Subscription Central 1-latest

Getting started with activation keys on the Hybrid Cloud Console

Subscription Central 1-latest Getting started with activation keys on the Hybrid Cloud Console

Red Hat Customer Content Services

Legal Notice

Abstract

Administrative users in your organization can create, configure, edit, and delete activation keys in the Red Hat Hybrid Cloud Console. When a preconfigured activation key is used to register a system from the command line, all of the system-level feature configurations set on the activation key are automatically applied to the system during the registration process.

Table of Contents

CHAPTER 1. CREATING AND MANAGING ACTIVATION KEYS

An activation key is a preshared authentication token that enables authorized users to register and auto-configure systems. Running a registration command with an activation key and organization ID combination, instead of a username and password combination, increases security and facilitates automation.

Administrative users in your organization can create and manage activation keys on the Red Hat Hybrid Cloud Console. When an authorized user enters a preconfigured activation key to register a system on the command line, all of the system-level settings configured on the activation key are automatically applied to the system during the registration process. You can also use an activation key in a Kickstart file to bulk-provision the registration of multiple Red Hat Enterprise Linux (RHEL) instances without exposing personal username and password values.

Your organization's activation keys and organization ID are displayed on the Activation Keys page in the Hybrid Cloud Console.

Each user's access to your organization's activation keys is managed through a role-based access control (RBAC) system for the Hybrid Cloud Console. For example:

- Only users with the RHC user role can view the activation keys on the Activation Keys page.

- Only users with the RHC administrator role can create, configure, edit, and delete activation keys.

- Only users with root privileges or their equivalent can enter an activation key and organization ID with a registration command to connect and automatically configure systems from the command line.

Users in the Organization Administrator group for your organization use the RBAC system to assign roles to other users in your organization. An Organization Administrator has the RHC administrator role by default. If you have questions about your access permissions, ask an Organization Administrator in your organization.

1.1. VIEWING AN ACTIVATION KEY

With the RHC user role, you can view your organization's numeric identifier (organization ID) and available activation keys on the Activation Keys page in the Hybrid Cloud Console. You can also view additional details, such as the Workload setting and additional enabled repositories for each activation key in your organization.

The **Key Name** column shows the unique name of the activation key.

The **Role** column shows the role value for the system purpose attribute set on the key. A potential role value is *Red Hat Enterprise Linux Server* .

The **SLA** column shows the service level agreement value for the system purpose attribute set on the key. A potential service level agreement value is *Premium*.

The **Usage** column shows the usage value for the system purpose attribute that is set on the key. A potential usage value is *Production*.

If the RHC administrator sets no system purpose attributes on the activation key, then the Role, SLA, and Usage columns show no values.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

- You have the RHC user or RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To view the activation keys for your organization in the Hybrid Cloud Console, complete the following step:

- From the Hybrid Cloud Console home page, click **Services** > **System Configuration** > **Activation Keys**.
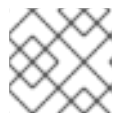
> **NOTE**
>
> Activation keys are listed alphabetically by default.

1.2. CREATING AN ACTIVATION KEY

With the RHC administrator role, you can use the Hybrid Cloud Console interface to create activation keys that root users in your organization can use as an authentication token. During the creation process, you can configure the activation key to set system-level features, such as system purpose attributes, to host systems. When an authorized user uses the preconfigured activation key to register a system to Red Hat, the selected attributes are automatically applied to the system during the registration process.

The activation key creation wizard guides you through the following fields:

- **Name**
  The activation key name uniquely identifies it. You can use this name to locate the key in the table on the **Activation Keys** page or to specify the key in a CLI command or automation script.

- **Workload**
  The workload associates the appropriate selection of repositories to the activation key. You can edit these repositories on the activation key details page after the key is created. When creating an activation key, you can select either **Latest release** or **Extended support** for the workload. **Latest release** is selected by default. If your account has subscriptions that are eligible for extended update support (EUS), then you can select **Extended support** and then select an EUS product and version available to your account. If your account does not have any subscriptions that are eligible for EUS, then the **Extended supported** option is disabled.

