



Red Hat Insights 1-latest

Red Hat Insights Remediations Guide

Fixing issues on RHEL systems with remediation playbooks

Red Hat Insights 1-latest Red Hat Insights Remediations Guide

Fixing issues on RHEL systems with remediation playbooks

Legal Notice

Copyright © 2024 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

Create and execute playbooks to remediate issues on any system registered with Insights. 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. REMEDIATIONS OVERVIEW	3
1.1. USER ACCESS SETTINGS IN THE RED HAT HYBRID CLOUD CONSOLE	3
1.1.1. Predefined User Access groups and roles	3
1.1.1.1. Predefined groups	3
1.1.1.2. Predefined roles assigned to groups	4
1.1.2. Access permissions	4
1.1.3. User Access roles for remediations users	4
CHAPTER 2. ENABLING HOST COMMUNICATION WITH INSIGHTS	5
2.1. ENABLING THE RHC CLIENT ON SYSTEMS DIRECTLY MANAGED BY INSIGHTS	5
2.2. ENABLING CLOUD CONNECTOR FOR CONTENT HOSTS MANAGED BY SATELLITE	6
2.2.1. Configuring Cloud Connector and uploading your Satellite Server content host inventory to Red Hat Insights	6
CHAPTER 3. CREATING AND MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS	8
3.1. CREATING A PLAYBOOK TO REMEDIATE A CVE VULNERABILITY ON RHEL SYSTEMS	8
3.1.1. Creating playbooks to remediate CVEs with security rules when recommended and alternate resolution options exist	9
3.2. MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS FOR RED HAT ENTERPRISE LINUX	13
3.2.1. Downloading a remediation playbook	13
3.2.2. Archiving a remediation playbook	13
3.2.3. Viewing archived remediation playbooks	13
3.2.4. Deleting a remediation playbook	14
3.2.5. Monitoring remediation status	14
CHAPTER 4. EXECUTING REMEDIATION PLAYBOOKS	15
4.1. EXECUTING REMEDIATION PLAYBOOKS FROM THE INSIGHTS USER INTERFACE	15
4.2. EXECUTING REMEDIATIONS FROM THE SATELLITE USER INTERFACE	15
CHAPTER 5. USING PATCH TEMPLATES FOR REMEDIATIONS	17
5.1. USING PATCH TEMPLATES WITH REMEDIATIONS	17
CHAPTER 6. REFERENCE	18
6.1. INSTALLING THE INSIGHTS CLIENT ON SATELLITE SERVER CONTENT HOSTS	18
6.2. CONFIGURING CLOUD CONNECTOR AFTER UPGRADING SATELLITE SERVER 6.10 TO 6.11	18
6.3. DISABLING DIRECT REMEDIATIONS ON A SATELLITE SERVER CONTENT HOST	19
6.4. DISABLING DIRECT REMEDIATION ON A SATELLITE SERVER CONTENT HOST GROUP	19
PROVIDING FEEDBACK ON RED HAT DOCUMENTATION	20

CHAPTER 1. REMEDIATIONS OVERVIEW

After identifying the highest remediation priorities in your Red Hat Enterprise Linux (RHEL) infrastructure, you can create, and then execute, remediation playbooks to fix those issues.

Subscription requirements

- Red Hat Insights for Red Hat Enterprise Linux is included with every RHEL subscription. No additional subscriptions are required to use Insights remediation features.

User requirements

- Access remediation capabilities in the Insights for Red Hat Enterprise Linux application on the Red Hat Hybrid Cloud Console (Hybrid Cloud Console).
- Access Red Hat Satellite-managed systems in the Console or in the Satellite application UI.
- All Insights users will automatically have access to read, create, and manage remediation playbooks.
- The ability to execute playbooks on remote systems requires the **Remediations administrator** predefined User Access role, granted by an Organization Administrator in Identity & Access Management settings on the Hybrid Cloud Console.

1.1. 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.

1.1.1. 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.

1.1.1.1. 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.

1.1.1.2. 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.

1.1.2. 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.

