



Red Hat Insights 2023

Remote Host Configuration and Management

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

Red Hat Insights 2023 Remote Host Configuration and Management

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

Legal Notice

Copyright © 2023 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[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] 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[®] 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 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	3
1.1. REMOTE CONFIGURATION COMPONENTS	3
CHAPTER 2. REGISTER AND CONNECT RHEL SYSTEMS USING THE RHC CLIENT	5
2.1. SETTING UP REMOTE HOST CONFIGURATION	6
2.2. DISCONNECTING A SYSTEM USING REMOTE HOST CONFIGURATION	6
2.3. USING ADDITIONAL CLI OPTIONS	6
CHAPTER 3. CONFIGURE CONNECTION TO INSIGHTS FOR RED HAT ENTERPRISE LINUX USING REMOTE HOST CONFIGURATION MANAGER	8
3.1. USER ACCESS FOR REMOTE HOST CONFIGURATION	8
3.1.1. User Access roles for remote host configuration manager	8
3.1.2. User Access roles for remediations users	9
3.1.3. Additional resources	9
3.2. OPENING THE REMOTE HOST CONFIGURATION MANAGER	9
3.3. EDITING SETTINGS IN THE REMOTE HOST CONFIGURATION MANAGER	9
CHAPTER 4. REMEDIATE ISSUES DIRECTLY FROM INSIGHTS FOR RED HAT ENTERPRISE LINUX	11
4.1. CREATING AND UPDATING A REMEDIATION PLAYBOOK	11
4.2. EXECUTING A REMEDIATION PLAYBOOK	11
CHAPTER 5. TROUBLESHOOTING REMOTE HOST CONFIGURATION ISSUES	13
5.1. NETWORKING CONSIDERATIONS	13
5.1.1. TCP ports and destinations	13
5.1.1.1. Subscription manager	13
5.1.1.2. Insights client	13
5.1.1.3. RHC client daemon	13
5.1.1.4. Adding a proxy for RHC to use for the connection	13
5.1.2. RHC client communication	14
5.2. CONSULTING AND INTERPRETING LOG FILES	14
5.3. KNOWN ISSUES	14
CHAPTER 6. CREATING AND MANAGING ACTIVATION KEYS IN THE RED HAT HYBRID CLOUD CONSOLE .	16
6.1. ACTIVATION KEY MANAGEMENT IN THE RED HAT HYBRID CLOUD CONSOLE	16
6.2. CREATING AN ACTIVATION KEY	16
6.3. VIEWING AN ACTIVATION KEY	17
6.4. USING AN ACTIVATION KEY TO REGISTER A SYSTEM WITH RED HAT SUBSCRIPTION MANAGER	18
6.5. USING AN ACTIVATION KEY TO REGISTER A SYSTEM WITH REMOTE HOST CONFIGURATION (RHC)	19
6.6. EDITING AN ACTIVATION KEY	19
6.7. DELETING AN ACTIVATION KEY	20
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	21

CHAPTER 1. INTRODUCING REMOTE HOST CONFIGURATION

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.
- A Red Hat Smart Management subscription is required to use remote host configuration.

1.1. REMOTE 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.

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 supported by the remote host configuration manager, 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 > Settings > Remote Host Configuration > Manage configuration](#). 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](#)
- [Introduction to Red Hat Subscription Management Workflows](#)
- [Performing an advanced RHEL installation](#)
- [Performing a standard RHEL installation](#)

- [Quick registration for RHEL](#)

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](#)

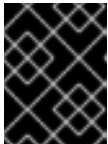
2.2. DISCONNECTING A SYSTEM USING REMOTE HOST CONFIGURATION

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 INSIGHTS FOR RED HAT ENTERPRISE LINUX USING REMOTE HOST CONFIGURATION MANAGER

The remote host configuration manager, located at [Red Hat Hybrid Cloud Console > Settings > Remote Host Configuration > Manage configuration](#), 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.

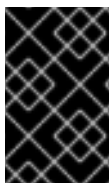
3.1. USER ACCESS FOR REMOTE HOST CONFIGURATION

Before account users can access certain features in the Red Hat Insights for Red Hat Enterprise Linux application, they must be added to the correct User Access group(s) in [Red Hat Hybrid Cloud Console > User Access > Users](#). The permissions that a user needs depend on their need to perform the tasks described in the following subsections. At a high level, an **Organization Administrator** or **User Access administrator** performs the following steps to create new groups, or to add roles or members to existing groups:

- Create a User Access **group** for each necessary role.
 - Add the **role** to the group.
 - Add **members** to the group.

Your organization might already have User Access groups with the proper roles added. Onboarding new members might be as easy as adding them to existing groups.

Existing groups can be searched, as well as the roles included in each group, in [Red Hat Hybrid Cloud Console > User Access > Groups](#).



IMPORTANT

Changes to User Access must be performed by an **Organization Administrator** on your Red Hat account, or a Red Hat Hybrid Cloud Console user with the **User Access administrator** role.

3.1.1. User Access roles for remote host configuration manager

There are currently two roles that are relevant for connector dashboard users. These roles determine if a user can change settings or simply view them:

- **RHC administrator.** Members in a group with this role can perform any operations in the rhc manager.
- **RHC viewer.** 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.

