Red Hat Insights 1-latest

Remote Host Configuration and Management

Using the remote host configuration and management features for Red Hat Insights

Last Updated: 2024-10-23

Red Hat Insights 1-latest Remote Host Configuration and Management

Using the remote host configuration and management features for Red Hat Insights

Legal Notice

Abstract

This guide is for RHEL system administrators who want to use remote host configuration to register RHEL systems with services on the Red Hat Hybrid Cloud Console platform. 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 .

Table of Contents

CHAPTER 1. INTRODUCING REMOTE HOST CONFIGURATION AND MANAGEMENT

Remote host configuration is a powerful tool that enables the following capabilities:

- **Easy registration.** With the rhc client, you can register systems to Red Hat Subscription Management (RHSM) and Red Hat Insights for Red Hat Enterprise Linux.
- **Configuration management.** Using the remote host configuration manager, you can configure the connection with Insights for Red Hat Enterprise Linux for all of the Red Hat Enterprise Linux (RHEL) systems in your infrastructure. You can enable or disable the rhc client, direct remediations, and other application settings from Insights for Red Hat Enterprise Linux.
- **Remediations from Insights for Red Hat Enterprise Linux.**When systems are connected to Insights for Red Hat Enterprise Linux with the rhc client, you can manage the end-to-end experience of finding and fixing issues. Registered systems can directly consume remediation playbooks executed from the Insights for Red Hat Enterprise Linux application.

Supported configurations

- The rhc client is supported on systems registered to Insights for Red Hat Enterprise Linux and running Red Hat Enterprise Linux (RHEL) 8.5 and later, and RHEL 9.0 and later.
- Single-command registration is supported by RHEL 8.6 and later, and RHEL 9.0 and later.

1.1. REMOTE HOST CONFIGURATION COMPONENTS

The complete remote host configuration solution comes with two main components: a client-side daemon and a server-side service to facilitate system management.

- **The remote configuration client.** The rhc client comes preinstalled with all Red Hat Enterprise Linux (RHEL) 8.5 and later installations, with the exception of minimal installation. The rhc client consists of the following utility programs:
  - The **rhcd** daemon runs on the system and listens for messages from the Red Hat Hybrid Cloud Console. It also receives and executes remediation playbooks for systems that are properly configured.
  - The **rhc** command-line utility for RHEL.
- **The remote host configuration manager.** With the remote host configuration manager user interface, you can enable or disable Insights for Red Hat Enterprise Linux connectivity and features.

To maximize the value of remote host configuration, you must install additional packages. To allow systems to be managed by remote host configuration manager and to support the execution of remediation playbooks, install the following additional packages:

- **ansible** or **ansible-core**
- **rhc-worker-playbook**

IMPORTANT

Starting with RHEL 8.6 and RHEL 9.0, the **ansible-core** and **rhc-worker-playbook** packages should automatically be installed in the background to make your system fully manageable from the remote host configuration manager user interface. However, a known bug is preventing the process from completing as expected. Thus, the packages must be installed manually after registration.

1.2. USER ACCESS SETTINGS IN THE RED HAT HYBRID CLOUD CONSOLE

User Access is the Red Hat implementation of role-based access control (RBAC). Your Organization Administrator uses User Access to configure what users can see and do on the Red Hat Hybrid Cloud Console (the console):

- Control user access by organizing roles instead of assigning permissions individually to users.
- Create groups that include roles and their corresponding permissions.
- Assign users to these groups, allowing them to inherit the permissions associated with their group's roles.

1.2.1. Predefined User Access groups and roles

To make groups and roles easier to manage, Red Hat provides two predefined groups and a set of predefined roles.

1.2.1.1. Predefined groups

The **Default access group** contains all users in your organization. Many predefined roles are assigned to this group. It is automatically updated by Red Hat.

NOTE

If the Organization Administrator makes changes to the **Default access** group its name changes to **Custom default access** group and it is no longer updated by Red Hat.