1.1.3. User Access roles for remediations users

The following roles enable standard or enhanced access to remediations features in Insights for Red Hat Enterprise Linux:

- **Remediations viewer.** The Remediations viewer role is included in the Default access group. The Remediation viewer role permits access to view existing playbooks for the account and to create new playbooks. Remediations viewers cannot execute playbooks on systems.
- **Remediations administrator.** The Remediations administrator role permits access to all remediations capabilities, including remotely executing playbooks on systems.

CHAPTER 2. ENABLING HOST COMMUNICATION WITH INSIGHTS

Before you can execute playbooks on remote systems from Red Hat Insights for Red Hat Enterprise Linux, your systems have to be able to communicate with Red Hat Insights.

- For Red Hat Enterprise Linux systems that are *not managed by Red Hat Satellite*, you should follow the procedure below to enable the `rhc` client on those systems.
- For systems that *are managed by Satellite*, you will configure Cloud Connector on the host servers for those systems. :context: host-communication-with-insights

2.1. ENABLING THE RHC CLIENT ON SYSTEMS DIRECTLY MANAGED BY INSIGHTS

To be able to execute remediation playbooks from Insights for Red Hat Enterprise Linux, the `rhc` client must be enabled on the systems in your infrastructure. The **`rhc connect`** command does this by registering (RHEL8.6 and later, and 9.0 and later) systems with Red Hat Subscription Manager and Red Hat Insights, and enabling remote host configuration (`rhc`) features in Insights for Red Hat Enterprise Linux.

Prerequisites

- Sudo access on the Red Hat Enterprise Linux host system

Connect `rhc` on RHEL8.5 systems

Remote host configuration on RHEL 8.5 has dependencies of **`ansible`** and **`rhc-worker-playbook`**. To install the dependencies, you must first register with Subscription Manager.

- Use the following commands to enable `rhc` on RHEL 8.5 systems.

```
[root]# subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-rpms
[root]# dnf -y install ansible rhc-worker-playbook-0.1.5-3.el8_4
[root]# rhc connect
```

Connect `rhc` on RHEL8.6 and later systems

- Use the following commands to enable `rhc` on RHEL8.6 and later systems.

```
[root]# dnf -y update rhc
[root]# dnf -y install rhc-worker-playbook
[root]# rhc connect
```

Connect `rhc` on RHEL9.0 and later systems

- Use the following commands to enable `rhc` on RHEL9.0 and later systems.

```
[root]# dnf -y install rhc rhc-worker-playbook
[root]# rhc connect
```

Additional resources

- After enabling `rhc`, you can manage the configuration at [Red Hat Hybrid Cloud Console > Red Hat Insights > Inventory > System Configuration > Remote Host Configuration \(RHC\)](#).
- For complete `rhc` documentation, see [Remote Host Configuration and Management](#).

2.2. ENABLING CLOUD CONNECTOR FOR CONTENT HOSTS MANAGED BY SATELLITE

You can remediate issues on Satellite-managed content hosts remotely from the Insights for Red Hat Enterprise Linux user interface in the Red Hat Hybrid Cloud Console. Remote remediation from Insights requires that you first configure the Cloud Connector plugin on the Satellite Server.



IMPORTANT

If you want to manage and execute host remediations completely from the Satellite web console, then you do not need to enable the Cloud Connector plugin.

The following prerequisites are comprehensive for Satellite Server configuration:

Prerequisites

- Satellite must be version 6.9 or later.
- You have root access to the Satellite server.
- The content hosts that are managed by the satellite should have the Insights client installed and turned on. See the reference section of this documentation for Insights client installation and enablement procedures.
- Import a Subscription Manifest into Satellite. For more information, see [Importing a Subscription Manifest into Satellite Server](#) in the Red Hat Satellite *Content Management Guide*.
- Register your hosts to Satellite using an activation key to attach Red Hat subscriptions. For more information, see [Registering Hosts](#) in the Red Hat Satellite *Managing Hosts* guide.

2.2.1. Configuring Cloud Connector and uploading your Satellite Server content host inventory to Red Hat Insights

Before you can run remediation playbooks remotely from Insights, you must install and configure the Cloud Connector plugin on Satellite Server. Perform the following tasks to install, configure, and verify the configuration of Cloud Connector.

Procedure

1. On Satellite Server, enable the **remote-execution** plugin by entering one of the following commands, based on your version of Satellite Server.

