

“Security”部分提供红帽产品安全中心 (<https://access.redhat.com/security/>) 的访问途径。此部分也提供有关重大安全问题的信息、红帽 CVE 数据库的访问途径、红帽博客的“安全”频道，以及有关红帽安全响应流程和如何评级和解决问题的资源。

最后，“Community”部分供红帽专家、客户和合作伙伴用于进行交流和协作。您可以在此处获得论坛、博客以及所在地区即将举办的活动的信息。



注意

您应完成“红帽入门 [<https://access.redhat.com/start>]”上的整个导览，包括有关如何个性化设置客户门户网站体验及探索红帽订阅权益的部分，从而全面了解客户门户网站。您的客户门户网站帐户需要至少有一个有效订阅，才能访问此页面。

使用红帽支持工具搜索知识库

红帽支持工具实用程序 **redhat-support-tool** 提供基于文本的界面，您可从系统的命令行使用此工具在客户门户网站上搜索知识库文章并提交支持案例。此工具没有图形界面；由于它会与红帽客户门户网站交互，因此需要接入互联网。使用任何终端或 SSH 连接运行 **redhat-support-tool** 命令。

redhat-support-tool 命令可以在交互模式中使用，也可加入选项和参数作为一个命令来调用。两种方式中该工具的语法均相同。默认情况下，其程序在交互模式中启动。使用 **help** 子命令来查看所有可用的命令。交互模式支持 Tab 补全，以及在父级 shell 中调用程序的功能。

```
[user@host ~]$ redhat-support-tool
Welcome to the Red Hat Support Tool.
Command (? for help):
```

第一次调用时，**redhat-support-tool** 会提示输入红帽客户门户网站订阅者登录信息。为避免重复提供此信息，工具会询问是否要将帐户信息存储在用户的主目录中 (`~/.redhat-support-tool/redhat-support-tool.conf`)。如果问题都通过特定的红帽客户门户网站帐户提交，`--global` 选项可以将帐户信息及其他系统范围的配置保存到 `/etc/redhat-support-tool.conf` 中。工具的 **config** 命令可修改工具配置设置。

redhat-support-tool 命令允许订阅者搜索和显示红帽客户门户网站中的知识库内容。知识库允许关键字搜索，与 **man** 命令相似。您可以输入错误代码、日志文件中的语法，或者任何关键字组合，以此生成相关解决方案文档的列表。

以下是初始配置和基本搜索演示：

```
[user@host ~]$ redhat-support-tool
Welcome to the Red Hat Support Tool.
Command (? for help): search How to manage system entitlements with subscription-
manager
Please enter your RHN user ID: subscriber
Save the user ID in /home/student/.redhat-support-tool/redhat-support-tool.conf
(y/n): y
Please enter the password for subscriber: password
Save the password for subscriber in /home/student/.redhat-support-tool/redhat-
support-tool.conf (y/n): y
```

在提示用户输入必要的用户配置后，工具将继续执行原先的搜索请求：

```
Type the number of the solution to view or 'e' to return to the previous menu.  
1 [ 253273:VER] How to register and subscribe a system to the Red Hat Customer  
Portal using Red Hat Subscription-Manager  
2 [ 265523:VER] Enabling or disabling a repository using Red Hat Subscription  
Management  
3 [ 100423:VER] Why does subscription-manager list return: "No Installed  
Products found" ?  
...output omitted...  
Select a Solution: 1
```

如上所述选择文章编号 1，系统将提示您选择要阅读的文档章节。最后，使用 **Q** 键退出您所在的章节，或重复使用它来退出 **redhat-support-tool** 命令。

```
Select a Solution: 1
```

```
Type the number of the section to view or 'e' to return to the previous menu.  
1 Title  
2 Issue  
3 Environment  
4 Resolution  
5 Display all sections  
End of options.  
Section: 1
```

```
Title  
=====
```

How to register and subscribe a system to the Red Hat Customer Portal using Red
Hat Subscription-Manager
URL: https://access.redhat.com/solutions/253273
Created On: None
Modified On: 2017-11-29T15:33:51Z

```
(END) q  
Section:  
Section: q
```

```
Select a Solution: q
```

```
Command (? for help): q  
[user@hosts ~]#
```

根据文档 ID 访问知识库文章

使用工具的 **kb** 命令及知识库文档 ID，直接查找在线文章。返回的文档在屏幕上滚动而不进行分页，但您可以将其重定向到文件以进行保存，并使用 **less** 一次滚动一个屏幕。

```
[user@host ~]$ redhat-support-tool kb 253273
```

```
Title  
=====
```

How to register and subscribe a system to the Red Hat Customer Portal using Red
Hat Subscription-Manager

URL: <https://access.redhat.com/solutions/253273>
Created On: None
Modified On: 2017-11-29T15:33:51Z

Issue

```
=====
* How to register a new `Red Hat Enterprise Linux` system to the Customer Portal
  using `Red Hat Subscription-Manager`
...output omitted...
```

用红帽支持工具管理支持案例

产品订阅的一个优点是能够通过红帽客户门户网站访问技术支持。根据系统的订阅支持级别，可以通过在线工具或电话联系红帽。请参见 https://access.redhat.com/site/support/policy/support_process 来了解详细信息。

准备错误报告

在联系红帽支持部门之前，务必要为错误报告收集相关的信息。

定义问题。能够清晰地陈述问题及其症状。尽可能具体。详述可重现该问题的步骤。

收集背景信息。受影响的产品和版本是什么？准备好提供相关的诊断信息。这可能包含 **sosreport** 的输出，该命令将在本节下文中予以介绍。对于内核问题，这可能包含系统的 **kdump** 崩溃转储或者崩溃系统的监控器上显示的内核回溯的数字照片。

