



Red Hat Insights 2023

使用 Ansible Playbook，通过修复方案进行系统 补丁

如何查看适用的公告和受影响的系统，并使用 Ansible playbook 修复

Red Hat Insights 2023 使用 Ansible Playbook, 通过修复方案进行系统补丁

如何查看适用的公告和受影响的系统, 并使用 Ansible playbook 修复

Red Hat Customer Content Services

法律通告

Copyright © 2023 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.

摘要

本文档演示了如何查看环境中的适用公告和受影响的系统，并使用 Ansible playbook 执行补救。红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 CTO Chris Wright 信息。

目录

第1章 补丁 (PATCH) 服务概述	3
1.1. 补丁和漏洞勘误标准	3
第2章 检查并过滤清单中的适用公告和系统	5
第3章 使用 ANSIBLE PLAYBOOK, 通过修复方案进行系统补丁	6
第4章 启用通知和集成	7
对红帽文档提供反馈	8

第1章 补丁 (PATCH) 服务概述

补丁利用红帽软件和管理自动化专家，为跨开放混合云的 Red Hat Enterprise Linux (RHEL)系统启用一致的补丁工作流。它为所有部署（无论是 Red Hat Satellite、托管 Red Hat Subscription Management (RHSM)或公有云）提供适用的公告的单一规范视图。

使用补丁，您可以：

- 有关您的 RHEL 系统检查 Insights 的信息，请查看所有适用的红帽及 Extra Packages for Enterprise Linux (EPEL)公告。
- 通过修复使用 Ansible playbook，使用一个或多个公告来修补任何系统。
- 请参阅自上次系统检查时，红帽和非红帽软件仓库可用的软件包更新。您的主机必须正在运行 Red Hat Enterprise Linux 7、Red Hat Enterprise Linux 8.6+ 或 Red Hat Enterprise Linux 9，它必须维护全新的 yum/dnf 缓存。



注意

- 在 [Red Hat Hybrid Cloud Console > Settings menu \(gear icon\) > Identity & Access Management > User Access](#).
- 有关此功能 [和示例用例的更多信息](#)，请参阅[基于角色的访问控制\(RBAC\)的用户访问配置指南](#)。

1.1. 补丁和漏洞勘误标准

补丁服务收集各种数据，以便为您的系统创建有意义的可操作勘误表。Insights 客户端会在每个检查中收集以下数据：

- 安装的软件包列表，包括名称、epoch、版本、发行和架构(NEVRA)
- 启用的模块列表(RHEL 8 及更新的版本)
- 启用的存储库列表
- **yum updateinfo -C** 或 **dnf updateinfo -C**的输出
- 从带有版本锁定的系统发行版本
- 系统架构（例如：**x86_64**）

另外，Insights for Red Hat Enterprise Linux 会从以下数据源收集元数据：

- 红帽内容交付网络(CDN)提供的产品软件仓库的元数据
- Extra Packages for Enterprise Linux (EPEL)软件仓库的元数据
- 红帽开放漏洞和评估语言(OVAL)源

Insights for Red Hat Enterprise Linux 将一组系统数据与收集的勘误和漏洞元数据进行比较，以便为每个系统生成一组可用的更新。这些更新包括软件包更新、红帽勘误以及常见漏洞和暴露(CVE)。

其他资源

有关常见漏洞和暴露(CVE)的更多信息，请参阅以下资源：

- [评估和监控 RHEL 系统上的安全漏洞](#)
- [Red Hat Enterprise Linux > Vulnerability > CVEs](#)

第 2 章 检查并过滤清单中的适用公告和系统

您可以看到所有适用的公告和已安装的软件包，用于检查 Red Hat Enterprise Linux 的 Red Hat Insights。

流程

1. 在 [Red Hat Hybrid Cloud Console](#) 上，导航到 [Red Hat Enterprise Linux > Patch > Advisories](#) 。
2. 您还可以使用搜索框按名称搜索公告，并通过以下方法过滤公告：
 - a. Type - Security, Bugfix, Enhancement, Unknown
 - b. 发布日期 - 最后 7 天、30 天、90 天、last 年或超过 1 年以上
3. 进入 [Red Hat Enterprise Linux > Patch > Systems](#) 以查看您可以使用适用的公告修补受影响的系统列表。您还可以使用搜索框搜索特定系统。
4. 进入 [Red Hat Enterprise Linux > Patch & gt; Patch](#) 软件包，查看环境中可用的更新软件包列表。您还可以使用搜索框搜索特定的软件包。