- a. On Satellite Server 6.12 and newer

```
[root]# satellite-installer --foreman-proxy-plugin-remote-execution-script-install-key true
```

- b. On Satellite Server 6.9 - 6.11

```
[root]# satellite-installer --foreman-proxy-plugin-remote-execution-ssh-install-key true
```

■

**NOTE**

Configuring Cloud Connector requires that the satellite perform a remote execution on itself. This is why the first step is to enable the **remote-execution** script or plugin.

- In the Satellite Server web UI, navigate to **Configure > Red Hat Cloud > Inventory Upload**. Verify that the **Automatic Inventory Upload** switch is turned **ON**, which is the default setting.
- Optionally:** Toggle the **Obfuscate host names** switch to the **ON** position to hide host names that Satellite Server reports to the Hybrid Cloud Console.

**NOTE**

The Obfuscate host names setting only affects **rh_cloud** reports. If you want to obfuscate hostnames *and* IP addresses, you should set obfuscation in the Insights client configuration. Satellite knows how to read this configuration, and will follow along. See [Client Configuration Guide for Red Hat Insights](#) sections, *Obfuscating the host name* and *Obfuscating the IPv4 address*.

Automatic inventory upload and **Obfuscate host names** are global settings. They affect content hosts that belong to all organizations.

- Click **Configure Cloud Connector**. A Notice dialog box warns you that this action also enables auto reports upload. Click **Confirm**.
- Wait for progress to finish. This should take about one minute. Go to **Jobs > Configure Cloud Connector** to see the job. Eventually, you will see the satellite in [Red Hat Hybrid Cloud Console > the Settings icon \(⚙\) > Integrations](#), in the **Red Hat** tab. Allow up to one hour after the job is visible in the Satellite web console.

The bottom of the **Inventory Uploads** page shows the name of your organization; hovering over it will turn the area grey. Clicking on the name will cause it to expand, showing a **Generating** tab and **Uploading** tab where one can monitor the progress of the upload.

- Click **Restart** to generate a data payload from each of the content hosts that have Insights client running, and upload your host inventory to Insights for Red Hat Enterprise Linux. Repeat this step, clicking **Restart** for each organization for which you want to upload a content host inventory.
- Set Auto sync for the organization under **Configure > Red Hat Cloud(after Sat 6.11) > Insights** using the toggle in the upper right of the screen.

Verification

To verify that the upload was successful, log into [Red Hat Hybrid Cloud Console > Red Hat Enterprise Linux > Red Hat Insights > Inventory](#) and search for the **satellite_id** tag for your content hosts.

Optionally, push the **Sync inventory status** button and wait for the task to finish. It will show you the number of content hosts recognized by Insights inventory.

CHAPTER 3. CREATING AND MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS

The workflow to create playbooks is similar in each of the services in Insights for Red Hat Enterprise Linux. In general, you will fix one or more issues on a system or group of systems.

Playbooks focus on issues identified by Insights services. A recommended practice for playbooks is to include systems of the same RHEL major/minor versions because the resolutions will be compatible.

3.1. CREATING A PLAYBOOK TO REMEDIATE A CVE VULNERABILITY ON RHEL SYSTEMS

Create a remediation playbook in the Red Hat Insights vulnerability service. The workflow to create a playbook is similar for other services in Insights for Red Hat Enterprise Linux.

Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console.



NOTE

No enhanced User Access permissions are required to create remediation playbooks.

Procedure

1. Navigate to the [Security > Vulnerability > CVEs](#) page.
2. Set filters as needed and click on a CVE.
3. Scroll down to view affected systems.
4. Select systems to include in a remediation playbook by clicking the box to the left of the system ID.



NOTE

Include systems of the same RHEL major/minor version, which you can do by filtering the list of affected systems.

5. Click the **Remediate** button.
6. Select whether to add the remediations to an *existing* or *new* playbook and take the following action:
 - a. Click **Add to existing playbook** and select the desired playbook from the dropdown list, OR
 - b. Click **Create new playbook** and add a playbook name.
 - c. Click Next.
7. Review the systems to include in the playbook, then click **Next**.
8. Review the information in the Remediation review summary.

