



Red Hat Hybrid Cloud Console 1-latest

基于角色的访问控制(RBAC)的用户访问配置指南

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

Red Hat Hybrid Cloud Console 1-latest 基于角色的访问控制(RBAC)的用户访问配置指南

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

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.

摘要

本指南适用于希望使用 User Access 功能为 Red Hat Hybrid Cloud Console 上托管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)的用户访问配置指南	3
1.1. 用户访问和软件即服务(SAAS)访问模型	3
1.2. 谁可以使用 USER ACCESS	3
1.3. 如何使用用户访问	3
第 2 章 配置用户访问的步骤	6
2.1. 创建用户访问管理员	6
2.2. 查看角色和权限	7
2.3. 查看用户权限	7
2.4. 使用角色和成员管理组访问权限	8
2.5. 限制对单个用户的服务访问	10
2.6. 在组中包含机构管理员	11
2.7. 禁用组访问	12
2.8. 用户访问的粒度权限	12
第 3 章 如何为红帽支持启用红帽帐户团队访问权限	19
3.1. 使用访问请求功能提供对客户帐户的访问	19
第 4 章 预定义的用户访问角色	23
对红帽文档提供反馈	28

第 1 章 基于角色的访问控制(RBAC)的用户访问配置指南

User Access 功能是基于角色的访问控制(RBAC)的一个实现，用于控制用户对 [Red Hat Hybrid Cloud Console](#) 上托管的各种服务的访问。您可以配置 User Access 功能，授予用户对在混合云控制台上托管的服务的访问权限。

1.1. 用户访问和软件即服务(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，但不是所有用户都需要对 [Red Hat Hybrid Cloud Console](#) 上提供的 SaaS 服务有相同的级别的访问权限。借助用户访问功能，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，机构中的所有用户可以查看信息，但只有机构管理员和集群所有者才能对集群执行操作。详情请参阅 [OpenShift Cluster Manager 文档中的在 OpenShift Cluster Manager 中配置集群的访问](#)。

1.2. 谁可以使用 USER ACCESS

要首先在 [Red Hat Hybrid Cloud Console](#) 上查看和管理用户访问权限，您必须是机构管理员。这是因为 User Access 需要从红帽客户门户网站指定的用户管理功能。<https://access.redhat.com> 这些功能仅属于机构管理员。

User Access 管理员角色 是一个特殊的角色，机构管理员可以为其分配它。此角色允许组织管理员用户在 [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按扩展方式分配给每个角色的组。您可以将用户分配给组。这意味着，组中的每个用户都被分配了该组中角色的权限。

通过创建不同的组并添加或删除该组的角色，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，用户可以执行该组允许的所有操作。

红帽为用户访问提供两个默认访问组：

- **默认 admin 访问组。** **Default admin access** 组仅限于您机构中机构管理员用户。您无法更改或修改 **Default admin access** 组中的角色。
- **默认访问组。** **Default access** 组包含您机构中的所有经过身份验证的用户。这些用户会自动继承所选预定义角色。



注意

您可以对 **Default access** 组进行更改。但是，当您这样做时，其名称会变为 **Custom default access** 组。

红帽提供了一组预定义角色。根据应用程序，每个支持的应用程序的预定义角色可能具有不同的权限，这些权限是为应用程序量身定制。

1.3.1. Default admin access 组

默认 **admin 访问 组** 由红帽在 [Red Hat Hybrid Cloud Console](#) 上提供。它包含一组角色，分配给系统上具有机构管理员角色的所有用户。此组中的角色在 [Red Hat Hybrid Cloud Console](#) 中进行了预定义。

Default admin access 组中的角色无法添加到或修改。由于此组是由红帽提供的，因此当红帽将角色分配给 **Default admin access** 组时，会自动更新它。