确定严重级别。红帽使用四个严重级别为问题分类。报告紧急和高严重级别问题后，应致电相关的当地支持中心（参见 <https://access.redhat.com/site/support/contact/technicalSupport>）。

严重性	描述
紧急（严重级别 1）	严重影响您在生产环境中使用该软件的问题。这包括生产数据丢失或生产系统故障。这种情况使您的业务运作暂停，也不存在其他可绕过问题的解决方法。
高（严重级别 2）	软件可以正常运行，但生产环境中的使用被严重削弱的问题。这种情况对您的业务运作有高度影响，也不存在其他可绕过问题的解决方法。
中（严重级别 3）	涉及生产环境或开发环境中软件部分的使用、非关键损失的问题。对于生产环境，您的业务会受到中低影响。业务可通过其他可绕过问题的解决方法继续正常运作。在开发环境中，这种情况将导致您的项目迁移至生产时出现问题。
低（严重级别 4）	一般使用问题，报告文档错误或未来产品增强或修改建议。在生产环境中，对您的业务或系统的性能或功能影响较低或没有影响。在开发环境中，对您的业务有中低级影响，但是业务可通过其他可绕过问题的解决方法继续正常运作。

通过 redhat-support-tool 管理错误报告

您可以通过 **redhat-support-tool** 创建、查看、修改和关闭红帽支持案例。当支持案例处于 **opened** 或 **maintained** 状态时，用户可以附上文件或文档，如诊断报告 (sosreport)。工具将上传并附加文件到案例中。

可以通过命令选项来指定产品名称、版本、摘要、描述、严重级别和案例组等案例详细信息，也可让工具提示输入必要的信息。下例中将打开一个新案例。已指定了 **--product** 和 **--version** 选项。

```
[user@host ~]$ redhat-support-tool
Welcome to the Red Hat Support Tool.
Command (? for help): opencase --product="Red Hat Enterprise Linux" --
version="7.0"
Please enter a summary (or 'q' to exit): System fails to run without power
Please enter a description (Ctrl-D on an empty line when complete):
When the server is unplugged, the operating system fails to continue.
1 Urgent
2 High
3 Normal
4 Low
Please select a severity (or 'q' to exit): 4
Would you like to assign a case group to this case (y/N)? N
Would see if there is a solution to this problem before opening a support case?
(y/N) N
-----
Support case 01034421 has successfully been opened.
```

如果未指定 **--product** 和 **--version** 选项，**redhat-support-tool** 将提供这些选项的选项列表。

```
[user@host ~]$ redhat-support-tool
Welcome to the Red Hat Support Tool.
Command (? for help): opencase
Do you want to use the default product - "Red Hat Enterprise Linux" (y/N)?: y
...output omitted...
29 7.4
30 7.5
31 7.6
32 8.0 Beta
Please select a version (or 'q' to exit): 32
Please enter a summary (or 'q' to exit): yum fails to install apache
Please enter a description (Ctrl-D on an empty line when complete):
yum cannot find correct repo
1 Urgent
2 High
3 Normal
4 Low
Please select a severity (or 'q' to exit): 4
Would you like to use the default (Ungrouped Case) Case Group (y/N)? : y
Would you like to see if there's a solution to this problem before opening a
support case? (y/N) N
-----
Support case 010355678 has successfully been opened.
```

将诊断信息附加到支持案例

包含诊断信息可以更快地解决问题。打开案例时附上 sosreport。**sosreport** 命令生成压缩的 tar 存档，内含从运行中的系统收集的诊断信息。如果之前创建过存档，则 **redhat-support-tool** 将提示包含该存档：

```
Please attach a SoS report to support case 01034421. Create a SoS report as
the root user and execute the following command to attach the SoS report
directly to the case:
redhat-support-tool addattachment -c 01034421 path to sosreport
```

```
Would you like to attach a file to 01034421 at this time? (y/N) N
Command (? for help):
```

如果不存在当前的 SoS 报告，管理员可以稍后生成并附加一份报告。使用 **redhat-support-tool addattachment** 命令来附加报告。

订阅者可以查看、修改和关闭支持案例：

```
Command (? for help): listcases

Type the number of the case to view or 'e' to return to the previous menu.
1 [Waiting on Red Hat] System fails to run without power
No more cases to display
Select a Case: 1

Type the number of the section to view or 'e' to return to the previous menu.
1 Case Details
2 Modify Case
3 Description
4 Recommendations
5 Get Attachment
6 Add Attachment
7 Add Comment
End of options.
Option: q

Select a Case: q

Command (? for help):q

[user@host ~]$ redhat-support-tool modifycase --status=Closed 01034421
Successfully updated case 01034421
[user@host ~]$
```

红帽支持工具具有高级应用诊断和分析功能。利用内核崩溃转储核心文件，**redhat-support-tool** 可以创建和提取回溯追踪。内核崩溃转储核心文件可通过 **kdump** 命令创建。回溯追踪是崩溃转储点处活动堆栈帧的报告，也能提供现场诊断。**redhat-support-tool** 的选项之一是打开支持案例。

该工具也提供日志文件分析功能。通过工具的 **analyze** 命令，可以解析许多类型的日志文件（如操作系统、JBoss、Python、Tomcat 和 oVirt）来识别问题症状。日志文件可以单独进行查看和诊断。与崩溃转储或日志文件等原始数据相比，提供预处理过的分析可以更加快速地创建支持案例并提交给工程师。

加入红帽开发者计划

红帽提供的另一个有用资源是红帽开发者计划。此计划托管于 <https://developer.redhat.com>，提供开发专用红帽软件订阅权利、相关文档，以及我们微服务、无服务器计算、Kubernetes 和 Linux 领域的专家推出的优质图书。另外，也提供博客、即将举办的活动与培训的信息链接和其他帮助资源，以及红帽客户门户网站的链接。

