Red Hat Customer Portal 1

サービスアカウントの作成と管理

サービスアカウントの作成および管理

Last Updated: 2024-06-22

Red Hat Customer Portal 1 サービスアカウントの作成と管理

サービスアカウントの作成および管理

法律上の通知

概要

このガイドでは、リソースにアクセスするためのサービスアカウントを作成および管理する方法を説明します。

目次

はじめに

サービスアカウントにより、システムサービスに特定のリソースにアクセスできるようになります。ユーザーはサービスアカウントを作成できますが、Organization Administrator ロールまたは User Access Admin ロールを持つユーザーのみが、サービスアカウントをユーザーグループに割り当てることができます。サービスアカウントには、ユーザーグループに付与されるアクセス許可が付与されます。

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。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

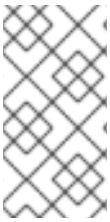
第1章 サービスアカウント

アカウントはユーザーアカウントまたはサービスアカウントのどちらかです。ユーザーアカウントで、組織内のユーザー (人) を認証します。サービスアカウントは、人間の介入なしにアプリケーションやサービスを認証します。以下の目的で、Red Hat Hybrid Cloud Console でサービスアカウントを作成します。

- アプリケーションまたはサービスは特定のリソースへのアクセスを必要である。
- アプリケーションまたはサービスは、人の介入を必要とせずにリソースにアクセスする必要がある。
- アプリケーションまたはサービスは、複数の場所からリソースにアクセスする必要がある。

Red Hat Hybrid Cloud Console のクラウドサービス API に接続するには、サービスアカウントを使用する必要があります。Red Hat の Basic 認証のサポートは 2024 年 12 月 31 日に終了予定で、その日以降はトークンベースの認証のみが許可されます。サービスアカウントは、トークンベースの認証をサポートします。

サービスアカウントの実装の詳細は、サービスアカウントを介した Basic 認証からトークンベース認証への Red Hat Hybrid Cloud ConsoleAPI の移行 を参照してください。



注記

API には、Red Hat Single Sign-On からのアクセストークンが必要です。トークンは 15 分 (900 秒) 後に期限切れになります。アクセストークンを取得するプロセスを 10 分 (600 秒) ごとに繰り返し、有効期限が切れる前にトークンがローテーションされるようにします。(RFC 6749, Section 4.1.4)

関連情報

- API インテグレーションの更新
- Red Hat Hybrid Cloud Console API の Basic 認証からサービスアカウントによるトークンベース認証への移行

第2章 サービスアカウントの作成および管理

サービスアカウントを使用すると、エンドユーザーの認証情報や直接の操作を必要とせずに、サービスやアプリケーションに安全かつ自動的に接続して認証できます。

Red Hat サービスアカウントを作成すると、**クライアント ID** と **シークレット** が生成されます。サービスアカウントは ID とシークレットを使用して Red Hat Hybrid Cloud Console のサービスにアクセスします。

- **クライアント ID** クライアント ID は、ユーザー名がユーザーを識別するのと同じように、リソースに対してサービスアカウントを識別します。
- **シークレット** シークレットは、パスワードと同様の機能を提供します。シークレットは、サービスアカウントを作成するときに一度表示されます。シークレットをコピーして保存し、パスワードと同じように保護します。

サービスアカウントを作成した後、該当するユーザーアクセスグループに追加します。(ユーザーアクセスは、ロールベースのアクセス制御の Red Hat 実装です。)ユーザーアクセスグループに割り当てられたロールによって、サービスアカウントが Red Hat Hybrid Cloud Console 上のアプリケーションおよびサービスに対して割り当てられるアクセスのレベルが決まります。

以下のタスクは、サービスアカウントを作成して User Access グループに追加する方法を示しています。

- 「サービスアカウントの作成」
- 「サービスアカウントのユーザーアクセスグループへの追加」
- 「ユーザーアクセスグループからのサービスアカウントの削除」

サービスアカウントのクライアント ID とシークレットを生成した後、次のタスクを実行できます。

- 「サービスアカウントシークレットのリセット」
- 「サービスアカウントの削除」

サービスアカウントをリセットまたは削除するには、サービスアカウントの所有者である必要があります。組織管理者は、任意のサービスアカウントをリセットまたは削除できます。

関連情報

- 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

2.1. サービスアカウントの作成

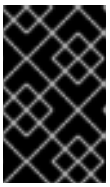
サービスアカウントを作成し、そのアカウントで使用するクライアント ID とシークレットを生成できます。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console から、設定アイコン(⚙)をクリックし、**Service Accounts** をクリックします。
2. **Create service account** をクリックしてアカウントを設定します。
3. Service account name および Short description を入力し、**Create** をクリックします。
4. 生成された **Client ID** と **Client secret** の値を安全な場所にコピーします。サービスへの接続を設定するときに、これらの認証情報を指定します。



重要

クライアントシークレット は 1 回しか表示されないため、認証情報ウィンドウを閉じる前に、コピーした認証情報が正常かつ安全に保存されたことを確認してください。

5. クライアント ID とシークレットを安全な場所に保存したら、認証情報ウィンドウで確認チェックボックスを選択し、ウィンドウを閉じます。
6. サービスアカウントとそのクライアント ID が **Service Accounts** ページに表示されます。

2.2. サービスアカウントのユーザーアクセスグループへの追加

組織管理者は、Red Hat Hybrid Cloud Console 上のサービスおよびアプリケーションにアクセスできる権限を持つユーザーアクセスグループにサービスアカウントを追加します。サービスアカウントは誰でも作成できますが、組織管理者またはユーザーアクセス管理者のみがサービスアカウントをグループに追加できます。

