



# OpenShift Container Platform 4.5

## Getting started with cost management

Learn about and configure cost management



# OpenShift Container Platform 4.5 Getting started with cost management

---

Learn about and configure cost management

## Legal Notice

Copyright © 2020 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 describes the initial steps to begin using cost management.

---

## Table of Contents

<b>CHAPTER 1. INTRODUCTION TO COST MANAGEMENT</b> .....	<b>3</b>
1.1. ABOUT COST MANAGEMENT	3
1.1.1. Terminology	3
1.2. PLANNING FOR COST MANAGEMENT	3
<b>CHAPTER 2. LIMITING ACCESS TO COST MANAGEMENT RESOURCES</b> .....	<b>5</b>
2.1. DEFAULT USER ROLES IN COST MANAGEMENT	5
2.2. ADDING A ROLE	5
2.3. ADDING A ROLE TO A GROUP	7
<b>CHAPTER 3. ADDING SOURCES TO COST MANAGEMENT</b> .....	<b>9</b>
3.1. ADDING AN AMAZON WEB SERVICES (AWS) SOURCE TO COST MANAGEMENT	9
3.1.1. Creating an S3 bucket for reporting	9
3.1.2. Activating AWS tags for cost management	10
3.1.3. Enabling minimal account access for cost and usage consumption	10
3.1.3.1. Enabling additional account access for cost and usage consumption	12
3.2. ADDING A MICROSOFT AZURE SOURCE TO COST MANAGEMENT	13
3.2.1. Creating an Azure resource group and storage account	13
3.2.2. Configuring Azure roles	14
3.2.3. Configuring a daily Azure data export schedule	14
3.3. ADDING AN OPENSIFT CONTAINER PLATFORM SOURCE TO COST MANAGEMENT	15
3.3.1. Installing the Cost Management Operator	15
3.3.2. Configuring the Cost Management Operator	16
<b>CHAPTER 4. NEXT STEPS FOR MANAGING YOUR COSTS</b> .....	<b>20</b>
4.1. CONFIGURE TAGGING FOR YOUR SOURCES	20
4.2. CONFIGURE COST MODELS TO ACCURATELY REPORT COSTS	20



# CHAPTER 1. INTRODUCTION TO COST MANAGEMENT

This document provides instructions to begin using cost management, including prerequisites and instructions for connecting your cloud environments, and configuring users and permissions.

After completing the setup described in this guide, you will be able to track cost and usage data for your Amazon Web Services (AWS), Microsoft Azure, and OpenShift Container Platform environments.

If you have a suggestion for improving this guide or have found an error, please submit a Bugzilla report at <http://bugzilla.redhat.com> against *Cloud Software Services (cloud.redhat.com)* for the **Cost Management** component.

## 1.1. ABOUT COST MANAGEMENT

Cost management is an OpenShift Container Platform service that enables you to better understand and track costs for clouds and containers. It is based on the upstream project Koku.

You can access the cost management application from <https://cloud.redhat.com/cost-management/>.

Cost management allows you to simplify management of resources and costs across various environments, including:

- Public clouds such as Amazon Web Services (AWS) and Microsoft Azure
- Container platforms such as OpenShift Container Platform

The cost management application allows you to:

- Visualize, understand and analyze the use of resources and costs
- Forecast your future consumption and compare them with budgets
- Optimize resources and consumption
- Identify patterns of usage that should be investigated
- Integrate with third party tools that can benefit from cost and resourcing data

### 1.1.1. Terminology

#### Source

A cloud provider account that is connected to cost management to be monitored, for example, an AWS or Azure account, or an OpenShift Container Platform deployment.

#### Organization Administrator

The highest permission level for Red Hat accounts, with full access to content and features. This is the only role that can manage users and control their access and permissions on an account. An account may have multiple Organization Administrators.

See [Roles and Permissions for Red Hat Subscription Management](#) for more details.

## 1.2. PLANNING FOR COST MANAGEMENT

When configuring cost management for your needs, consider the scope of your environments that you want to manage costs for, and the users who will have access to the data.

Some considerations in creating a new Red Hat organization and users for different customer types include:

**Scope:**

- Customer company wide
- Customer division or organization wide
- Partner company managing several tenants

**Data:**

- How does your business need the data? Do you want information about projects, or users, for example?
- Planning AWS tags to reflect previous use cases.
- Enforcement: Is there any way for you to ensure that the proper tags and metadata are included in each item of the inventory?

