Abstract

This guide provides an overview of the features available in the cloud platform (cloud.redhat.com) that can help administrator users with the planning and usage of a service or application that uses these features in your hybrid cloud environment.
# Table of Contents

**PART I. PLANNING YOUR RED HAT CLOUD PLATFORM INITIATIVES** .......................... 3

**CHAPTER 1. WHAT IS USER ACCESS**  ........................................................................ 4
  1.1. WHO CAN USE USER ACCESS  ................................................................. 4
  1.2. ADDITIVE ACCESS  .................................................................................. 4
  1.3. THE USER ACCESS GROUPS, ROLES, AND PERMISSIONS  .................... 4

**CHAPTER 2. SETTING USER PREFERENCES** ......................................................... 5

**CHAPTER 3. HOOKS INTEGRATION IN CLOUD.REDHAT.COM (BETA)**  ................. 6
  3.1. HOW HOOKS SENDS NOTIFICATIONS ABOUT CHANGES IN YOUR INSIGHTS SYSTEM INVENTORY  .............................................................. 6

**CHAPTER 4. SYSTEM TAGS AND GROUPS** ........................................................ 7
  4.1. TAG STRUCTURE  ...................................................................................... 8

**CHAPTER 5. SYSTEM STALENESS AND DELETION** ........................................... 9
  5.1. RULES FOR SYSTEM STALENESS AND DELETION  ............................... 9
  5.2. VIEWING STALE SYSTEM SUMMARY  ..................................................... 9
  5.3. FILTERING SYSTEM INVENTORY  ......................................................... 9

**CHAPTER 6. CONFIGURING SOURCES FOR RED HAT SERVICES** ...................... 11
  6.1. ABOUT SOURCES  .................................................................................. 11
  6.2. ADDING CLOUD SOURCES  ................................................................. 11
  6.3. ADDING RED HAT SOURCES  .............................................................. 14
  6.4. SOURCES REFERENCE MATERIAL  ....................................................... 14
PART I. PLANNING YOUR RED HAT CLOUD PLATFORM INITIATIVES

This guide provides an overview of the features available in the cloud platform (cloud.redhat.com) that can help administrator users with the planning and usage of a service or application that uses these features in your hybrid cloud environment.
CHAPTER 1. WHAT IS USER ACCESS

The User Access feature is an implementation of role-based access control (RBAC) that controls user access to various services hosted at cloud.redhat.com. You configure the User Access feature to grant or deny user access to services hosted on cloud.redhat.com.

1.1. WHO CAN USE USER ACCESS

To initially view and manage User Access on cloud.redhat.com, you must be an Organization Administrator (org admin). This is because User Access requires user management capabilities that are designated from the Red Hat Customer Portal at Customer Portal. Those capabilities belong solely to the org admin.

The User Access administrator role is a special role that the org admin can assign. This role allows users who are not org admin users to manage User Access on cloud.redhat.com.

1.2. ADDITIVE ACCESS

User access on cloud.redhat.com uses an additive model, which means that there are no deny roles. In other words, actions are only permitted. You control access by assigning the appropriate roles with the desired permissions to groups then adding users to those groups. The access permitted to any individual user is a sum of all roles assigned to all groups to which that user belongs.

1.3. THE USER ACCESS GROUPS, ROLES, AND PERMISSIONS

User Access uses the following categories to determine the level of user access that an org admin can grant to the supported cloud.redhat.com services. The access provided to any authorized user depends on the group that the user belongs to and the roles assigned to that group.

- **Group**: A collection of users belonging to an account which provides the mapping of roles to users. An org admin can use groups to assign one or more roles to a group and to include one or more users in a group. You can create a group with no roles and no users.

- **Roles**: A set of permissions that provide access to a given service, such as Insights. The permissions to perform certain operations are assigned to specific roles. Roles are assigned to groups. For example, you might have a read role and a write role for a service. Adding both roles to a group grants all members of that group read and write permissions to that service.