Default admin access 组的好处是它允许将角色自动分配给机构管理员。

如需 **Default admin access** 组中包含的角色，请参阅 [预定义的用户访问角色](#)。

1.3.2. Default access 组

默认访问组 由红帽在 [Red Hat Hybrid Cloud Console](#) 上提供。它包含一组在 [Red Hat Hybrid Cloud Console](#) 中预定义的角色。**Default access** 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 包含所有预定义角色的子集。如需更多信息，请参阅 **Default admin access group** 中包含的角色的预定义 [用户访问 角色](#) 部分。

作为机构管理员，您可以添加角色来并从 **Default 访问 组** 中删除角色。当这样做时，其名称会更改为 **Custom default access** 组。您对此组所做的更改会影响您机构中所有经过身份验证的用户。

1.3.3. Custom default access 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。

从那时起，机构管理员负责对 **自定义默认访问组的所有更新和更改**。该组不再由 [Red Hat Hybrid Cloud Console](#) 管理或更新。



重要

您不能删除 **Default access 组** 或 **Custom default access 组**。
您可以恢复 **Default 访问 组**，它会删除 **Custom default access 组** 以及您所做的任何更改。请参阅 [恢复 Default access 组](#)。

1.3.4. User Access groups、角色和权限

用户访问使用以下类别来确定机构管理员可以授予受支持的 [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，提供角色与用户的映射。机构管理员可以使用组为组分配一个或多个角色，并在组中包含一个或多个用户。您可以创建一个没有角色且没有用户的组。
- **角色**：一组提供给定服务访问权限的权限，如 Insights。对特定角色分配执行某些操作的权限。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中，将该组的所有成员授予该服务的读写权限。

- **权限**：可以请求的离散操作。权限分配给角色。

机构管理员向组中添加或删除角色和用户。组可以是机构管理员创建的新组，或者组可以是现有组。通过创建一个或多个特定角色的组，然后将用户添加到该组，您可以控制该组及其成员如何与 [Red Hat Hybrid Cloud Console](#) 服务进行交互。

当您将用户添加到组中时，它们会成为该组的成员。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. 可添加的访问

[Red Hat Hybrid Cloud Console](#) 上的用户访问使用额外的模型，这意味着没有 **拒绝** 角色。换句话说，只允许操作。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。允许访问任何单个用户的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

下图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**：角色可以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。

在其初始默认配置中，所有 User Access 帐户用户都会继承 **Default access** 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 User Access 管理员，您可以点  > Identity & Access Management 查看、配置和修改 User Access 组、角色和权限。

2.1. 创建用户访问管理员

User Access 管理员 是一个特殊的角色，机构管理员会分配给组。此组中的所有用户都可以执行 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 管理员角色 无法创建或修改 User Access 管理员组。只有机构管理员可以创建、修改或删除被分配了 User Access 管理员角色 的组。



注意

User Access 管理员角色 不授予查看和批准客户访问请求的权限。

通过拥有 User Access 管理员角色，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功能。User Access 管理员角色 不会继承 Default admin access 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到 [Red Hat Hybrid Cloud Console](#)。

流程

1. 进入 [Red Hat Hybrid Cloud Console > Settings > 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. 使用可识别的名称命名组：**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 管理员角色**，然后单击选择框，将此角色添加到组中。（可选）选择附加角色。
 - e. 单击 **Next** 按钮，将成员添加到组中。



注意

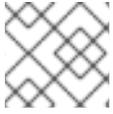
您添加的任何成员都必须是机构帐户的活跃成员。

- f. 在为组选择成员后，单击 **Next** 按钮来查看详情。
- g. 您可以单击 **Back** 按钮返回并进行更改，或者 **Cancel** 按钮取消该操作。

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](#) 中查看用户访问权限的角色和权限。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 管理员角色** 的组的成员。

流程

1. 进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#)。此时会显示用户访问角色。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 Price List Viewer** 角色，您会看到以下信息：

