Red Hat Insights 2023

评估和监控 RHEL 系统上的安全漏洞

了解您的环境暴露于 Potential Security Threats

Last Updated: 2023-10-01

Red Hat Insights 2023 评估和监控 RHEL 系统上的安全漏洞

了解您的环境暴露于 Potential Security Threats

法律通告

摘要

使用漏洞服务评估和监控 RHEL 系统中安全漏洞的状态，了解基础架构公开程度，并计划采取行动。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 RHEL 漏洞服务的 INSIGHTS 概述

此漏洞服务支持快速评估和全面监控 RHEL 基础架构对常见漏洞和暴露(CVE)的监控，以便您可以更好地了解最重要的问题和系统，并有效地管理补救。

通过上传到漏洞服务的数据，您可以过滤并排序系统和 CVE 组，以优化和优化您的视图。您还可以给各个 CVE 添加上下文，以防对系统造成特殊风险。了解您的风险后，向适当的利益相关者报告 CVE 的状态，然后创建 Ansible Playbook 以修复问题来保护您的机构的安全。

先决条件

此漏洞服务适用于所有支持的 RHEL 6 版本 7、8 和 9。在使用漏洞服务前，必须满足以下条件：

- **每个系统都已安装 Insights 客户端，并注册到 Insights for Red Hat Enterprise Linux 应用程序。**按照 Red Hat Insights for Red Hat Enterprise Linux，获取入门说明 来安装客户端并注册您的系统。
- **此漏洞服务完全支持由 Red Hat Subscription Management (RHSM)和 Satellite 6 及更新版本管理的 RHEL 系统。**使用任何其他方法获取软件包更新，除了 Satellite 6 以外的 RHSM 使用 subscription.redhat.com 注册 RHSM （客户门户网站）可能会导致误导结果。
- **安全漏洞服务补救没有被完全支持，且可能无法在 Satellite 5 和 Spacewalk 托管 RHEL 系统中正常工作。**
- **有些功能需要您机构管理员提供的特殊权限。**具体来说，查看与特定 CVE 和系统关联的红帽安全公告(RHSA)，并在 Red Hat Enterprise Linux 补丁服务中查看并修补这些漏洞，需要通过用户访问获得权限。

其他资源

- *使用漏洞服务和 Ansible Playbook 修复安全风险*
- *生成安全漏洞服务报告*

1.1. 漏洞服务的工作方式

漏洞服务使用 Insights 客户端收集有关 RHEL 系统的信息。客户端收集有关系统的信息并将其上传到漏洞服务。

然后，这个漏洞服务会根据 Red Hat CVE 数据库和安全公告来评估数据，以确定是否有可能影响系统的未完成的 CVE，并提供这些比较的结果。

分析数据后，您可以查看并排序显示的结果，评估漏洞的风险和优先级，报告其状态，以及创建和部署 Ansible Playbook 以修复它们。漏洞服务的目标是启用可重复的流程，防止 RHEL 基础架构的安全性弱点。

第 2 章 安全漏洞服务用户的用户访问

在访问 Red Hat Insights for Red Hat Enterprise Linux 应用程序中的一些功能前，您必须具有正确的权限，这些权限在 Red Hat Hybrid Cloud Console > {SETTINGS (gear icon)} > Identity & Access Management > User Access > Groups 赋予。机构管理员或 **用户访问权限管理员必须** 作为成员添加到具有所需角色的 User Access 组中。

默认情况下，Red Hat Hybrid Cloud Console 上的用户访问（User Access）具有预配置的 **漏洞管理员（Vulnerability administrator）**（所有访问权限）和**漏洞视图（Vulnerability viewer）**（只读访问）角色。如果您的组织确定预定义的角色提供不足的访问权限，则 **User Access 管理员可以配置** 自定义角色，以提供一组用户需要的特定权限。

本章的以下部分介绍了漏洞服务用户的每个预定义角色。

重要

改为 User Access 需要由机构管理员在您的红帽帐户中执行，或者由一个是 User Access 组的成员，并带有 **User Access administrator** 角色的用户执行。

其他资源

- *基于角色的访问控制(RBAC)的用户访问权限配置指南*

2.1. 漏洞管理员角色

Vulnerability 管理员角色 是 **Default access 组的默认** 角色。您的帐户中的所有 Red Hat Enterprise Linux 用户都是 **Default 访问组的成**员。在默认配置中，具有 **Vulnerability 管理员角色** 的组成员可以访问所有漏洞服务资源。

您的机构可能会决定默认角色太有限，或者太宽松。要限制对某些功能的访问权限，或者添加额外的权限，**用户访问管理员可以** 自定义角色，并使用任何权限进行配置。通过自定义预配置的角色，**将替换 Default 访问组**。

2.2. 安全漏洞视图角色

在默认配置中，**Vulnerability viewer** 角色可以读取任何安全漏洞服务资源。这是一个预配置的角色，但没有包含在 **Default 访问组中**。**Vulnerability viewer** 角色包括以下权限：

- 查看并分类所有漏洞服务结果、页面和列表。
- 查看哪些系统已选择向 Red Hat Insights for Red Hat Enterprise Linux 报告结果。
- 为 .JSON 和 .CSV 输出设置过滤器和导出数据。
- 在 Security > Vulnerability > Reports 中查看并创建高级报告。

