Red Hat Customer Portal 1

Creating and Managing Service Accounts

Create and manage service accounts

Last Updated: 2024-06-21

Red Hat Customer Portal 1 Creating and Managing Service Accounts

Create and manage service accounts

Legal Notice

Abstract

This guide explains how to create and manage service accounts for accessing resources.

Table of Contents

PREFACE

A service account grants a system service access to specific resources. While users can create service accounts, only an Organization Administrator or a user with the User Access Admin role can assign service accounts to user groups. The service account will have the permissions that are granted to the user group.

Making open source more inclusive

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message .

CHAPTER 1. SERVICE ACCOUNTS

An account can be either a user account or a service account. A user account authenticates human users in your organization. A service account authenticates applications or services without human intervention. You create service accounts on Red Hat Hybrid Cloud Console for the following reasons:

- An application or service needs access to specific resources.
- The application or service needs to access resources without the need for human intervention.
- The application or service needs to access resources from multiple locations.

You must use service accounts to connect to cloud service APIs on Red Hat Hybrid Cloud Console. Red Hat support for basic authentication ends on December 31, 2024 and will only permit token-based authentication after that date. Service accounts support token-based authentication.

For more information about service account implementation, see Transition of Red Hat Hybrid Cloud Console APIs from basic authentication to token-based authentication via service accounts.

NOTE

APIs require an access grant token from Red Hat Single Sign-On. The token expires after 15 minutes (900 seconds). Repeat the process of obtaining an access token every 10 minutes (600 seconds) so that the token is rotated prior to expiration. RFC 6749, Section 4.1.4

Additional resources

- Update Your API Integration
- Transition of Red Hat Hybrid Cloud Console APIs from basic authentication to token-based authentication via service accounts

CHAPTER 2. CREATING AND MANAGING A SERVICE ACCOUNT

Use service accounts to securely and automatically connect and authenticate services or applications without requiring an end user's credentials or direct interaction.

When you create a Red Hat service account, you generate a **client ID** and a **secret**. The service account uses the ID and secret to access services on the Red Hat Hybrid Cloud Console.

- **Client ID** The client ID identifies the service account to the resource, much like a username identifies a user.
- **Secret** The secret provides a similar function as does a password. The secret appears once when you create the service account. Copy and save the secret and protect it as you would any password.

After you create a service account, you add it to the applicable User Access group. (User Access is the Red Hat implementation of role-based access control.) The roles assigned to a User Access group determine the level of access the service account has to applications and services on the Red Hat Hybrid Cloud Console.

The following tasks show you how to create service accounts and add them to a User Access group:

- Section 2.1, "Creating a service account"
- Section 2.2, "Adding service accounts to a User Access group"
- Section 2.3, "Deleting service accounts from a User Access group"

You can perform the following tasks after you generate a client ID and a secret for a service account:

- Section 2.4, "Resetting a service account secret"
- Section 2.5, "Deleting a service account"

You must be the owner of a service account if you want to reset it or delete it. The Organization Administrator can reset or delete any service account.

Additional resources

- User Access Configuration Guide for Role-based Access Control (RBAC)

2.1. CREATING A SERVICE ACCOUNT

You can create a service account and generate the client ID and secret to use with that account.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

Procedure

1. From the Red Hat Hybrid Cloud Console, Click the settings icon (⚙) and click **Service Accounts**.

2. Click **Create service account** to set up the account.
3. Enter a Service account name and a Short description and click **Create**.
4. Copy the generated **Client ID** and **Client secret** values to a secure location. You'll specify these credentials when configuring a connection to a service.

IMPORTANT

The **Client secret** is displayed only once, so ensure that you've successfully and securely saved the copied credentials before closing the credentials window.

5. After you save the Client ID and secret to a secure location, select the confirmation check box in the credentials window and close the window.
6. The service account and its Client ID appear on the **Service Accounts** page.

