



Red Hat OpenShift API Management 1

Adding users in Red Hat OpenShift API Management

Adding users in Red Hat OpenShift API Management.

Red Hat OpenShift API Management 1 Adding users in Red Hat OpenShift API Management

Adding users in Red Hat OpenShift API Management.

Legal Notice

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.

Abstract

This guide provides information about how you can get started with adding users in Red Hat OpenShift API Management.

Table of Contents

| | |
|---------------------------------------------------------------------|----------|
| MAKING OPEN SOURCE MORE INCLUSIVE | 3 |
| CHAPTER 1. ADDING USERS IN OPENSIFT API MANAGEMENT | 4 |
| 1.1. ROLES IN OPENSIFT API MANAGEMENT | 4 |
| 1.2. GRANTING 3SCALE ADMINISTRATOR PRIVILEGES TO DEVELOPERS | 5 |
| 1.3. REMOVING A USER FROM OPENSIFT API MANAGEMENT FROM YOUR CLUSTER | 6 |

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. ADDING USERS IN OPENSHIFT API MANAGEMENT

1.1. ROLES IN OPENSHIFT API MANAGEMENT

OpenShift API Management includes administrator and developer roles. These roles determine the actions a user can perform.

All OpenShift API Management users belong to the **rhoam-developers** group. Additionally, administrators are members of the **dedicated-admins** group and are granted the **dedicated-admin** role in OpenShift Dedicated. Administrators are managed using the **dedicated-admins** group in the OpenShift Dedicated cluster and have elevated privileges in OpenShift API Management.

Administrator role

An administrator has rights to view and modify resources in OpenShift API Management and can assign cluster roles to control who has various access levels and permissions in OpenShift API Management, Red Hat 3scale API Management, and Red Hat Single Sign-On. Administrators in OpenShift API Management manage users, and the API gateway, APIcast, which is the interface that handles calls to an API. The onboarding process creates an administrator with the highest level of access in OpenShift API Management and with **admin** privileges in 3scale.

As an administrator, you can perform the following tasks:

- [Red Hat Single Sign-On](#)
 - Manage users and permissions in the master realm.
 - Create realms.
 - Administer user-created realms.
- [Red Hat 3scale API Management](#)
 - Elevate permissions of developers to an administrator level.
 - Edit routes.
 - View pod logs in the 3scale namespace.
 - Create a product in the 3scale console.

Developer role

Developers have access to the services in OpenShift API Management. With the developer role, you can use the Red Hat Single Sign-On instance to secure your applications and you have basic member access in 3scale. Developers, which are referred to as API providers in 3scale, make APIs accessible by adding them to OpenShift API Management, configuring their use, and publishing them.

As a developer, you can perform the following tasks:

- [Red Hat Single Sign-On](#)
 - Access the console.
 - Create realms.

- [Red Hat 3scale API Management](#)
 - Access the 3scale Admin Portal.
 - Access the 3scale Developer Portal.

An OpenShift API Management administrator can grant 3scale **admin** privileges to developers.

Additional resources

- [Roles in OpenShift Dedicated](#)
- [Managing OpenShift Dedicated administrators](#)
- [Inviting users and managing rights in 3scale](#)

1.2. GRANTING 3SCALE ADMINISTRATOR PRIVILEGES TO DEVELOPERS

As an administrator in OpenShift API Management, you also have **admin** privileges in 3scale. However, the developer role in OpenShift API Management only has **member** privileges in 3scale and limited access to 3scale features.

An administrator must explicitly grant 3scale **admin** permissions to OpenShift API Management developers.

Prerequisites

- You are an administrator in OpenShift API Management.
- You have a developer you want to grant **admin** privileges to in 3scale.

Procedure

1. Log in to the Red Hat 3scale API Management console **Admin Portal**.
2. Click **Dashboard**.
3. In the **Dashboard** drop-down menu, click **Accounts Settings**.
4. In the menu, click **Users** > **Listing**. The **Users** page is displayed.
5. Choose a user.
6. Click **Edit** for the user whose permission you would like to modify. The **Edit User** page opens.
7. In the **ADMINISTRATIVE** section of the **Edit User** page, choose **Admin (full access)** to grant **admin** privileges to the selected user.
8. Click **Update User**.

Verification

1. Navigate to the **Users** page. In the menu, click **Users** > **Listing**.
2. On the **Users** page, find the user whose permissions you modified.

3. In the **Role** column, ensure **admin** is displayed in the row of the chosen user.

Additional resources

- [Giving new users rights in 3scale](#)

1.3. REMOVING A USER FROM OPENSIFT API MANAGEMENT FROM YOUR CLUSTER

To completely remove a user from Red Hat OpenShift API Management, you must remove them from the allowed group in your OpenShift identity provider (IDP) and then delete the user custom resource (CR).

Prerequisites

- You have added an identity provider (IDP) to your cluster.
- You have the IDP user name for the user whose privileges you are revoking.
- You are logged in to the OpenShift Cluster Manager console using the OpenShift Cluster Manager account that you used to create the cluster or the administrator user.

Procedure

1. You can enter the following command to identify all users:

```
oc get users
```

2. Enter the following command to delete a specific user.

```
oc delete user <username>
```

3. Delete the desired user from the configured IDP.
4. Delete the user CR.
5. In OpenShift Cluster Manager, delete references to the user in the Access Control section. Ensure the user is removed from both the **Cluster Roles and Access** and the **Roles and Access** section.