如果您的组织确定 Vulnerability viewer 角色的默认配置不低，则用户访问管理员可以创建具有所需特定权限的自定义角色。

第 3 章 常见漏洞和暴露(CVE)

通用漏洞和暴露(CVE)是在公开发布的软件包中发现的安全漏洞。CVE 由国家 Cybersecurity FFRDC (NCF)标识和列出，由 Mitre 公司进行的研究和开发中心标识并列出，并来自美国美国美国安全诊断的国家 Cyber Security Division。CVE 的完整列表位于 https://cve.mitre.org。

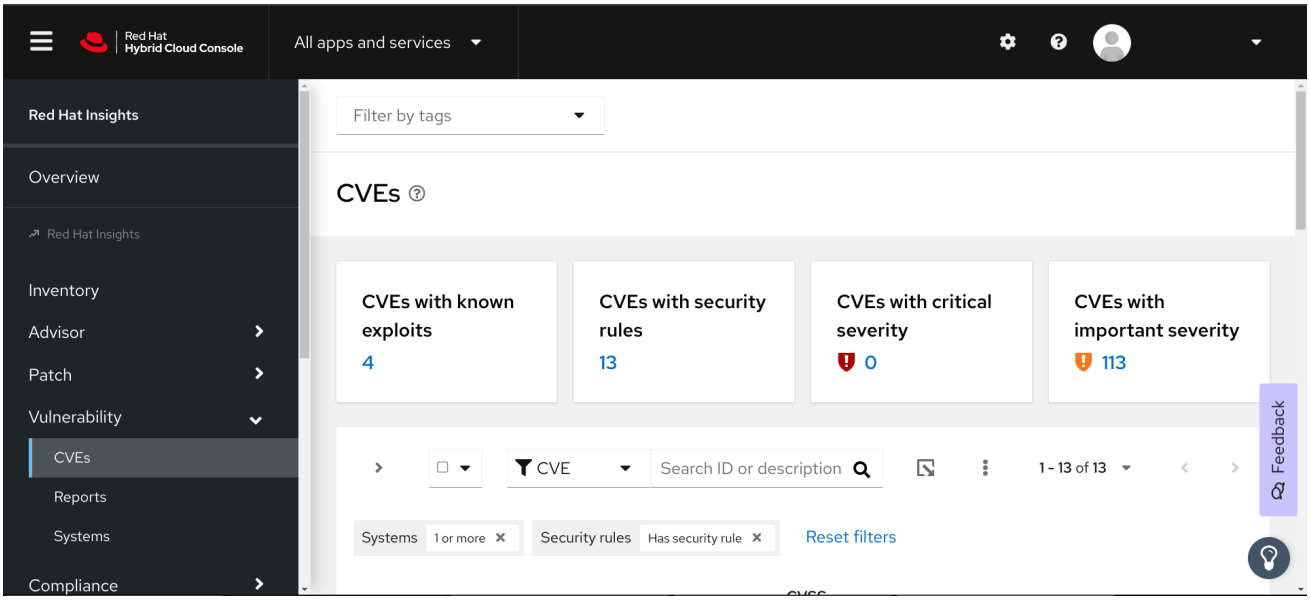
通过突出显示与 CVE 相关的公开已知漏洞和安全规则的 CVE，漏洞服务会增强威胁智能信息，以帮助确定哪些 CVE 给 RHEL 环境带来最大潜在风险，从而让用户能够有效地解决其最重要的问题。

重要

漏洞服务不包含 https://cve.mitre.org 的条目列表中包含的每个 CVE。只有红帽 CVE，那些红帽发布安全公告(RHSA)的 CVE 包括在漏洞服务中。