2.2. ADDING SERVICE ACCOUNTS TO A USER ACCESS GROUP

The Organization Administrator adds a service account to a User Access group that has the permissions that allow a service account to access services and applications on the Red Hat Hybrid Cloud Console. Any user can create a service account but only the Organization Administrator or a User Access administrator can add service accounts to groups.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as the Organization Administrator or as a user with User Access administrator permissions.
- One or more service accounts are associated with your Red Hat organization account. Section 2.1, "Creating a service account"

Procedure

1. From the Red Hat Hybrid Cloud Console, click the settings icon (⚙) and click **User Access**.
2. To add the service account to a preexisting group, click the **Groups** tab and click the name of the group that you want to add the service account to.
3. When the group name window appears, click the **Service accounts** tab.
4. Click **Add service account**. A list appears of all service accounts associated with your Red Hat organization account.
5. Click the service accounts you want to add to the User Access group and click **Add to group**.
6. The service accounts appear on the **Service accounts** tab.

Additional resources

- User Access Configuration Guide for Role-based Access Control (RBAC)
- Section 2.3, "Deleting service accounts from a User Access group"

2.3. DELETING SERVICE ACCOUNTS FROM A USER ACCESS GROUP

The Organization Administrator can delete a service account from a User Access group on the Red Hat Hybrid Cloud Console. Any user can create a service account but only the Organization Administrator or a User Access administrator can delete service accounts from groups.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console as the Organization Administrator or as a user with User Access administrator permissions.
- One or more service accounts are associated with your Red Hat organization account. Section 2.1, “Creating a service account”

Procedure

1. From the Red Hat Hybrid Cloud Console, click the settings icon (⚙) and click **User Access**.
2. To delete the service account from a group, click the **Groups** tab and click the name of the group that includes the service account.
3. When the group name window appears, click the **Service accounts** tab. All service accounts in that group appear.
4. Remove a single service account.
    a. Click the options icon (⋮) in the Name row and click **Remove**.
    b. Acknowledge the **Remove service account?** message and click **Remove service account**
5. Remove multiple service accounts.
    a. Click the check box next to each account to remove.
    b. Click the options icon (⋮) in any Name row of the selected service accounts and click **Remove**.
    c. Acknowledge the **Remove service account?** message and click **Remove service account**
6. Verify that the selected service account does not appear on the **Service accounts** tab.

Additional resources

- Section 2.2, “Adding service accounts to a User Access group”

2.4. RESETTING A SERVICE ACCOUNT SECRET

You can reset the secret for a service account. When you do so, the client ID does not change. You must be the owner of a service account if you want to reset it or delete it. The Organization Administrator user can reset or delete any service account.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

Procedure

1. From the Red Hat Hybrid Cloud Console, Click the settings icon (⚙) and click **Service Accounts**.
2. On the list of existing service accounts, select the service account you want to reset and click the options icon (⋮).
3. Verify that you want to reset this account and click **Reset credentials**.
4. Copy the updated **Client secret** values to a secure location. You'll specify these credentials when configuring a connection to a service.

IMPORTANT

The generated credentials are displayed only once, so ensure that you've successfully and securely saved the copied credentials before closing the credentials window.

5. After you save the generated credentials to a secure location, select the confirmation check box in the credentials window and close the window.

2.5. DELETING A SERVICE ACCOUNT

You can delete a service account. You must be the owner of a service account if you want to reset it or delete it. The Organization Administrator user can reset or delete any service account.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

Procedure

1. From the Red Hat Hybrid Cloud Console, Click the settings icon (⚙) and click **Service Accounts**.
2. Identify the service account you want to delete and click the options icon (⋮).
3. Verify that you want to delete this account and click **Delete service account**

CHAPTER 3. USING SERVICE ACCOUNTS WITH SERVICES

The following information briefly describes how to use service accounts with services and the CLIENT_ID and CLIENT_SECRET variables. It is provided as a reference guideline only.

1. Create a new Service account: Red Hat Hybrid Cloud Console Service accounts

2. Paste the following information on a terminal, replacing the CLIENT_ID and CLIENT_SECRET variables:

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

3. Get a token for the service account with

```
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}"
```

   If you have **jq** installed (a command-line JSON processor), you can save the token to an env var:

```
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. Send a request to an application that supports service accounts:

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

5. The response should be empty, or unprivileged depending on the app. Try adding the service account to an RBAC group, and adding roles to that group. User Access Groups

6. After roles are added to the service account group, repeat step 3 to grab a fresh token and attempt the request again. You should now have more privileges and get proper responses from applications.