注册免费，可在 <https://developer.redhat.com/register> 完成。



参考文献

[sosreport\(1\) man page](#)

红帽 Access：红帽支持工具

<https://access.redhat.com/site/articles/445443>

红帽支持工具首次使用

<https://access.redhat.com/site/videos/534293>

联系红帽技术支持

https://access.redhat.com/site/support/policy/support_process/

帮助 - 红帽客户门户网站

<https://access.redhat.com/site/help/>

► 指导练习

从红帽客户门户网站获取帮助

在本练习中，您将使用 Web 控制台生成诊断报告。

成果

您应能够使用 Web 控制台生成诊断报告，该报告可作为支持案例的一部分提交到红帽客户门户网站。

在你开始之前

在 workstation 上，以 student 用户身份并使用 student 作为密码进行登录。

从 workstation，运行 **lab support-portal start** 命令。该命令将运行一个起始脚本，它将确定 servera 是否可从网络访问。它还在 servera 上启动并启用 Web 控制台。

```
[student@workstation ~]$ lab support-portal start
```

- 1. 从 workstation，使用 ssh 命令以 student 用户身份登录 servera。

```
[student@workstation ~]$ ssh student@servera
Web console: https://servera.lab.example.com:9090/ or https://172.25.250.10:9090/
[student@servera ~]$
```

- 2. 使用 systemctl 命令确认 cockpit 服务处于运行状态。系统提示输入密码时，输入 student。

```
[student@servera ~]$ sudo systemctl status cockpit.socket
[sudo] password for student: student
● cockpit.socket - Cockpit Web Service Socket
    Loaded: loaded (/usr/lib/systemd/system/cockpit.socket; enabled; vendor preset:
              disabled)
    Active: active (listening) since Thu 2019-05-16 10:32:33 IST; 4min 37s ago
      Docs: man:cockpit-ws(8)
      Listen: [::]:9090 (Stream)
    Process: 676 ExecStartPost=/bin/ln -snf active.motd /run/cockpit/motd
              (code=exited, status=0/SUCCESS)
    Process: 668 ExecStartPost=/usr/share/cockpit/motd/update-motd localhost
              (code=exited, status=0/SUCCESS)
      Tasks: 0 (limit: 11405)
     Memory: 1.5M
        CGroup: /system.slice/cockpit.socket
...output omitted...
```

- 3. 从 servera 注销。

```
[student@servera ~]$ exit  
[student@workstation ~]$
```

- 4. 在 **workstation** 上，打开 Firefox，再以 **root** 用户身份并使用 **redhat** 作为密码登录 **servera.lab.example.com** 上运行的 Web 控制台界面。
- 4.1. 打开 Firefox，再访问 **https://servera.lab.example.com:9090** 地址。
 - 4.2. 如有提示，将自签名证书添加为例外来接受它。
 - 4.3. 以 **root** 用户身份并使用 **redhat** 作为密码进行登录。您现在以特权用户身份登录，这是创建诊断报告所必需的。
 - 4.4. 单击左侧导航栏中的 **Diagnostic Reports**。单击 **Create Report**。创建报告需要几分钟时间。
- 5. 报告准备好后，单击 **Download report**。保存该文件。
- 5.1. 单击 **Download report** 按钮，然后单击 **Save File** 按钮。
 - 5.2. 单击 **Close** 按钮。
 - 5.3. 从 Web 控制台界面注销。

完成

在 **workstation** 上，运行 **lab support-portal finish** 脚本来完成本练习。

```
[student@workstation ~]$ lab support-portal finish
```

本引导式练习到此结束。

通过红帽智能分析工具检测和解决问题

培训目标

学完本节后，您应能够使用红帽智能分析工具分析服务器问题，修复或解决问题，并确认解决方案是否有效。

红帽智能分析工具简介

红帽智能分析工具是一种预测分析工具，可帮助您识别和修复基础架构中运行红帽产品的系统的安全性、性能、可用性和稳定性威胁。红帽智能分析工具作为软件即服务 (SaaS) 产品提供，因此您可以快速部署和扩展它，没有额外的基础架构要求。此外，这意味着您可以立即利用特定于已部署系统的红帽最新建议和更新。

红帽会定期更新红帽智能分析工具使用的知识库，这些知识库基于常见的支持风险、安全漏洞、已知错误的配置，以及红帽识别的其他问题。缓解或修复这些问题的措施会得到红帽的检验和验证。这样，您可以在问题成为更大问题之前主动识别问题，确定其优先级并加以解决。

对于检测到的每个问题，红帽智能分析工具提供所呈现风险的估测以及有关如何缓解或修复问题的建议。这些建议可提供诸如 Ansible Playbook 或易于阅读的分步骤说明等资料来帮助您解决问题。

红帽智能分析工具建议面向注册到服务的每个系统进行定制。安装各个客户端系统时会一同安装一个代理，它将收集有关系统运行时配置的元数据。您使用 **sosreport** 向红帽支持部门提供数据时应包含这一数据，以便能解决支持票据。您可以限制或模糊处理客户端发送的数据。这会使某些分析规则无法运作，具体取决于您的限制。

在您注册服务器并且服务器完成初始系统元数据同步之后不久，就能够在红帽云门户网站上的红帽智能分析工具控制台中看到您的服务器和对应的建议。

红帽智能分析工具目前为下列红帽产品提供预测分析和建议：

- 红帽企业 Linux 6.4 及更高版本
- 红帽企业虚拟化 4 及更高版本
- 红帽 OpenShift 容器平台
- 红帽 OpenStack 平台 7 及更高版本

