Red Hat Insights 2022

System Patching Using Ansible Playbooks via Remediations

How to review applicable advisories and affected systems and remediate using Ansible playbooks

Last Updated: 2022-12-22

Red Hat Insights 2022 System Patching Using Ansible Playbooks via Remediations

How to review applicable advisories and affected systems and remediate using Ansible playbooks

Red Hat Customer Content Services

Legal Notice

Abstract

This document demonstrates how to review applicable advisories and affected systems in your environment and perform remediation using Ansible playbooks.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

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.

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 that be Red Hat Satellite, hosted Red Hat Subscription Management (RHSM), or the public cloud.

Using Patch you can:

- 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 Ansible playbooks via Remediations.
- 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 7, Red Hat Enterprise Linux 8.6+ or Red Hat Enterprise Linux 9 and it must maintain a fresh yum/dnf cache.

NOTE

- Configure Role Based Access Control (RBAC) in Red Hat Insights for Red Hat Enterprise Linux > Settings > User Access.
- 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), reference the following resources:

- *Assessing and Monitoring Security Vulnerabilities on RHEL Systems*
- Red Hat Enterprise Linux > Vulnerability > CVEs

CHAPTER 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 Red Hat Enterprise Linux > Patch > 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 Red Hat Enterprise Linux > 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 Red Hat Enterprise Linux > Patch > Patch packages to see a list of packages with updates available in your environment. You can also search for specific packages using the search box.

CHAPTER 3. SYSTEM PATCHING USING ANSIBLE PLAYBOOKS VIA REMEDIATIONS

The following steps demonstrate the patching workflow via the **Advisories** tab:

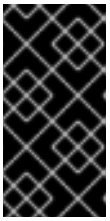
Procedure

1. On Red Hat Hybrid Cloud Console, navigate to Red Hat Enterprise Linux > Patch > 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. As a bulk operation, you can click the options menu located next to a system, then click **Apply all applicable advisories** to patch the system with all applicable advisories at once.
3. Alternatively, select the system(s) you want to patch with this particular advisory, then click **Remediate**.
4. On the Remediate with Ansible page, you can choose to modify an existing Playbook or create a new one to remediate with Ansible. 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. You will then see a summary of the action and resolution. Your system will auto reboot by default. If you desire to disable this functionality, click on the blue link that states "turn off auto reboot." Click **Submit**.
6. On the left navigation, click on Remediations.
7. Click on the playbook name to see the playbook details, or simply select and click **Download playbook**.

The following steps demonstrate the patching workflow via the **Systems** tab:

1. Click the **Systems** tab to see a list of affected systems. As a bulk operation, you can click the options menu located next to a system, then click **Apply all applicable advisories** to patch the system with all applicable advisories at once.
2. Alternatively, click the system you want to patch. You will see the system details and a list of applicable advisories for remediation, along with additional details such as the advisory publish date, type, and synopsis. Select the advisories you want to apply to the system, then click **Remediate**.
3. On the Remediate with Ansible page, you can either modify an existing Playbook or create a new one to remediate with Ansible. Accordingly, click **Existing Playbook** and select the playbook name from the drop-down list, then click **Next**. Or, click **Create new Playbook**, enter a name for your playbook, then click **Next**.
4. You will then see a summary of the action and resolution. Your system will auto reboot by default. If you desire to disable this functionality, click on the blue link that states "turn off auto reboot." Click **Submit**.
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**.



IMPORTANT

Review and test any recommended actions and the playbook, and if you deem appropriate, deploy on your systems running Red Hat software. Red Hat is not responsible for any adverse outcomes related to these recommendations or Playbooks.

CHAPTER 4. 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 in other ways:

- Using an authenticated client to query Red Hat Insights APIs for event data
- Using webhooks to send events to third-party applications that accept inbound requests
- Integrating notifications with applications such as Splunk to route patch advisories to the application dashboard

Additional resources

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

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.