The **Default admin access** group contains only users who have Organization Administrator permissions. This group is automatically maintained and users and roles in this group cannot be changed.

On the Hybrid Cloud Console navigate to Red Hat Hybrid Cloud Console > the **Settings** icon (⚙) > Identity & Access Management > User Access > Groups to see the current groups in your account. This view is limited to the Organization Administrator.

1.2.1.2. Predefined roles assigned to groups

The **Default access** group contains many of the predefined roles. Because all users in your organization are members of the **Default access** group, they inherit all permissions assigned to that group.

The **Default admin access** group includes many (but not all) predefined roles that provide update and delete permissions. The roles in this group usually include **administrator** in their name.

On the Hybrid Cloud Console navigate to Red Hat Hybrid Cloud Console > the **Settings** icon (⚙) > Identity & Access Management > User Access > Roles to see the current roles in your account. You can see how many groups each role is assigned to. This view is limited to the Organization Administrator.

See *User Access Configuration Guide for Role-based Access Control (RBAC)* for additional information.

1.2.2. Access permissions

The **Prerequisites** for each procedure list which predefined role provides the permissions you must have. As a user, you can navigate to Red Hat Hybrid Cloud Console > the **Settings** icon (⚙) > My User Access to view the roles and application permissions currently inherited by you.

If you try to access Insights for Red Hat Enterprise Linux features and see a message that you do not have permission to perform this action, you must obtain additional permissions. The Organization Administrator or the User Access administrator for your organization configures those permissions.

Use the Red Hat Hybrid Cloud Console Virtual Assistant to ask "Contact my Organization Administrator". The assistant sends an email to the Organization Administrator on your behalf.

1.2.3. User Access roles for remote host configuration and management

There are several User Access roles that are relevant for Red Hat Insights for Red Hat Enterprise Linux users. These roles determine if an Insights user can simply view settings or change them, and use remediation features.

User Access roles for using the Remote Host Configuration Manager in the Insights for Red Hat Enterprise Linux web console

- **RHC administrator.** Members in a group with this role can perform any operations in the rhc manager.
- **RHC user.** This is a default permission for all users on your organization's Red Hat Hybrid Cloud Console account, allowing anyone to see the current status of the configuration.

User Access roles for using remediation features in the Insights for Red Hat Enterprise Linux web console

- **Remediations administrator.** Members in a group with this role can perform any available operation against any remediations resource, including direct remediations.
- **Remediations user.** Members in a group with this role can create, view, update, and delete operations against any remediations resource. This is a default permission given to all Hybrid Cloud Console users on your account.

CHAPTER 2. REGISTER AND CONNECT RHEL SYSTEMS USING THE RHC CLIENT

The rhc client performs critical system tasks, such as registering your system to the Red Hat Hybrid Cloud Console, retrieving the current configuration of various services that the remote host configuration manager supports, and updating the current configuration of services. It also maintains a history of configuration changes, and ensures that newly connected systems are kept up to date with the latest configuration.

The rhc client updates a system through a change in the remote host configuration manager, and through a new remote host configuration connection event from Red Hat Insights for Red Hat Enterprise Linux inventory.

NOTE

Currently, settings apply to all systems connected with the rhc client. You cannot configure a system or group of systems independently.

Before configuring your system to connect using the rhc client, review the configuration in Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Remote Host Configuration (RHC). The remote host configuration manager settings determine your system's configuration.

RHEL version considerations

Setup procedures for the rhc client differ depending on the Red Hat Enterprise Linux (RHEL) version on the system.

- RHEL 8.6 and later, and RHEL 9.0 and later support simplified registration to Red Hat Subscription Management (RHSM) and Insights for Red Hat Enterprise Linux .
- RHEL 8.5 supports the other features of remote host configuration, but configuration and setup involve a few more steps.