**User access:**

- What level of access do you want your users to have?
- Do you want some users to have access to all cost data, while other users can view only a portion of the environment or certain sources?



## CHAPTER 2. LIMITING ACCESS TO COST MANAGEMENT RESOURCES

You may not want users to have access to all cost data, but instead only data specific to their projects or organization. Using role-based access control, you can limit the visibility of resources involved in cost management reports. For example, you may want to restrict a user's view to only AWS sources, instead of the entire environment.

Role-based access control works by organizing users into groups, which can be associated with one or more roles. A role defines a permission and a set of resource definitions.

By default, a user who is not an account administrator will not have access to data, but instead must be granted access to resources. Account administrators can view all data without any further role-based access control configuration.



### NOTE

A Red Hat account user with Organization Administrator entitlements is required to configure Red Hat account users. This Red Hat login allows you to look up users, add them to groups, and to assign roles that control visibility to resources.

For more information about Red Hat account roles, see [Roles and Permissions for Red Hat Subscription Management](#) and [How To Create and Manage Users](#).

### 2.1. DEFAULT USER ROLES IN COST MANAGEMENT

You can configure custom user access roles for cost management, or assign each user a predefined role.

To use a default role, determine the required level of access to permit your users based on the following predefined roles in cost management:

#### Administrator roles

- Cost Administrator: has read and write permissions to all resources in cost management
- Cost Price List Administrator: has read and write permissions on price list rates

#### Viewer roles

- Cost Cloud Viewer: has read permissions on cost reports related to cloud sources
- Cost OpenShift Viewer: has read permissions on cost reports related to OpenShift sources
- Cost Price List Viewer: has read permissions on price list rates


### 2.2. ADDING A ROLE

Create a new role to manage and limit the scope of information that users can see within cost management.

#### Prerequisites

- You must be an Account Administrator or a member of a group with the *RBAC Administrator* role to create a role.

## Procedure

1. From cost management, click  (**Settings**) to navigate to **User Access**.
2. Click the **Roles** tab.
3. Click **Create Role** to open the **Add role** wizard.
4. In the **Name and Description** screen, enter a name for the new role, and optionally, a description. Click **Next**.
5. In the **Permission** screen, specify the Red Hat Cloud Services application you are creating the role for (in this case, cost management) as well as the resource and permission type:
  - a. For **Application**, enter *cost-management*.
  - b. For **Resource type**, specify the resource this permission will be used to access from the following list:
    - *aws.account*
    - *aws.organizational\_unit*
    - *azure.subscription\_guid*
    - *openshift.cluster*
    - *openshift.node*
    - *openshift.project*
  - c. For **Permission**, specify *read* as all cost resource data is read-only. For example, to create a role with read-only permissions to AWS account data, set *aws.account* as the **Resource type** and *read* as the **Permission**. In the next step, you can specify the AWS account to apply this role to.
6. In the **Resource definitions** screen, you can provide more details about the resources the permission will be used for. For example, to grant this role access to a specific AWS account, enter the following and click **Add to definitions**:
  - **Key:** *aws.account*
    - Options for **Key** are: *aws.account*, *azure.subscription\_guid*, *openshift.cluster*, *openshift.node*, *openshift.project*
  - **Operation:** *equal*
    - Use *equal* if you know the exact value, or *list* to see a list of values that will work for this role.
  - **Value:** Your AWS account number or account alias.

- This is specific to the resource defined in the **Key** field. Examples include the AWS account ID or alias, Azure subscription ID, OpenShift cluster ID, OpenShift node name, or OpenShift project name.  
You can also enter \* in this field as a wildcard to create a role that matches everything of the resource type defined in **Key**.

7. Add more resource definitions if desired and click **Next** when finished.

8. Review the details for this role and click **Confirm** to create the role.

Your new role will be listed in the **Roles** tab on the **User Access Management** screen.

### Next steps

- Add this role to a group to provide the role with access to resources.


## 2.3. ADDING A ROLE TO A GROUP

Add your role to a group to manage and limit the scope of information that users in that group can see within cost management.

### Prerequisites

- You must be an Account Administrator or a member of a group with the *RBAC Administrator* role to create a role.