[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



注意

星号 * 表示通配符权限。通配符权限授予所有资源类型的访问权限，并允许角色中应用程序的所有操作。

2.3. 查看用户权限

您可以从用户详情页面查看用户的权限和其他与访问权限相关的信息。

先决条件

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。

流程

1. 进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users](#) 来查看机构中的用户列表。
2. 点 **Username** 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
 - 用户电子邮件地址
 - 混合云控制台（也称为 Red Hat 登录）上的用户的用户名。
 - 与用户关联的角色列表。查看每个角色的更多详情：
 - 单击 **Groups** 列中的计数，以显示分配了此角色的组。
 - 单击 **Permissions** 列中的计数，以显示角色提供的权限。



注意

如果您不是机构管理员，您可以通过进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > My User Access](#) 来查看您自己的不同服务的权限。

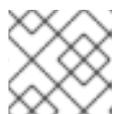
2.4. 使用角色和成员管理组访问权限

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

Members 选项卡显示您可以添加到组中的所有用户。当您用户添加到组中时，它们会成为该组的成员。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 管理员角色** 的组的成员。



注意

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

流程

1. 进入 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#) 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，请编辑组并添加其他角色。

2.4.1. 在组中添加角色

向现有组添加一个角色，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

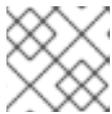
您可以从 **Users** 页面将角色添加到组，或者从 **Groups** 页面中编辑组。这些步骤演示了如何从用户详情页面编辑组。

先决条件

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。

流程

1. 进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users](#) 来打开 **Users** 列表。
2. 点 **用户名** 来打开用户详情页面。
3. 点角色的 **Groups** 列中的数量。这显示了用户所属的组，该角色已分配有此角色。



注意

您可以通过点 **Permissions** 列中的 count 来查看角色提供的权限。

4. 点组名称旁边的 **Add role to this group**，为组添加额外的角色。这将打开 **Add roles** 对话框。
5. 选中您要添加到组的每个角色的复选框。（仅列出尚未与组关联的角色。）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。

这个组现在在控制台中具有这些额外权限。

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时，这非常有用，您想要为其提供所有必要权限。



注意

您可以从 **Users** 页面将用户添加到组中，或者从 **Groups** 页面中编辑组。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

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。

流程

流程

1. 进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Users](#) 来打开 **Users** 列表。
2. 点您要编辑的用户的用户名。
3. 在用户详情页面中，单击 **Add user to a group**。此时会打开一个对话框，显示用户不是其成员的组列表。
4. 选中一个或多个要将用户添加到的组的复选框，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所授予的权限。

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。您添加的角色提供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，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用户访问权限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。

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。

当您添加用户到新组中时，用户会获取新组的权限，同时继承他们所属的所有其他组的权限。新组的权限被添加到其现有权限中。



重要

在此过程中，您将修改 **Default** 访问组。修改后，**默认访问** 组名称会更改为 **Custom default access**。现在，Red Hat 从 [Red Hat Hybrid Cloud Console](#) 中推送的更改，不再更新 **Custom default access** 组。

提示

您可以恢复 **Default** 访问组，它会删除 **Custom default access** 组以及您所做的任何更改。请参阅 [恢复 Default access 组](#)。

先决条件

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。

流程

1. 进入 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#)。此时会显示 **Groups** 页面。
2. 从 **Default access** 组删除所有角色。
因为您的机构中的所有用户都属于 **Default** 访问模式，所以您无法在 **Default access** 中添加或删除单个用户来创建访问控制。通过删除所有角色，用户不会从 **Default access** 继承角色权限。
 - a. 选中角色列表上方的复选框，以选择组中的所有角色。

- b. 单击更多选项图标(HBAC)> **Remove**。
 - c. 单击 **Remove roles** 进行确认。
3. 将更改保存到 **Default access** 组。对 **Custom default access** 的名称会改变。
4. 创建一个新组，其中包含允许访问权限的用户和角色。
例如，创建一个组 **Security Admin**，其中包含对漏洞服务具有完全访问权限的用户。
 - a. 创建组 **Security Admin**。
 - b. 从 **Members** 列表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 **Organization Administrator** 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，请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

此流程假设您要修改现有组，并将机构管理员添加到组中。另外，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 管理员角色** 的组的成员。
- 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权限](#)。
- 有关如何为行为组配置通知的详情，请参考[配置通知行为组](#)。

