Fixing issues on RHEL systems with remediation playbooks
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 CONSIDERATIONS ............................................................... 3
    1.1.1. 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 ON HOSTS MANAGED BY SATELLITE ....................... 6
    2.2.1. Uploading your host inventory from Satellite to Insights ......................... 6
    2.2.2. Installing the Insights client on hosts managed by Satellite ..................... 7
    2.2.3. Configuring Cloud Connector on Satellite Server .................................... 8
      2.2.3.1. Creating the Cloud Connector configuration playbook ......................... 8
      2.2.3.2. Enabling Cloud Connector operation on Satellite ............................... 8
      2.2.3.3. Verifying Satellite and Insights communication ................................... 8
      2.2.3.4. Enabling Auto Sync and perform initial manual sync ............................ 8
      2.2.3.5. Disabling direct remediations on a host ........................................... 9
      2.2.3.6. Disabling direct remediation on a host group .................................... 9
      2.2.3.7. Configuring inventory uploads ....................................................... 9
      2.2.3.8. Verifying successful configuration ................................................. 10
    2.2.4. Configuring Cloud Connector after upgrading Satellite Server 6.10 to 6.11 ............. 10
    2.2.5. Configuring Insights recommendations on Satellite .................................... 10

CHAPTER 3. CREATING AND MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS ............... 11
  3.1. CREATING A PLAYBOOK TO REMEDIATE A CVE VULNERABILITY ON RHEL SYSTEMS ......... 11
  3.2. MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS FOR RED HAT ENTERPRISE LINUX ..... 12
    3.2.1. Downloading a remediation playbook ................................................... 12
    3.2.2. Archiving a remediation playbook ...................................................... 12
    3.2.3. Viewing archived remediation playbooks .............................................. 13
    3.2.4. Deleting a remediation playbook ....................................................... 13
    3.2.5. Monitoring remediation status ............................................................ 13

CHAPTER 4. EXECUTING REMEDIATION PLAYBOOKS ................................................. 14
  4.1. EXECUTING REMEDIATION PLAYBOOKS FROM INSIGHTS FOR RED HAT ENTERPRISE LINUX .... 14

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION ............................................ 15
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 CONSIDERATIONS

An Organization Administrator on your account configures settings in User Access to control access to Red Hat Insights for Red Hat Enterprise Linux features. All users on your account have access to most of the data in Insights for Red Hat Enterprise Linux. However, performing some actions requires users to have elevated access.

Access is granted in User Access in the Red Hat Hybrid Cloud Console. To grant or change access, an Organization Administrator or User Access administrator must add you to a User Access group with the required roles in Red Hat Hybrid Cloud Console > Settings menu (gear icon) > Identity & Access Management > User Access.

IMPORTANT

In this documentation, prerequisites for procedures declare whether you need elevated access to perform the procedure.

Important predefined groups and roles relevant to understanding User Access are:

- Default access group
- Default admin group
- Organization Administrator role

Brief overview about some predefined groups and roles

The following predefined groups and roles are relevant to access:
- **Default access group.** All users on the account are members of the Default access group. Members of the Default access group have read-only access, which allows you to view most information in Insights for Red Hat Enterprise Linux.

- **Default admin access group.** All users on the account who are Organization Administrators are members of this group. Users cannot modify the roles in the Red Hat-managed Default admin access group. Members of the Default admin access group have read-write access, which allows you to view and perform other actions in Insights for Red Hat Enterprise Linux.

- **Organization Administrator role.** All users on the account who are Organization Administrators can create and modify User Access groups and grant access to other account users. To find out whether you are an Organization Administrator, click your name in the Red Hat Hybrid Cloud Console header, in the upper right of your screen, and see whether the words “Org. Administrator” show under your username.

**IMPORTANT**

**Requesting elevated access** If you do not have access to features that you need, you can:

- Contact [Customer Service](#) to get Organization Administrator details for your account.
  - Provide your account number when you send the request.

- Contact the Organization Administrator and ask for access, providing the following information:
  - The name of the role you need access to, for example, Remediations administrator
  - A link to [full User Access documentation](#), to help inform the Organization Administrator about how to give you access.

### 1.1.1. 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.

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-playbook-worker. To install the dependencies, you must first register with Subscription Manager.

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

  ```bash
  [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.