漏洞服务标识了影响 RHEL 系统的 CVE，表示严重性，并可让您有效地分类对最关键的安全漏洞。短划线将提醒您进入以下类型的 CVE：

- 已知的漏洞
- 安全规则
- 严重严重性
- 重要严重性

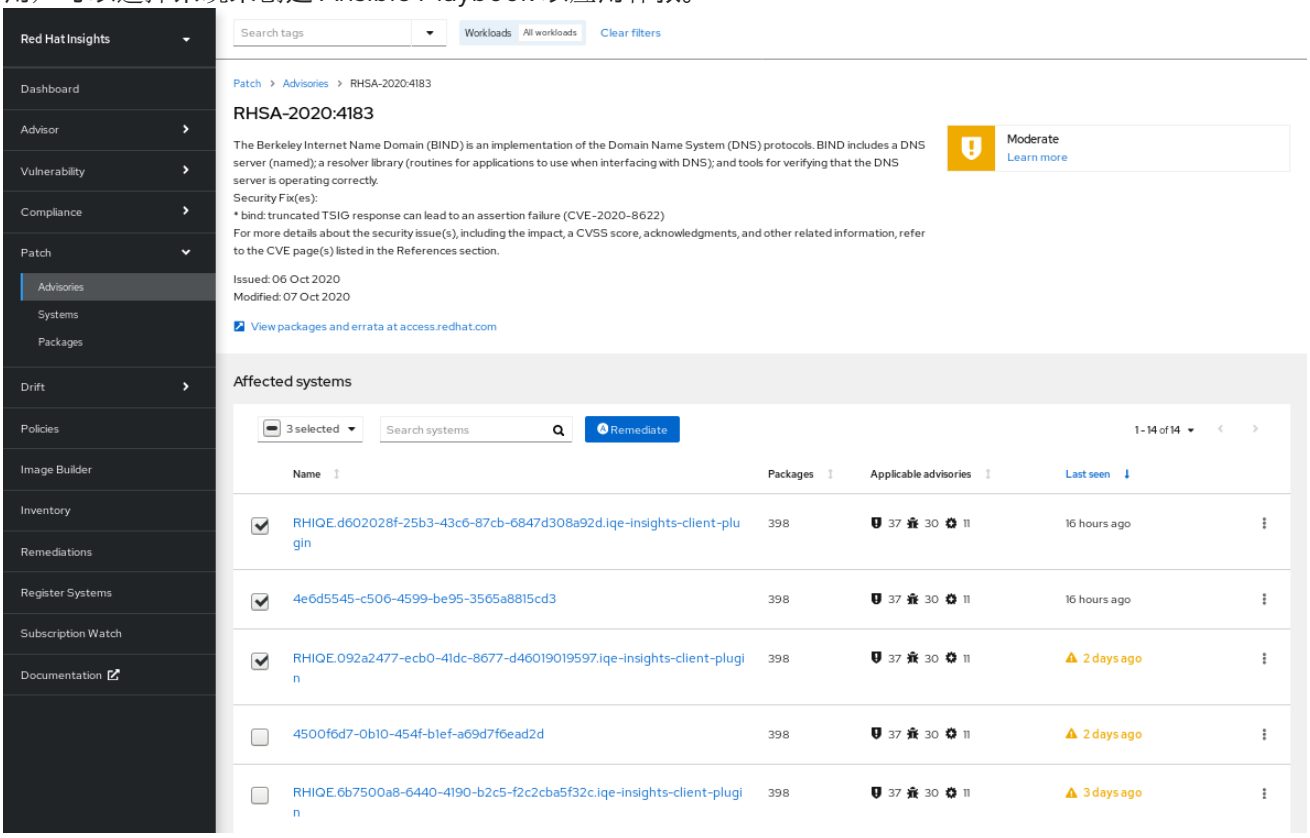


3.1. 红帽安全公告(RHSA)

红帽安全公告(RHSA)勘误记录了红帽产品中的安全漏洞。Red Hat Enterprise Linux 漏洞服务显示与向 CVE 公开的每个系统相关联的公告标识符。

选择 CVE 并在安全规则卡中选择 **Filter by affected** system 链接来查看此信息。如果系统存在公告，则 RHSA ID 会在 **Exposed systems** 列表中的的 **Advisory** 列的系统旁会显示一个链接。如果没有这样的公告，则 Advisory 列不可见，否则会显示 "Not available"。

当某个系统的公告存在时，用户可以查看有关 RHSA 的更多信息，包括受影响系统列表。在补丁服务中，用户可以选择系统来创建 Ansible Playbook 以应用补救。



3.2. 安全规则

安全规则的 CVE 可能会因为提升的风险并暴露了与其关联的风险导致了额外的可见性。这些安全漏洞可能收到大量媒体覆盖，并由红帽产品安全团队团队提供，使用产品 安全事件响应计划 工作流来帮助确定您的 RHEL 环境。这些安全规则允许您采取适当的操作来保护您的机构。

除了分析系统上运行的 RHEL 版本外，安全规则提供了深入威胁。通过分析 Insights 客户端收集的系统元数据，手动策展安全规则，以确定您是否容易受到安全威胁的影响。如果漏洞服务将系统识别为暴露于安全规则，则可能会提高安全风险，并且问题应该通过紧急处理。

重要

解决公开系统上的安全规则应该是您的最高优先级。

最后，并非所有暴露于 CVE 的系统也会暴露给与该 CVE 关联的安全规则。虽然您可能在运行存在安全漏洞的软件版本，但其他环境条件可能会降低威胁；例如，一个特定的端口已关闭，或者如果您正在运行 SELinux。