### Procedure

1. From cost management, click  (**Settings**) to navigate to **User Access**.
2. Click the **Groups** tab.
3. Click **Create group**.
4. In the **General information** screen, enter a name for the new group, and optionally, a description. Click **Next**.
5. In the **Add members** screen, select the user(s) in your organization to add to the new group. Click **Next**.
6. (Optional) In the **Select roles** screen, select one or more role(s) to add to the group. Default roles available for cost management are:
  - *Cost Administrator* : grants read and write permissions
  - *Cost Cloud Viewer* : grants read permissions on cost reports related to cloud sources
  - *Cost OpenShift Viewer* : grants read permissions on cost reports related to OpenShift sources
  - *Cost Price List Administrator* : grants read and write permissions on price list rates
7. Review the details for this group and click **Confirm** to create the group.

Your new group will be listed in the **Groups** list on the **User Access** screen.

To verify your configuration, log out of the cost management application and log back in as a user added to the group.

## CHAPTER 3. ADDING SOURCES TO COST MANAGEMENT

To use cost management to monitor your cloud costs, you must first connect a data source to the cost management application.

Currently, cost management can track costs for Amazon Web Services (AWS), Microsoft Azure, and Red Hat OpenShift Container Platform sources.

### 3.1. ADDING AN AMAZON WEB SERVICES (AWS) SOURCE TO COST MANAGEMENT

To add an AWS account to cost management, you must configure your AWS account to provide metrics, then add your AWS account as a source from the cost management user interface.

This creates a read-only connection to AWS in order to collect cost information hourly in cost management, but does not make any changes to the AWS account.



#### IMPORTANT

You must use an AWS master account for this procedure, as a linked AWS account does not have sufficient access to create billing accounts. After you add the master account as a source, cost management will collect data from any linked accounts as well.

Before you can add your AWS account to cost management as a data source, you must configure the following services on your AWS account to allow cost management access to metrics:

1. An S3 bucket to store cost and usage data reporting for cost management
2. An Identity Access Management (IAM) policy and role for cost management to process the cost and usage data

As you will complete some of the following steps in the AWS console, and some steps in the cost management user interface, keep both applications open in a web browser.

Add your AWS source to cost management from the settings area at <https://cloud.redhat.com/settings/sources/>.



#### NOTE

As non-Red Hat products and documentation can change without notice, instructions for configuring the third-party sources provided in this guide are general and correct at the time of publishing. See the [AWS documentation](#) for the most up-to-date and accurate information.

#### 3.1.1. Creating an S3 bucket for reporting

Cost management requires an Amazon S3 bucket with permissions configured to store billing reports.

Log into your AWS master account to begin configuring cost and usage reporting:

1. In the AWS S3 console, create a new S3 bucket or use an existing bucket. If you are configuring a new S3 bucket, accept the default settings.

2. In the AWS Billing console, create a Cost and Usage Report that will be delivered to your S3 bucket. Specify the following values (and accept the defaults for any other values):

Report name: `<any-name>` (note this name as you will use it later)  
 Additional report details: Include resource IDs  
 S3 bucket: `<the S3 bucket you configured previously>`  
 Time granularity: Hourly  
 Enable report data integration for: Amazon Redshift, Amazon QuickSight (do not enable report data integration for Amazon Athena)  
 Compression type: GZIP  
 Report path prefix: (leave blank)



#### NOTE

See the *AWS Billing and Cost Management* documentation for more details on configuration.

3. In the cloud.redhat.com platform, open the **Sources** menu (<https://cloud.redhat.com/settings/sources/>) to begin adding an AWS source to cost management:
  - a. Navigate to **Sources** and click **Add a source** to open the Sources wizard.
  - b. Enter a name for your source and click **Next**.
  - c. Select **Cost Management** as the application and **Amazon Web Services (AWS)** as the source type. Click **Next**.
  - d. Paste the name of your S3 bucket and click **Next**.

### 3.1.2. Activating AWS tags for cost management

To use tags to organize your AWS resources in the cost management application, activate your tags in AWS to allow them to be imported automatically.

#### Procedure

1. In the AWS Billing console:
  - a. Open the *Cost Allocation Tags* section.
  - b. Select the tags you want to use in the cost management application, and click **Activate**.
2. In the cloud.redhat.com **Sources** wizard, click **Next** to move to the next screen.

