



# Red Hat OpenShift API Management 1

## Getting Started with Red Hat OpenShift API Management

Getting started with your Red Hat OpenShift API Management installation.



# Red Hat OpenShift API Management 1 Getting Started with Red Hat OpenShift API Management

---

Getting started with your Red Hat OpenShift API Management installation.

## 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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 start working with Red Hat OpenShift API Management.

---

## Table of Contents

<b>MAKING OPEN SOURCE MORE INCLUSIVE .....</b>	<b>3</b>
<b>CHAPTER 1. INTRODUCTION TO RED HAT OPENSIFT API MANAGEMENT .....</b>	<b>4</b>
1.1. WHAT IS OPENSIFT API MANAGEMENT	4
Understanding Red Hat 3scale API Management	4
Understanding Red Hat Single Sign-On	4
Red Hat OpenShift API Management considerations	5
1.2. HOW TO SET UP OPENSIFT API MANAGEMENT	6
Configure an identity provider	7
Add OpenShift API Management	7
Configure 3scale API provider account permissions	7
1.3. HOW TO USE OPENSIFT API MANAGEMENT	7
Get started with 3scale	7
Create and configure an API	7
Configure APIcast policies	8
Secure your API	8
Set up a 3scale Developer Portal	8
Set up monitoring and analytics for your API	9
Launch the API product	9
Monitor your API	9
1.4. GET OPENSIFT API MANAGEMENT	9



## 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. INTRODUCTION TO RED HAT OPENSIFT API MANAGEMENT

Learn about the features and functions available in the Red Hat OpenShift API Management cloud service.

## 1.1. WHAT IS OPENSIFT API MANAGEMENT

Red Hat OpenShift API Management is a cloud service for creating, securing, and publishing your APIs. The OpenShift API Management service is an add-on for Red Hat OpenShift Dedicated and Red Hat OpenShift Service on AWS. The service is based on the Red Hat 3scale API Management platform and also includes an implementation of Red Hat Single Sign-On.

### Understanding Red Hat 3scale API Management

Application Programming Interface (API) management refers to the processes of distributing, controlling, and analyzing the APIs that connect applications and data across cloud environments.

Red Hat OpenShift API Management provides a management platform that allows users to share, secure, distribute, control, and monetize APIs. After setting up authentication and user accounts, OpenShift API Management developers, also referred to as API providers, can configure, and publish their APIs.

The main OpenShift API Management components include:

- APIcast - the 3scale API gateway
- Admin Portal - the 3scale console that API providers work in
- Developer Portal - the interface for API consumers
- Red Hat Single Sign-On - for authenticating access to the Developer Portal as well as to APIs

API providers are developers who work in the 3scale Admin Portal, for which an administrator has given them accounts. API providers also work in the OpenShift Dedicated cluster to deploy applications, such as a backend for service API requests. API providers create and publish APIs, and can configure Red Hat Single Sign-On authentication to secure APIs. 3scale separates APIs into two main groups:

- *Backends* are internal APIs bundled in a product. Backends grant API providers the freedom to map internal API organization structures to 3scale. A backend contains a private URL for an internal API. It is exposed through mapping rules and the public URL of one or more 3scale products.
- *Products* are customer-facing APIs. Products facilitate the creation of robust yet simplified offerings for API consumers. A product includes application plans and configuration of the APIcast gateway. A product can bundle multiple backends.

When a 3scale product is ready for use, an API provider publishes it in the Developer Portal. API consumers visit the Developer Portal to subscribe to a plan that enables them to use the 3scale product that contains that API. Consumers can then call the API's operations, subject to any usage policies that may be in effect.

### Understanding Red Hat Single Sign-On

Red Hat Single Sign-On provides single sign-on (SSO) authentication to secure web applications. You use this SSO implementation to control access to 3scale Developer Portals and to 3scale API products. It is not supported as a company-wide SSO solution.



## Red Hat OpenShift API Management considerations

Red Hat OpenShift API Management introduces several product considerations that need to be thoroughly understood before proceeding with the installation and configuration of the service:

- **Authentication Options:** OpenShift API Management provides various authentication options within the service to ensure secure access control and identity verification:
  - **OAuth 2.0:** An authorization framework that enables secure and delegated access to APIs. OAuth 2.0 allows users and applications to obtain limited, scoped access tokens, which can be used to authenticate and authorize API requests.
  - **OpenID Connect:** An identity layer built on top of OAuth 2.0 that provides additional features for authentication, such as user profile information and identity federation. OpenID Connect allows users to authenticate using their existing accounts from various identity providers.
  - **LDAP (Lightweight Directory Access Protocol):** A protocol commonly used for accessing and managing directory information. LDAP integration enables organizations to leverage their existing user directories for authentication within OpenShift API Management.
  - **Token-based authentication:** A mechanism that involves exchanging a token for authentication purposes. Tokens are typically issued by an identity provider or authentication service and can be used to validate and authorize API requests.
- **CIDR (Classless Inter-Domain Routing):** CIDR is a method used to allocate and manage IP addresses more efficiently. It replaces the older system of class-based IP addressing and enables flexible allocation of IP address blocks. CIDR notation is used to define network ranges and subnets. Understanding CIDR is important for correctly configuring networking components, such as IP whitelisting, firewall rules, and defining network policies for secure communication. The CIDR range must not overlap with any network you would like to peer within the OpenShift cluster VPC. If you do not specify a CIDR value, you can click the link in the OpenShift Cluster Manager to apply the default CIDR range. After submitting the initial configuration, you cannot modify the CIDR range. If you want to change the CIDR range, you must delete and reinstall Red Hat OpenShift API Management. The CIDR prefix length range must be between **/16** and **/26**. Only CIDR values within this range are permitted. You can use **10.1.0.0/26** as the default CIDR range.
- **Custom Wildcard Domain:** A wildcard domain name allows you to handle dynamic routing of API traffic across various endpoints and services within your infrastructure. By using a wildcard DNS record (for example **\*.example.com**), you can ensure that any subdomain under the specified domain is automatically routed to the corresponding API service or endpoint. This flexibility is particularly useful when dealing with multiple APIs or microservices, as it simplifies the management of API endpoints and enables dynamic scaling and routing. To configure a custom wildcard domain name with 3scale and Red Hat OpenShift API Management, you would typically do the following:
  - **Obtain a registered domain:** You need to have a registered domain name that you own and have administrative control over.
  - **Configure DNS settings:** Update your DNS settings for the domain to include a wildcard DNS record pointing to the appropriate IP address or load balancer associated with your API infrastructure.
  - **Obtain an SSL/TLS certificate:** Obtain an SSL/TLS certificate for your custom wildcard domain name to ensure secure communication between clients and your API services. This certificate can be either self-signed or issued by a trusted certificate authority (CA).

- Configure 3scale and OpenShift API Management: In the configuration settings of both 3scale and OpenShift API Management, specify the custom wildcard domain name as the endpoint for your APIs. This ensures that API requests made to any subdomain under the wildcard domain are correctly routed and processed by the respective API services.
- **SMTP (Simple Mail Transfer Protocol)** SMTP is a widely used standard protocol for email transmission. In the context of OpenShift API Management, SMTP configuration allows you to specify the email server settings required for email notifications, alerts, and communication within the system. By providing the necessary SMTP details, such as the server address, port number, authentication credentials, and encryption settings, you enable the platform to send emails seamlessly. To successfully apply an SMTP configuration, you must enter values for all related fields. Values for all Custom SMTP fields are required, if you specify values for any of the fields. Entering an SMTP configuration is optional. Red Hat OpenShift API Management default values are applied if you leave the SMTP configuration fields blank. You can enter values for the following fields:
  - **Custom SMTP Mail Server Address**- The remote mail server as a relay
  - **Custom SMTP From Address**- Email address of the outgoing mail
  - **Custom SMTP Username**- The mail server username
  - **Custom SMTP Password**- The mail server password
  - **Custom SMTP Port**- The port on which the mail server is listening for new connections
- **VPC Configurations:** A VPC (Virtual Private Cloud) is a virtual network infrastructure that allows you to provision and manage network resources within a logically isolated environment. OpenShift API Management supports the option to bring your own VPC, which means you can use your existing VPC setup instead of relying on the default networking configuration. The following Availability Zone (AZ) scenarios represent the tested configurations. Configurations that differ from the following, may not work as expected and are not supported.
  - **Single-AZ installation:** The tested architecture includes a VPC with an internet gateway, an availability zone containing a public subnet, and a private subnet.
  - **Multi-AZ installation:** The tested architecture includes a VPC with an internet gateway, up to three availability zones (with each containing one public subnet), and a private subnet.
  - **PrivateLink Multi-AZ installation:** The tested architecture includes connections to clusters using AWS PrivateLink endpoints instead of public endpoints for OpenShift Service on AWS (ROSA) or OpenShift Dedicated (OSD).

#### Additional resources

- [Supported bring-your-own VPC architectures](#)

## 1.2. HOW TO SET UP OPENSIFT API MANAGEMENT

A Red Hat OpenShift Dedicated cluster administrator sets up the cluster and identity provider and adds the OpenShift API Management service to a cluster. Then, you configure the service users.

If desired, you can customize APIcast, which is the interface that handles calls to a 3scale API product.