Timing of registration

To register the system to Red Hat Subscription Management (RHSM) and Insights for Red Hat Enterprise Linux with a single command, it might make sense to run the **rhc connect** command during the RHEL installation workflow, following network configuration. For RHEL 8.6 and later, this step will take care of the registration to Red Hat Subscription Management (RHSM), but you may still use RHSM for advance configurations.

If you have already installed and registered the RHEL installation with RHSM, or registered with Insights for Red Hat Enterprise Linux, you can still use **rhc connect** to enable the rhc client at any time to get the benefits of the remote host configuration manager and direct remediations.

Additional resources

- Client Configuration Guide for Red Hat Insights
- Creating Red Hat Customer Portal Activation Keys
- Getting Started with RHEL System Registration
- Performing an advanced RHEL installation

- Performing a standard RHEL installation
- Registration Assistant - a registration method that uses a guided lab in *Red Hat Customer Portal Labs*.

2.1. SETTING UP REMOTE HOST CONFIGURATION

The remote host configuration tool is evolving rapidly for multiple major and minor versions of Red Hat Enterprise Linux. For the latest installation instructions, see the knowledge article, Registering your host using RHC. The article will be updated as changes are made for various RHEL versions.

Additional resources

- Product Documentation for Red Hat Enterprise Linux 8
- Product Documentation for Red Hat Enterprise Linux 9

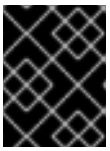
2.2. DISCONNECTING A SYSTEM USING REMOTE HOST CONFIGURATION

Prerequisites

- You are logged in to the system as **root** or have sudo permissions.

Procedure

- Run the following command on each Red Hat Enterprise Linux (RHEL) system that you want to remove from the remote host configuration manager.



IMPORTANT

Disconnecting through the rhc client unregisters your system from both the Red Hat Customer Portal and Red Hat Insights for Red Hat Enterprise Linux.

```
# rhc disconnect

Disconnecting <$HOSTNAME> from console.redhat.com.
This might take a few seconds.

• Deactivated the Red Hat connector daemon

Manage your Red Hat connector systems: https://red.ht/connector
```

2.3. USING ADDITIONAL CLI OPTIONS

View additional options for the **rhc** command.

Prerequisites

- You are logged in to the system as **root** or have sudo permissions.

Procedure

- Run **ps** and pipe through **grep** to display the connector **rhcd** process.

```
PID TTY TIME COMMAND
14992 ? 0:00 /usr/sbin/rhcd
```

- Run **systemctl status rhcd** to view the on/off status of the **rhcd daemon**.

```
# systemctl status rhcd
```

- Enter **rhc --help** with no other options.

```
GLOBAL OPTIONS:
   --version, -v  print the version (default: false)
```

CHAPTER 3. CONFIGURE CONNECTION TO RED HAT INSIGHTS USING REMOTE HOST CONFIGURATION MANAGER

The remote host configuration manager, located at Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Remote Host Configuration (RHC), is where you can control Red Hat Enterprise Linux system connections to Red Hat Insights for Red Hat Enterprise Linux. From the remote host configuration manager, you control the connection to your RHEL infrastructure, and how the Insights for Red Hat Enterprise Linux services are configured on the remote systems.

Changes in the remote host configuration manager create a playbook that is fetched by the rhc client. The connected rhc client monitors for remote host configuration manager to send playbooks and will execute them instantaneously. The remote host configuration manager provides a log that shows you the playbook runs.

With the rhc client and the remote host configuration manager, there is no fine control over individual system connections, and there is no additional control over the data that is packaged on your systems and uploaded to Insights for Red Hat Enterprise Linux.

To control the type of data that each system provides to Insights for Red Hat Enterprise Linux, you must use the Insights client configuration options. For example, if you want to apply data obfuscation or data redaction to the system information that is sent to Insights for Red Hat Enterprise Linux, you must configure the obfuscation and redaction values in the Insights client configuration file on each system.