3.2.1. 在 RHEL 仪表板中识别 Insights 中的安全规则

使用以下步骤查看您的基础架构暴露于安全规则。

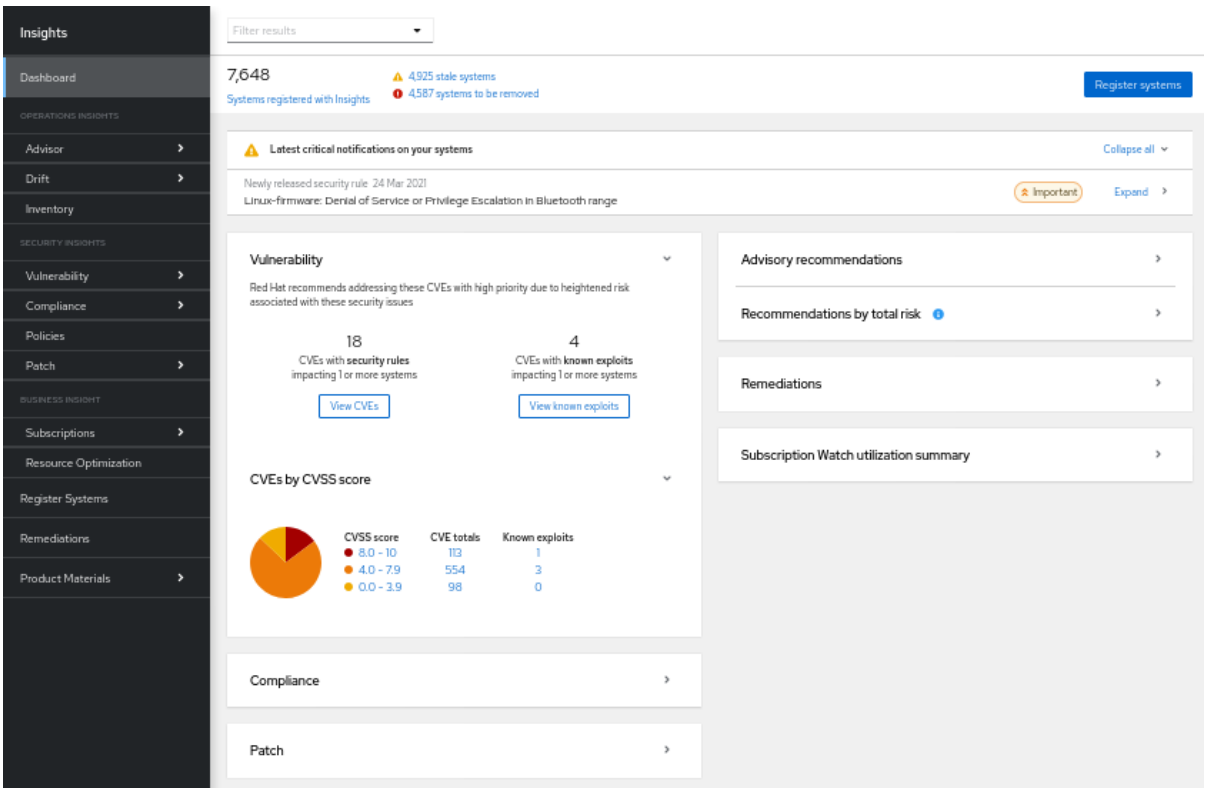
流程

1. 导航到 Red Hat Insights for Red Hat Enterprise Linux 仪表板 。

注意

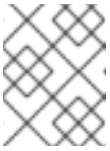
为简单起见，以下屏幕截图中可最小化与安全漏洞评估相关的服务的面板。

:



2. 查看您的系统面板中的**最新的关键通知**。这些是安全规则，升级的严重性评级为 "Important" 或 "Critical"。 这些是您的最重要的问题，应该优先选择进行补救。

   a. 在每个通知右侧，点 **Expand** 按钮来查看关联的 CVE 和您的基础架构中公开的系统数量。



注意

您可能会在关键通知中看到安全规则，但公开了零个系统。在这种情况下，即使 CVE 存在于您的基础架构中，则安全规则条件可能不存在。

   b. 在安全规则的名称下，并在关联的 CVE 下点击 CVE ID 链接。

   c. 查看哪些系统会受到安全规则 CVE 的影响，并选择性地选择公开系统来创建 playbook。

3. 接下来，查看 **漏洞** 卡中的信息。

   a. 请注意“CVEs with **security rules** impacting systems.”的数。 这个数字包括任何影响至少一个系统的严重性的安全规则。

      i. 点 **View CVEs**。根据高严重性安全规则，请考虑您的第二个最高优先级进行补救的最高安全规则。

3.3. 已知的漏洞

红帽分析 Metasploit 数据，以确定代码是否公开利用 CVE，或者 CVE 已公开利用。漏洞服务将"已知漏洞"标签应用到满足该条件的 CVE。

这种增强的威胁评估可帮助用户识别并解决首先出现最重要的风险的 CVE。红帽建议用户查看具有高优先级的"已知利用(Known exploit) "标签的 CVE，并解决这些问题。

重要

漏洞服务可让您了解在基础架构的系统上存在已知的 CVE。"已知利用"标签并不意味着漏洞已在 RHEL 系统中被利用。这个漏洞服务不会进行判断。

3.4. 常见漏洞和暴露性通过 TRIAGE 功能提供深入威胁

漏洞服务为您提供了有关各个常见漏洞和暴露(CVE)的数据，以及它们对注册到 Insights 的系统的影响。CVE 被归类为 **存在安全漏洞** 或 **受影响，但不存在安全漏洞。**此级别的安全威胁智能功能适用于具有 **Security Rule** 标签或已通过红帽产品安全团队严格分析的 CVE。

这提高了威胁智能功能，您可以首先解决最严重的问题。在管理大量服务器时，这转换为快速保护和显著的技术。

受影响的但不受漏洞的 CVE 状态意味着您正在运行有漏洞 但目前无法被利用的软件。这个系统需要补救，但不需要立即关注。

存在安全漏洞的 CVE 状态表示带有可利用开放路径的安全漏洞代码。开放的路径可以是允许以下之一的端口或操作系统版本：机密信息被泄漏，系统的完整性会被破坏或可用。

我们查看 **存在安全漏洞的** 服务器的一个示例与 **受影响的服务器，但不受到攻击** 的服务器：

假设 **服务器 A** 运行有漏洞的软件，允许 root 访问该系统。**服务器 A** 将被视为存在安全漏洞，需要立即修补。

相反，假设 **服务器 B** 的当前配置会阻止漏洞进行清单，即使存在于受影响的代码中。**服务器 B** 将被视为 **受影响，但不被视为存在安全漏洞**。这意味着，**服务器 B** 可以重新设置为 to-do 列表，以便更立即威胁，**可以修复服务器 A**。

重要信息：在 **Server A** 得到解决后，您应该对 **Server B** 进行补丁，因为它正在运行可能存在安全漏洞的代码。版本更新以及其他事件可能会导致它在以后存在安全漏洞。

