



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 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

Copyright © 2020 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

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

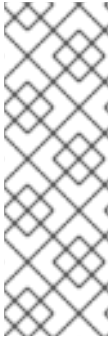
CHAPTER 1. OVERVIEW	3
CHAPTER 2. REVIEWING AND FILTERING APPLICABLE ADVISORIES AND SYSTEMS IN THE INVENTORY	4
CHAPTER 3. SYSTEM PATCHING USING ANSIBLE PLAYBOOKS VIA REMEDIATIONS	5

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



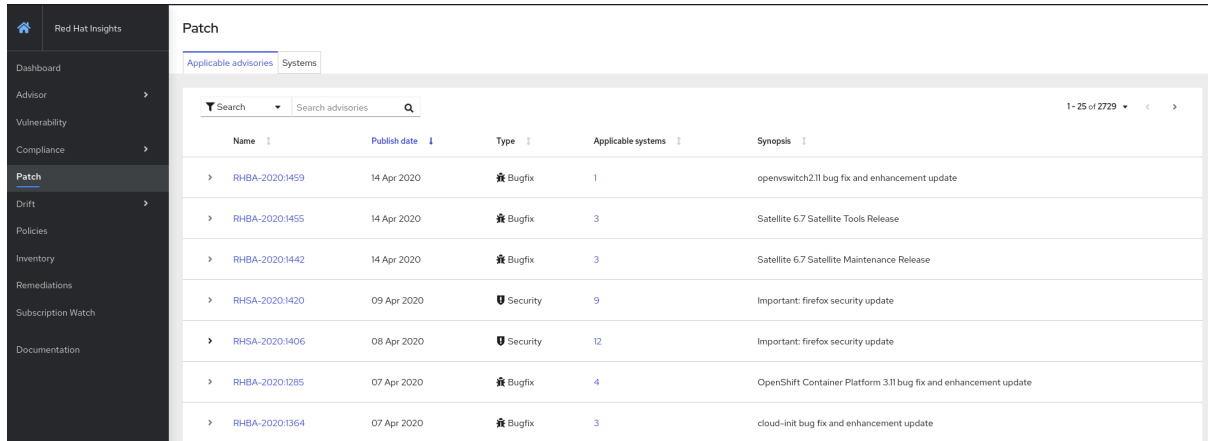
NOTE

- 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).



The screenshot shows the 'Patch' section of the Red Hat Insights interface. The 'Applicable advisories' tab is selected. A search bar is visible at the top. Below it is a table with columns for Name, Publish date, Type, Applicable systems, and Synopsis. The table lists several advisories, including RHBA-2020-1459, RHBA-2020-1455, RHBA-2020-1442, RHSA-2020-1420, RHSA-2020-1406, RHBA-2020-1285, and RHBA-2020-1364.


Name	Publish date	Type	Applicable systems	Synopsis
> RHBA-2020-1459	14 Apr 2020	Bugfix	1	openswitch2.11 bug fix and enhancement update
> RHBA-2020-1455	14 Apr 2020	Bugfix	3	Satellite 6.7 Satellite Tools Release
> RHBA-2020-1442	14 Apr 2020	Bugfix	3	Satellite 6.7 Satellite Maintenance Release
> RHSA-2020-1420	09 Apr 2020	Security	9	Important: firefox security update
> RHSA-2020-1406	08 Apr 2020	Security	12	Important: firefox security update
> RHBA-2020-1285	07 Apr 2020	Bugfix	4	OpenShift Container Platform 3.11 bug fix and enhancement update
> RHBA-2020-1364	07 Apr 2020	Bugfix	3	cloud-init bug fix and enhancement update

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.

[Patch](#) > [Advisories](#) > RHSA-2020:1420

RHSA-2020:1420

Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 68.7.0 ESR.

Security Fix(es):


- * Mozilla: Uninitialized memory could be read when using the WebGL copyTexSubImage method (CVE-2020-6821)
- * Mozilla: Memory safety bugs fixed in Firefox 75 and Firefox ESR 68.7 (CVE-2020-6825)
- * Mozilla: Out of bounds write in GMPDecodeData when processing large images (CVE-2020-6822)

















For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

Issued: 09 Apr 2020

Modified: 09 Apr 2020

[View packages and errata at access.redhat.com](#)

 **Important**
[Learn more](#)

Affected systems			
Name	Applicable advisories	Last seen	
<input checked="" type="checkbox"/> rhel7yeokh	 6  137  43	2 days ago	
<input checked="" type="checkbox"/> rh-pivote.minpublico.cl	 7  123  50	14 hours ago	
<input type="checkbox"/> localhost	 6  144  55	4 hours ago	
<input checked="" type="checkbox"/> dysattest.dytest123.com	 6  130  42	2 days ago	

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**.

Remediate with Ansible x

Playbook name: Demo playbook


Action ↑	Resolution	Reboot required ↓	Systems ↓	Type ↓
RHSA-2020:1420	Apply RHSA-2020:1420	✓	3	Patch

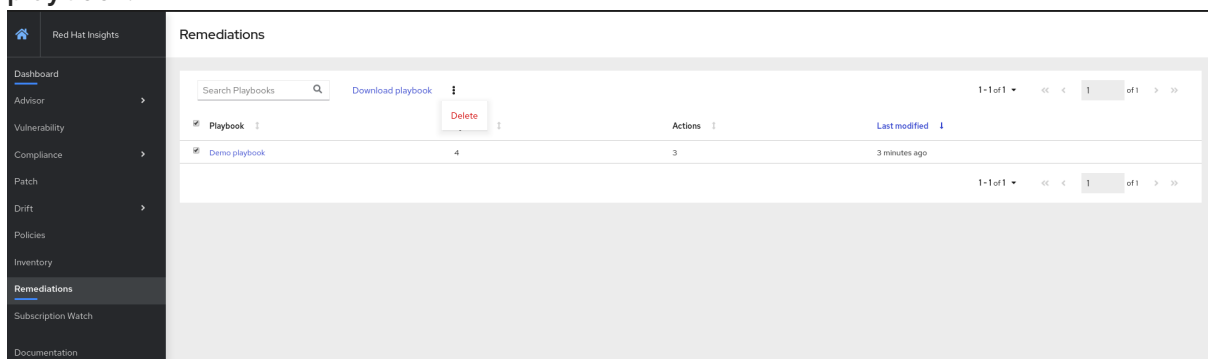
System reboot is required

Auto reboot

- In the Red Hat Insights user interface, click [Remediations](#) in the left-side menu.
- 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:

- 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.
- 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**.
- 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**.
- 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**.
- In the Red Hat Insights user interface, click [Remediations](#) in the left-side menu.
- 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.