Red Hat Insights 1-latest

System Patching Using Remediation Playbooks with FedRAMP

How to review applicable advisories and affected systems

Last Updated: 2024-05-10

Red Hat Insights 1-latest System Patching Using Remediation Playbooks with FedRAMP

How to review applicable advisories and affected systems

Red Hat Customer Content Services

Legal Notice

Abstract

This document demonstrates how to review applicable advisories and affected systems with FedRAMP® in your environment and perform remediations. 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.

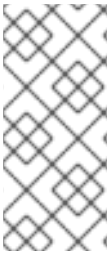
Table of Contents

CHAPTER 1. PATCH SERVICE OVERVIEW

Patch leverages Red Hat software and management automation expertise to enable consistent patch workflows for Red Hat Enterprise Linux (RHEL) systems across the open hybrid cloud. It provides a single canonical view of applicable advisories across all of your deployments, whether they be Red Hat Satellite, hosted Red Hat Subscription Management (RHSM), or the public cloud.

Use the Insights patch service to

- see all of the applicable Red Hat and Extra Packages for Enterprise Linux (EPEL) advisories for your RHEL systems checking into Insights.
- patch any system with one or more advisories by using remediation playbooks.
- see package updates available for Red Hat and non-Red Hat repositories as of the last system checkin. Your host must be running Red Hat Enterprise Linux (RHEL) 7, RHEL 8.6+ or RHEL 9 and it must maintain a fresh **yum**/**dnf** cache.



NOTE

- Configure Role Based Access Control (RBAC) in Red Hat Hybrid Cloud Console > the **Settings** icon (⚙) > Identity & Access Management > User Access > Users .
- See *User Access Configuration Guide for Role-based Access Control (RBAC)* for more information about this feature and example use cases.

1.1. CRITERIA FOR PATCH AND VULNERABILITY ERRATA

The patch service collects a variety of data to create meaningful and actionable errata for your systems. The Insights client collects the following data on each checkin:

- List of installed packages, including name, epoch, version, release, and architecture (NEVRA)
- List of enabled modules (RHEL 8 and later)
- List of enabled repositories
- Output of **yum updateinfo -C** or **dnf updateinfo -C**
- Release version from systems with a version lock
- System architecture (eg. **x86_64**)

Additionally, Insights for Red Hat Enterprise Linux collects metadata from the following data sources:

- Metadata from product repositories delivered by the Red Hat Content Delivery Network (CDN)
- Metadata from Extra Packages for Enterprise Linux (EPEL) repositories
- Red Hat Open Vulnerability and Assessment Language (OVAL) feed

Insights for Red Hat Enterprise Linux compares the set of system data to the collected errata and vulnerability metadata in order to generate a set of available updates for each system. These updates include package updates, Red Hat errata, and Common Vulnerabilities and Exposures (CVEs).

Additional resources

For more information about Common Vulnerabilities and Exposures (CVEs), refer to the following resources:

- *Assessing and Monitoring Security Vulnerabilities on RHEL Systems*
- Security > Vulnerability > CVEs

1.2. REVIEWING AND FILTERING APPLICABLE ADVISORIES AND SYSTEMS IN THE INVENTORY

You can see all of the applicable advisories and installed packages for systems checking into Red Hat Insights for Red Hat Enterprise Linux.

Procedure

1. On Red Hat Hybrid Cloud Console , navigate to Content > Advisories.
2. You can also search for advisories by name using the search box, and filter advisories by:
   a. Type - Security, Bugfix, Enhancement, Unknown
   b. Publish date - Last 7 days, 30 days, 90 days, Last year, or More than 1 year ago
3. Navigate to Content > Patch > Systems to see a list of affected systems you can patch with applicable advisories. You can also search for specific systems using the search box.
4. Navigate to Content > Packages to see a list of packages with updates available in your environment. You can also search for specific packages using the search box.