- **System purpose**
  The subscriptions service uses system purpose values to filter and identify hosts. You can set values for the **Role**, **Service Level Agreement (SLA)**, and **Usage** attributes to ensure that subscriptions are accurately reported for the system. You can select the system purpose values that are available to your account from the drop-down menus.

- **Review**
  You can review your entries and selections for each field before creating the activation key. If you do not select a value for an optional field, then the default value is **Not defined**.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To create an activation key in the Hybrid Cloud Console, complete the following steps:

1. From the Hybrid Cloud Console home page, click **Services** > **System Configuration** > **Activation Keys**.

2. From the Activation Keys page, click **Create activation key**.

3. In the **Name** field, enter a unique name for the activation key. Click **Next**.

   > **NOTE**
   >
   > If you enter a name that already exists for an activation key in your organization, then you will receive an error message and the key will not be created.

4. Select a workload option to associate the appropriate selection of repositories with the activation key. Click **Next**.

5. Optional: In the **Role**, **Service Level Agreement (SLA)**, and **Usage** fields, select the system purpose attribute value that you want to set on the activation key. Click **Next**.

   > **NOTE**
   >
   > Only the system purpose attributes that are available to your organization's account are selectable.

6. Review the information that you entered into each field. If the information is correct, click **Create**.

7. To make changes to the activation key settings or to enable additional repositories, click **View activation key**.
   The activation key details page opens.

Verification

The new activation key is listed on the Activation Keys page of the Hybrid Cloud Console.

1.3. ENABLING ADDITIONAL REPOSITORIES ON AN ACTIVATION KEY

By default, your system has access to content repositories that contain software packages that you can use to set up and manage your system. However, enabling additional repositories gives your system access to features and capabilities beyond the default repositories.

It is no longer necessary to use command line tools to manually enable your system to access additional content repositories or to use automation scripts after the system is registered. With the RHC administrator role, you can use the Red Hat Hybrid Cloud Console interface to add selected repositories to an exisiting activation key. When a root user uses a preconfigured activation key to register a system from the command line, any content repositories that have been added to the activation key are automatically enabled for system access during the registration process.

Using an activation key to automate the repository enablement process allows you to configure multiple system settings in one place for simplified system management. You can also use activation keys to apply system settings to multiple instances of Red Hat Enterprise Linux (RHEL) for automated bulk provisioning.

Users with the RHC user role can see all the repositories that are associated with each activation key, but only users with the RHC administrator role can perform management functions, such as adding or deleting repositories on an activation key. If you have questions about your access permissions, contact a user in your organization with the Organization Administrator role in the Hybrid Cloud Console role-based access control (RBAC) system.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To enable additional repositories on an activation key in the Hybrid Cloud Console, complete the following steps:

1. From the Hybrid Cloud Console home page, click **Services** > **System Configuration** > **Activation Keys**.

2. From the **Activation Keys** table, click the name of the activation key that you want to configure with additional repositories.

   > **NOTE**
   >
   > Only users with the RHC user role can click an activation key to view its details. If you have questions about your access permissions, contact a user in your organization with the Organization Administrator RBAC role.

3. From the **Additional repositories** table, click **Add repositories**.

   > **NOTE**
   >
   > Only users with the RHC administrator role can add or delete enabled repositories on an activation key. If you do not have sufficient access permissions to complete this step, **Add repositories** is disabled. If you have questions about your access permissions, contact a user in your organization with the Organization Administrator RBAC role.

4. Select each additional repository that you want to enable with the activation key.

5. Click **Save Changes**.

Result

If a RHC administrator has enabled additional repositories on an activation key, then those repositories are listed in the **Additional repositories** table for the selected activation key.

1.4. EDITING AN ACTIVATION KEY

With the RHC administrator role, you can use the Hybrid Cloud Console interface to edit the activation keys on the **Activation Keys** page. Specifically, you can add, change, or remove the following configurations on an existing activation key:

- System purpose attributes

- Workload, such as the release version of your system

- Additional enabled repositories

> **NOTE**
>
> You cannot edit the name of the activation key after it has been created.

