。

3.1.1. 批准对您的帐户的访问

作为客户和机构管理员，您可以通过批准红帽访问请求来授予您的帐户的访问权限。当机构管理员登录并收到请求时，Red Hat Hybrid Cloud Console 上会出现一个访问请求通知弹出窗口。

您可以查看系统的所有帐户访问请求列表，以及 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Red Hat Access Requests。

注意

只有机构管理员才能批准或拒绝访问请求。User Access administrator 角色不提供批准或拒绝访问请求的权限。

先决条件

与红帽支持工程师合作，并提供以下信息，以便支持工程师能够为您的批准创建访问请求。

- 以具有机构管理员 权限的用户身份登录 Red Hat Hybrid Cloud Console 。
- 您的红帽客户帐户号。
- 系统访问的开始日期。
- 系统访问的结束日期。
- 了解访问请求将授予红帽支持工程师的用户访问角色。

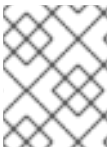
流程

1. 进入 Red Hat Hybrid Cloud Console > Settings menu (gear icon)> Identity & Access Management > User Access > Red Hat Access Requests。此时会显示所有访问请求的列表。
2. 推荐的方法是点 Request ID 号，它是一个十六进制数字的字符串。
3. 仔细检查请求详情和请求的角色。
4. 点 **Approve** 批准请求。已确认该操作，状态更改为 Approved。
5. 使用 edit 功能更改您的响应。

3.1.2. 拒绝访问您的帐户

作为客户和机构管理员，您可以通过拒绝红帽访问请求来拒绝访问您的帐户。

您可以通过 Red Hat Hybrid Cloud Console 中的 (**Settings**) 查看所有账户访问请求以及它们的状态的列表。



注意

只有机构管理员才能批准或拒绝访问请求。User Access administrator 角色不提供批准或拒绝访问请求的权限。

先决条件

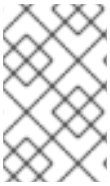
- 红帽支持工程师创建了访问请求。
- 访问请求会出现在 **Red Hat Account Requests**列表中。

流程

1. 进入 Red Hat Hybrid Cloud Console > Settings 菜单(gear 图标) > Identity & Access Management > User Access > Red Hat Access Requests 窗口。
   此时会显示所有访问请求的列表。
2. 推荐的方法是点 Request ID 号，它是一个十六进制数字的字符串。
3. 仔细检查请求详情和请求的角色。
4. 点 **Deny** 批准请求。已确认该操作，状态更改为 Denied。
5. 使用 edit 功能更改您的响应。

3.1.3. 请求客户帐户（红帽支持团队）

红帽支持团队的成员使用访问请求功能访问 Red Hat Hybrid Cloud Console 上的客户帐户。在收到访问请求后，客户可以批准或拒绝请求。



注意

访问请求功能仅适用于具有验证的红帽关联用户帐户的红帽人员。在未关联的情况下，访问请求功能不可见。这些信息可作为红帽大客户经理(TAM)或红帽客户体验与参与支持工程师的协助，并增强客户和红帽支持团队之间的要求通信。

先决条件

在开始任何访问请求操作前，请确保验证以下信息。

- 客户帐户号
- 客户机构 ID
- 访问的持续时间，其中包括最长持续时间，最多 12 个月
- 客户希望获得红帽支持团队的用户访问角色

流程

1. 使用以下方法之一获取客户机构 ID：
   - 询问客户提供它。
   - 在 Red Hat Subscription Admin 页面中，按客户帐户号进行搜索。

     注意

     您必须在 Red Hat VPN 上进行红帽关联，才能查看 Red Hat Subscription Admin 页面。
2. 登录到 Red Hat Hybrid Cloud Console 。
3. 点 Red Hat Hybrid Cloud Console 窗口右上角的用户 avatar。此时会出现下拉列表。
4. 在下拉列表中，单击 **Internal**。
5. 出现 **Internal** 窗口后，单击 **Access Requests**。
6. 点 **Create request**。向导指导您完成这些步骤。
7. 创建访问请求后，在客户批准或拒绝请求之前，您可以编辑请求或取消请求。

验证

您有权访问的帐户列表出现在 Red Hat Hybrid Cloud Console 帐户的 masthead 中的上下文切换器中。此列表包括您的个人帐户。

当您从上下文切换器选择另一个帐户时，会在 Red Hat Hybrid Cloud Console 窗口中出现横幅，例如："查看为帐户 654321"。

提示

Access Requests 窗口显示您提交的所有访问请求的状态。帐户请求链接到您的用户名，并对您是唯一的。没有其他红帽关联可以查看或对您创建的请求做出反应。

第 4 章 预定义的用户访问角色

下表列出了用户提供的预定义角色。一些预定义的角色包含在 **Default 访问** 组中，其中包括您机构中的所有经过身份验证的用户。

只有机构中的机构管理员用户才会继承 **Default admin 访问** 组中的角色。由于此组由红帽提供，因此当红帽为 **Default admin 访问权限** 组分配角色时，会自动更新它。