3.1. OPENING THE REMOTE HOST CONFIGURATION MANAGER

Use the remote host configuration manager to view connection settings.

The first time you open the manager, it shows a pane for **rhc** command syntax that you can fill in and copy. This will simplify command entry on your Red Hat Enterprise Linux (RHEL) systems if they are not already running the remote host configuration utility. You can close this pane, but it cannot be reopened.

Prerequisites

- You must be logged into the Red Hat Hybrid Cloud Console.
- You must have **RHC user** privileges, assigned in User Access, to perform this procedure.

Procedure

- Navigate to Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Remote Host Configuration (RHC) to view the Red Hat Insights for Red Hat Enterprise Linux connection settings.

3.2. EDITING SETTINGS IN THE REMOTE HOST CONFIGURATION MANAGER

Use the remote host configuration manager to edit remote host configuration settings. You can enable or disable whether your RHEL systems receive remediation playbooks and rhc client configuration changes from remote host configuration manager. If you want to maintain your client configurations manually, or with your own configuration management system, you may disable the system configuration management settings.

You can enable settings to use OpenSCAP for compliance policies and Cloud Connector to fix issues directly from Red Hat Insights for Red Hat Enterprise Linux. Enabling OpenSCAP automatically installs the OpenSCAP and RHEL System Security Guide (SSG), required to use the compliance service.

Prerequisites

- You must be logged into the Red Hat Hybrid Cloud Console.
- You must have **RHC administrator** privileges, assigned in User Access, to perform this procedure.

Procedure

1. Navigate to Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Remote Host Configuration (RHC) to view the current settings.
2. Click **Change settings**.
3. Use the slider buttons to select Red Hat Insights for Red Hat Enterprise Linux settings for your connected systems. The changes are applied to all connected systems and to all future systems that connect through the rhc client.

3.3. MAINTAINING A CONNECTION BETWEEN REMOTE HOST CONFIGURATION AND RED HAT HYBRID CLOUD CONSOLE

To maintain a strong connection between remote host configuration(rhc) and Red Hat Hybrid Cloud Console, it is recommended that you set an option for a 10 second reconnect delay.

Prerequisites

- You have root-level access to the system or **sudo** permissions.
- You have a rhc version installed that is at least version 0.2.4 but less than version 0.3.

Procedure

- Open the following file: **/etc/rhc/config.toml**
- Add this option to the file **mqtt-reconnect-delay = "10s"**
- Save your changes.
- Type the following command in your terminal: # **systemctl restart rhcd.service**

Verification step

Run the following command in your terminal:

```
#`systemctl status rhcd.service`
```

If the option was added successfully, you should see the following statement returned:

```
# `Active: active (running)` followed by a timestamp.
```

Additional resources

For information about registering rhc, see the following:

Registering your host using rhc

CHAPTER 4. REMEDIATE ISSUES DIRECTLY FROM INSIGHTS FOR RED HAT ENTERPRISE LINUX

Remote host configuration (rhc) allows you to remediate issues on your Red Hat Enterprise Linux (RHEL) systems directly from Insights for Red Hat Enterprise Linux. Direct remediation is available when you have the rhc client installed on your RHEL 8.5 and later system.

For complete remediations documentation for Red Hat Insights, see the *Red Hat Insights Remediations Guide*.

CHAPTER 5. TROUBLESHOOTING REMOTE HOST CONFIGURATION ISSUES

System logs are a useful source of information when troubleshooting a remote host configuration issue. In addition, it is helpful to be aware of any known issues.

5.1. TCP PORTS AND DESTINATIONS

The complete remote host configuration solution currently relies on existing clients; your system will be communicating with Red Hat in different ways.

