Red Hat Insights 1-latest

Red Hat Insights Remediations Guide with FedRAMP

Fixing issues on RHEL systems with remediation playbooks

Last Updated: 2024-06-27

Red Hat Insights 1-latest Red Hat Insights Remediations Guide with FedRAMP

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 playbooks to remediate issues on any system registered with Insights with FedRAMP®. 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
1.1.2. User Access roles for remediations users 3

CHAPTER 2. CREATING AND MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS 4
2.1. CREATING A PLAYBOOK TO REMEDIATE A CVE VULNERABILITY ON RHEL SYSTEMS 4
2.1.1. Creating playbooks to remediate CVEs with security rules when recommended and alternate resolution options exist 5
2.2. MANAGING REMEDIATION PLAYBOOKS IN INSIGHTS FOR RED HAT ENTERPRISE LINUX 9
2.2.1. Downloading a remediation playbook 9
2.2.2. Archiving a remediation playbook 9
2.2.3. Viewing archived remediation playbooks 9
2.2.4. Deleting a remediation playbook 10
2.2.5. Monitoring remediation status 10

CHAPTER 3. USING PATCH TEMPLATES FOR REMEDIATIONS 11
3.1. USING PATCH TEMPLATES WITH REMEDIATIONS 11

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION 12

CHAPTER 1. REMEDIATIONS OVERVIEW

After identifying the highest remediation priorities in your Red Hat Enterprise Linux (RHEL) infrastructure, you can create remediation playbooks that 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

- All Insights users will automatically have access to read, create, and manage remediation playbooks.

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

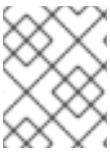
All users on your account have access to most of the data in Insights for Red Hat Enterprise Linux.

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.

1.1.2. User Access roles for remediations users

The Remediations Viewer role enables standard or enhanced access to remediations features in Insights for Red Hat Enterprise Linux. 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.

CHAPTER 2. 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.

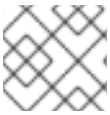
Playbooks focus on issues identified by Insights services. A recommended practice for playbooks is to include systems of the same RHEL major/minor versions because the resolutions will be compatible.

2.1. 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.

2.1.1. 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

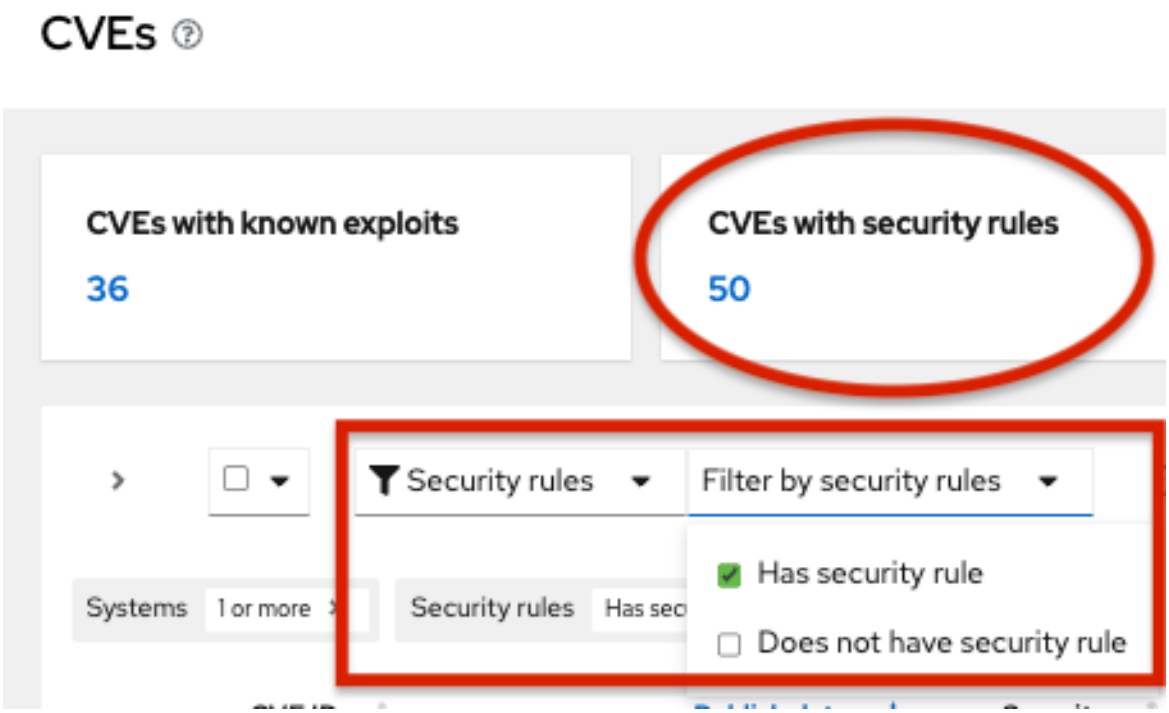
- You are logged into the Red Hat Hybrid Cloud Console.

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.



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.