  ```bash
  [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.

  ```bash
  [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 > Settings > Remote Host Configuration > Manage configuration.

For complete rhc documentation, see Remote Host Configuration and Management.

2.2. ENABLING CLOUD CONNECTOR ON HOSTS MANAGED BY SATELLITE

Before you can remediate issues in your Satellite infrastructure, you must connect your hosts to Insights for Red Hat Enterprise Linux and configure Cloud Connector on Satellite Server.

IMPORTANT

If you want to manage and execute host remediations completely from Satellite, then you do not need to enable Cloud Connector. Cloud Connector enables the remediation of Satellite-managed hosts remotely, from Insights for Red Hat Enterprise Linux.

The following prerequisites are comprehensive for Satellite configuration:

Prerequisites

- Satellite must be version 6.9 or later.
- Import a Subscription Manifest into Satellite. Only hosts in organizations with a valid Red Hat certificate can be connected to Red Hat Hybrid Cloud Console. 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.
- Enable remote execution on your hosts so that Satellite can run remediation playbooks on them. For more information, see Distributing SSH Keys for Remote Execution in the Red Hat Satellite Managing Hosts guide.
- Ensure Enable auto upload is checked on the Configure > Inventory upload page
- Ensure that Sync automatically is checked on the Configure > Insights page.

NOTE

This step also shows recommendation counts on Satellite’s hosts list page and the recommendations tab on the host details page.

2.2.1. Uploading your host inventory from Satellite to Insights

Use this procedure to upload your host inventory from Red Hat Satellite to Red Hat Insights for Red Hat Enterprise Linux.

Prerequisites

- Register your hosts to Satellite using an activation key to attach Red Hat subscriptions.
- You have root access to the Satellite service.
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
      ```

2. In the Satellite web UI, navigate to **Configure > Inventory Upload**. The **Automatic Inventory Upload** switch is **ON** by default.

3. Click **Configure Cloud Connector**. A Notice dialog box warns you that your inventory will be automatically uploaded. Click **Confirm**.

4. Navigate to **Configure > Inventory Upload** and select your organization.

5. Click **Restart** to upload your host inventory to Red Hat Insights for Red Hat Enterprise Linux. Repeat this step for each organization from which you want to upload a host inventory.

6. **Optional**: Toggle the **Obfuscate host names** switch to the **ON** position to hide host names that Satellite reports to the Red Hat Hybrid Cloud Console. 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.

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

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 hosts.

Optionally, push the **Sync inventory status** button and wait for the task to finish. It will show you the amounts of Satellite hosts recognized also on the cloud side.

### 2.2.2. Installing the Insights client on hosts managed by Satellite

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

```
# 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.

2.2.3. Configuring Cloud Connector on Satellite Server

Before you can remotely run remediation playbooks on your Satellite-managed infrastructure, you must install and configure the Cloud Connector on Satellite Server. Perform the following tasks to install, configure, and verify the configuration of Cloud Connector.

2.2.3.1. Creating the Cloud Connector configuration playbook

A Satellite administrator can install and configure the Cloud Connector by activating the Configure Cloud Connector button. This automatically creates the service user that the Cloud Connector will use to trigger remediation jobs on Satellite, then runs the Cloud Connector installation playbook using the service-user credentials.

2.2.3.2. Enabling Cloud Connector operation on Satellite

To ensure that the Cloud Connector operates, verify that Automatic Inventory Upload (Configure > Inventory Upload) and Sync Automatically (Configure > Insights) are turned ON.

For more information about running remediations from Satellite, see section, Creating an Insights Plan for Hosts, in Managing Hosts Red Hat Satellite 6.12.

2.2.3.3. Verifying Satellite and Insights communication

Perform these tasks manually to verify the system functions. Refer to the following steps:

- **By uploading the report:** Select the required organization from the inventory page, and click Restart. This step is asynchronous and it may take time to be processed by the cloud.

- **By syncing Insights information:** Select the three dots menu from the Insights page, and click Sync Recommendations.

- **Optional; verify the status of the new source record:** The source record would look like Satellite <UUID> organization <org_name> under Red Hat Hybrid Cloud Console > Settings > Sources. The source should indicate “Available” before the remediations are able to run.

2.2.3.4. Enabling Auto Sync and perform initial manual sync

Click Sync Inventory Status and enable Auto Sync for the organization.

**IMPORTANT**

Make sure to sync manually for the first time before it starts.
It is normal that while syncing the inventory, you might get a notification indicating the number of hosts that are in disconnected status or not uploaded to your Hybrid Cloud Console inventory. At this stage, you must re-sync the inventory. In some cases, the host processing at Hybrid Cloud Console can take some time to remediate.

2.2.3.5. Disabling direct remediations on a host

By default the parameter is not set on each host. It is set to 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 be executed.

To ensure the playbook run does not get invoked from the cloud on a single host, set the enable_cloud_remediations parameter to False on that host.

2.2.3.6. Disabling direct remediation on a host group

By default the parameter is not set in the system. It is set to 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.

2.2.3.7. Configuring inventory uploads

1. In the Satellite web UI, navigate to Configure > Inventory Upload.
2. Click on the **Configure Cloud Connector** button.

### 2.2.3.8. Verifying successful configuration

To verify that the playbook was successful, log into Red Hat Hybrid Cloud Console > Settings > Sources and search for your Satellite Server.

### 2.2.4. 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.

### 2.2.5. Configuring Insights recommendations on Satellite

You can use Red Hat Satellite synchronization to provide Insights for Red Hat Enterprise Linux recommendations for Satellite-managed hosts. Use this procedure to configure Insights synchronization on Red Hat Satellite.

**Procedure**

1. Navigate to **Configure > Insights** to manually synchronize Insights for Red Hat Enterprise Linux recommendations. Click the **more options** icon and choose **Sync recommendations**.

2. Optionally, toggle the **Synchronize Automatically** switch to the **ON** position to enable Satellite to download Insights recommendations from the Hybrid Cloud Console automatically, once a day.

You have now configured Red Hat Insights for Red Hat Enterprise Linux Synchronization on Satellite.

In the Satellite web UI, navigate to **Hosts > All Hosts** to see Insights for Red Hat Enterprise Linux recommendations for each Satellite-managed host.
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 one Insights service. For example, a playbook created using the vulnerability service will only contain resolutions for vulnerability-service CVEs and not also advisor-service recommendations.

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

**Verification step**

1. Navigate to **Automation Toolkit > Remediations**.

2. Search for your playbook. You should see your playbook.

### 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 More 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 playbook 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 organizations Ansible workflow, or execute the playbook on remote systems from the Insights for Red Hat Enterprise Linux application.

4.1. EXECUTING REMEDIATION PLAYBOOKS FROM INSIGHTS FOR RED HAT ENTERPRISE LINUX

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.
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.