5.1.1. Subscription manager

For subscription-manager, the system must be able to reach the following destination and TCP ports:

- subscription.rhn.redhat.com:443 (https)
- subscription.rhsm.redhat.com:443 (https)
- cdn.redhat.com:443 (https)
- *.akamaiedge.net:443 (https)
- *.akamaitechnologies.com:443 (https)

5.1.2. Insights client

For Red Hat Insights for Red Hat Enterprise Linux data collection to work correctly, the system must be able to reach the following destination and TCP ports:

- api.access.redhat.com:443 (https)
- cert-api.access.redhat.com:443 (https)

5.1.3. RHC client daemon

For the rhc daemon, **rhcd**, to communicate with the MQTT message broker, the system must be able to reach the following:

- connect.cloud.redhat.com:443 (https)

5.1.4. Adding a proxy for RHC to use for the connection

Use the following commands to add a proxy for **rhc** to use to connect to Red Hat.

```
# mkdir -p /etc/systemd/system/rhcd.service.d
# cat /etc/systemd/system/rhcd.service.d/proxy.conf
[Service]
Environment=HTTPS_PROXY=http://proxy.corp.com:8888
# systemctl daemon-reload
# systemctl restart rhcd
```

5.2. RHC CLIENT COMMUNICATION

The communication technology behind the rhc daemon, **rhcd**, is MQTT. The client establishes a connection to the Red Hat message broker and waits for new messages. The new messages are then read and converted into playbook execution. While the messages are consumed almost instantaneously, the communication is always established by the client. There is no communication initiated from the Red Hat services to your environment.

5.3. CONSULTING AND INTERPRETING LOG FILES

Troubleshooting an issue often starts by looking at the logs to see what happened during a given event.

- Use the following command to consult logs:

```
# journalctl -u rhcd
```

- Use **-f**, **--follow**, to show only the most recent journal entries, and continuously print new entries as they are appended to the journal:

```
# journalctl -u rhcd -f
```

5.4. KNOWN ISSUES

There are occasionally issues that the user or org admin should be aware of when working with their systems.

The following known issues are documented for remote host configuration:

- Remote host configuration is stuck in the **checking** status if a Red Hat Satellite-connected system is also in the remediation plan.
  If you have a remediation plan that contains one or more remote host configuration systems and one or more Red Hat Satellite-connected systems, when you click the **Execute Playbook** button on the remote host configuration manager. The remote host configuration system will be stuck at **checking**. You will not be able to execute the remediation plan on the remote host configuration system.

  See RHC stuck at "checking" if a Satellite-connected system is also in the remediation plan for more information.

- The **insights-client** command is not invoked after executing remediation with remote host configuration.
  Playbooks generated by Remediations generally have the following structure:

  - Fix the problems listed in the remediation.
  - Optionally reboot the system.
  - Execute the **insights-client** command so that Red Hat Insights for Red Hat Enterprise Linux has an updated version of the system's state.
    If a playbook is invoked by clicking **Execute playbook** in the **Remediations** UI, and if the targeted system is running rhc client (as opposed to being managed by a Satellite), the final step is missing. As a result, Insights for Red Hat Enterprise Linux never receives an updated view of the system's state.

- The current temporary solution is to manually run: **insights-client** on the system OR wait 24 hours for the next upload.
- See insights-client not invoked after executing remediation via RHC for more information.

CHAPTER 6. CREATING AND MANAGING ACTIVATION KEYS IN THE RED HAT HYBRID CLOUD CONSOLE

Your organization's activation keys are listed on the Activation Keys page in the Red Hat Hybrid Cloud Console. You can use an activation key as an authentication token to register a system with Red Hat hosted services, such as Red Hat Subscription Manager or remote host configuration (RHC). Administrators can create, edit, and delete activation keys for your organization. They also have the option to set system-level features, such as system purpose, on an activation key. When you use a preconfigured activation key to register a system, all the selected attributes are automatically applied at the time of registration.

6.1. ACTIVATION KEY MANAGEMENT IN THE RED HAT HYBRID CLOUD CONSOLE

An activation key is a preshared authentication token that enables authorized users to register and configure systems. It eliminates the need to store, use, and share a personal username and password combination, which increases security and facilitates automation. For example, you can use a preconfigured activation key to automatically register a system with all the required system-level features. Additionally, you can put preconfigured activation keys in Kickstart scripts to bulk -provision the registration of multiple systems.