- **Permissions**: A discrete action that can be requested of a service. Permissions are assigned to roles.

An org admin adds or deletes roles and users to groups. The group can be a new group created by an org admin or the group can be an existing group. By creating a group that has one or more specific roles and then adding users to that group, you control how that group and its members interact with the cloud.redhat.com services.

When you add users to a group, they become members of that group. A group member inherits the roles of all other groups they belong to. The user interface lists users in the Members tab.
CHAPTER 2. SETTING USER PREFERENCES

You can set or update your email preferences as follows.

Procedure

1. Click the user menu located on the upper-right side, then go to User preferences → Email preferences. The Email preferences screen opens.

    Alternatively, on the {PRODUCTNAME} dashboard, in the left-side navigation panel at the top, click “Red Hat Insights”, and then click “User Preferences”. The Email preferences screen opens.

2. Depending on your email notification preference, you can subscribe to Instant notification emails for each system with triggered policies and/or Daily digest (summary) of all systems with triggered policies. On this page, you can also select your preference for other https://cloud.redhat.com emails you want to receive.

    NOTE

    Subscribing to instant notification can result in receiving many emails on large inventories, that is, one email per system checking in.

3. Click Submit.
3.1. HOW HOOKS SENDS NOTIFICATIONS ABOUT CHANGES IN YOUR INSIGHTS SYSTEM INVENTORY

**IMPORTANT**

Hooks integration on cloud.redhat.com currently is only available as Beta.

Webhooks, or simply hooks, enables Red Hat Insights to send event-driven notifications to a customer’s own hooks-compatible tooling as those events occur. These real-time event notifications free administrators from having to check the Insights user interface routinely to look for notifications. The automatic notifications enable Insights to have an event-driven monitoring strategy.

Policies integrate with Insights webhooks for their actions. Webhooks are responsible for sending POST messages as notifications to third-party applications that support incoming webhooks integration. Examples of such applications include instant messaging platforms and external ticketing systems. This enables users to integrate cloud.redhat.com into the operational workflow used at their site.

**NOTE**

- Use the Role Based Access Control (RBAC) capability in [https://cloud.redhat.com](https://cloud.redhat.com) (Settings > User access) to control user access for Policies.

- See [Role Based Access Control for Red Hat Insights and cloud management services for Red Hat Enterprise Linux](https://cloud.redhat.com) for more information about this feature and example use cases.
CHAPTER 4. SYSTEM TAGS AND GROUPS

Red Hat Insights enables administrators to filter systems in inventory and in individual services using group tags. Groups are identified by the method of system data ingestion to Insights. Insights enables filtering groups of systems by those running SAP workloads, by Satellite host group, and by custom tags that are defined by system administrators with root access to configure the Insights client on the system.

NOTE

As of Fall 2020, Inventory, Advisor, Vulnerability, Patch, Drift, and Policies enable filtering by groups and tags. Other services will follow.

Use the global, Search tags box to filter by SAP workloads, Satellite host groups, or custom tags added to the Insights client configuration file.

Prerequisites

The following prerequisites and conditions must be met to use the tagging features in Red Hat Insights:

- The Red Hat Insights client is installed and registered on each system.
To create custom tags, root permissions, or their equivalent, are required to add to or change the `/etc/insights-client/tags.yaml` file.

### 4.1. TAG STRUCTURE

Tags use a **namespace/key=value** paired structure.

- **Namespace.** The namespace is the name of the ingestion point, *insights-client*, and cannot be changed. The `tags.yaml` file is abstracted from the namespace, which is injected by the client before upload.

- **Key.** The key can be a user-chosen key or a predefined key from the system. You can use a mix of capitalization, letters, numbers, symbols and whitespace.

- **Value.** Define your own descriptive string value. You can use a mix of capitalization, letters, numbers, symbols and whitespace.
CHAPTER 5. SYSTEM STALENESS AND DELETION

System deletion is the automated removal of systems from the Red Hat Insights inventory after all sources stop reporting information about it for a defined period of time.