- a. By default, **autoreboot** is enabled. You can disable this option by clicking **Turn off autoreboot**.
- b. Click **Submit**.

Verification step

1. Navigate to [Automation Toolkit > Remediations](#).
2. Search for your playbook. You should see your playbook.

3.1.1. Creating playbooks to remediate CVEs with security rules when recommended and alternate resolution options exist

Most CVEs in Red Hat Insights for RHEL will have one remediation option for you to use to resolve an issue. Remediating a CVE with security rules might include more than one resolution a recommended and one or more alternate resolutions. The workflow to create playbooks for CVEs that have one or more resolution options is similar to the remediation steps in the advisor service.

For more information about security rules, see [Security rules](#), and [Filtering lists of systems exposed to security rules](#) in [Assessing and Monitoring Security Vulnerabilities on RHEL Systems](#) .

Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console.



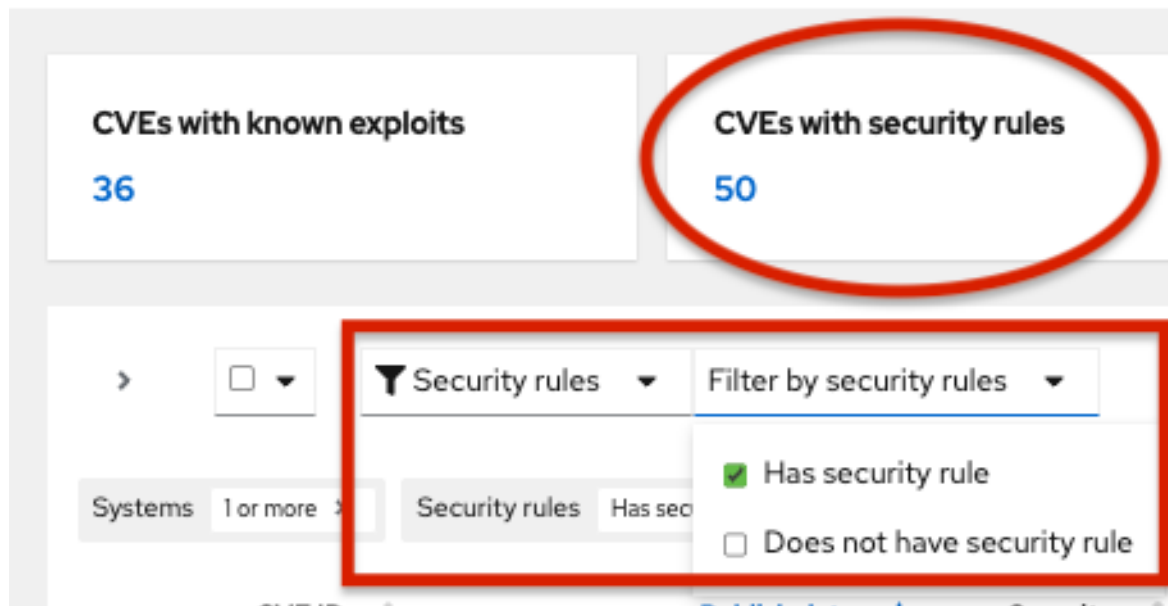
NOTE

You do not need enhanced User Access permissions to create remediation playbooks.

Procedure

1. Navigate to [Security > Vulnerability > CVEs](#)
2. Set filters if needed (for example, filter to see **CVEs with security rules** to focus on issues that have elevated risk associated with them). Or, click the CVEs with security rules tile on the dashbar. Both options show in the example image.

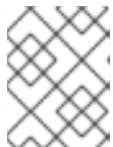
CVEs ?



3. Click a CVE in the list.



4. Scroll to view affected systems, and select systems you want to include in a remediation playbook by clicking the box to the left of the system ID on the **Review systems** page. (Selecting one or more systems activates the Remediate button.)



NOTE

Recommended: Include systems of the same RHEL major or minor version by filtering the list of affected systems.

