Red Hat Insights 2020-10

System Patching Using Ansible Playbooks via Remediations

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

Last Updated: 2020-11-02

Red Hat Insights 2020-10 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. Providing Feedback: If you have a suggestion to improve this document or find an error, submit a Bugzilla report at http://bugzilla.redhat.com against Cloud Software Services (cloud.redhat.com) for the Patch component.

Table of Contents

CHAPTER 1. 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 advisories for your RHEL systems checking into Insights
- patch any system with one or more advisories by using Ansible playbooks via Remediations

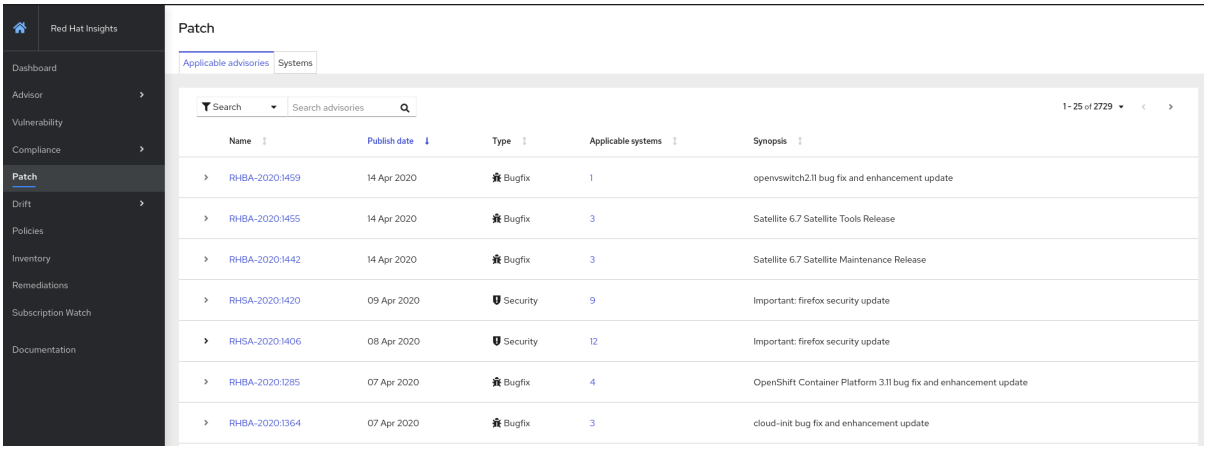
NOTE

- Use the Role Based Access Control (RBAC) capability in https://cloud.redhat.com (Settings  > User access) to control user access for Patch.
- See Role Based Access Control for Red Hat Insights and cloud management services for Red Hat Enterprise Linux for more information about this feature and example use cases.

CHAPTER 2. REVIEWING AND FILTERING APPLICABLE ADVISORIES AND SYSTEMS IN THE INVENTORY

You can see all of the applicable advisories for systems checking into Red Hat Insights.

1. In the cloud.redhat.com platform, click Patch under Red Hat Insights. You can see a list of applicable advisories under the **Applicable advisories** tab (shown by default).



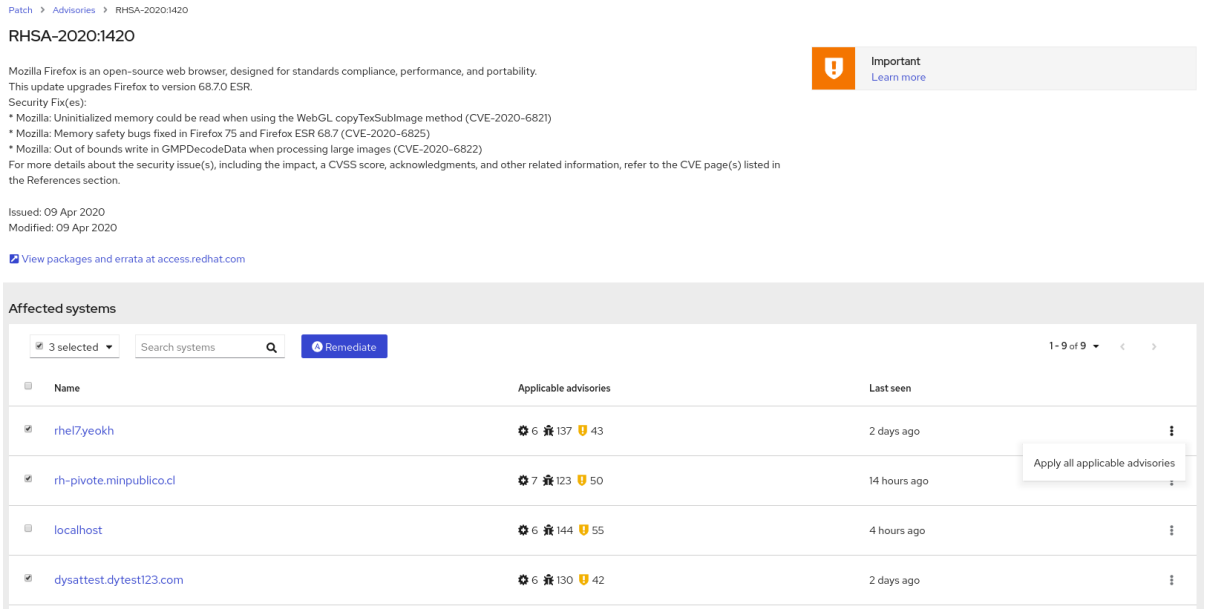
2. You can also search for advisories by name using the search box, and filter advisories by:
   a. Type - Security, Bugfix, Enhancement, Unknown
   b. Publish date - Last 7 days, 30 days, 90 days, Last year, or More than 1 year ago
3. Click on the **Systems** tab to see a list of affected systems you can patch with applicable advisories. You can also search for specific systems using the search box.