System staleness is reporting when a system has missed check-ins for a defined period of time but is not yet deleted.

5.1. RULES FOR SYSTEM STALENESS AND DELETION

The inventory reporting service, as part of their messaging, includes a timestamp for when the report about the host is considered stale. This timestamp is determined by the reporting service and defaults to a value set by the user account.

When various reporters contribute data to the host in the host inventory, staleness states are recalculated.

Systems in the inventory have the following three fields related to staleness and deletion:

- "stale_timestamp": "2019-12-13T19:36:30.979Z"
- "stale_warning_timestamp": "2019-12-13T19:36:30.979Z"
- "culled_timestamp": "2019-12-13T19:36:30.978Z"

Rules:

- Before the stale_timestamp is reached, a system is considered fresh
- Between the stale_timestamp and stale_warning_timestamp, a system is considered stale
- Between the stale_warning_timestamp and culled_timestamp, a system is considered in the “stale warning” state and is scheduled for deletion
- After the culled_timestamp is reached, a system and all associated data are automatically deleted

5.2. VIEWING STALE SYSTEM SUMMARY

You can see stale systems and the ones scheduled for deletion in the following places in the Red Hat Insights user interface:

Dashboard: In the Red Hat Insights dashboard summary, you can see the number of stale systems and the number of systems scheduled for deletion displayed under System inventory. Click on the respective links to see the list of stale systems and the ones marked for deletion.

Inventory: On the last seen column, you will see systems marked for deletion with a warning icon. Hover on the last seen information to see if a system will be removed from the inventory in the next x days or if it is already scheduled for deletion.

5.3. FILTERING SYSTEM INVENTORY

You can filter the inventory by system status: Fresh, Stale, and Stale warning. Note that by default fresh and stale systems are listed, but stale warning systems are not shown in the user interface. You can also select the source, which is Insights by default, and filter by system name. You can remove a particular
filter in effect, or clear all at once.
CHAPTER 6. CONFIGURING SOURCES FOR RED HAT SERVICES

A data source is a service, application, or provider that supplies data to a Red Hat cloud platform application or service. Sources comprise cloud sources and Red Hat sources.

6.1. ABOUT SOURCES

Sources are how the services and applications on cloud.redhat.com connect with public cloud providers and other services or tools to collect information for the service or application. You add and manage sources in the Sources application located within the Settings bundle. You can access Settings by clicking the gear icon in the masthead on cloud.redhat.com.

The Sources menu uses a wizard to help you add cloud sources and Red Hat sources. For cloud sources, you can associate the provider with Red Hat applications, such as Cost Management and the RHEL management bundle. For Red Hat sources, you can add Red Hat OpenShift Container Platform. Adding applications is optional for cloud sources but is required for Red Hat sources.

6.2. ADDING CLOUD SOURCES

The Add a cloud source wizard steps you through creating a source. You can add Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. The wizard provides detailed information for each public cloud provider.

Amazon Web Services

The workflow for adding AWS as a cloud source includes the following high-level steps:

1. Selecting the source type
2. Naming the source
3. Selecting the configuration
4. Selecting applications
5. Configuring cost and usage reporting (for Cost Management)
6. Identifying tags, aliases, and organizational units (for Cost Management)
7. Enabling account access
8. Reviewing details
9. Adding the source

You have two choices for the configuration mode: * Account authorization (recommended) * Manual configuration

If you select Account authorization, you provide your AWS account credentials (Access key ID and Secret key ID) and Red Hat configures and manages your source for you. This option automatically selects the Cost Management and RHEL management applications. You can deselect these applications.
If you select **Manual configuration**, you choose **Cost Management**, **RHEL management** bundle, or **No application**.