3.4.1. 在 Red Hat Insights for RHEL 仪表板中识别已知的 CVE

使用以下步骤识别 Red Hat Enterprise Linux 仪表板漏洞卡中已知的 CVE。

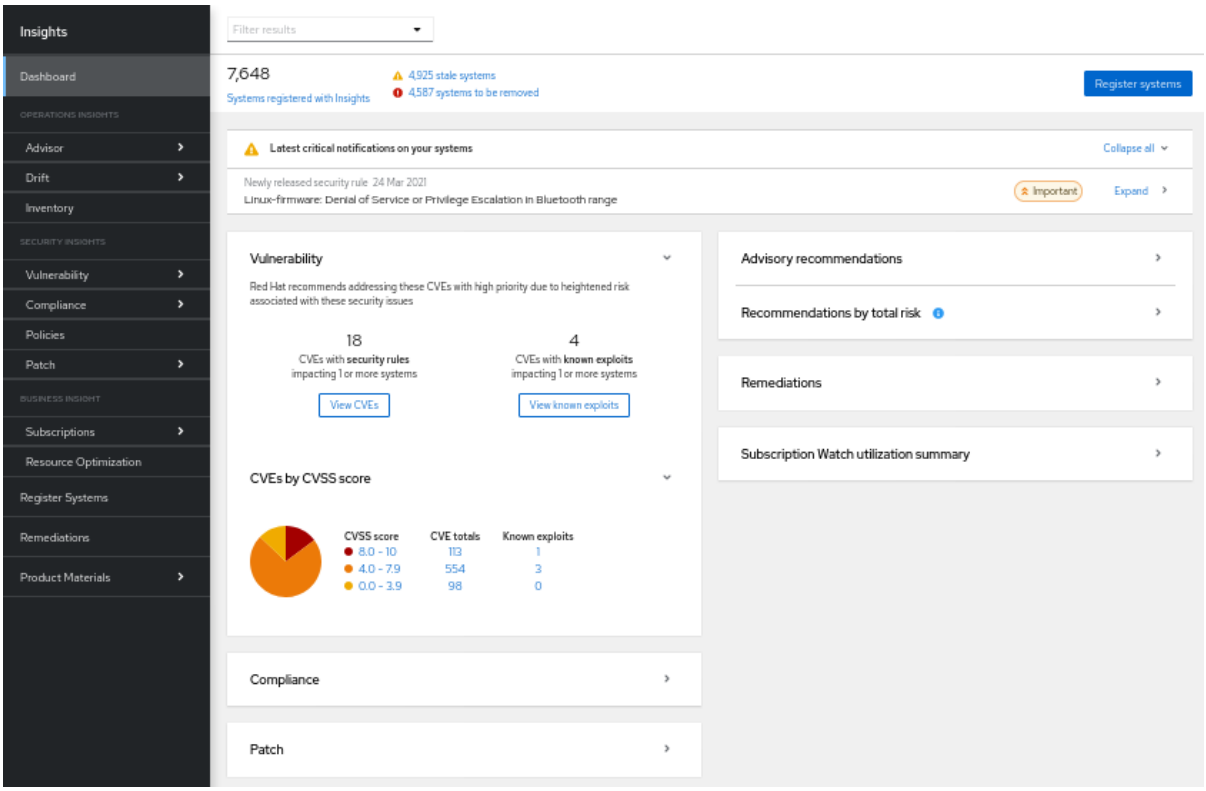
流程

1. 导航到 Red Hat Insights for Red Hat Enterprise Linux 仪表板 。

注意

为简单起见，以下屏幕截图中可最小化与安全漏洞评估相关的服务的面板。

:



2. 在 **漏洞** 卡中，请注意 **带有已知漏洞的 CVE 会影响 1 个或更多系统，以及显示的数字。**
3. 点 **View Known exploits。**
4. 查看 CVE 列表中 Known-exploit CVE 的过滤列表。