描述红帽智能分析工具架构

您可以通过红帽云门户网站将系统注册到红帽智能分析工具。注册系统时，它会向红帽智能分析工具提供有关其当前配置的元数据。此数据在发送到红帽智能分析工具时会使用 TLS 加密进行传输保护。它在发送之前也是匿名的。

根据红帽智能分析工具规则引擎提供的建议，分析结果会显示在红帽云门户网站中的红帽智能分析工具控制台上，网址为：<https://cloud.redhat.com/insights>。

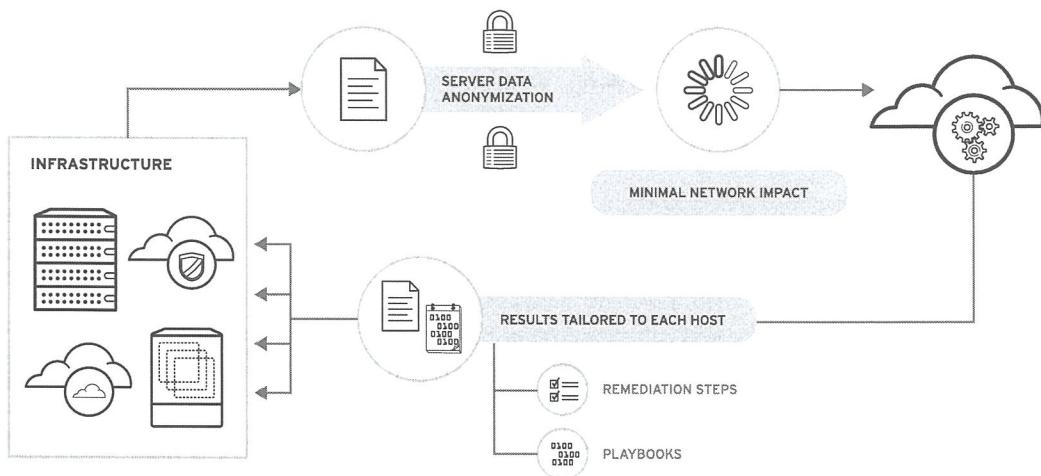


图 16.34: 红帽智能分析工具高级架构

安装红帽智能分析工具客户端

红帽智能分析工具已作为订阅的一部分随附于红帽企业 Linux 8 中。旧版的红帽企业 Linux 服务器需要在系统上安装 insights-client 软件包。



重要

自红帽企业 Linux 7.5 起，insights-client 软件包取代了旧版 redhat-access-insights 软件包。

如果您的系统通过客户门户网站订阅管理服务注册了软件权利，则可以使用一个命令来激活红帽智能分析工具。使用 **insights-client --register** 命令来注册系统。

```
[root@demo ~]# insights-client --register
```

智能分析工具客户端定期更新提供给红帽智能分析工具的元数据。您随时可以使用 **insights-client** 命令刷新客户端的元数据。

```
[root@demo ~]# insights-client
Starting to collect Insights data for demo.lab.example.com
Uploading Insights data.
Successfully uploaded report from 773b351b-dfb1-4393-afa8-915cc2875e06 to
account XXXXX.
```

将 RHEL 系统注册到红帽智能分析工具

将 RHEL 服务器注册到红帽智能分析工具时，整个过程如下：

1. 使用红帽订阅管理服务，以交互方式注册系统。

```
[root@demo ~]# subscription-manager register --auto-attach
```

必须将红帽智能分析工具的有效权利与系统关联，您可能会在红帽企业 Linux 订阅中收到该权利。

- 确保系统上已安装 insights-client 软件包。在 RHEL 7 中，此软件包位于 `rhel-7-server-rpms` 频道中。



注意

在红帽企业 Linux 8 系统上不需要此步骤。

```
[root@demo ~]# yum install insights-client
```

- 使用 `insights-client --register` 命令，将系统注册到红帽智能分析工具服务并上传初始系统元数据。

```
[root@demo ~]# insights-client --register
```

- 验证 <https://cloud.redhat.com/insights> 上是否可看到系统。

The screenshot shows the Red Hat Insights dashboard. At the top, there's a navigation bar with 'Red Hat' and a user profile. Below it is a sidebar with links for 'Overview', 'Rules', 'Inventory', 'Remediations', and 'Documentation'. The main area has three main sections: 'Rule hits by severity' (1 Medium affecting 2 systems), 'Rule hits by category' (Availability 0, Stability 0, Performance 0, Security 1), and 'Get started with Red Hat Insights' which includes 'Connect your first systems' (with a note to connect at least 10 systems), 'Remediate Insights findings with Ansible' (with a note to generate an Ansible playbook), and 'Deploy Insights at scale' (with a note to get more out of Insights with more systems). There are also 'Download Ansible Playbook' and 'Learn how to connect a system to Insights' buttons.

图 16.35: 云门户网站上的红帽智能分析工具概览

查看红帽智能分析工具提供的报告

红帽智能分析工具报告显示系统在不同时间的状态。通过这些报告，您可以轻松查看当前的风险评估并确定历史趋势，从而改进您的决策制定。

红帽智能分析工具界面为您提供包括如下内容的信息：

- 基于您注册的系统的当前总体风险评分。
- 建议对系统采取的操作，进一步细分为不同的类别和严重性。
- 有关系统最近在何时签入到红帽智能分析工具的信息。
- 根据其影响需要优先处理的问题。

红帽智能分析工具控制台导航

云门户网站上的红帽智能分析工具控制台包含以下页面：

概述

Overview 页面提供对已注册基础架构当前风险的概览。Overview 提供了一个视角，用于调查特定规则如何影响已注册的系统，或了解对所选系统构成风险的所有规则。

该页面允许您根据严重性来查看规则，并根据类别对基础架构风险进行分类。每个规则均根据对操作的以下方面之一的潜在影响进行分类：**Availability**、**Stability**、**Performance** 和 **Security**