3.1.2. User Access roles for remediations users

There are two roles that are relevant for remediations users and determine whether a user can view remediations details or execute direct remediations from Insights for Red Hat Enterprise Linux:

- **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.

3.1.3. Additional resources

- [User Access Configuration Guide for Role-based Access Control \(RBAC\)](#)

3.2. 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 viewer** privileges, assigned in User Access, to perform this procedure.

Procedure

- Navigate to [Red Hat Hybrid Cloud Console > Settings > Remote Host Configuration > Manage configuration](#) to view the Red Hat Insights for Red Hat Enterprise Linux connection settings.

3.3. 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 > Settings > Remote Host Configuration > Manage configuration](#) 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.

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.



NOTE

Use of remote host configuration features, including direct remediations, requires a single Red Hat Smart Management subscription at the Red Hat account level.

4.1. CREATING AND UPDATING A REMEDIATION PLAYBOOK

Creating playbooks in Red Hat Insights for Red Hat Enterprise Linux follows roughly the same steps, regardless of the service you are working in. To create or update playbooks, use the procedures described in the following Insights for Red Hat Enterprise Linux documentation:

- Advisor service: [Remediating Configuration Issues Using Red Hat Insights and Ansible Playbooks](#)
- Compliance service: [Remediating Security-Policy Compliance issues using Ansible Playbooks](#)
- Patch service: [System Patching Using Ansible Playbooks via Remediations](#)
- Vulnerability service: [Remediating Security Exposures using the Vulnerability Service and Ansible Playbooks](#)

4.2. EXECUTING A REMEDIATION PLAYBOOK

Execute a playbook directly from the Red Hat Insights for Red Hat Enterprise Linux application.

Prerequisites

- You must be logged into the Red Hat Hybrid Cloud Console.
- You must have **Remediations administrator** privileges, assigned in User Access, to perform this procedure.
- Your organization's Red Hat account must have at least one Red Hat Smart Management subscription.
- Remediations are enabled in the remote host configuration manager.

Procedure

1. Navigate to [Red Hat Enterprise Linux > Red Hat Insights > Toolkit > Remediations](#) and locate the remediation playbook to be executed.
2. Open the playbook to review its details (Action, Systems, Activity) or directly run the playbook.
3. Click **Execute playbook**. This action displays a summary of the type of connection to use when pushing the playbook. **Direct connection** refers to the system connecting through the rhc client.

Verification

1. The remediation playbook successfully executed.
2. The issue was marked as resolved in [Red Hat Enterprise Linux > Red Hat Insights > Toolkit > Remediations](#).
3. The issue was resolved on the system.

CHAPTER 5. TROUBLESHOOTING REMOTE HOST CONFIGURATION ISSUES

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

5.1. NETWORKING CONSIDERATIONS

You must have access to `cert.cloud.redhat.com`.

5.1.1. 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.

5.1.1.1. 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)`

5.1.1.2. 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)`

5.1.1.3. 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)`

5.1.1.4. 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/yggd.service.d
# cat /etc/systemd/system/yggd.service.d/proxy.conf << EOF
[Service]
Environment=HTTPS_PROXY=http://proxy.corp.com:8888
```

```
EOF
```

```
# systemctl daemon-reload  
# systemctl restart rhcd
```

5.1.2. 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.

5.2. 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
```

5.3. 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 a preconfigured activation key is used 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 viewer and RHC administrator, to users within your organization. An RHC viewer 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 [Using system purpose](#) in the *Using Red Hat Subscription Management* guide.

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. Log in to your Red Hat Hybrid Cloud Console account at console.redhat.com.
2. From the Hybrid Cloud Console navigation menu, click **Remote Host Configuration > Activation Keys**.
3. From the Activation Keys page, click **Create activation key**.
4. 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.

5. 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.

6. 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 viewer, 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 viewer 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. Log in to your Red Hat Hybrid Cloud Console Account at console.redhat.com.
2. From the Hybrid Cloud Console navigation menu, click **Remote Host 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. Log in to your Red Hat Hybrid Cloud Console account at console.redhat.com.
2. From the Hybrid Cloud Console navigation menu, click **Remote Host Configuration > Activation Keys**.

3. 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.
4. 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.
5. 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. Log in to your Red Hat Hybrid Cloud Console account at console.redhat.com.
2. From the Hybrid Cloud Console navigation menu, click **Remote Host Configuration > Activation Keys**.
3. 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.
4. 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 your feedback on our documentation. To provide feedback, highlight text in a document and add comments.

Prerequisites

- You are logged in to the Red Hat Customer Portal.
- In the Red Hat Customer Portal, the document is in the **Multi-page HTML** viewing format.

Procedure

To provide your feedback, perform the following steps:

1. Click the **Feedback** button in the top-right corner of the document to see existing feedback.



NOTE

The feedback feature is enabled only in the **Multi-page HTML** format.

2. Highlight the section of the document where you want to provide feedback.
3. Click the **Add Feedback** pop-up that appears near the highlighted text.
A text box appears in the feedback section on the right side of the page.
4. Enter your feedback in the text box and click **Submit**.
A documentation issue is created.
5. To view the issue, click the issue link in the feedback view.