1.3. SYSTEM PATCHING USING INSIGHTS REMEDIATION PLAYBOOKS

The following steps demonstrate the patching workflow from the Content > Advisories page in Red Hat Insights for Red Hat Enterprise Linux:

Procedure

1. On Red Hat Hybrid Cloud Console , navigate to Content > Advisories.
2. Click the advisory you want to apply to affected systems. You will see a description of the advisory, a link to view packages and errata at access.redhat.com, and a list of affected systems. The total number of applicable advisories of each type (Security, Bugfix, Enhancement) against each system are also displayed.
3. Select the system(s) for which you want to create a playbook, then click **Remediate**.
4. You can choose to modify an existing Playbook or create a new one. Accordingly, select **Existing Playbook** and the playbook name from the drop-down list, then click **Next**. Or, select **Create new Playbook** and enter a name for your playbook, then click **Next**.
5. On the left navigation, click on Remediations.
6. Click on the playbook name to see the playbook details, or simply select and click **Download playbook**.

1.4. UPDATING ERRATA FOR SYSTEMS MANAGED BY RED HAT SATELLITE

Insights for Red Hat Enterprise Linux calculates applicable updates based on the packages, repositories, and modules that a system reports when it checks in. Insights combines these results with a client-side evaluation, and stores the resulting superset of updates as applicable updates.

A system check-in to Red Hat Insights includes the following content-related data:

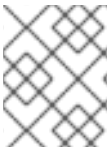
- Installed packages
- Enabled repositories
- Enabled modules
- List of updates, which the client determines using the **dnf updateinfo -C** command. This command primarily captures package updates for non-Red Hat repositories

Insights uses this collection of data to calculate applicable updates for the system.

Sometimes Insights calculates applicable updates for systems managed by Red Hat Satellite and reports inaccurate results. This issue can manifest in two ways:

- Insights shows installable updates that cannot be installed on the Satellite-managed system.
- Insights shows applicable updates that match what can be installed on the system immediately after patching, but shows outdated or missing updates a day or two later. This can occur when the system is subscribed to RHEL repositories that have been renamed.

Insights now provides an optional check-in command to provide accurate reporting for applicable updates on Satellite-managed systems. This option rebuilds the **yum**/**dnf** package caches and creates a refreshed list of applicable updates for the system.



NOTE

Satellite-managed systems are not eligible to have Red Hat Insights content templates applied.

Prerequisites

- Admin-level access to the system

Procedure

- To rebuild the package caches from the command line, enter the following command:

```
# insights-client --build-packagecache
```

The command regenerates the **dnf**/**yum** caches and collects the relevant installable errata from Satellite. **insights-client** then generates a refreshed list of updates and sends it to Insights.

NOTE

The generated list of updates is equivalent to the output from the command **dnf updateinfo list**.

1.4.1. Configuring automatic check-in for insights-client

You can edit the **insights-client** configuration file on your system (**/etc/insights-client/insights-client.conf**) to rebuild the package caches automatically each time the system checks in to Insights.

Procedure

1. Open the **/etc/insights-client/insights-client.conf** file in a text editor.
2. Look in the file for the following comment:

```
#Set build_packagecache=True to refresh the yum/dnf cache during the insights-client check-in
```

3. Add the following line after the comment:

```
build_packagecache=True
```

4. Save your edits and exit the editor.

When the system next checks in to Satellite, **insights-client** executes a **yum/dnf** cache refresh before collecting the output of the client-side evaluation. Insights then reports the client-side evaluation output as installable updates. The evaluation output, based on what has been published to the CDN, is reported as applicable updates.

Additional resources

- For more information about the **--build-packagecache** options, see the following KCS article: https://access.redhat.com/solutions/7041171
- For more information about managing errata in Red Hat Satellite, see https://access.redhat.com/documentation/en-us/red_hat_satellite/6.15/html/managing_content/managing_errata_content-management.

1.5. ENABLING NOTIFICATIONS AND INTEGRATIONS

You can enable the notifications service on Red Hat Hybrid Cloud Console to send notifications whenever the patch service detects an issue and generates an advisory. Using the notifications service frees you from having to continually check the Red Hat Insights for Red Hat Enterprise Linux dashboard for advisories.