CHAPTER 3. SYSTEM PATCHING USING ANSIBLE PLAYBOOKS VIA REMEDIATIONS

The following steps demonstrate the patching workflow via the **Applicable advisories** tab:

1. In the cloud.redhat.com platform, click Patch under Red Hat Insights. You will see a list of applicable advisories under the **Applicable advisories** tab (shown by default).

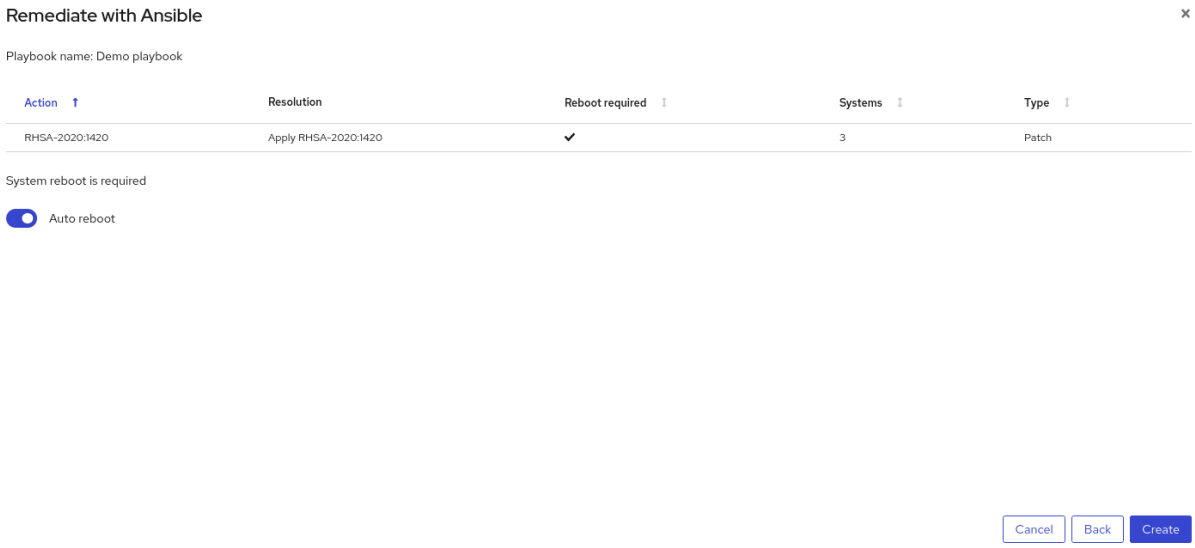
2. Click the advisory you want to apply to affected systems. You will see a description of the advisory, a link to view packages and errata at access.redhat.com, and a list of affected systems. The total number of applicable advisories of each type (Security, Bugfix, Enhancement) against each system 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. If you want to reboot the system upon remediation, click the toggle switch to activate **Auto reboot**. Click **Create**.



6. In the Red Hat Insights user interface, click Remediations in the left-side menu.

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.

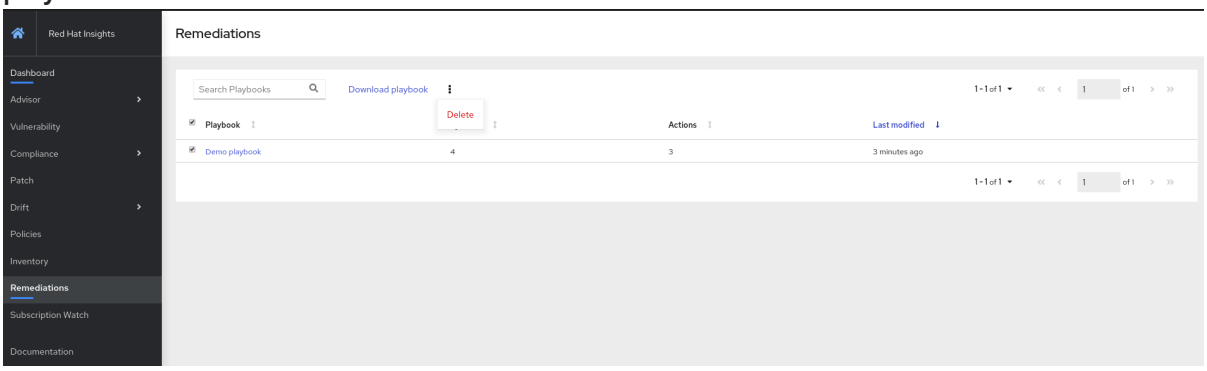
2. Alternatively, click the system you want to patch. You will see the system details and a list of applicable advisories for remediation, along with additional details such as the advisory publish date, type, and synopsis. Select the advisories you want to apply to the system, then click **Remediate**.

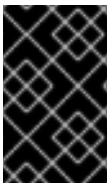
3. On the Remediate with Ansible page, you can either modify an existing Playbook or create a new one to remediate with Ansible. Accordingly, click **Existing Playbook** and select the playbook name from the drop-down list, then click **Next**. Or, click **Create new Playbook**, enter a name for your playbook, then click **Next**.

4. You will then see a summary of the action and resolution. If you want to reboot the system upon remediation, click the toggle switch to activate **Auto reboot**. Click **Create**.

5. In the Red Hat Insights user interface, click Remediations in the left-side menu.

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.