流程

1. 进入 **Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups**。此时将显示 **Groups** 页面。
2. 单击组 **Name** 以显示组的详细信息。
3. 在组详情页面上，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. 在出现的 **组** 页面中，找到 **Organization Administrator** 用户名，再单击名称旁边的复选框。
例如，如果 **Organization Administrator** 用户名是 **smith-jones**，找到该名称，然后单击 **smith-jones** 旁边的复选框。您可以添加额外的名称。

- 验证名称列表是否已完成，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权限。由于角色及其权限决定了被授予对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权限。

前提条件

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。

流程

- 进入 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#)。此时会显示 **Groups** 页面。
- 点要修改的 **Group Name**。
- 点 **Roles** 选项卡。
- 点您要删除的 **roles Name** 旁边的复选框。
您可以单击 **Name** 列顶部的复选框来选择所有角色。
- 点 **Add role** 标签页旁的更多选项菜单图标 ，然后点 **Remove from group**。
- 在出现的确认窗口中，单击 **Remove role** 或 **Cancel** 以完成该操作。



注意

组不能包含角色，也不能包含任何成员，仍然是有效的组。

2.8. 用户访问的粒度权限

细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。许多预定义角色都提供通配符权限，这等同于超级用户角色，具有对所有操作的完整访问权限。

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

例如，比较成本管理员和成本价格视图的预定义角色。

角色	Application（应用程序）	资源	操作
Cost Administrator	cost-management	*(all)	*(all)
成本价格列表查看器	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

用户访问提供了很多可以添加到组的预定义角色。除了使用预定义的角色外，您还可以创建和管理自定义用户访问角色，其具有一个或多个应用程序的粒度权限。

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

Default 访问 组包含所有预定义角色的子集。如需更多信息，请参阅 [预定义的用户访问角色](#)。



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 管理员角色** 的组的成员。

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. 进入到 [Red Hat Hybrid Cloud Console > Settings > 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

在您要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单个角色，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

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。
- 您启动了 **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，则必须提供不同的名称，然后才能继续。
5. 使用 **Add permissions** 窗口选择要包含在您的角色中的应用程序权限。默认情况下，应用程序列出权限。
6. （可选）使用过滤器下拉列表根据应用程序、资源或操作过滤。

提示

使用向导页面顶部的列表来查看添加到角色的所有权限。您可以点权限删除它。

7. 点 **Next** 按钮查看详情。您可以点击 **Submit** 按钮提交角色，**返回返回** 并进行更改，或者 **Cancel** 按钮取消该操作。

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并且需要更改、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

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。
- 您启动了 **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边的按钮。
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，则必须提供不同的名称，然后才能继续。
6. 使用 **Add permissions** 窗口选择要包含在您的角色中的应用程序权限。默认情况下，应用程序列出权限。

提示

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

7. (可选) 使用过滤器下拉列表根据应用程序、资源或操作过滤。

提示

使用向导页面顶部的列表来查看添加到角色的所有权限。您可以点权限删除它。

8. 点 **Next** 按钮查看详情。您可以点击 **Submit** 按钮提交角色，**返回返回** 并进行更改，或者 **Cancel** 按钮取消该操作。

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

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。
- 您启动了 **Create role** 向导。
- 您处于向导中的 **Add permissions** 步骤。

流程

1. 在 **Add permissions** 窗口中，点 **Filter by application** 字段。
2. 通过键入应用程序名称的前几个字母来选择应用程序。向导显示该应用程序的匹配权限。
3. (可选) 使用导航工具滚动可用应用程序和权限的列表。
4. 点特定应用程序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** 按钮提交角色，**返回返回** 并进行更改，或者 **Cancel** 按钮取消该操作。

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。其他应用角色不提供该选择。

先决条件

- 安装和配置成本管理 Operator。
- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。
- 至少配置一个云集成用于成本管理。