For example, you can configure the notifications service to automatically send an email message whenever the patch service generates an advisory.

Enabling the notifications service requires three main steps:

- First, an Organization Administrator creates a User Access group with the Notifications-administrator role, and then adds account members to the group.
- Next, a Notifications administrator sets up behavior groups for events in the notifications service. Behavior groups specify the delivery method for each notification. For example, a behavior group can specify whether email notifications are sent to all users, or just to Organization Administrators.

- Finally, users who receive email notifications from events must set their user preferences so that they receive individual emails for each event.

In addition to sending email messages, you can configure the notifications service to send event data using an authenticated client to query Red Hat Insights APIs.

Additional resources

- For more information about how to set up notifications for patch advisories, see *Configuring notifications on the Red Hat Hybrid Cloud Console with FedRAMP*.

CHAPTER 2. APPLYING PATCHES TO SYSTEMS IN THE RED HAT HYBRID CLOUD CONSOLE

The Red Hat Insights patch application supports scheduled patching cycles. 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.

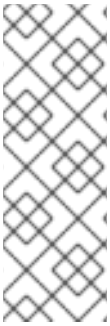
2.1. HOW PATCH TEMPLATES WORK

The Red Hat Insights patch application supports scheduled patching cycles. 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.

Use patch templates to enter criteria that limit the scope of advisories that apply to your systems. For example, you can create a template to show only applicable advisories that were published up to the date of your current patching cycle. After you create the template, use the wizard to add systems and select the date of the patching cycle. When you have finished adding systems to the patch template, you can remediate all the installable advisories for the selected group of systems.

If a system already has a patch template applied, applying a different patch template overrides the existing template. A system can only have one patch template at a time.

For more information about remediations, see the *Red Hat Insights Remediations Guide* .



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* .

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.

2.2. CREATING A PATCH TEMPLATE

You can create a patch template to limit the scope of advisories that apply to your systems. For example, you can ignore advisories that were published after the date of your current patching cycle.

Prerequisites

- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Templates .
2. Click **Create a template**. The Create patch template wizard opens and displays the **Create content template** page.

3. Click the date icon to select the Patch template date. The patch template applies advisories published up to the selected date. Click **Next**.
4. Enter a unique name for the template in the **Name** field.
5. **Optional:** Add a description for the template in the **Description** field.
6. Click **Next**. The **Apply to systems** page displays.
7. **Optional:** Select the systems that you want to assign to the template and click **Next**. The **Review** page displays.
8. Review the template information. When you have finished reviewing, click **Submit**.

A few minutes after you have finished creating the template, the system updates its list of installable advisories. The update time depends on the number of systems in your installation.

Additional resources

- For more information about remediations, see the *Red Hat Insights Remediations Guide* .

2.3. EDITING AN EXISTING PATCH TEMPLATE

Edit the patch template to update the patch template name or description, set a new date for your next patching cycle, or add or remove systems.

Prerequisites

- You have already created a patch template.
- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Templates . The list of available patch templates displays.
2. Locate the patch template that you want to edit.
3. Click the menu button on the far right side of the row that contains the template. A pop-up menu appears.
4. Select **Edit template**. The Edit template wizard opens and displays the **Edit content template** page.
5. **Optional:** Edit the patch template date. Click **Next**. The **Edit template details** page displays.
6. **Optional:** Edit the template name and description. Click **Next**. The **Apply to systems** page displays.
7. Add or remove systems assigned to the template and then click **Next**. The **Review** page displays.
8. Review the updated template information. When you have finished reviewing, click **Submit**.

If you edited the patch template date or added or removed assigned systems from the template, the system updates its list of installable advisories within a few minutes. The update time depends on the number of systems in your installation.

2.4. ADDING OR REMOVING SYSTEMS FROM THE PATCH TEMPLATE

To add systems to the patch template or to remove systems from the template, use the Edit template wizard.