第 4 章 修正了 VULNERABILITY-SERVICE 结果

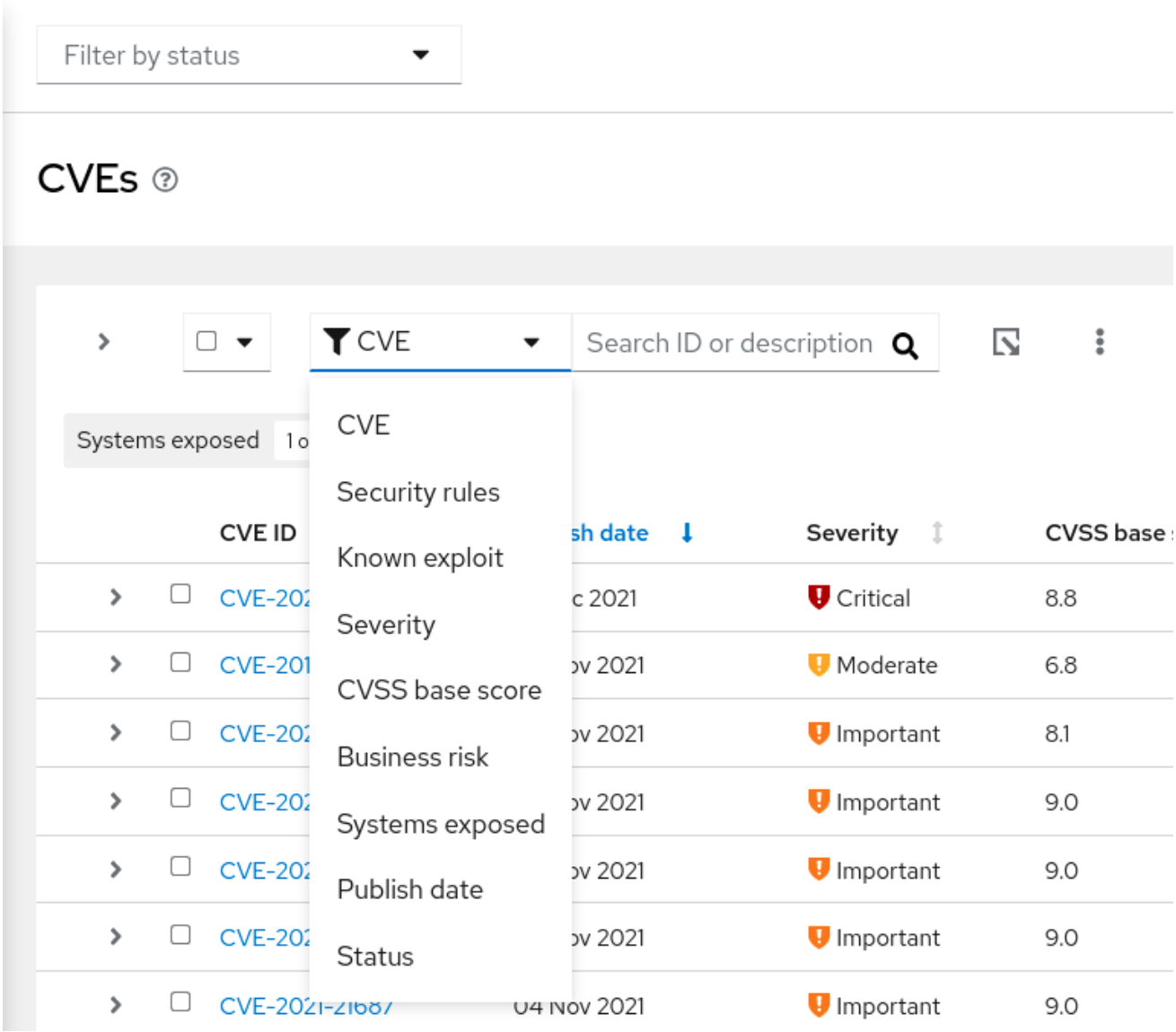
无论向利益相关者报告结果还是优先考虑补救系统，漏洞服务都允许许多方法来优化您的数据视图，帮助您和其它方面专注于最重要的系统、工作负载或问题。以下小节描述了您的数据的组织以及可用于优化和增强结果的排序、过滤和上下文功能。

4.1. CVE-LIST 和 SYSTEM-LIST 过滤器

过滤缩小 CVE 和相关系统的可见列表，可帮助您专注于特定问题。将过滤器应用到 CVEs 列表，以便按严重程度或业务风险专注于 CVE。选择单独的 CVE 后，对受影响的系统列表应用过滤器，以专注于特定 RHEL 主版本或次版本的用户，例如：