- 您启动了 **Create role** 向导。

流程

这个步骤描述了如何从头开始创建具有成本管理权限的角色。

1. 在 **Create role** 窗口中，单击 单选按钮 **从头开始创建角色**。
2. 输入 **Role name**（必需）和 **Role 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，然后点 **cost-management** 复选框。
5. 出现 **Add permissions** 窗口时，单击此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 **Define Cost Management resources**窗口。
7. 您将看到您添加到角色的每个应用程序权限的可用资源 **定义** 的下拉列表。您必须点击每个成本管理权限中至少一个资源的复选框。
8. 点 **Next** 按钮查看详情。您可以点击 **Submit** 按钮提交角色，**返回返回** 并进行更改，或者 **Cancel** 按钮取消该操作。

2.8.5.1. 从头开始创建角色的成本管理示例

先决条件

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 **User Access 管理员角色** 的组的成员。
- 至少配置一个云集成用于成本管理。
- 您启动了 **Create role** 向导。

流程

1. 启动 **Create role** 向导，再单击 **从头开始创建角色**。
2. 为 **角色名称**输入 **AWS 机构单元成本查看器**，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，然后点 **cost-management** 复选框。
4. 点包含 **aws.organizational_unit** 的行上的复选框，然后点 **Next** 按钮为权限 显示可用资源定义的下拉列表。
5. 单击 **资源定义** 列表中列出的至少一个资源的复选框，然后单击 **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 **Permissions** 页面更改自定义角色的名称。

先决条件

- * 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 User Access 管理员角色的组的成员。
- 必须存在一个或多个自定义角色。

流程

1. 进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#)。此时会出现 Roles 窗口。在 Roles 窗口中，自定义角色的名称右侧具有  (更多选项)。
2. 点  (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，然后点角色名称右侧的  (更多选项)访问 Edit 和 Delete 操作。

5. 此时会出现确认窗口。确认此操作无法撤消后，自定义角色将被删除。

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 管理员角色的组的成员。
- 必须存在一个或多个自定义角色。

流程

1. 进入到 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Roles](#)。此时会出现 Roles 窗口。在 Roles 窗口中，自定义角色的名称右侧具有  (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 Default 访问组

您可以将 Default 访问组恢复到红帽提供的状态。当这样做时，自定义默认访问组将删除，以及对该组所做的任何更改。

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

恢复 Default 访问组的原因：

- 您更改了没有预期的 Default 访问组。
- 您需要使用 Default access 组开始。
- 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 Custom 默认访问组。



注意

一个默认组(Default access 组或 Custom default access 组)始终存在于系统中。

先决条件

- 以具有机构管理员权限的用户身份登录到 [Red Hat Hybrid Cloud Console](#)。
- 如果您不是机构管理员，则必须是分配了 User Access 管理员角色的组的成员。
- Custom default access 组必须存在。

流程

1. 进入 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > User Access > Groups](#)。此时会显示 Groups 页面。
2. 在 Groups 页面上点 Custom default access。
3. 点 Restore to default，接受小心消息。Default access 会出现在 Groups 页面中。

第 3 章 如何为红帽支持启用红帽帐户团队访问权限

当客户对 [Red Hat Hybrid Cloud Console](#) 的帐户有疑问时，他们可以为该帐户授予红帽员工的临时访问权限，通常是红帽大客户经理(TAM)或红帽客户体验与参与支持工程师。客户授予帐户访问权限后，红帽 TAM 或支持工程师可以登录客户帐户，并像客户帐户的成员一样访问 [Red Hat Hybrid Cloud Console](#) 的帐户信息。

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请求对客户帐户的访问时，他们可以看到和执行哪些用户访问角色被分配给访问请求，并且仅限于 [Red Hat Hybrid Cloud Console](#) 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 [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

当屏幕截图和远程查看会话无法成功时，直接访问客户帐户可以帮助解决问题。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持续时间的客户合作。