Prerequisites

- You have already created a patch template.
- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Templates. The list of available patch templates displays.
2. Locate the patch template that you want to edit.
3. Click the menu button on the far right side of the row that contains the template. A pop-up menu appears.
4. Select **Edit template**. The Edit template wizard opens and displays the **Edit content template** page.
5. **Optional:** Edit the Patch template date.
6. Click **Next**. The **Edit template details** page displays.
7. **Optional:** Edit the template name and description.
8. Click **Next**. The **Apply to systems** page displays.
9. Add or remove systems assigned to the template and then click **Next**. The **Review** page displays.
10. Review the updated template information. When you have finished reviewing, click **Submit**.

The system updates its list of installable advisories within a few minutes. The update time depends on the number of systems in your installation.

2.5. APPLYING AN EXISTING PATCH TEMPLATE TO SELECTED SYSTEMS

You can apply an existing patch template to individual systems that you select from a list.

Prerequisites

- You have already created a patch template.
- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Systems . The list of available systems displays.
2. Select a system or systems to which you want to apply the patch template.
3. Click the More options menu beside the Remediate button and Export icon.
4. Select **Assign to a template**. The Apply template dialog box displays.
5. Click **Select an existing template**, and then select a template from the drop-down list.
6. Click **Apply template** to apply the template to the selected systems.

The selected systems update within a few minutes. The update time depends on the number of systems in your installation.

2.6. REMOVING A PATCH TEMPLATE

You might want to remove a patch template if you want to assign a system or systems to a different patch template, or if you want the systems to receive patches and updates that have creation dates outside the boundaries of the current patch template.

Prerequisites

- You have already created a patch template.
- The template has systems assigned to it.
- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Templates . The list of available patch templates displays.
2. Locate the patch template that you want to remove.
3. Click the menu button on the far right side of the row that contains the template. A pop-up menu appears.
4. Select **Remove patch template**.

A few minutes after you have removed the template, the system updates its list of installable advisories. The update time depends on the number of systems in your installation.

2.7. APPLYING A NEW PATCH TEMPLATE TO SELECTED SYSTEMS

After you select individual systems from a list, you can create a new patch template to apply to the selected systems.

Prerequisites

- You have already created a patch template.

- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Systems . The list of available systems displays.
2. Select a system or systems for which you want to create a new patch template.
3. Click the More options (three dots) menu beside the Remediate button and the Export icon.
4. Select **Assign to a template**. The Apply template dialog box displays.
5. Click the **Create** button. The Create content template wizard opens and displays the **Define template content** page.
6. Click the date icon. Select a date to apply all installable advisories published up to that date, and then click **Next**. The **Details** page displays.
7. Enter a unique name for the template in the **Name** field.
8. **Optional:** Add a description for the template in the **Description** field.
9. Click **Next**. The **Apply to systems** page appears, and shows the list of systems that you selected.

NOTE

If a system already has an assigned patch template, the new patch template overrides the previous template.

10. Click **Next**. The **Review** page displays.
11. Review the template information. When you have finished reviewing, click **Submit**.

The selected systems update within a few minutes. The update time depends on the number of systems in your installation.

2.8. REMOVING A PATCH TEMPLATE FROM SELECTED SYSTEMS

You can select systems from a list and remove an applied patch template from those systems. Removing the template from the systems does not delete the template.

Prerequisites

- You have already created a patch template.
- The patch template has been applied to systems in your installation.
- You are logged into the Red Hat Hybrid Cloud Console as an Organization Administrator.

Procedure

1. Use the left menu to navigate to Content > Patch > Systems . The list of available systems displays. The Template column in the list shows the systems that have applied patch templates, as well as the names of the templates.
2. Select a system or systems for which you want to create a new patch template.
3. Click the More options (three dots) menu beside the Remediate button and the Export icon.
4. Select **Remove from a template**. The **Remove systems from a patch template**dialog box displays.
5. Click the **Remove** button. A success message appears.

The selected systems show a status of **No template** in the Template column. The update time depends on the number of systems in your installation.

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.