**NOTE**

In Red Hat OpenShift API Management documentation, ignore content for 3scale Hosted (SaaS). It does not apply to OpenShift API Management.

**Configure an identity provider**

If an identity provider is already configured, there is no need to configure another one. Otherwise, you must choose and configure an identity provider, which can be LDAP, GitHub, GitHub Enterprise, Google, or OpenID Connect.

Instructions:

- [Configuring identity providers](#)

**Add OpenShift API Management**

Adding OpenShift API Management to a cluster makes the service available for use by 3scale API providers. You can add OpenShift API Management to an OpenShift Dedicated cluster, or to a ROSA cluster.

Instructions:

- [Adding OpenShift API Management to your cluster](#)
- [Adding OpenShift API Management to your Red Hat OpenShift Service on AWS cluster](#)

**Configure 3scale API provider account permissions**

In the 3scale Admin Portal, configure account permissions so that API providers in your organization can create, configure, and launch 3scale API products.

When a new user logs in to the OpenShift Dedicated cluster by using the configured identity provider, the user automatically receives an OpenShift account with permission to access OpenShift API Management.

You manage these accounts in the 3scale Admin Portal.

By default, Single Sign-On is configured for 3scale in OpenShift API Management.

Instructions:

- [Red Hat Single Sign-On for the 3scale Admin Portal](#)

## 1.3. HOW TO USE OPENSIFT API MANAGEMENT

Use OpenShift API Management to create, secure, and publish your APIs.

**Get started with 3scale**

You can use the 3scale wizard to start learning about how to add and test a 3scale API product.

Instructions:

- [First steps with 3scale](#)

**Create and configure an API**

In the 3scale Admin Portal, create and configure an API to ensure that access is protected by API keys, tracked, and monitored by 3scale with basic rate limits and controls in place.

This involves the following steps:

- Create API backends
- Create API products
- Create mapping rules and application plans to define a customer-facing API product
- Capture metrics
- Configure API access rules

Mapping rules define the metrics or methods to report. Application plans define the rules such as limits, pricing, and features for using an API product. An application subscribes to an application plan.

Instructions:

- [Adding and configuring APIs](#)

### Configure APIcast policies

APIcast is the 3scale API gateway, which is the endpoint that accepts API product calls and routes them to bundled backends. OpenShift API Management provides APIcast staging for developing and testing APIs and also APIcast production, for published APIs.

APIcast policies are units of functionality that modify how APIcast operates. Policies can be enabled, disabled, and configured to control APIcast behavior. Use custom policies to add functionality that is not available in a default APIcast deployment.

Instructions:

- [APIcast policies](#)

### Secure your API

If you want to secure your API by using OpenID and OAuth, then in the Red Hat Single Sign-On Admin Console, create a Red Hat Single Sign-On realm. An SSO realm is required to manage authentication for access to the Developer Portal and 3scale API products.

In the 3scale Admin Portal, set up authentication to control access to your API product and to the 3scale Developer Portal.

Instructions:

- [Enabling and disabling authentication through Red Hat Single Sign-On](#)

### Set up a 3scale Developer Portal

A well-structured developer portal and great documentation are key elements to assure adoption. A developer portal is the main hub for managing interactions with API consumers and for API consumers to access their API keys in a secure way.

In the 3scale Admin Portal, add OpenAPI Specification 3.0 conforming documents for use in a Developer Portal. API consumers use the Developer Portal to access the APIs defined in these documents.

Then, configure the Developer Portal and add your APIs.

Instructions:

- [Providing APIs in the Developer Portal](#)
- [Discover and import APIs available in your OpenShift Dedicated cluster](#)
- [Summary: from zero to hero Developer Portal](#)

### **Set up monitoring and analytics for your API**

You can designate methods in your API and add metrics to set access limits for any of an API product's application plans. For an API backend, methods and metrics can be used to set access limits in the application plan of any API product that bundles the backend.

Instructions:

- [Designating methods and adding metrics for capturing usage details](#)
- [API analytics](#)

### **Launch the API product**

After you have configured and secured your API and created a Developer Portal, you can launch your API so that consumers can begin to use it.

Instructions:

- [Going live](#)

### **Monitor your API**

After your API is launched, you can monitor metrics that indicate how it is being used. Knowing how a 3scale API product is used is a crucial step for managing traffic, provisioning for peaks, and identifying the users who most often send requests to the API product.

Instructions:

- [Viewing 3scale built-in traffic analytics for applications](#)

## **1.4. GET OPENSIFT API MANAGEMENT**

To get OpenShift API Management, you can add it to your OpenShift Dedicated cluster or ROSA cluster. To learn more, go to <https://cloud.redhat.com/application-services/overview>.