在典型的情况下，客户会在红帽支持团队中创建一个支持问题单。红帽支持团队与客户合作来安排客户帐户的访问权限，并登录其 [红帽混合云控制台](#)。

确保在开始任何访问请求操作前验证以下信息：

- 客户帐户号。
- 访问持续时间，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发出请求的支持团队的唯一用户名相关联。这意味着，每个红帽访问请求仅对发出请求的红帽员工可见，并且只有该关联可以访问客户系统。如果将不同的红帽支持工程师引入到支持问题单中，则需要对该唯一红帽用户名进行新的访问请求操作。

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权限来授予对客户帐户的访问权限。当机构管理员登录并接受请求时，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 > Identity & Access Management > User Access > Red Hat Access Requests](#) 的状态。



注意

只有机构管理员才可以批准或拒绝访问请求。User Access 管理员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到 [Red Hat Hybrid Cloud Console](#)。
- 您的红帽客户帐号。
- 系统访问的开始日期。
- 系统访问的结束日期。
- 了解访问请求将向 Red Hat 支持工程师授予哪些用户访问角色。

流程

1. 进入 [Red Hat Hybrid Cloud Console > Settings > 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. 仔细检查请求详情以及请求的角色。
4. 点 Approve 批准请求。这个操作已被确认，状态更改为 Approved。
5. 使用 edit 功能更改您的响应。

3.1.2. 拒绝对您的帐户的访问

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对帐户的访问。

您可以从 [Red Hat Hybrid Cloud Console > Settings > Identity & Access Management > Red Hat Access Requests](#) 中查看所有帐户访问请求及其状态的列表。



注意

只有机构管理员才可以批准或拒绝访问请求。User Access 管理员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 > 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. 仔细检查请求详情以及请求的角色。
4. 点 Deny 批准请求。这个操作已被确认，状态更改为 Denied。
5. 使用 edit 功能更改您的响应。

3.1.3. 请求访问客户帐户（红帽支持团队）

红帽支持团队的成员使用访问请求功能来获取对客户帐户的访问权限。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已验证的红帽关联用户帐户的红帽员工。访问请求功能对非关联不可见。这些信息有助于红帽大客户经理(TAM)或红帽客户体验与参与支持工程师提供，并增强客户与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
- 访问持续时间，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权限角色

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，按客户帐户号搜索。



注意

您必须是红帽 VPN 上的红帽关联，才能查看 [Red Hat Subscription Admin](#) 页面。

2. 登录到 [Red Hat Hybrid Cloud 控制台](#)。
3. 点 [Red Hat Hybrid Cloud Console](#) 窗口右上角的用户 avatar。此时会出现一个下拉列表。
4. 在下拉列表中点 Internal。
5. 出现 Internal 窗口后，点 Access Requests。
6. 点 Create request。向导将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中选择另一个帐户时，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。帐户请求会链接到您的用户名，并与您的唯一。没有其他红帽员工可以查看或操作您创建的请求。

第 4 章 预定义的用户访问角色

下表列出了通过 User Access 提供的预定义角色。一些预定义角色包含在 Default access 组中，其中包含您机构中的所有经过身份验证的用户。

只有您所在机构的机构管理员用户会继承 Default admin access 组中的角色。由于此组是由红帽提供的，因此当红帽将角色分配给 Default admin access 组时，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

预定义角色由红帽更新和修改，且无法修改。表可能不包含所有当前可用的预定义角色。

表 4.1. 由用户访问提供的预定义角色

角色名称	描述	默认访问组	默认 admin 访问组
Ansible Wisdom Admin Dashboard 用户	一个 Ansible Wisdom Admin Dashboard 用户角色，为所有图表授予机构管理员读取权限。		X
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 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。		
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，以及读取工作流。	X	
自动化分析管理员	授予 ALL 权限的 Automation Analytics Administrator 角色。		
自动化分析编辑器	授予读写权限的 Automation Analytics Editor 角色。	X	
自动化分析视图	授予读取权限的 Automation Analytics Viewer 角色。		
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	