有关查看预定义角色的更多信息，请参阅 第 2 章 *配置用户访问的步骤*。

注意

预定义的角色由红帽更新和修改，不可修改。表可能不包含所有当前可用的预定义角色。

表 4.1. 为用户提供访问权限的预定义角色

角色名称	描述	默认访问组	默认管理员访问组
Approval Administrator（批准管理员）	批准管理员角色，授予管理工作流、请求、操作和模板的权限。		
Approval User（批准用户）	批准用户角色，授予创建/读取/取消请求的权限，并读取工作流。	X	
Approval Approver（批准批准员）	批准的批准者角色，具有授予读取和批准请求的权限。		
自动化分析管理员	授予所有权限的自动分析管理员角色。		
Automation Analytics Editor	一个 Automation Analytics Editor 角色，用于授予读写权限。	X	
自动化分析视图	一个 Automation Analytics Viewer 角色，用于授予读取权限。		
Automation Services Catalog 管理员	目录管理员角色授予创建、读取、更新、删除和订购权限		
Automation Services Catalog 用户	目录用户角色授予读和订购权限	X	
Compliance Administrator	一个 Compliance 角色，授予任何 Compliance 资源的完整访问权限。		X

角色名称	描述	默认访问组	默认管理员访问组
Compliance viewer	一个 Compliance 角色，授予任何 Compliance 资源的读取访问权限。	X	
RHC 管理员	在 RHC 管理器上执行任何操作		X
RHC viewer	可以查看 RHC 管理器上的当前配置	X	
仓库管理员	对任何软件仓库资源执行任何可用的操作。		X
软件仓库查看器	对存储库资源执行只读操作。	X	
Cost Administrator	授予读写权限的成本管理管理员角色。		X
成本管理列表管理员	对成本模型授予读写权限的成本管理角色。		
成本增强列表查看器	一个成本管理角色，用于授予成本模型的读取权限。		
成本云查看器	一个成本管理角色，用于授予与云源相关的成本报告的读取权限。		
成本 OpenShift Viewer	一个成本管理角色，用于授予与 OpenShift 源相关的成本报告的读取权限。		
偏移分析管理员	对任何 Drift Analysis 资源执行任何可用的操作。		X
偏移查看器	对 Drift Analysis 资源执行只读操作。	X	
RHEL Advisor 管理员	对任何 RHEL Advisor 资源执行任何可用的操作。	X	
清单管理员	对任何 Inventory 资源执行任何可用的操作。		

角色名称	描述	默认访问组	默认管理员访问组
清单主机管理员	能够读取并编辑清单主机数据。	X	X
清单主机查看器	能够读取清单主机数据。		
清单组管理员	能够读取并编辑清单组数据。		X
清单组查看器	能够读取清单组数据。		
恶意软件检测管理员	对任何 malware-detection 资源执行任何可用的操作。		X
malware 检测查看器	读取任何 malware-detection 资源。		
迁移分析管理员	对任何 Migration Analytics 资源执行任何可用的操作。	X	
通知管理员	对通知和集成应用程序执行任何可用的操作。		X
通知视图	只读访问通知和集成应用程序。		
OCM 集群编辑器	授予编辑集群的权限		
OCM Idp Editor	授予编辑 idps 的权限		
OCM 机器池编辑器	授予编辑机器池的权限		
OCM 集群置备器	授予置备集群的权限	X	
OCM 集群查看器	授予权限查看集群	X	
OCM 机构管理员	授予与机构的集群关联的管理权限		
OCP Advisor 管理员	对任何 OCP Advisor 资源执行任何可用的操作。	X	
补丁管理员	对任何 Patch 资源执行任何可用的操作。		X

角色名称	描述	默认访问组	默认管理员访问组
Patch viewer	阅读任何补丁资源。	X	
策略管理员	对任何策略资源执行任何可用的操作。		X
策略视图	对任何策略资源执行只读操作。	X	
用户访问管理员	授予非机构管理员完全访问权限，以配置和管理 console.redhat.com 上托管的服务的访问权限。此角色只能由机构管理员查看和分配。		
User Access principal viewer	授予非机构管理员对用户访问权限内的主体的读访问权限。		
补救管理员	对任何修复资源执行任何可用的操作		
补救用户	对任何 Remediations 资源执行 create, view, update, delete 操作。	X	
资源优化管理员	对任何资源优化资源执行任何可用的操作。		X
资源优化用户	赋予只读权限的资源优化用户角色。	X	
源管理员	对任何源执行任何可用的操作		X
订阅管理员	对任何订阅资源执行任何可用的操作。		X
订阅用户	查看任何订阅资源。	X	
任务管理员	对任何任务资源执行任何可用的操作。		X
漏洞管理员	对任何安全漏洞资源执行任何可用的操作。	X	

角色名称	描述	默认访问组	默认管理员访问组
安全漏洞查看器	阅读任何安全漏洞资源。		

对红帽文档提供反馈

我们感谢您对我们文档的反馈。要提供反馈，请突出显示文档中的文本并添加注释。

先决条件

- 已登陆到红帽客户门户网站。
- 在红帽客户门户网站中，文档采用 **Multi-page HTML** 查看格式。

流程

要提供反馈，请执行以下步骤：

1. 点击 **文档** 右上角的反馈按钮查看现有的反馈。

注意

反馈功能仅在多页 HTML 格式中启用。

2. 高亮标记您要提供反馈的文档中的部分。
3. 点在高亮文本旁弹出的 **Add Feedback**。
   文本框会出现在页面右侧的反馈部分中。
4. 在文本框中输入您的反馈，然后点 **Submit**。
   已创建一个文档问题。
5. 要查看问题，请点击反馈视图中的问题链接。