前提条件

- 組織管理者またはユーザーアクセス管理者権限を持つユーザーとして Red Hat Hybrid Cloud Console にログインしている。
- 1 つ以上のサービスアカウントが Red Hat 組織アカウントに関連付けられている。「サービスアカウントの作成」 を参照してください。

手順

1. Red Hat Hybrid Cloud Console から、設定アイコン (⚙) をクリックし、**ユーザーアクセス** をクリックします。
2. サービスアカウントを既存のグループに追加するには、**Groups** タブをクリックし、サービスアカウントを追加するグループの名前をクリックします。
3. グループ名ウィンドウが表示されたら、**Service accounts** タブをクリックします。
4. **Add service account** をクリックします。Red Hat の組織アカウントに関連付けられているすべてのサービスアカウントのリストが表示されます。
5. ユーザーアクセスグループに追加するサービスアカウントをクリックし、**Add to group** をクリックします。
6. サービスアカウントが **Service accounts** タブに表示されます。

関連情報

- 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
- 「ユーザーアクセスグループからのサービスアカウントの削除」

2.3. ユーザーアクセスグループからのサービスアカウントの削除

組織管理者は Red Hat Hybrid Cloud Console のユーザーアクセスグループからサービスアカウントを削除できます。すべてのユーザーがサービスアカウントを作成できますが、グループからサービスアカウントを削除できるのは組織管理者またはユーザーアクセス管理者だけです。

前提条件

- 組織管理者またはユーザーアクセス管理者権限を持つユーザーとして Red Hat Hybrid Cloud Console にログインしている。
- 1 つ以上のサービスアカウントが Red Hat 組織アカウントに関連付けられている。「サービスアカウントの作成」 を参照してください。

手順

1. Red Hat Hybrid Cloud Console から、設定アイコン (⚙) をクリックし、 **ユーザーアクセス** をクリックします。
2. グループからサービスアカウントを削除するには、**Groups** タブをクリックして、サービスアカウントが含まれるグループの名前をクリックします。
3. グループ名ウィンドウが表示されたら、**Service accounts** タブをクリックします。そのグループ内のすべてのサービスアカウントが表示されます。
4. 単一のサービスアカウントを削除します。
    a. Name 行のオプションアイコン (⋮) をクリックし、**Remove** をクリックします。
    b. **Remove service account?** メッセージを確認し、**Remove service account** をクリックします。
5. 複数のサービスアカウントを削除します。
    a. 削除する各アカウントの横にあるチェックボックスをクリックします。
    b. 選択したサービスアカウントのいずれかの Name 行にあるオプションアイコン (⋮) をクリックし、**Remove** をクリックします。
    c. **Remove service account?** メッセージを確認し、**Remove service account** をクリックします。
6. 選択したサービスアカウントが **Service accounts** タブに表示されないことを確認します。

関連情報

- 「サービスアカウントのユーザーアクセスグループへの追加」

2.4. サービスアカウントシークレットのリセット

サービスアカウントのシークレットをリセットできます。シークレットをリセットしても、クライアン

ト ID は変更されません。サービスアカウントをリセットまたは削除するには、サービスアカウントの所有者である必要があります。組織管理者ユーザーは、任意のサービスアカウントをリセットまたは削除できます。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console から、設定アイコン(⚙)をクリックし、**Service Accounts** をクリックします。
2. 既存のサービスアカウントのリストで、リセットするサービスアカウントを選択し、オプションアイコン (⋮) をクリックします。
3. このアカウントをリセットすることを確認し、**Reset credentials** をクリックします。
4. 更新された **Client secret** の値を安全な場所にコピーします。サービスへの接続を設定するときに、これらの認証情報を指定します。

重要

生成された認証情報は 1 回しか表示されないため、認証情報ウィンドウを閉じる前に、コピーした認証情報が正常かつ安全に保存されたことを確認してください。

5. 生成されたクレデンシャルを安全な場所に保存したら、認証情報ウィンドウで確認チェックボックスを選択し、ウィンドウを閉じます。

2.5. サービスアカウントの削除

サービスアカウントを削除できます。サービスアカウントをリセットまたは削除するには、サービスアカウントの所有者である必要があります。組織管理者ユーザーは、任意のサービスアカウントをリセットまたは削除できます。

前提条件

- Red Hat Hybrid Cloud Console にログインしている。

手順

1. Red Hat Hybrid Cloud Console から、設定アイコン(⚙)をクリックし、**Service Accounts** をクリックします。
2. 削除するサービスアカウントを特定し、オプションアイコン (⋮) をクリックします。
3. このアカウントを削除することを確認し、**Delete service account** をクリックします。

第3章 サービスでのサービスアカウントの使用

以下の情報は、サービスと CLIENT_ID および CLIENT_SECRET 変数でサービスアカウントを使用する方法を簡単に説明します。参考ガイドラインとしてのみ提供されています。

1. 新しいサービスアカウント (Red Hat Hybrid Cloud Console サービスアカウント) を作成します。

2. 次の情報を端末に貼り付けて、CLIENT_ID 変数と CLIENT_SECRET 変数を置き換えます。

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

3. サービスアカウントのトークンを取得します。

```
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 (コマンドライン JSON プロセッサー) がインストールされている場合は、トークンを環境変数に保存できます。

```
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. サービスアカウントをサポートするアプリケーションにリクエストを送信します。

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

5. レスポンスは空であるか、アプリケーションによっては特権のないアカウントが指定されているはずです。サービスアカウントを RBAC グループに追加し、ロールをそのグループに追加してみてください。(ユーザーアクセスグループ)

6. ロールがサービスアカウントグループに追加されたら、手順 3 を繰り返して新しいトークンを取得し、リクエストを再試行します。これで、さらに権限が付与され、アプリケーションから適切な応答が得られるようになります。