Red Hat Customer Portal 1

创建和管理服务帐户

创建和管理服务帐户

Last Updated: 2024-06-22

Red Hat Customer Portal 1 创建和管理服务帐户

创建和管理服务帐户

法律通告

摘要

本指南说明了如何创建和管理用于访问资源的服务帐户。

目录

前言

服务帐户授予系统服务对特定资源的访问权限。虽然用户可以创建服务帐户，但只有机构管理员或具有 User Access Admin 角色的用户才能将服务帐户分配给用户组。服务帐户将具有授予用户组的权限。

使开源包含更多

红帽承诺替换我们的代码、文档和网页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 的信息。

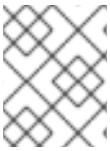
第 1 章 服务帐户

帐户可以是用户帐户或服务帐户。用户帐户在您的机构中对人用户进行身份验证。服务帐户在无需人工干预的情况下对应用程序或服务进行身份验证。您可以在 Red Hat Hybrid Cloud Console 上创建服务帐户，理由如下：

- 应用程序或服务需要访问特定资源。
- 应用程序或服务需要访问资源，而无需人为干预。
- 应用程序或服务需要从多个位置访问资源。

您必须使用服务帐户连接到 Red Hat Hybrid Cloud Console 上的云服务 API。红帽对基本身份验证的支持于 2024 年 12 月 31 日结束，并且仅在该日期之后允许基于令牌的身份验证。服务帐户支持基于令牌的身份验证。

有关服务帐户实施的更多信息，请参阅通过 服务帐户将 Red Hat Hybrid Cloud Console API 从基本身份验证转换到基于令牌的身份验证。



注意

API 需要来自 Red Hat Single Sign-On 的访问令牌。令牌在 15 分钟后过期(900 秒)。重复一次 10 分钟(600 秒)获取访问令牌的过程，以便在过期前轮转令牌。RFC 6749, 4.1.4 节

其他资源

- 更新您的 API 集成
- 通过服务帐户将 Red Hat Hybrid Cloud Console API 从基本身份验证转换到基于令牌的身份验证

第 2 章 创建和管理服务帐户

使用服务帐户安全并自动连接和验证服务或应用程序，而无需最终用户的凭证或直接交互。

在创建红帽服务帐户时，您可以生成 **客户端 ID** 和 **secret**。服务帐户使用 ID 和 secret 来访问 Red Hat Hybrid Cloud Console 上的服务。

- **客户端 ID** 标识资源的服务帐户，就像用户名标识用户一样。
- **Secret** secret 提供与密码类似的功能。创建服务帐户后，secret 会出现一次。复制并保存该机密，并进行保护。

创建服务帐户后，您可以将其添加到适用的 User Access 组中。（用户访问是红帽实施基于角色的访问控制。）分配给 User Access 组的角色决定了服务帐户对 Red Hat Hybrid Cloud Console 上的应用程序和服务的访问级别。

以下任务演示了如何创建服务帐户并将其添加到 User Access 组中：

- 第 2.1 节 “创建一个服务帐户”
- 第 2.2 节 “将服务帐户添加到用户访问组中”
- 第 2.3 节 “从 User Access 组删除服务帐户”

您可以在为服务帐户生成客户端 ID 和 secret 后执行以下任务：

- 第 2.4 节 “重置服务帐户 secret”
- 第 2.5 节 “删除一个服务帐户”

只有服务账户的所有者才能重置或删除服务帐户。机构管理员可以重置或删除任何服务帐户。

其他资源

- 基于角色的访问控制(RBAC)的用户访问配置指南

2.1. 创建一个服务帐户

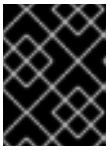
您可以创建一个服务帐户，并生成客户 ID 和 secret，以用于该帐户。

先决条件

- 您已登录到 Red Hat Hybrid Cloud Console。

流程

1. 在 Red Hat Hybrid Cloud Console 中，点设置图标(iwl)，然后点 **Service Accounts**。
2. 点 **Create service account** 设置帐户。
3. 输入 Service account name 和 Short description，再点 **Create**。
4. 将生成的 **Client ID** 和 **Client secret** 值保持到一个安全的位置。在配置与服务的连接时，您将使用这些凭证。



重要

Client secret 仅显示一次，因此请确保在关闭凭证窗口前成功并安全地保存复制的凭证。

5. 将客户端 ID 和 secret 保存到安全位置后，在凭证窗口中选择确认复选框并关闭该窗口。
6. 服务帐户及其客户端 ID 会出现在 **Service Accounts** 页面中。

2.2. 将服务帐户添加到用户访问组中

机构管理员将服务帐户添加到具有访问权限的用户访问组中，允许服务帐户访问 Red Hat Hybrid Cloud Console 上的服务和应用程序。任何用户都可以创建服务帐户，但只有机构管理员或 User Access 管理员可以将服务帐户添加到组中。

先决条件

- 以机构管理员或具有 User Access 管理员权限的用户身份登录到 Red Hat Hybrid Cloud Console。
- 一个或多个服务帐户与您的红帽机构帐户关联。第 2.1 节 “创建一个服务帐户”

流程

1. 在 Red Hat Hybrid Cloud Console 中，点设置图标(iwl)，然后点 **User Access**。
2. 要将服务帐户添加到预先存在的组中，请点 **Groups** 选项卡，然后点击您要将服务帐户添加到的组名称。
3. 当显示组名称窗口时，点 **Service accounts** 选项卡。
4. 单击 **Add service account**。列出与您的红帽机构帐户关联的所有服务帐户。
5. 单击您要添加到 User Access 组的服务帐户，然后单击 **Add to group**。
6. 服务帐户显示在 **Service accounts** 选项卡上。