### 3.1.3. Enabling minimal account access for cost and usage consumption

To provide data within the web interface and API, cost management needs to consume the Cost and Usage Reports produced by AWS. For cost management to obtain this data with a minimal amount of access, create an IAM policy and role for cost management to use. This configuration provides access to the stored information and nothing else.

#### Procedure

1. From the AWS Identity and Access Management (IAM) console, create a new IAM policy for the S3 bucket you configured previously.
  - a. Select the JSON tab and paste the following content in the JSON policy text box:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "s3:HeadBucket",
        "cur:DescribeReportDefinitions"
      ],
      "Resource": "*"
    }
  ]
}
```

- a. Provide a name for the policy and complete the creation of the policy. Keep the AWS IAM console open as you will need it for the next step.
  1. In the cloud.redhat.com **Sources** wizard, click **Next** to move to the next screen.
  2. In the AWS IAM console, create a new IAM role:
- b. For the type of trusted entity, select **Another AWS account**
- c. Enter *589173575009* as the Account ID to provide the cost management application with read access to the AWS account cost data.
- d. Attach the IAM policy you just configured.
- e. Enter a role name (and description if desired) and finish creating the policy.
  1. In the cloud.redhat.com **Sources** wizard, click **Next** to move to the next screen.
  2. In the AWS IAM console under Roles, open the summary screen for the role you just created and copy the Role ARN (a string beginning with *arn:aws:*).
  3. In the cloud.redhat.com **Sources** wizard, paste your Role ARN and click **Next**.
  4. Review the details and click **Finish** to add the AWS account to cost management.

Cost management will begin collecting cost and usage data from your master AWS account and any linked AWS accounts.

The data can take a few days to populate before it shows on the cost management dashboard (<https://cloud.redhat.com/cost-management/>).

### 3.1.3.1. Enabling additional account access for cost and usage consumption

Cost management can display additional data that might be useful. For example:

- Include the Action `iam:ListAccountAliases` to display an AWS account alias rather than an account number in cost management.
- Include the Actions `organization:List*` and `organizations:Describe*` to obtain the display names of AWS member accounts if you are using consolidated billing rather than the account ID.

The following configuration provides access to additional stored information and nothing else.

#### Procedure

1. From the AWS Identity and Access Management (IAM) console, create a new IAM policy for the S3 bucket you configured previously.
2. Select the JSON tab and paste the following content in the JSON policy text box:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": [
        "arn:aws:s3:::bucket",
        "arn:aws:s3:::bucket/*"
      ]
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "iam:ListAccountAliases",
        "s3:HeadBucket",
        "cur:DescribeReportDefinitions",
        "organizations:List*",
        "organizations:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```



The remainder of the configuration steps are the same as in [Section 3.1.3.1, “Enabling additional account access for cost and usage consumption”](#).

You have completed adding your AWS account as a source.

## 3.2. ADDING A MICROSOFT AZURE SOURCE TO COST MANAGEMENT

This section describes how to configure your Microsoft Azure account to allow cost management access.

Configuring your Azure account to be a cost management source requires:

1. Creating a storage account and resource group
2. Configuring a Storage Account Contributor and Reader roles for access
3. Scheduling daily cost exports



### NOTE

As non-Red Hat products and documentation can change without notice, instructions for configuring the third-party sources provided in this guide are general and correct at the time of publishing. See the [Microsoft Azure documentation](#) for the most up-to-date and accurate information.

Add your Azure source to cost management from <https://cloud.redhat.com/settings/sources/>.

### 3.2.1. Creating an Azure resource group and storage account

Cost export data is written to a storage account, which exists within a resource group. The resource group must be accessible by cost management in order to read the Azure cost data.

Create a new storage account in Azure to contain the cost data and metrics that cost management will collect. This requires a resource group; Red Hat recommends creating a dedicated resource group for this storage account.

1. In the cloud.redhat.com platform, open the **Sources** menu (<https://cloud.redhat.com/settings/sources/>) to begin adding an Azure source to cost management:
  - a. Navigate to **Sources** and click **Add a source** to open the Sources wizard.
  - b. Enter a name for your source and click **Next**.
  - c. Select **Cost Management** as the application and **Microsoft Azure** as the source type. Click **Next**.
2. Create a resource group and storage account in your Azure account using the instructions in the See [Azure documentation](#) *Create a storage account*.

Make a note of the resource group and storage account. They will be needed in subsequent steps.

1. In the cloud.redhat.com **Sources** wizard, enter the **Resource group name** and **Storage account name** and click **Next**.

### 3.2.2. Configuring Azure roles

Red Hat recommends configuring dedicated credentials to grant cost management read-only access to Azure cost data. Configure a Storage Account Contributor and Reader role in Azure to provide this access to cost management.

1. In Azure Cloud Shell, run the following command to obtain your Subscription ID:

```
$ az account show --query "{subscription_id: id}"
```

2. In the cloud.redhat.com **Sources** wizard, enter your **Subscription ID**. Click **Next** to move to the next screen.
3. In Azure Cloud Shell, run the following command to create a Cost Management Storage Account Contributor role, and obtain your tenant ID, client (application) ID, and client secret:

```
$ az ad sp create-for-rbac -n "CostManagement" --role "Storage Account Contributor" --query '{"tenant": tenant, "client_id": appld, "secret": password}'
```

4. In the cloud.redhat.com **Sources** wizard, enter your Azure **Tenant ID**, **Client ID**, and **Client Secret**.
5. In Azure Cloud Shell, run the following command to create a Cost Management Reader role with your subscription ID. Copy the full command from the cloud.redhat.com **Sources** wizard, which will automatically substitute your Azure subscription ID obtained earlier for `<SubscriptionID>`:

```
$ az role assignment create --role "Cost Management Reader" --assignee http://CostManagement --subscription <SubscriptionID>
```

6. Click **Next**.

### 3.2.3. Configuring a daily Azure data export schedule

Create a recurring task to export your cost data on a daily basis automatically to your Azure storage account, where cost management will retrieve the data.

1. In Azure, add a new export as described in the instructions in the [Azure article](#) *Create and manage exported data*.
  - For **Export type**, select **Daily export of billing-period-to-date costs**
  - For **Storage account**, select the account you created earlier.
  - Enter any value for the container name and directory path for the export. These values provide the tree structure in the storage account where report files are stored.
  - Click **Run now** to start exporting data to the Azure storage container.
2. In the cloud.redhat.com **Sources** wizard, click **Next** when you have created the export schedule and review the source details.
3. Click **Finish** to complete adding the Azure source to cost management.

After the schedule is created, cost management will begin polling Azure for cost data, which will appear on the cost management dashboard (<https://cloud.redhat.com/cost-management/>).

You have completed adding your Azure account as a source.

### 3.3. ADDING AN OPENSIFT CONTAINER PLATFORM SOURCE TO COST MANAGEMENT

To add an OpenShift Container Platform cluster as a source to cost management, you must first configure your cluster to provide usage data (metrics) using the Cost Management Operator.

The Cost Management Operator (**cost-mgmt-operator**) collects the metrics required for cost management by:

- Using Operator Metering to create usage reports specific to cost management.
- Collecting and packaging these reports to a tarball which is uploaded to cost management through [cloud.redhat.com](https://cloud.redhat.com).



#### NOTE

An OpenShift Container Platform 4.3 or newer cluster is required to use the Cost Management Operator.

To add your OpenShift Container Platform cluster as a cost management source:

1. Install the Cost Management Operator in OpenShift from OperatorHub
2. Configure the Cost Management Operator to collect OpenShift usage data (metrics) using Operator Metering
3. Provide the cluster identifier to cost management

As you will complete some of the following steps in OpenShift Container Platform, and some steps in the [cloud.redhat.com](https://cloud.redhat.com/settings/sources/) platform (<https://cloud.redhat.com/settings/sources/>), have both applications open in a web browser, as well as a terminal to access the command line interface (CLI).

#### 3.3.1. Installing the Cost Management Operator

The Cost Management Operator collects the metrics required for cost management.

Begin adding your OpenShift Container Platform cluster as a source to cost management, then install the Cost Management Operator from OperatorHub.



#### NOTE

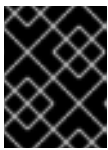
See [Operators](#) in the OpenShift documentation for more information about Operators and OperatorHub.

#### Prerequisites

- OpenShift Container Platform 4.3 or newer

#### Procedure

1. In the cloud.redhat.com platform, open the **Sources** menu (<https://cloud.redhat.com/settings/sources/>) to begin adding an OpenShift source to cost management:
  - a. Navigate to **Sources** and click **Add source** to open the Sources wizard.
  - b. Enter a name for your source and click **Next**.
  - c. Select **Cost Management** as the application and **OpenShift Container Platform** as the source type. Click **Next**.
2. In OpenShift, create a namespace called **openshift-metering** if one does not exist, and label the namespace with **openshift.io/cluster-monitoring=true**.
3. In OpenShift, install the Cost Management Operator in the **openshift-metering** namespace, using either the OpenShift web console (search for *cost management* in OperatorHub) or the CLI.



### IMPORTANT

You must install the Cost Management Operator in the **openshift-metering** namespace. Other namespaces are not supported for installation.

See [Adding operators to a cluster](#) in the OpenShift documentation for instructions for installing an Operator.

### Additional resources

- See [Metering](#) in the OpenShift documentation for more information about installing Metering.

## 3.3.2. Configuring the Cost Management Operator

The Cost Management Operator (**cost-mgmt-operator**) collects the metrics required for cost management.

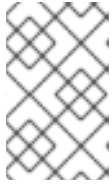
After installing the Cost Management Operator, configure authentication and the **operator-metering** namespace, then configure the Cost Management Operator.

### Prerequisites

- OpenShift Container Platform 4.3 or newer
- The Cost Management Operator installed in the **openshift-metering** namespace
- A user with access to the **openshift-config** namespace

### Procedure

1. Configure authentication inside the **openshift-metering** project. This allows you to upload OpenShift data to cloud.redhat.com.

**NOTE**

You can use token authentication or basic authentication to upload the usage reports (metrics) to cost management. The default and recommended method is token authentication.

- a. Copy the following into a file called **auth\_secret.yaml**:

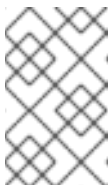
```
kind: Secret
apiVersion: v1
metadata:
  name: auth-secret-name
  namespace: openshift-metering
  annotations:
    kubernetes.io/service-account.name: cost-mgmt-operator
data:
  username: >-
    Y2xvdWQucmVkaGF0LmNvbSB1c2VybmFtZQ==
  password: >-
    Y2xvdWQucmVkaGF0LmNvbSBwYXNzd29yZA==
  token: >-
    Y2xvdWQucmVkaGF0LmNvbSB0b2t1bG==
```

- b. Choose a name for your authentication secret and replace the **metadata.name** value with it.
- c. To configure token authentication (the default method), obtain the correct *auth* token and then edit the secret to replace the token value:
- i. Install the **jq** JSON processor.
  - ii. Change to the **openshift-config** namespace:

```
$ oc project openshift-config
```

- iii. Replace the token value in **auth\_secret.yaml** with the authentication token for *cloud.openshift.com*. Obtain the token by running the following command, and copy only the "tokenvalue" to **auth\_secret.yaml** (excluding the quotation marks):

```
$ oc get secret pull-secret -o "jsonpath={.data.\.dockerconfigjson}" | base64 --decode
| jq '.auths."cloud.openshift.com".auth'
```

**NOTE**

To use basic authentication, edit the secret to replace the username and password values with your base64-encoded username and password for connecting to *cloud.redhat.com*.

- d. Deploy the secret to your OpenShift cluster in the **openshift-metering** namespace:

```
$ oc create -f auth-secret.yaml
```

For both methods of authentication, the name of the secret should match the *authentication\_secret\_name* set in the **CostManagement** custom resource configured in the next steps.

2. Configure the Metering Operator.  
Cost management uses the Metering Operator to create, collect, package, and upload metrics to cost management. In order for metering to work properly, configure **operator-metering** using the [OpenShift documentation](#) to create a MeteringConfig resource.
3. Configure the Cost Management Operator by creating the **CostManagement** and **CostManagementData** custom resources.  
Creating these resources also starts the roles that create the resources to obtain the usage reports (metrics). This takes about an hour to run and the reports are collected, packaged, and uploaded every six hours.

**NOTE**

The Cost Management Operator requires the **clusterID**, **reporting\_operator\_token\_name**, and **authentication\_secret\_name** to be specified in a **CostManagement** custom resource.

- a. Copy the following **CostManagement** resource template and save it to a file called **cost-mgmt-resource.yaml**:

```
apiVersion: cost-mgmt.openshift.io/v1alpha1
kind: CostManagement
metadata:
  name: cost-mgmt-setup
spec:
  clusterID: '123a45b6-cd8e-9101-112f-g131415hi1jk'
  reporting_operator_token_name: 'reporting-operator-token-123ab'
  validate_cert: 'false'
  authentication: 'basic'
  authentication_secret_name: 'basic_auth_creds-123ab'
```

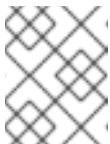
- b. Edit the following values in your **cost-mgmt-resource.yaml** file:

- The **clusterID** value to your cluster ID. Obtain your cluster ID by running:

```
$ oc get clusterversion -o jsonpath='{.items[].spec.clusterID}'
```

- The **reporting\_operator\_token\_name** to the **reporting-operator-token** secret name inside the **openshift-metering** namespace. Obtain this by running:

```
$ oc get secret -n openshift-metering | grep reporting-operator-token
```

**NOTE**

Depending on your configuration, this command can return two token names. You can use either to configure the Cost Management Operator.

- Specify the authentication type you are using (**token** or **basic**). If you are using **token** authentication, you can remove the authentication field as token authentication is the default.
- Change the **authentication\_secret\_name** to the name of your authentication secret you created earlier.

- c. Deploy the **CostManagement** resource:

```
$ oc create -f cost-mgmt-resource.yaml
```

- d. Create a **CostManagementData** resource to start the collection. Copy the following template and save it as **cost-mgmt-data-resource.yaml**:

```
apiVersion: cost-mgmt-data.openshift.io/v1alpha1
kind: CostManagementData
metadata:
  name: cost-mgmt-data-example
```

- e. Deploy the **CostManagementData** resource:

```
$ oc create -f cost-mgmt-data-resource.yaml
```

The Cost Management Operator will now create, collect, package, and upload your OpenShift usage reports to cost management.

4. When configuration is complete, enter the cluster identifier into the cloud.redhat.com **Sources** wizard, click **Next**.



#### NOTE

The cluster identifier can be found in **Help > About** in OpenShift.

5. In the cloud.redhat.com **Sources** wizard, review the details and click **Finish** to add the OpenShift Container Platform cluster to cost management.

#### Additional resources

- See [Operators](#) in the OpenShift documentation for more information about Operators and OperatorHub

Cost management will begin collecting usage data (metrics) from your OpenShift Container Platform cluster. The data can take a few days to populate before it shows on the cost management dashboard.

You have completed adding your OpenShift Container Platform cluster as a source.

## CHAPTER 4. NEXT STEPS FOR MANAGING YOUR COSTS

After adding your infrastructure and cloud sources, in addition to showing cost data by source, cost management will automatically show AWS and Azure cost and usage related to running your OpenShift Container Platform clusters on AWS or Azure.

On the cost management **Overview** page, use the **Perspective** options for different views of your cost data.

Use the **Details** menu to look more closely at your costs.

### 4.1. CONFIGURE TAGGING FOR YOUR SOURCES

The cost management application tracks cloud and infrastructure costs using tags (called labels in OpenShift), which you can refine to filter and attribute to resources. Tags in cost management allow you to organize your resources by cost and to allocate the costs to different parts of your cloud infrastructure.



#### IMPORTANT

Tags and labels can only be configured directly on a source. You cannot edit tags and labels in the cost management application.

See [Managing cost data using tagging](#) to learn more about:

- Planning your tagging strategy to organize your view of cost data
- Understanding how cost management associates tags
- Configuring tags and labels on your sources

### 4.2. CONFIGURE COST MODELS TO ACCURATELY REPORT COSTS

Now that you have configured your sources to collect cost and usage data into cost management, you can configure cost models to associate prices to metrics and usage, and fine-tune the costs of running your cloud.

A cost model is a framework used to define the calculations for the costs stored in cost management, using raw costs and metrics. Costs generated by a cost model can be recorded, categorized and distributed to specific customers, business units or projects.

From the [Cost models](#) area of cost management, you can:

- Classify your costs as infrastructure or supplementary costs
- Capture monthly costs for OpenShift nodes and clusters
- Apply a markup to account for additional support costs
- Learn how to configure a cost model in [Using cost models](#).