5. Click **Remediate**.
6. Decide whether to add the remediations to an existing or new playbook by taking one of the following actions:
 - Choose **Add to existing playbook** and select the desired playbook from the dropdown list, OR
 - Choose **Create new playbook**, and add a playbook name. For this example, HCCDOC-392.
7. Click **Next**. A list of systems shows on the screen.
8. Review the systems to include in the playbook (deselect any systems that you do not want to include).
9. Click **Next** to see the **Review and edit actions** page, which shows you options to remediate the CVE. The number of items to remediate can vary. You will also see additional information (that you can expand and collapse) about the CVE, such as:
 - **Action:** Shows the CVE ID.

- **Resolution:** Displays the recommended resolution for the CVE. Shows if you have alternate resolution options.
- **Reboot required:** Shows whether you must reboot your systems.
- **Systems:** Shows the number of systems you are remediating.

10. On the **Review and edit actions** page, choose one of two options to finish creating your playbook:

- **Option 1:** To review all of the recommended and alternative remediation options available (and choose one of those options):
 - a. Select **Review and/or change the resolution steps for this 1 action** or similar based on your actual options.

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 **Review and edit actions**
4 Remediation review

Review and edit actions

You have selected 1 item to remediate. 1 of 1 item allows for you to chose from multiple resolution steps.

- Review and/or change the resolution steps for this 1 action.

Action	Resolution	Reboot required	Systems
> CVE-2021-4034	[TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap 1 alternate resolution	Not required	6

Accept all recommended resolution steps for all actions
You may modify reboot status to manual reboot in the next step, or from the playbook.

b. Click **Next**.

- c. On the **Choose action: <CVE information>** page, click a tile to select your preferred remediation option. The bottom edge of the tile highlights when you select it. The recommended solution is highlighted by default.

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 Review and edit actions
4 **Choose actions**
CVE_2021_4034_POLKIT
5 Remediation review

Choose action: CVE_2021_4034_POLKIT

Review the possible resolution steps and select which to add to your playbook.

Resolution affects 6 systems

[TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap

Resolution from "CVE-2021-4034"

Reboot **not** required

Update polkit to fix CVE-2021-4034

Resolution from "CVE-2021-4034"

Reboot **not** required

Next

d. Click **Next**.

- **Option 2:** To accept all recommended remediations:
 - Choose **Accept all recommended resolutions steps for all actions**

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 **Review and edit actions**
4 Remediation review

Review and edit actions

You have selected 1 item to remediate. 1 of 1 item allows for you to chose from multiple resolution steps.

Review and/or change the resolution steps for this 1 action.

Action	Resolution	Reboot required	Systems
> CVE-2021-4034	[TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap 1 alternate resolution	Not required	6

Accept all recommended resolution steps for all actions
You may modify reboot status to manual reboot in the next step, or from the playbook.

11. Review information about your selections and change options for autoreboot of systems on the **Remediations review** page. The page shows you the:

- Issues you are adding to your playbook.
- Options for changing system autoreboot requirements.
- Summary about CVEs and resolution options that to fix them.

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 Review and edit actions
4 Choose actions
 CVE_2021_4034_PO
 LKIT
5 **Remediation review**

Remediation review

Issues listed below will be added to the playbook HCCDOC-392.

The playbook HCCDOC-392 **does not** auto reboot systems.

[Turn on autoreboot](#)

Action	Resolution	Reboot required	Systems
> CVE-2021-4034	[TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap	Not required	6

[Submit](#) [Back](#) [Cancel](#)

12. Optional. Change autoreboot options on the **Remediation review** page, if needed. (Autoreboot is enabled by default, but your settings might vary based on your remediation options.)
13. Click **Submit**. A notification displays that shows the number of remediation actions added to your playbook, and other information about your playbook.

Verification step

1. Navigate to [Automation Toolkit > Remediations](#)

2. Search for your playbook.
3. To run (execute) your playbook, see [Executing remediation playbooks from Insights for Red Hat Enterprise Linux](#).

3.2. MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS FOR RED HAT ENTERPRISE LINUX

You can download, archive, and delete existing remediation playbooks for your organization. The following procedures describe how to perform common playbook-management tasks.

Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console.



NOTE

No enhanced permissions are required to view, edit, or download information about existing playbooks.

3.2.1. Downloading a remediation playbook

Use the following procedure to download a remediation playbook from the Insights for Red Hat Enterprise Linux application.