规则

Rules 页面提供智能分析工具规则和受影响主机的列表。

在 Rules 页面中，您会注意到其中有些问题在 Ansible 徽标栏下面标有勾号。这表示该问题具有可用的 Ansible 修复 playbook。无勾号的问题没有 Ansible 修复 playbook，但可能在问题详细信息中提供手动缓解或修复的说明。

您可以单击规则名称以查看所有受影响的系统。每个问题都提供了有关如何在系统上显示此问题的说明，并且提供 Remediate with Ansible 以创建修复 Playbook。

The screenshot shows the Red Hat Insights interface with the 'Rules' tab selected. The main content area displays three security-related rules:

Rule	Added	Total Risk	Systems	Ansible
Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)	a year ago	0	1	✓
Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre, CVE-2017-5754/Meltdown)	a year ago	0	1	✓
Kernel vulnerable to side-channel attacks in modern microprocessors using Speculative Store Bypass when CPU microcode is outdated (CVE-2019-3639)	a year ago	0	3	✓

图 16.36: 红帽智能分析工具控制台中的 Rules 页面

清单

Inventory 页面中提供您已注册到红帽智能分析工具的系统列表。

您可以针对特定系统轻松过滤清单。Last Sync 列中显示各个系统最近一次更新元数据的时间。

The screenshot shows the Red Hat Insights interface with the 'Inventory' tab selected. The main content area displays a list of registered systems:

Name	Last Sync
rhe01.test.lab.redhat.com	2/28/2019, 6:10:37 AM
rhe01.test.lab.redhat.com	2/28/2019, 6:13:31 AM
rhe01.les1.lab.redhat.com	3/9/2019, 11:47:36 AM
rhe02.les1.lab.redhat.com	4/2/2019, 12:02:08 PM

图 16.37: 红帽智能分析工具控制台中的 Inventory 页面

调控措施

Remediations 页面提供所创建的 Ansible Playbook 列表，并允许下载这些 Playbook。

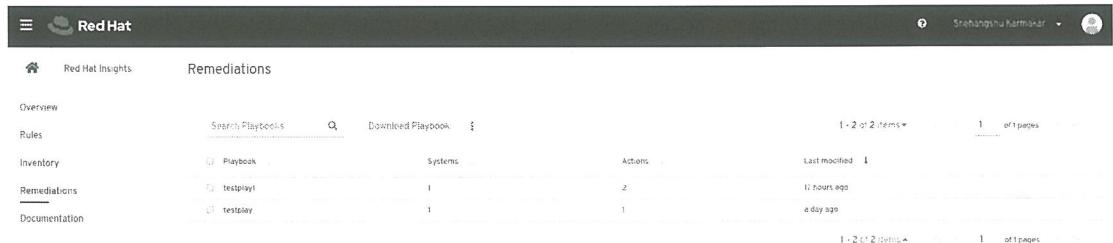


图 16.38: 红帽智能分析工具控制台中的 Remediations 页面

查看红帽智能分析工具报告的问题

查看红帽智能分析工具报告的问题时，整个过程如下：

1. 登录红帽云门户网站，再访问位于 <https://cloud.redhat.com/insights> 的红帽智能分析工具页面。
2. 在门户网站中，前往 **Inventory** 页面。
3. 选择 **Rule hits by severity**，从而按它们对已注册的基础设施施加的 **Total Risk** 来查看规则。或者，选择 **Rule hits by category** 以根据类别查看风险的类型。
4. 滚动规则列表以查看有关风险、暴露的系统以及 Ansible Playbook 可用性的高级别信息，以便自动进行修复。
5. 单击规则查看规则的更多描述，单击链接阅读相关的知识库文章，并查看所有受影响主机的列表。
6. 单击主机可查看有关检测到的问题的具体信息以及解决问题的步骤。

解读红帽智能分析工具报告

在红帽智能分析工具中，其规则决定了它在您的系统上查找的问题。红帽经常向红帽智能分析工具添加新规则，以检查新发现的问题。规则可能会查找系统上发生的指示问题的事件，或者它们可能会根据系统的当前配置主动预测问题。

如果规则与您的系统匹配（即表明存在问题），会随同规则提供附加信息，以帮助您了解问题，确定解决问题的工作的优先级，确定可用的缓解或补救措施，以及协助自动解决问题。

每个规则按类型分类，具有摘要名称，并通过较长的描述来解释问题所在。规则通常链接到客户门户网站上的知识库文章以及其他信息。知识库文章可能提供有关缓解或修复问题的不同方法的信息，规则也可能提供 Ansible Playbook 或其他材料来帮助自动缓解和修复问题。

有些问题很难解决，完整的修复可能需要重新引导或停机。在这种情况下，可以选择通过降低风险作为临时措施来缓解这些问题。规则将在几个不同的类别中提供问题所呈现的风险的分数。

例如，某一安全问题需要更新内核软件包并重新引导系统才能修复，但也可能很难通过某些临时配置更改来利用。您可以选择立即应用临时更改，并推迟重新引导系统，直到您可以安排紧急维护窗口。

红帽智能分析工具将问题带给系统的风险分为四类。它使用以下等级来评估风险的级别：**Low**、**Moderate**、**Important** 和 **Critical**。

Likelihood、**Impact**、**Total Risk** 和 **Risk of Change** 类别预测订阅的系统上检测到问题的风险系数。

影响
表示此问题对系统的预计影响程度。

Likelihood

表示给定问题影响系统的可能性。

Total Risk

利用一个四点评级（低等、中等、重要及严重）以及通用漏洞评估系统 (CVSS) 基础评分，指示红帽产品中发现的安全问题的影响。它们可以提供一种优先级风险评估，以帮助您针对每个问题给基础架构带来的风险做出明智的决定。