You can use an activation key and a numeric organization identifier (organization ID) to register a system with Red Hat hosted services, such as Red Hat Subscription Manager or remote host configuration (RHC). 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 the activation keys in the Hybrid Cloud Console is managed through a role-based access control (RBAC) system. Users in the Organization Administrator group for your organization use the RBAC system to assign roles, such as RHC user and RHC administrator, to users within your organization. An RHC user can view the activation keys in the table on the Activation Keys page. Only an RHC administrator is authorized to use the Hybrid Cloud Console user interface to create, edit, and delete activation keys. An RHC administrator also has the option to configure an activation key to apply system purpose attributes (role, service level agreement, or usage) to the system during the registration process. An Organization Administrator has the RHC administrator role by default.

In the terminal, users with root privileges can use the activation key and the organization ID to register the system with a single command. If the activation key has been preconfigured with system purpose attributes, the specified attributes are automatically applied to the system upon registration.

Additional resources

- For more information about RBAC roles, see *User Access Configuration Guide for Role-based Access Control (RBAC)*.
- For more information about system purpose, see System purpose configuration in *Getting Started with RHEL System Registration*.

6.2. CREATING AN ACTIVATION KEY

As an RHC administrator, you can use the Hybrid Cloud Console interface to create preconfigured activation keys that authorized users in your organization can use to register systems to Red Hat hosted services, such as Red Hat Subscription Manager or remote host configuration (RHC). An activation key requires a unique name that enables users to use the activation key by entering the activation key name and organization ID, without requiring a username or password. An activation key can also contain

system purpose attributes that can be automatically applied to individual systems at the time of registration. The activation keys that you create can be viewed in the table on the Activation Keys page and used to register systems in the terminal.

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

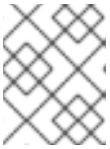
To create an activation key in the Hybrid Cloud Console, perform the following steps:

1. Navigate to Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > 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.

NOTE

Your activation key name must be unique, may contain only numbers, letters, underscores, and hyphens, and contain fewer than 256 characters. If you enter a name that already exists in your organization, you will receive an error message and the key will not be created.

4. Optional: To add system purpose attributes to the activation key, navigate to the system purpose field that you want to populate. From the drop-down list, select the attribute value that you want to apply to the system.



NOTE

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

5. When you have populated all the required fields, click **Create**.

NOTE

=== The **Create activation key**button is disabled until a valid name is entered into the Name field. If the button remains disabled after populating the Name field, check that the name meets the noted criteria and that you are logged in to the Hybrid Cloud Console with the required RBAC role. For questions regarding your RBAC role, contact an Organization Administrator. ===

6.3. VIEWING AN ACTIVATION KEY

As an RHC user, you can view your organization's numeric identifier (organization ID) and available activation keys on the Activation Keys page in the Hybrid Cloud Console. The activation keys and their respective details are presented in a table. The **Name** column contains the name of the activation key. The **Role** column contains 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 contains 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 contains the usage value for the system purpose attribute set on the key. A potential usage value is *Production*. If no system purpose attribute is set on the activation key, the respective field contains no value.

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 an activation key in the Hybrid Cloud Console, perform the following steps:

1. Navigate to Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Activation Keys.

6.4. USING AN ACTIVATION KEY TO REGISTER A SYSTEM WITH RED HAT SUBSCRIPTION MANAGER

The activation keys that you create in the Hybrid Cloud Console combine all the system registration steps into one secure, automated process.

As a user with root privileges you can register the system, apply pre-configured system purpose attributes, and enable repositories with a single command. Root users can pass an activation key and a numeric organization identifier (organization ID) to the command line tools used to register a system to Red Hat hosted services such as Red Hat Subscription Manager or remote host configuration (RHC). If an RHC administrator has preconfigured the activation key to apply selected system purpose attributes, those attributes are automatically applied to the system during the registration process.