第 3 章 使用 ANSIBLE PLAYBOOK, 通过修复方案进行系统补丁

以下步骤演示了通过 **Advisories** 选项卡修补工作流：

流程

1. 在 [Red Hat Hybrid Cloud Console](#) 上, 导航到 [Red Hat Enterprise Linux > Patch > Advisories](#) 。
2. 点击您要应用到受影响的系统的公告。您将看到公告的描述、查看 [access.redhat.com](#) 中的软件包和勘误的链接, 以及受影响系统的列表。另外, 每个系统都会显示每种类型的适用公告 (安全、bugfix、增强)。作为批量操作, 您可以点击系统旁的选项菜单, 然后点 **Apply all applicable advisories** 来一次性使用所有适用的公告来修补系统。
3. 或者, 选择您要使用这个特定公告修补的系统, 然后点 **Remediate**。
4. 在 Remediate with Ansible 页面中, 您可以选择修改现有 Playbook 或创建新 Playbook 来使用 Ansible 修复。相应地, 从下拉列表中选择 **Existing Playbook** 和 playbook name, 然后单击 **Next**。或者, 选择 **Create new Playbook**, 再为您的 playbook 输入名称, 然后单击 **Next**。
5. 然后您将看到操作和分辨率摘要。您的系统默认将自动重启。如果要禁用此功能, 请单击蓝色链接该链接, 该链接 "Demo off auto reboot"。点 **Submit**。
6. 在左侧导航中, 点 [Remediations](#)。
7. 点 playbook 名称查看 playbook 详情, 或者只需选择并单击 **Download playbook**。

以下步骤演示了通过 **Systems** 选项卡修补工作流：

1. 点 **Systems** 选项卡查看受影响的系统列表。作为批量操作, 您可以点击系统旁的选项菜单, 然后点 **Apply all applicable advisories** 来一次性使用所有适用的公告来修补系统。
2. 或者, 点您要修补的系统。您将看到系统详情和用于补救的适用公告列表, 以及公告发布日期、类型和语法等其他详情。选择您要应用到该系统的公告, 然后点 **Remediate**。
3. 在 Remediate with Ansible 页面中, 您可以修改现有 Playbook 或创建新 Playbook 来使用 Ansible 修复。相应地, 点 **Existing Playbook**, 然后从下拉列表中选择 playbook 名称, 然后单击 **Next**。或者, 单击 **Create new Playbook**, 输入您的 playbook 名称, 然后单击 **Next**。
4. 然后您将看到操作和分辨率摘要。您的系统默认将自动重启。如果要禁用此功能, 请单击蓝色链接该链接, 该链接 "Demo off auto reboot"。点 **Submit**。
5. 在左侧导航中, 点 [Remediations](#)。
6. 点 playbook 名称查看 playbook 详情, 或者只需选择并单击 **Download playbook**。



重要

检查并测试所有推荐的操作和 playbook, 如果您认为适合, 请在运行红帽软件的系统上部署。红帽不负责与这些建议或 Playbook 相关的任何结果。

第 4 章 启用通知和集成

您可以在 Red Hat Hybrid Cloud Console 上启用通知服务，以便在补丁服务检测到问题并生成公告时发送通知。使用通知服务可自由地检查 Red Hat Insights for Red Hat Enterprise Linux 仪表板是否存在公告。

例如，您可以将通知服务配置为在补丁服务生成公告时自动发送电子邮件消息。

启用通知服务需要三个主要步骤：

- 首先，机构管理员使用 Notifications-administrator 角色创建一个 User Access 组，然后将帐户成员添加到组中。
- 接下来，通知管理员为通知服务中的事件设置行为组。行为组指定每个通知的交付方法。例如，行为组可以指定是否向所有用户发送电子邮件通知，还是只发送给机构管理员。
- 最后，从事件接收电子邮件通知用户必须设置其用户首选项，以便接收每个事件的独立电子邮件。

除了发送电子邮件信息外，您还可以将通知服务配置为以其他方式发送事件数据：

- 使用经过身份验证的客户端查询 Red Hat Insights API 以了解事件数据
- 使用 Webhook 将事件发送到接受入站请求的第三方应用程序
- 将通知与 Splunk 等应用程序集成，将补丁公告路由到应用程序仪表板

其他资源

- 有关如何为补丁公告设置通知的更多信息，请参阅在 [Red Hat Hybrid Cloud Console 上配置通知和集成](#)。

对红帽文档提供反馈

我们感谢您对我们文档的反馈。要提供反馈，请突出显示文档中的文本并添加注释。

先决条件

- 已登陆到红帽客户门户网站。
- 在红帽客户门户网站中，文档采用 **Multi-page HTML** 查看格式。

流程

要提供反馈，请执行以下步骤：

1. 点击 **文档** 右上角的反馈按钮查看现有的反馈。



注意

反馈功能仅在多页 HTML 格式中启用。

2. 高亮标记您要提供反馈的文档中的部分。
3. 点在高亮文本旁弹出的 **Add Feedback**。
文本框会出现在页面右侧的反馈部分中。
4. 在文本框中输入您的反馈，然后点 **Submit**。
已创建一个文档问题。
5. 要查看问题，请点击反馈视图中的问题链接。