通过从左侧的过滤器下拉列表中选择主过滤器，然后从右侧的过滤器列表中选择二级子过滤器来激活过滤器。所选过滤器在过滤器菜单下可见，可通过单击每个的 X 来停用。

CVEs 列表过滤器

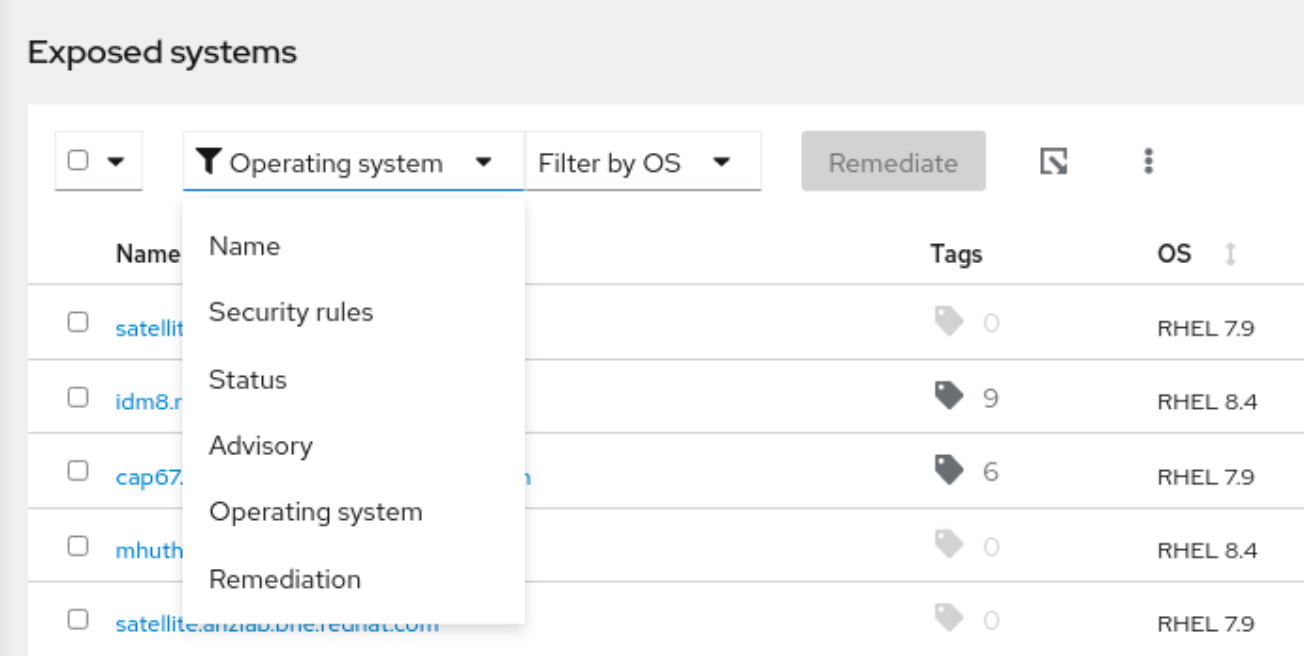


以下主要过滤器可从 CVE 页面访问。选择主过滤器，然后在 subfilter 中定义参数：

- **CVE.**搜索 ID 或描述。
- **安全规则。**仅显示带有 "Security rule" 标签的 CVE。

- **已知的漏洞利用。**仅显示带有 "Known exploit" 标签的 CVE。
- **严重性。**选择一个或多个值：Critical, Important, Moderate, Low, 或 Unknown。
- **CVSS 基本分数.**选择一个或多个范围： All, 0.0-3.9, 4.0-7.9, 8.0-10.0, N/A （不适用）
- **业务风险。**选择一个或多个值： High, Medium, Low, Not defined。
- **Systems exposed .**选择仅显示当前影响的系统的 CVE，或者没有影响系统。
- **发布日期。**从 All, Last 7 days, Last 30 days, Last 90 days, Last year, 或 More than 1 年以上选择。
- **状态。**选择一个或多个值：Not review, In review, On-hold, Scheduled for patch, Resolved, No action - risk accepted, Resolved by mitigation.

系统列表过滤器



以下主要过滤器可从 CVE 详情页面的系统列表的顶部访问：

- **名称。**输入 CVE ID 来查找特定的 CVE。
- **安全规则。**如果 CVE 关联了一个安全规则，则根据其他系统进行过滤，容易受到同一安全规则的影响，或者显示不受安全规则的影响。
- **状态。**以特定状态或工作流类别显示系统。
- **公告。**显示红帽公告适用于此 CVE 的系统。
- **操作系统。**显示运行特定 RHEL （次）版本的系统。
- **补救。**显示 Ansible Playbook、手动补救或者未包含在当前补救计划中的系统。

4.2. 过滤安全规则 CVE

特别是高严重性安全规则的安全规则会对您的基础架构带来最大的潜在威胁，并应考虑识别和补救的最高优先级。使用以下步骤仅在 CVE 列表中查看高严重性安全规则 CVE 并确定受影响的系统。

注意

并非所有暴露于 CVE 的系统也会暴露给与该 CVE 关联的安全规则。虽然您可能在运行存在安全漏洞的软件版本，但其他环境条件可能会降低威胁；例如，特定端口关闭或者启用 SELinux。

流程

1. 进入 Red Hat Insights for Red Hat Enterprise Linux 中的 Security > Vulnerability > CVEs。
2. 点工具栏中的过滤器下拉列表。
   a. 应用 **Security rules** 过滤器。
   b. 应用 **Has 安全规则** 子过滤器。
3. 向下滚动以查看安全规则 CVE。带有安全规则的 CVE 会显示位于 CVE ID 下的 security-rule 标签。

4.3. 使用 RHEL 系统上的安全规则修复漏洞

具有安全规则的 CVE 是红帽优先级的 CVE，因为他们专注于系统有提升风险的问题。修复这些问题有助于支持安全状态，确定您的组织中最重要的问题。通过使用漏洞服务和补救服务，您可以对系统进行优先排序并修复一些最重要的威胁：

- 专注于具有安全规则的 CVE。有关安全规则的更多信息，请参阅 安全规则，以及 过滤公开给安全规则的系统列表。
- 修复 CVE.有关修复 CVE 的更多信息，请参阅 Red Hat Insights 修复指南 。

4.4. 过滤已知的 CVE

带有"已知利用"标签的 CVE 由红帽决定，以利用这些技术中存在的漏洞；代码会公开利用利用 CVE，或者已知漏洞已公开发生。因此，在识别和补救时，应该优先选择已知的 CVE。

重要

红帽不会确定您的任何注册的系统是否已被利用。我们只是识别可能会带来特殊风险的 CVE。

使用以下步骤过滤 CVE 列表中已知的 CVE：

流程

1. 进入 Red Hat Insights for Red Hat Enterprise Linux 中的 Security > Vulnerability > CVEs。
2. 点工具栏中的过滤器下拉列表。
   a. 应用 **Known exploit** 过滤。
   b. 应用 **Has a known exploit** 子过滤。
3. 向下滚动以查看已知的可被利用的 CVE 列表。

4.5. 过滤公开给安全规则的系统列表

在过滤 CVE 列表以只查看您的最重要的威胁后，选择一个 CVE 来查看公开系统列表，并将过滤器应用到列表中。

流程

1. 选择安全规则 CVE 后，向下滚动到 **Exposed systems** 列表。并非列表中的每个系统都存在 CVE 的安全规则条件，以便 CVE 成为安全规则。应用以下过滤器，仅查看存在安全规则条件的系统。
2. 从主过滤器下拉列表中选择 **Security rules** 过滤器。
3. 选中二级子过滤器下拉列表中的 **Has 安全规则** 框。
4. 查看暴露了该 CVE 的系统，这些 CVE 也存在安全规则的条件。