1.4.1. Editing system purpose settings on an activation key

You can change the system purpose configuration on an existing activation key by selecting a different system purpose attribute value from the **Role**, **Service Level Agreement (SLA)**, or **Usage** drop-down list. Possible selections for each attribute include the following values:

Role

- Red Hat Enterprise Linux Server

- Red Hat Enterprise Linux Workstation

- Red Hat Enterprise Linux Compute Node

- Not defined

Service Level Agreement (SLA)

- Premium

- Standard

- Self-Support

- Not defined

Usage

- Production

- Development/Test

- Not defined

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To edit the system purpose attributes on an activation key, complete the following steps:

1. From the Hybrid Cloud Console home page, click **Services** > **System Configuration** > **Activation Keys**.

2. From the **Activation Keys** table, click the name of the activation key that you want to edit.

3. From the System Purpose section of the activation key details page, click **Edit**.

4. Select the value from the Role, SLA, or Usage drop-down list that you want to set on the activation key. Click **Save changes**.

1.4.2. Editing workload settings on an activation key

You can change the workload configuration on an existing activation key by selecting a different value from the **Release version** drop-down list. Possible selections for the workload include the following RHEL release versions:

- 8.1

- 8.2

- 8.4

- 8.6

- 8.8

- 9.0

- 9.2

- Not defined

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To edit the workload setting on an activation key, complete the following steps:

1. From the Hybrid Cloud Console home page, click **Services** > **System Configuration** > **Activation Keys**.

2. From the **Activation Keys** table, click the name of the activation key that you want to edit.

3. From the Workload section of the activation key details page, click **Edit**.

4. Select the value from the **Release version** drop-down list that you want to set on the activation key.

5. Click **Save changes**.

1.5. DELETING AN ACTIVATION KEY

With the RHC administrator role, you can use the Hybrid Cloud Console interface to delete an activation key from the table on the Activation Keys page. You might want to delete an unwanted or compromised activation key for security or maintenance purposes. However, deleting an activation key that is

referenced in an automation script will impact the ability of that automation to function. To avoid any negative impacts to your automated processes, complete one of the following actions:

- Remove the unwanted activation key from the automation script.

- Retire the automation script prior to deleting the key.

Prerequisites

- You are logged in to the Red Hat Hybrid Cloud Console.

- You have the RHC administrator role in the role-based access control (RBAC) system for the Red Hat Hybrid Cloud Console.

Procedure

To delete an activation key in the Hybrid Cloud Console, complete the following steps:

1. From the Hybrid Cloud Console home page, click **Services** > **System Configuration** > **Activation Keys**.

2. From the Activation Keys page, locate the row containing the activation key that you want to delete. Click the **Delete** icon.

3. In the Delete Activation Key window, review the information about deleting activation keys. If you want to continue with the deletion, click **Delete**.

CHAPTER 2. USING ACTIVATION KEYS

With root privileges, you can use an activation key with a registration command to connect your system to Red Hat from the command line. Using an activation key and organization ID combination instead of a username and password combination increases security and facilitates automation. If an RHC administrator has preconfigured the activation key with system-level features, then the selected features are automtically applied to the system during the registration process.

Additional resources

- For more information about using activation keys to register your system to Red Hat, see Registering a RHEL system with command line tools in Getting Started with RHEL System Registration

- For more information about using activation keys with automation scripts, see Automating RHEL system registration with a Kickstart file in Getting Started with RHEL System Registration

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. To provide feedback, open a Jira issue that describes your concerns. Provide as much detail as possible so that your request can be addressed quickly.

Prerequisites

- You have a Red Hat Customer Portal account. This account enables you to log in to the Red Hat Jira Software instance. If you do not have an account, you will be prompted to create one.

Procedure

To provide your feedback, perform the following steps:

1. Click the following link: Create Issue.

2. In the **Summary** text box, enter a brief description of the issue.

3. In the **Description** text box, provide more details about the issue. Include the URL where you found the issue.

4. Provide information for any other required fields. Allow all fields that contain default information to remain at the defaults.

5. Click **Create** to create the Jira issue for the documentation team.

A documentation issue will be created and routed to the appropriate documentation team. Thank you for taking the time to provide feedback.