角色名称	描述	默认访问组	默认 admin 访问组
云管理员	对任何源执行任何可用操作。		X
合规管理员	授予对任何 Compliance 资源的完全访问权限的 Compliance 角色。		X
Compliance viewer	授予对任何 Compliance 资源的读取访问权限的 Compliance 角色。	X	
Cost Administrator	授予读和写权限的成本管理管理员角色。		X
成本云查看器	成本管理角色，授予与云源相关的成本报告读取权限。		
OpenShift Viewer 成本	成本管理角色，授予与 OpenShift 源相关的成本报告读取权限。		
成本价格列表管理员	为成本管理角色授予成本模型的读写权限。		
成本价格列表查看器	具有成本管理角色，以授予成本模型的读取权限。		
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	
Hybrid Committed Spend viewer	查看任何混合提交报告。		
清单组管理员	能够读取和编辑清单组数据。		X
清单组查看器	能够读取清单组数据。		
清单主机管理员	能够读取和编辑清单主机数据。	X	X
清单主机查看器	能够读取清单主机数据。		

角色名称	描述	默认访问组	默认 admin 访问组
清单管理员	对任何清单资源执行任何可用的操作。		
启动管理员	赋予读写权限的启动管理员角色。		X
启动查看器	在启动保留和相关资源时授予读取权限的 launch 角色。	X	
在 AWS 用户中启动	一个 AWS 启动角色，它授予启动保留和相关资源的写入权限。		
在 Azure User 上启动	Azure 启动角色，授予启动保留和相关资源的写入权限。		
在 Google Cloud User 上启动	Google Cloud 启动角色，授予启动保留和相关资源的写入权限。		
恶意软件检测管理员	对任何恶意软件检测资源执行任何可用操作。		X
malware 检测查看器	读取任何恶意软件检测资源。		
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
通知查看器	只读访问通知和集成应用程序。	X	
OCM Cluster Autoscaler Editor	授予编辑集群自动扩展的权限		
OCM 集群编辑器	授予编辑集群的权限		
OCM Cluster Provisioner	授予置备集群的权限	X	
OCM 集群查看器	授予查看集群的权限	X	
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		

角色名称	描述	默认访问组	默认 admin 访问组
OCM 机构管理员	授予关联的机构集群的管理权限		
OCP Advisor 管理员	对任何 OCP Advisor 资源执行任何可用的操作。	X	
Organization Staleness and Deletion Administrator	能够读取和编辑组织可扩展性和删除数据。		X
机构 Staleness 和 Deletion Viewer	能够读取组织 Staleness 和 Deletion 数据。	X	
补丁管理员	对任何 Patch 资源执行任何可用的操作。		X
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
policies viewer	对任何策略资源执行只读操作。	X	
RHC 管理员	在 RHC 管理器上执行任何操作		X
RHC 用户	可以查看 RHC 管理器上的当前配置，并写入激活码	X	
RHEL Advisor 管理员	对任何 RHEL Advisor 资源执行任何可用的操作。	X	
补救管理员	针对任何 Remediations 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	
仓库管理员	对任何仓库资源执行任何可用的操作。		X
仓库查看器	对存储库资源执行只读操作。	X	

角色名称	描述	默认访问组	默认 admin 访问组
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	
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
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 上托管的服务的用户访问权限。此角色只能由机构管理员查看和分配。		X
用户访问主体查看器	授予非机构管理员对用户访问权限内主体的读取访问权限。		
漏洞管理员	对任何漏洞资源执行任何可用的操作。	X	
漏洞查看器	读取任何漏洞资源。		

对红帽文档提供反馈

我们感谢您对我们文档的反馈。尽可能提供详细信息，以便可以解决您的请求。

先决条件

- 您有红帽帐户。
- 您已登录到您的红帽帐户。

流程

1. 要提供反馈，请点击以下链接：[Create Issue](#)
2. 在 Summary 文本框中描述问题或功能增强。
3. 在 Description 文本框中提供有关问题或功能增强的更多详细信息。
4. 如果您的红帽用户名没有自动显示在 Reporter 文本框中，请输入它。
5. 滚动到页面底部，然后单击 Create 按钮。创建文档问题并路由到适当的文档团队。

感谢您花时间来提供反馈。