Risk of Change

表示建议的修复措施可能导致系统中断的风险。

要在红帽智能分析工具中查看各种规则的风险系数预测，请前往 Overview 或 Rules 页面。每个规则都显示 Total Risk 和 Risk of Change 图标。

The screenshot shows a detailed view of a security rule in the Red Hat Intelligent Analysis tool. At the top, it says 'Rules > Kernel Vulnerable To Side-Channel Attacks In Modern Microprocessors (CVE-2017-5715/Spectre)'. Below that, it lists the rule name, 'Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)', and the publish date, '1/17/2018'. The rule description states: 'A vulnerability was discovered in modern microprocessors supported by the kernel, whereby an unprivileged attacker can use this flaw to bypass restrictions to gain read access to privileged memory. The issue was reported as CVE-2017-5715 / Spectre.' A 'Knowledgebase Article' link is provided. On the right, there are two main sections: 'Total Risk' and 'Risk of Change'. 'Total Risk' is marked as 'Medium' with a 'Moderate' icon. It notes that the likelihood is medium and impact would be high if it occurred. 'Risk of Change' is also marked as 'Moderate' with a 'Moderate' icon. It states that these changes will likely require an outage window and might require a reboot. Below these sections, under 'Affected systems', it shows one system listed: 'servera.lab.example.com'. A 'Remediate with Ansible' button is available for this system. At the bottom, there are navigation links for 'Affected systems', 'Last Sync' (5/14/2019, 12:01:41 PM), and 'Sync'.

图 16.39: 应用于主机的红帽智能分析工具规则

确定了要解决的问题后，您可以手动或自动解决问题。在问题得到解决，并且红帽智能分析工具客户端上传了新的元数据后，规则应不再与系统匹配，问题也应该会从建议操作列表中消失。

手动修复红帽智能分析工具报告的问题

手动修复红帽智能分析工具报告的问题时，整个过程如下：

1. 登录红帽云门户网站，再访问位于 <https://cloud.redhat.com/insights> 的红帽智能分析工具页面。
2. 导航到 Rules 页面。单击要解决问题的规则的名称。
3. 在 Name 列下，单击受影响的系统链接之一。页面中将显示有关问题对系统造成的影响的说明，以及解决系统问题的步骤。按照 Steps to resolve 中的说明进行操作，以修复系统上的问题。

The screenshot shows the Red Hat Insights interface for a host named 'servera.lab.example.com'. A specific rule, 'Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5715/Spectre)', has been identified. The 'Impact' section indicates a potential risk, and the 'Risk of Change' section provides details on how to remediate the issue using Ansible.

Detected issues:

- This machine is vulnerable, because it runs a vulnerable kernel.
- An unprivileged attacker could use the vulnerability to read privileged memory by conducting targeted cache side-channel attacks, including memory locations that cross the `syscall` boundary or the guest/host boundary, or potentially arbitrary host memory addresses.

Steps to resolve:

Red Hat recommends that you update the kernel:

```
# yum update kernel
# reboot
```

If additional steps to update the kernel are necessary, they are detailed in the separate insights rule `Kernel vulnerable to side-channel attacks in modern microprocessors (CVE-2017-5753/Spectre, CVE-2017-5715/Spectre, CVE-2017-5754/Meltdown)`. Fixes require CPU microcode/firmware to activate.

In addition:

Subscribers are advised to contact their hardware OEM to receive the appropriate microcode/firmware for their processor. Red Hat may be providing `microcode_ctl` and `linux_firmware` packages that will cover the limited subset of chipsets we were able to test, but this will not address many CPUs that you may have in use in your server fleet. Again, contacting your hardware vendor will ensure you have the appropriate software to enable the protections for Variant 2 of this issue.

图 16.40: 手动修复系统规则

- 对受影响系统执行这些步骤，以解决此问题。
- 应用修复步骤后，在系统上以 `root` 用户身份运行以下命令，以将更改报告到红帽智能分析工具：

```
[root@demo ~]# insights-client
Starting to collect Insights data for demo.lab.example.com
Uploading Insights data.
Successfully uploaded report from 773b351b-dfb1-4393-afa8-915cc2875e06 to
account xxxxxx.
```

- 在红帽智能分析工具控制台中，导航到 `Rules` 页面。单击规则并向下滚动到 `Affected systems`，然后验证问题不再出现在受影响的系统列表中。



参考文献

insights-client (8) 和 **insights-client.conf** (5) man page。

有关更多信息，请参阅《红帽智能分析工具 1.0 快速入门指南》中的快速入门章节，网址为：

<https://access.redhat.com/products/red-hat-insights/#getstarted>

有关红帽智能分析工具功能更新的更多信息，请访问：

https://access.redhat.com/documentation/en-us/red_hat_insights/1.0/html-single/release_notes/#release_information

有关红帽智能分析工具收集的数据的信息，请访问：

红帽智能分析工具收集的系统信息

<https://access.redhat.com/articles/1598863>

有关红帽智能分析工具如何排除收集的数据的信息，请访问：

选择不从红帽智能分析工具客户端发送元数据

<https://access.redhat.com/articles/2025273>

► 小测验

通过红帽智能分析工具检测和解决问题

选择以下问题的正确答案：

► 1. 在使用红帽智能分析工具管理红帽企业 Linux 系统时，会以何种顺序发生以下事件？

1. 红帽智能分析工具分析系统元数据，以确定适用的问题和建议。
 2. 智能分析工具客户端将系统元数据上传到红帽智能分析工具服务。
 3. 管理员在红帽智能分析工具客户门户网站中查看建议的操作。
 4. 红帽智能分析工具在红帽企业 Linux 系统上收集系统元数据。
- a. 1, 2, 3, 4
 - b. 4, 2, 1, 3
 - c. 4, 2, 3, 1
 - d. 4, 1, 2, 3