The **Cost Management** application allows you to perform financially related tasks, such as:

- Visualizing, understanding, and analyzing the use of resources and costs
- Forecasting your future consumption and comparing them with budgets
- Optimizing resources and consumption
- Identifying patterns of usage for further analysis
- Integrating with third-party tools that can benefit from cost and resourcing data

The **RHEL management** bundle includes the following items:

- Red Hat gold images
- High precision subscription watch data
- Autoregistration

Cost Management and RHEL management require you to enable account access. You accomplish this by creating an IAM policy, an IAM role, and entering your Amazon Resource Name (ARN). An ARN is a generic name for an Amazon resource and has a common format depending on the service involved. In this case, it is the identity and access management (IAM) service and Role resource-type.

If you select **No application**, you choose which credentials to supply:

- AWS Secret key
- Cost Management ARN
- Subscription Watch ARN

**Google Cloud**

The workflow for adding Google Cloud as a cloud source includes the following high-level steps:

1. Selecting the source type
2. Naming the source
3. Selecting applications
4. Adding a project
5. Enabling account access
6. Creating a dataset
7. Setting up billing export information
8. Reviewing details
9. Adding the source
Cost Management is the only application choice. You must create an IAM role and assign access.

The **Cost Management** application allows you to perform financially related tasks, such as:

- Visualizing, understanding, and analyzing the use of resources and costs
- Forecasting your future consumption and comparing them with budgets
- Optimizing resources and consumption
- Identifying patterns of usage for further analysis
- Integrating with third-party tools that can benefit from cost and resourcing data

If you select **No application**, you provide the Project ID and the Service Account JSON as credentials.

**Microsoft Azure**

The workflow for adding Microsoft Azure as a cloud source includes the following high-level steps:

1. Selecting the source type
2. Naming the source
3. Selecting applications
4. Creating a resource group and a storage account (for Cost Management)
5. Entering a Subscription ID (for Cost Management)
6. Creating roles (for Cost Management)
7. Setting up daily exports (for Cost Management)
8. Providing credentials
9. Reviewing details
10. Adding the source

Application choices include **Cost Management**, **RHEL management** bundle, or **No application**.

The **Cost Management** application allows you to perform financially related tasks, such as:

- Visualizing, understanding, and analyzing the use of resources and costs
- Forecasting your future consumption and comparing them with budgets
- Optimizing resources and consumption
- Identifying patterns of usage for further analysis
- Integrating with third-party tools that can benefit from cost and resourcing data

The **RHEL management** bundle includes the following items:

- Red Hat gold images
Autoregistration

You create a dedicated resource group and a storage account in the Azure Portal so you can collect cost data and metrics for cost management. You then use your subscription ID to create a Cost Management Storage Account Contributor role in the Cloud Shell. Using the subscription ID to run a second command in the Cloud Shell gives you the tenant (directory) ID, client (application) ID, and client secret necessary to complete setting up that role.

NOTE

Configure dedicated credentials to grant cost management read-only access to Azure cost data.

6.3. ADDING RED HAT SOURCES

The workflow for adding Red Hat OpenShift Container Platform as a cloud source includes the following high-level steps:

1. Selecting the source type and application
2. Naming the source
3. Installing and configuring the operator
4. Reviewing the details
5. Adding the source

Cost Management is the only application choice. The Cost Management application allows you to perform financially related tasks, such as:

- Visualizing, understanding, and analyzing the use of resources and costs
- Forecasting your future consumption and comparing them with budgets
- Optimizing resources and consumption
- Identifying patterns of usage for further analysis
- Integrating with third-party tools that can benefit from cost and resourcing data

NOTE

For Red Hat OpenShift Container Platform 4.6 and later, install the costmanagement-metrics-operator from the OpenShift Container Platform web console. For more information, see Adding an OpenShift Container Platform source to cost management.

6.4. SOURCES REFERENCE MATERIAL

Getting started with cost management
Getting Started with Subscription Watch
Adding sources for public cloud metering
Getting started with Automation Services Catalog

Bucket restrictions and limitations

Bucket naming rules