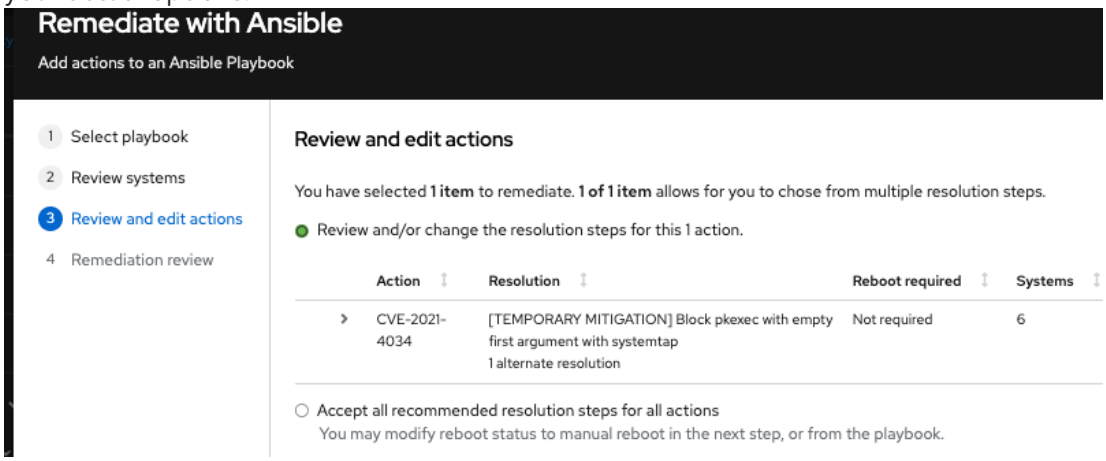
8. Review the systems to include in the playbook (deselect any systems that you do not want to include).

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.

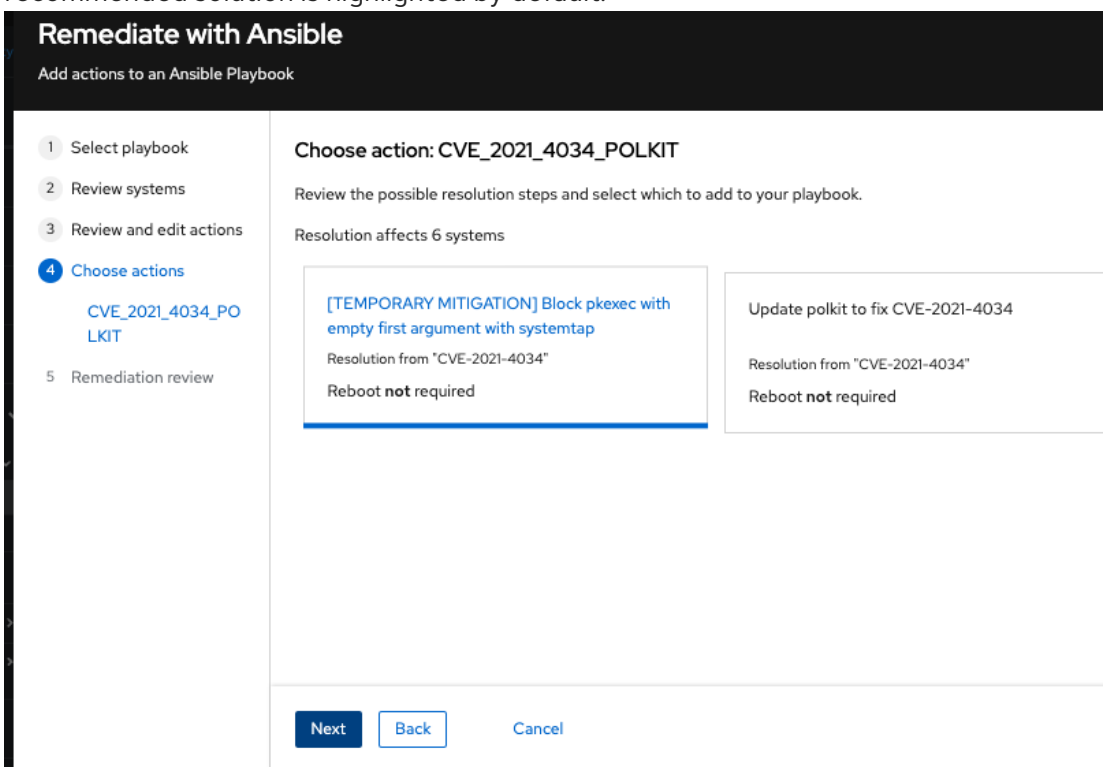
- **Resolution:** Displays the recommended resolution for the CVE. Shows if you have alternate resolution options.
- **Reboot required:** Shows whether you must reboot your systems.
- **Systems:** Shows the number of systems you are remediating.

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.