► 2. 哪一个命令用于将客户端注册到红帽智能分析工具？

- a. `insights-client --register`
- b. `insights-client --no-upload`
- c. `subscription-manager register`
- d. `insights-client --unregister`

► 3. 红帽智能分析工具控制台中的哪两个页面允许您根据风险类别使用过滤器来显示规则列表？（请选择两项。）

- a. 概述
- b. 清单
- c. 规则
- d. Remediation

► 解决方案

通过红帽智能分析工具检测和解决问题

选择以下问题的正确答案：

► 1. 在使用红帽智能分析工具管理红帽企业 Linux 系统时，会以何种顺序发生以下事件？

1. 红帽智能分析工具分析系统元数据，以确定适用的问题和建议。
 2. 智能分析工具客户端将系统元数据上传到红帽智能分析工具服务。
 3. 管理员在红帽智能分析工具客户门户网站中查看建议的操作。
 4. 红帽智能分析工具在红帽企业 Linux 系统上收集系统元数据。
- a. 1, 2, 3, 4
b. 4, 2, 1, 3
c. 4, 2, 3, 1
d. 4, 1, 2, 3

► 2. 哪一个命令用于将客户端注册到红帽智能分析工具？

- a. `insights-client --register`
- b. `insights-client --no-upload`
- c. `subscription-manager register`
- d. `insights-client --unregister`

► 3. 红帽智能分析工具控制台中的哪两个页面允许您根据风险类别使用过滤器来显示规则列表？（请选择两项。）

- a. 概述
- b. 清单
- c. 规则
- d. Remediation

总结

在本章中，您学到了：

- Web 控制台是一个基于 Web 的服务器管理界面，它的基础是开源 Cockpit 服务。
- Web 控制台提供系统性能图表、用于管理系统配置和检查日志的图形工具，以及交互式终端界面。
- 通过红帽客户门户网站，您可以访问红帽产品的文档、下载项目、优化工具、支持案例管理，以及订阅和权利管理。
- **redhat-support-tool** 是一个命令行工具，可用于从服务器命令行查询知识库并操作支持案例。
- 红帽智能分析工具是一种基于 SaaS 的预测分析工具，可帮助您识别和修复系统的安全性、性能、可用性和稳定性威胁。

章 17

总复习

目标

回顾 红帽系统管理一 中的任务

培训目标

· 回顾 红帽系统管理一 中的任务

章节

· 总复习

实验

- 实验：从命令行管理文件
- 实验：管理用户和组、权限以及进程
- 实验：配置和管理服务器
- 实验：管理网络
- 实验：挂载文件系统和查找文件

总复习

培训目标

学完本节后，学员应该回顾并温习了在 红帽系统管理一 中学到的知识和技能。

复习 红帽系统管理一

在开始进行本课程总复习前，学员应当熟悉各章节涉及的主题。

请尽管向讲师寻求有关这些主题的额外指导或解释。

第 1 章 红帽企业 Linux 入门

描述和定义开源、Linux、Linux 发行版和红帽企业 Linux。

- 定义和解释 Linux 的用途、开源、Linux 发行版和红帽企业 Linux。

第 2 章 访问命令行

登录 Linux 系统并使用 shell 运行简单的命令。

- 在本地文本控制台中登录 Linux 系统，并使用 shell 运行简单的命令。
- 使用 GNOME 3 桌面环境登录 Linux 系统，并在终端程序中从 shell 提示符运行命令。
- 通过使用 Tab 补全、命令历史记录和命令编辑快捷键在 Bash shell 中运行命令来节省时间。

第 3 章 从命令行管理文件

在从 Bash shell 操作时，复制、移动、创建、删除和组织文件。

- 描述 Linux 如何组织文件，以及文件系统层次结构中各种目录的用途。
- 指定文件相对于当前工作目录的位置和绝对位置，确定并更改工作目录，以及列出目录的内容。
- 创建、复制、移动和删除文件及目录。
- 使用硬链接和符号（或“软”）链接，使多个文件名引用同一文件。
- 通过使用 Bash shell 的模式匹配功能，高效地运行影响很多文件的命令。

第 4 章 在红帽企业 Linux 中获取帮助

通过利用本地帮助系统来解决问题。

- 在本地 Linux 系统手册页中查找信息。
- 从 GNU Info 中的本地文档查找信息。

第 5 章 创建、查看和编辑文本文件

通过命令行输出或在编辑器中创建、查看和编辑文本文件。

- 通过 shell 重定向将命令输出或错误保存到文件中，并利用管道通过多步程序处理命令输出。

- 使用 **vim** 编辑器创建和编辑文本文件。
- 使用 shell 变量来帮助运行命令，并编辑 Bash 启动脚本以设置 shell 和环境变量，从而修改 shell 以及从 shell 运行的程序的行为。

第 6 章 管理本地用户和组

创建、管理和删除本地用户和组，以及管理本地密码策略。

- 描述 Linux 系统上用户和组的用途。
- 切换到超级用户帐户来管理 Linux 系统，并使用 **sudo** 命令授予其他用户超级用户访问权限。
- 创建、修改和删除本地定义的用户帐户。
- 创建、修改和删除本地定义的组帐户。
- 为用户设置密码管理策略，并且手动锁定和解锁用户帐户。

第 7 章 控制对文件的访问

设置文件的 Linux 文件系统权限，并解释不同权限设置的安全效果。

- 列出文件和目录的文件系统权限，并解释这些权限对用户和组访问权限的影响。
- 利用命令行工具更改文件的权限和所有权。
- 控制用户创建的新文件的默认权限，解释特殊权限的影响，并使用特殊权限和默认权限设置在特定目录中创建的文件的组所有者。