Procedure

1. Navigate to [Automation Toolkit > Remediations](#).
2. Locate the playbook you want to manage and click on the name of the playbook. The playbook details are visible.
3. Click the **Download playbook** button to download the playbook YAML file to your local drive.

3.2.2. Archiving a remediation playbook

You can archive a remediation playbook that is no longer needed, but the details of which you want to preserve.


Procedure

1. Navigate to [Automation Toolkit > Remediations](#).
2. Locate the playbook you want to archive.
3. Click on the options icon (`:`) and select **Archive playbook**. The playbook is archived.

3.2.3. Viewing archived remediation playbooks

You can view archived remediation playbooks in Insights for Red Hat Enterprise Linux.


Procedure

1. Navigate to [Automation Toolkit > Remediations](#).
2. Click the **More options** icon  that is to the right of the Download playbook button and select Show archived playbooks.

3.2.4. Deleting a remediation playbook

You can delete a playbooks that is no longer needed.

Procedure

1. Navigate to [Automation Toolkit > Remediations](#).
2. Locate and click on the name of the playbook you want to delete.
3. On the playbook details page, click the **More options** icon  and select **Delete**.

3.2.5. Monitoring remediation status

You can view the remediation status for each playbook that you execute from the Insights for Red Hat Enterprise Linux remediations service. The status information tells you the results of the latest activity and provides a summary of all activity for playbook execution. You can also view log information for playbook execution.

Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console.

Procedure

1. Navigate to [Automation Toolkit > Remediations](#). The page displays a list of remediation playbooks.
2. Click on the name of a playbook.
3. From the **Actions** tab, click any item in the **Status** column to view a pop-up box with the status of the resolution.

To monitor the status of a playbook in the Satellite web UI, see [Monitoring Remote Jobs](#) in the Red Hat Satellite *Managing Hosts* guide.

CHAPTER 4. EXECUTING REMEDIATION PLAYBOOKS

After you create a remediation playbook, you can download and run the playbook using your organization's Ansible workflow, or execute the playbook on remote systems from the Insights for Red Hat Enterprise Linux application.

4.1. EXECUTING REMEDIATION PLAYBOOKS FROM THE INSIGHTS USER INTERFACE

After installing the rhc client on systems in your infrastructure, you can execute remediation playbooks on remote RHEL systems, directly from the Insights for Red Hat Enterprise Linux application.

Prerequisites

- You must be logged in to the Red Hat Hybrid Cloud Console.
- You must be a member of a User Access group with the **Remediations administrator** role.

Procedure

1. Navigate to [Automation Toolkit > Remediations](#).
2. Select a remediation playbook to run and click on the playbook name.
3. Click the **Execute playbook** button.
4. On the popup, click on the **Execute playbook on systems** button. The playbook runs on those systems.

4.2. EXECUTING REMEDIATIONS FROM THE SATELLITE USER INTERFACE

You can also remediate using the Satellite User Interface.

Prerequisites

- You are a **Sources Administrator**.
- You are a **Remediations Administrator**.
- You have completed Host registration using the Insights client.

For specific instructions, see [Creating an Insights Remediation Plan for Hosts](#) in the Satellite Managing Hosts documentation.

**NOTE**

When you introduce a new host into your Satellite inventory, by means of provisioning or registration, two automatic background tasks will initiate. It will take 24 hours for these tasks to complete. This is a typical time frame for the automatic synchronization.

If you identify security issues or another scenario that warrants not waiting 24 hours for the automatic sync, you can manually synchronize by clicking the sync button in the UI. This manual sync will complete in a few minutes.

To see the procedures for enabling automatic and manual synchronization, see the [Configuring Synchronization of Insights Recommendations for Hosts](#) in the Satellite documentation.

CHAPTER 5. USING PATCH TEMPLATES FOR REMEDIATIONS

The Red Hat Insights patch application supports scheduled patching cycles.

Patch templates do not affect **yum/dnf** operations on the host, but they allow you to refine your patch status reporting in Red Hat Insights. You can use the templates to create remediation playbooks for simple patch cycles.