Prerequisites

- You have root privileges or their equivalent to run the commands in the following procedure.
- You have the numeric identifier for your organization (organization ID).

Procedure

To use an activation key to register a system with Subscription Manager, perform the following steps:

1. From the terminal, enter the following command where *<activation_key_name>* is the name of the activation key you want to use and *<1234567>* is your organization ID:

```
subscription-manager register --activationkey=<activation_key_name> --org=<1234567>
```

2. The expected output confirms that your system is registered. For example:

```
The system has been registered with id:
62edc0f8-855b-4184-b1b8-72a9dc793b96
```

6.5. USING AN ACTIVATION KEY TO REGISTER A SYSTEM WITH REMOTE HOST CONFIGURATION (RHC)

The activation keys that you create in the Hybrid Cloud Console combine all the system registration steps into one secure, automated process.

As a user with root privileges you can register the system, apply pre-configured system purpose attributes, and enable repositories with a single command. Root users can pass an activation key and a numeric organization identifier (organization ID) to the command line tools used to register a system to Red Hat hosted services such as Red Hat Subscription Manager or remote host configuration (RHC). If an RHC administrator has pre-configured the activation key to apply selected system purpose attributes, those attributes are automatically applied to the system during the registration process.

Prerequisites

- You have root privileges or their equivalent to run the commands in the following procedure.
- You have the numeric identifier for your organization (organization ID).

Procedure

To use an activation key to register a system with RHC, perform the following steps:

1. From the terminal, enter the following command where *<activation_key_name>* is the name of the activation key you want to use and *<1234567>* is your organization ID:

```
rhc connect --activation-key <activation_key_name> --organization <1234567>
```

6.6. EDITING AN ACTIVATION KEY

As an RHC administrator, you can use the Hybrid Cloud Console interface to edit the activation keys on the Activation Keys page. Specifically, you can add, update, or remove the system purpose attributes on an existing activation key. However, you cannot edit the name of the activation key itself.

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 an activation key in the Hybrid Cloud Console, perform the following steps:

1. Navigate to Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Activation Keys.
2. From the Activation Keys page, locate the row that contains the activation key that you want to edit. Click **More options** and select **Edit** from the overflow menu.
3. To update a system purpose attribute on the activation key, navigate to the system purpose field that you want to change. From the drop-down list, select the attribute value that you want to apply to the system.

4. To remove a system purpose attribute from the activation key, navigate to the system purpose field that you want to clear and deselect the unwanted value from the drop-down list. To update the activation key, click **Save changes**.

6.7. DELETING AN ACTIVATION KEY

As an RHC administrator, 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, either remove the unwanted activation key from the script or 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, perform the following steps:

1. Navigate to Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Activation Keys.
2. From the Activation Keys page, locate the row containing the activation key that you want to delete. Click **More options** and select **Delete** from the overflow menu.
3. In the Delete Activation Key window, review the information about deleting activation keys. If you want to continue with the deletion, click **Delete**.

IMPORTANT

=== Deleting this activation key will impact any automation that references it. To avoid any negative consequences of deleting this key, retire any automation script that uses this key or remove any references of this key from your Kickstart scripts.

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate and prioritize your feedback regarding our documentation. Provide as much detail as possible, so that your request can be quickly addressed.

Prerequisites

- You are logged in to the Red Hat Customer Portal.

Procedure

To provide feedback, perform the following steps:

1. Click the following link: Create Issue
2. Describe the issue or enhancement in the **Summary** text box.
3. Provide details about the issue or requested enhancement in the **Description** text box.
4. Type your name in the **Reporter** text box.
5. Click the **Create** button.

This action creates a documentation ticket and routes it to the appropriate documentation team. Thank you for taking the time to provide feedback.