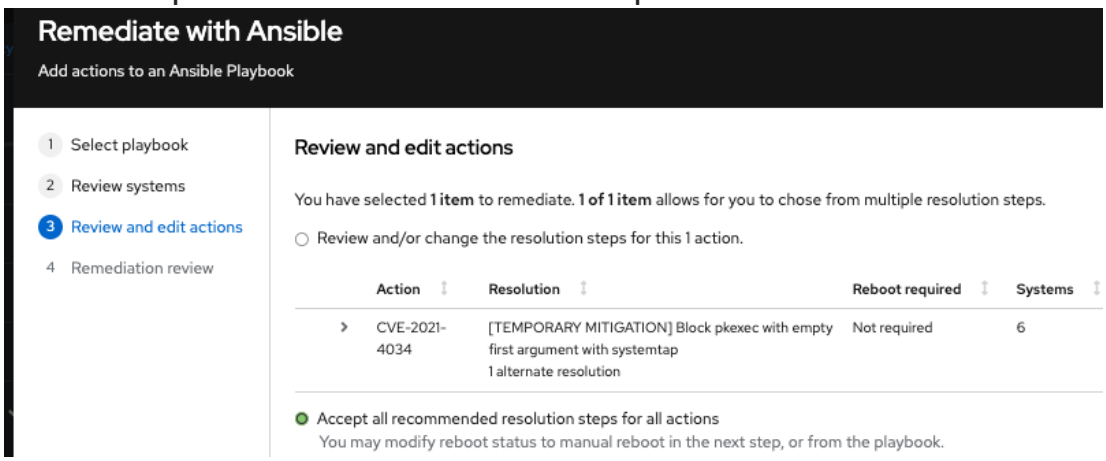
        b. Click **Next**.

        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.

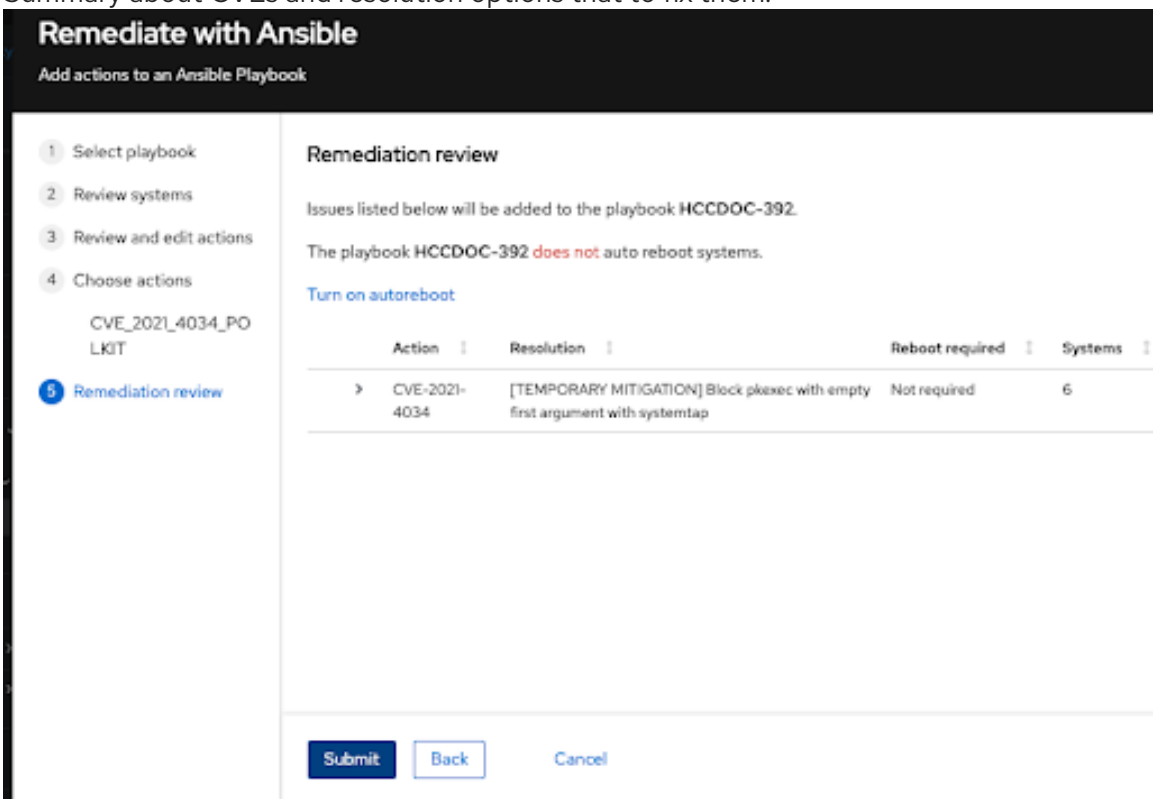


        d. Click **Next**.

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



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.



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.

2.2. 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.

2.2.1. 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.

2.2.2. 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.

2.2.3. 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.

2.2.4. 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**.

2.2.5. Monitoring remediation status

You can view the remediation status for each playbook. The status information tells you the results of the latest activity and provides a summary of all activity for that playbook. You can also view log information.

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 3. USING PATCH TEMPLATES FOR REMEDIATIONS

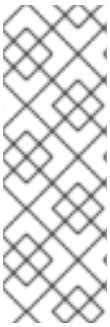
The Red Hat Insights patch application supports scheduled patching cycles.

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.

3.1. 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 with FedRAMP* .

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.