第 8 章 监控和管理 Linux 进程

评估和控制运行在红帽企业 Linux 系统上的进程。

- 获取有关在系统上运行的程序的信息，以便您可以确定状态、资源使用情况和所有权，从而对它们进行控制。
- 使用 Bash 作业控制来管理从同一终端会话启动的多个进程。
- 控制和终止与 shell 无关的进程，以及强行结束用户会话和进程。
- 描述负载平均值的定义，并确定对服务器上高资源使用量负责的进程。

第 9 章 控制服务和守护进程

使用 Systemd 控制和监控网络服务与系统守护进程。

- 列出由 **systemd** 服务启动的系统守护进程和网络服务，以及套接字单元。
- 使用 **systemctl** 控制系统守护进程和网络服务。

第 10 章 配置和保护 SSH

使用 OpenSSH 配置远程系统上的安全命令行服务。

- 使用 **ssh** 登录远程系统并运行命令。
- 为用户帐户配置基于密钥的身份验证，以便其无需密码就能安全登录远程系统。
- 限制直接以 root 身份登录，并为 OpenSSH 服务禁用基于密码的身份验证。

第 11 章 分析和存储日志

查找和准确解读系统事件的日志，以满足故障排除之需。

- 描述红帽企业 Linux 用于记录事件的基本日志架构。
- 解读相关 syslog 文件中的事件，以排除故障或查看系统状态。
- 查找和解读系统日志中的条目，以排除故障或查看系统状态。
- 配置系统日志，以便在服务器系统重启时保留事件记录。
- 利用 NTP 维护准确的时间同步，并且配置时区以确保系统日志和日志记录的事件标有正确的时间戳。

第 12 章 管理网络

配置红帽企业 Linux 服务器上的网络接口和设置。

- 描述服务器的网络寻址和路由的基本概念。
- 使用命令行实用程序，测试并检查当前的网络配置。
- 使用 **nmcli** 管理网络设置和设备。
- 通过编辑配置文件修改网络设置。
- 配置服务器的静态主机名及其名称解析，并测试结果。

第 13 章 归档和传输文件

将文件归档，并从一个系统复制文件到另一系统。

- 使用 **tar** 将文件和目录归档到压缩文件中，以及提取现有 **tar** 存档的内容。
- 通过 SSH，与远程系统安全地来回传输文件。
- 将本地文件或目录的内容与远程服务器上的副本同步。

第 14 章 安装和更新软件包

从红帽和 Yum 软件包存储库下载、安装、更新和管理软件包。

- 将系统注册到您的红帽帐户，并使用红帽订阅管理为其分配软件更新和支持服务的权利。
- 说明如何以 RPM 软件包形式提供软件，并使用 Yum 和 RPM 调查系统上安装的软件包。
- 使用 **yum** 命令查找、安装和更新软件包。
- 启用和禁用红帽或第三方 YUM 存储库。
- 说明如何借助模块安装特定版本的软件，如何列出、启用和切换模块流，以及如何从模块安装和更新软件包。

第 15 章 访问 Linux 文件系统

访问、检查和使用附加至 Linux 服务器的存储上的现有文件系统。

- 说明块设备的定义，解释存储设备的文件名，并且识别文件系统用于特定目录或文件的存储设备。

- 通过将文件系统附加到文件系统层次结构中的目录来访问文件系统。
- 通过 **find** 和 **locate** 命令搜索已挂载文件系统上的文件。

第 16 章 分析服务器和获取支持

在基于 Web 的管理界面中调查和解决问题，并从红帽获取支持以帮助解决问题。

- 激活 Web 控制台管理界面，以远程管理和监控红帽企业 Linux 服务器的性能。
- 描述可通过红帽客户门户网站使用的重要资源，并在红帽文档和知识库中查找信息。
- 分析服务器问题，修复或解决问题，以及使用红帽智能分析工具确认解决方案。

▶ 开放研究实验

从命令行管理文件

在本复习中，您将管理文件，将文本文件中特定的几行重定向到另一个文件，并且编辑文本文件。

成果

您应能够：

- 从命令行管理文件
- 显示文本文件中一定数量的行，并将输出重定向到另一个文件。
- 编辑文本文件。

在你开始之前

在重置之前，将想要保留的任何文件或工作复制到其他系统中。现在重置 `workstation`、`servera` 和 `serverb` 系统。稍等片刻，直到 `workstation`、`servera` 和 `serverb` 系统启动。

以 `student` 用户身份并使用 `student` 作为密码登录 `workstation`。

在 `workstation` 上，运行 `lab rhcsa-rh124-review1 start` 以开始总复习。此脚本会创建必要的文件，以正确设置环境。

```
[student@workstation ~]$ lab rhcsa-rh124-review1 start
```

说明

在 `serverb` 上完成下列任务，以完成练习。

- 创建新目录 `/home/student/grading`。
- 在 `/home/student/grading` 目录中创建以下三个空文件：`grade1`、`grade2` 和 `grade3`。
- 将 `/home/student/bin/manage-files` 文件的前五行采集到 `/home/student/grading/manage-files.txt` 文件中。
- 将 `/home/student/bin/manage-files` 的最后三行附加到 `/home/student/grading/manage-files.txt` 文件。您不得覆盖 `/home/student/grading/manage-files.txt` 文件中已存在的任何文本。
- 将 `/home/student/grading/manage-files.txt` 复制到 `/home/student/grading/manage-files-copy.txt`。
- 编辑 `/home/student/grading/manage-files-copy.txt` 文件，使其包含显示有文本 `Test JJ` 的两个连续行。
- 编辑 `/home/student/grading/manage-files-copy.txt` 文件，使得该文件中不含 `Test HH` 文本行。