其他资源

- 基于角色的访问控制(RBAC)的用户访问配置指南
- 第 2.3 节 “从 User Access 组删除服务帐户”

2.3. 从 USER ACCESS 组删除服务帐户

机构管理员可从 Red Hat Hybrid Cloud Console 上的 User Access 组删除服务帐户。任何用户都可以创建服务帐户，但只有机构管理员或 User Access 管理员可以从组中删除服务帐户。

先决条件

- 以机构管理员或具有 User Access 管理员权限的用户身份登录到 Red Hat Hybrid Cloud Console。
- 一个或多个服务帐户与您的红帽机构帐户关联。第 2.1 节 “创建一个服务帐户”

流程

1. 在 Red Hat Hybrid Cloud Console 中，点设置图标(iwl)，然后点 **User Access**。
2. 要从组中删除服务帐户，点 **Groups** 选项卡，再点包含服务帐户的组的名称。
3. 当显示组名称窗口时，点 **Service accounts** 选项卡。此时会出现该组中的所有服务帐户。
4. 删除单个服务帐户。
   a. 点 Name 行中的选项图标(HBAC)，然后点 **Remove**。
   b. 确认 **Remove service account?** 消息，然后单击 **Remove service account**。
5. 删除多个服务帐户。
   a. 单击要删除的每个帐户旁边的复选框。
   b. 点所选服务帐户的任何 Name 行中的选项图标(HBAC)，然后点 **Remove**。
   c. 确认 **Remove service account?** 消息，然后单击 **Remove service account**。
6. 验证所选服务帐户没有出现在 **Service accounts** 选项卡中。

其他资源

- 第 2.2 节 “将服务帐户添加到用户访问组中”

2.4. 重置服务帐户 SECRET

您可以为服务帐户重置 secret。当这样做时，客户 ID 不会改变。只有服务账户的所有者才能重置或删除服务帐户。Organization Administrator 用户可以重置或删除任何服务帐户。

先决条件

- 您已登录到 Red Hat Hybrid Cloud Console 。

流程

1. 在 Red Hat Hybrid Cloud Console 中，点设置图标(iwl)，然后点 **Service Accounts**。
2. 在现有服务帐户列表中，选择您要重置的服务帐户，然后点击选项图标(RCU)。
3. 验证您是否要重置此帐户，然后单击 **重置凭据**。
4. 将更新的 **Client secret** 值复制到一个安全的位置。在配置与服务的连接时，您将使用这些凭证。

重要

生成的凭证仅显示一次，因此在关闭凭证窗口前请确定已成功并安全地保存了凭证。

5. 将生成的凭证保存到安全位置后，在凭证窗口中选择确认复选框并关闭该窗口。

2.5. 删除一个服务帐户

您可以删除一个服务帐户。只有服务账户的所有者才能重置或删除服务帐户。Organization Administrator 用户可以重置或删除任何服务帐户。

先决条件

- 您已登录到 Red Hat Hybrid Cloud Console 。

流程

1. 在 Red Hat Hybrid Cloud Console 中，点设置图标(iwl)，然后点 **Service Accounts**。
2. 找到您要删除的服务帐户，然后点选项图标 (⋮)。
3. 验证您是否要删除此帐户，然后单击 **Delete service account**。

第 3 章 将服务帐户与服务搭配使用

以下信息简要描述了如何将服务帐户与服务和 CLIENT_ID 和 CLIENT_SECRET 变量一起使用。它仅作为参考指南行提供。

1. 创建新服务帐户： Red Hat Hybrid Cloud Console 服务帐户
2. 在终端中粘贴以下信息，替换 CLIENT_ID 和 CLIENT_SECRET 变量：

```
export HOST='https://sso.redhat.com' CLIENT_ID='<client_id>'
CLIENT_SECRET='<client_secret>' SCOPES='openid api.iam.service_accounts'
```

3. 获取服务帐户的令牌

```
curl "${HOST}/auth/realms/redhat-external/protocol/openid-connect/token" \
        --data-urlencode "grant_type=client_credentials" \
        --data-urlencode "client_id=${CLIENT_ID}" \
        --data-urlencode "client_secret=${CLIENT_SECRET}" \
        --data-urlencode "scope=${SCOPES}"
```

如果您安装了 **jq** （命令行 JSON 处理器），您可以将令牌保存到 env var 中：

```
export ACCESS_TOKEN=$( \
    curl "${HOST}/auth/realms/redhat-external/protocol/openid-connect/token" \
        --data-urlencode "grant_type=client_credentials" \
        --data-urlencode "client_id=${CLIENT_ID}" \
        --data-urlencode "client_secret=${CLIENT_SECRET}" \
        --data-urlencode "scope=${SCOPES}" \
    | jq -r '.access_token')
```

4. 将请求发送到支持服务帐户的应用程序：

```
curl --header "Authorization:Bearer ${ACCESS_TOKEN}" --location
"https://console.redhat.com/api/rbac/v1/access/?application=inventory"
```

5. 响应应为空，或者根据应用没有特权。尝试将服务帐户添加到 RBAC 组，并将角色添加到该组。用户访问组
6. 将角色添加到服务帐户组后，重复步骤 3 以获取新的令牌，然后再次尝试请求。现在，您应该具有更多权限，并从应用程序获得正确的响应。