5.1. USING PATCH TEMPLATES WITH REMEDIATIONS

Patch templates can include one or more remediations that you want to apply to multiple systems. You can create a patch template to update a group of systems in a test environment, and use the same patch template to update systems in a production environment on a different day.

For more information about creating and using patch templates with remediations, refer to [System Patching Using Remediation Playbooks](#).



NOTE

After you apply a patch template to the systems you assign, you will not see more recently published advisories that apply to those systems. Use Red Hat Hybrid Cloud Console notifications to ensure that you remain aware of newly published advisories that might affect your infrastructure.

For more information about notifications in the Red Hat Hybrid Cloud Console, see [Configuring notifications on the Red Hat Hybrid Cloud Console](#).

CHAPTER 6. REFERENCE

The following topics are related to the configuration, creation, and management of Insights remediation playbooks.

6.1. INSTALLING THE INSIGHTS CLIENT ON SATELLITE SERVER CONTENT HOSTS

The Insights client comes preinstalled on most versions of Red Hat Enterprise Linux; however, if you have to install it, use this procedure to install the Insights client on each system.

Prerequisites

- Register your hosts to Satellite
If you already have Red Hat Enterprise Linux hosts, you can use the Global Registration Template to register them to Satellite. For more information, see [Registering hosts to Satellite](#).

Procedure

1. Install the Insights for Red Hat Enterprise Linux client:

```
# yum install insights-client
```

2. Register the host to Insights for Red Hat Enterprise Linux:

```
# insights-client --register
```

3. Repeat these steps on each host.

Alternatively, you can use the **RedHatInsights.insights-client** Ansible role to install the Insights client and register the hosts. For more information, see [Using Red Hat Insights with Hosts in Satellite](#) in the Red Hat Satellite *Managing Hosts* guide.

6.2. CONFIGURING CLOUD CONNECTOR AFTER UPGRADING SATELLITE SERVER 6.10 TO 6.11



NOTE

This only applies to upgrades from Satellite version 6.10 to 6.11. Refer to the [Upgrading and Updating Red Hat Satellite](#) guide for more information.

To configure Cloud Connector after upgrading the Satellite Server, click **Configure Cloud Connector** button from **Configure > RH Cloud - Inventory Upload** to enable it on the new version of Satellite Server. Simultaneously, you are required to remove the previous source from the cloud manually on the Red Hat Hybrid Cloud Console after upgrading your Satellite Server.

Once the Cloud Connector is configured, it will remove the receptor bits and install the RHC bits. At the same time, the Cloud Connector announces all the organizations in the Satellite to the source and is ready to receive the connections.

6.3. DISABLING DIRECT REMEDIATIONS ON A SATELLITE SERVER CONTENT HOST

By default the parameter is not set on each host. It is **True** *for the hostgroup* to allow the execution of playbooks by default on the Cloud Connector. Note that all the hosts that are present in that particular organization inherit the same parameters.

When the Satellite receives the remediation playbook run request from Cloud Connector, that request has a list of hosts where it should execute.

Complete the following step to ensure the playbook run does not get invoked from the cloud on a single host.

Procedure

1. Go to **Hosts menu** > **All Hosts** in the Satellite web UI.
2. Locate the host and click the **Edit button** > **Parameters tab** and set the **enable_cloud_remediations** parameter to **False** on that host.

6.4. DISABLING DIRECT REMEDIATION ON A SATELLITE SERVER CONTENT HOST GROUP

By default the parameter is not set in the *system*. It is **True** *for the host group* to allow the execution of playbooks by default with the Cloud Connector.



NOTE

All the hosts that are present in that particular organization will inherit the same parameters.

Optionally, an Organization Administrator can disable the cloud remediations for the whole organization or host group. To disable remediations, change the **Global Parameter** in the Red Hat Satellite User Interface. Use the following steps to make this edit.

Procedure

1. Navigate to the [Satellite Dashboard](#).
2. Click **Configure** on the left navigation.
3. Click **Global Parameters**.
4. Click **Create Parameter**.
5. In the **Name** field, enter **enable_cloud_remediations**.
6. In the **Value** field, enter **false**.
7. Click **Submit**.

Verification step

Find your new parameter listed in the **Global Parameters** table.

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.