4.6. INSIGHTS FOR RHEL 组过滤器

通过根据系统或工作负载组过滤漏洞服务结果的功能，用户只能查看标记为属于特定组的系统。这些可以是由 Satellite 主机组运行 SAP 工作负载（或 SAP ID）的系统，也可以通过添加到 Insights 客户端配置文件中的自定义标签。

可以使用位于 Red Hat Enterprise Linux 应用程序整个页面顶部的 **Filter 结果** 框在 Insights for Red Hat Enterprise Linux 的 Insights 中全局设置组过滤。从服务更改为服务并将页面更改为页面时，组选择会保留。但是，这个功能因 Red Hat Enterprise Linux 服务的不同 Insights 而异。

组过滤可在漏洞仪表板和漏洞服务 CVE 和系统列表中工作。

参阅本文档的 标签和 *系统组部分了解更多有关组标签和配置* 自定义标签的信息。

4.6.1. 按组过滤仪表板、CVE 和系统列表

使用以下步骤根据组过滤安全漏洞服务 CVE 和系统列表。

流程

1. 导航到 Red Hat Hybrid Cloud Console 并登录。
2. 打开 Red Hat Enterprise Linux 应用程序的 Red Hat Insights。
3. 点 Insights 应用中任何页面顶部的 **Filter 结果** 框的下箭头。
4. 选择要过滤您的系统的组。
   搜索或滚动以查看可用的标签。要浏览可用标签的完整列表，请滚动到列表的底部，然后单击 **View more**。

   （可选）

   a. 选择 SAP 工作负载。

   b. 根据特定的 SAP ID 选择系统。

   c. 选择 Satellite 主机聚合。

   d. 选择由自定义组标签标识的系统。

要了解更多有关创建自定义标签的信息，请参阅本文档中的 **自定义系统标记** 部分。

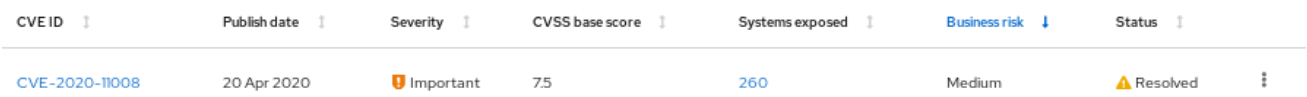
5. 进入该服务，仅查看属于您选择的组或组的系统或 CVE。

4.7. 为 CVE 定义业务风险

通过这个漏洞服务，您可以使用以下选项定义 CVE 的风险： High、Medium、low 或 Not Defined （默认）。

虽然 CVE 列表显示每个 CVE 的严重性，但分配业务风险可让您根据可能对您的组织的影响对 CVE 进行等级排序。这可让您更好地控制在大型环境中高效地管理风险，并让您做出更好的操作决策。

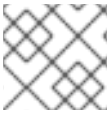
默认情况下，特定 CVE 的业务风险字段被设置为 **Not Defined**。设置业务风险后，会在 CVE 行的 Security > Vulnerability > CVEs 列表中可见。



每个 CVE 的详细信息卡中也会看到业务风险，其中显示更多信息并列出受影响的系统。

4.7.1. 为单个 CVE 设置业务风险

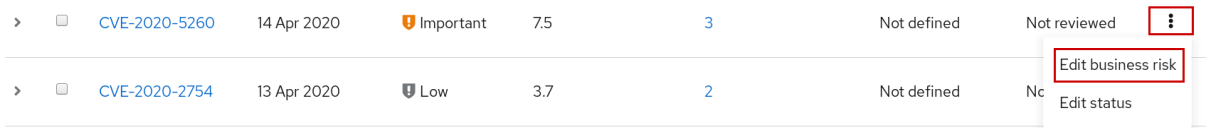
完成以下步骤，为单个 CVE 设置业务风险：



注意

CVE 的企业风险在受其 *影响的所有* 系统上都是相同的。

1. 进入 Security > Vulnerability > CVEs 页面，并在需要时登录。
2. 确定要为其设置业务风险的 CVE。
3. 点 CVE 行右侧的 **more-actions** 图标（三个垂直点），然后单击 **Edit business risk**。



4. 为适当的级别设置业务风险值，并（可选）为您的风险评估添加说明。
5. 点击 **Save**。

4.7.2. 为多个 CVE 设置业务风险

完成以下步骤，在您选择的多个 CVE 上设置相同的业务风险：

1. 进入 Security > Vulnerability > CVEs 并在需要时登录。
2. 选中您要为其设置业务风险的 CVE 框。
3. 执行以下步骤设定业务风险：
   a. 点工具栏中过滤器下拉菜单右侧的 **more-actions** 图标（三个垂直点），然后单击 **Edit business risk**。
   b. 设置适当的业务风险价值，并选择性地为您的风险评估添加说明。
   c. 点击 **Save**。

4.8. 将系统从漏洞服务分析中排除

漏洞服务允许您在漏洞分析中排除特定的系统。这可节省时间，并注意与您的机构目标无关的系统中的检查和重新检查问题。

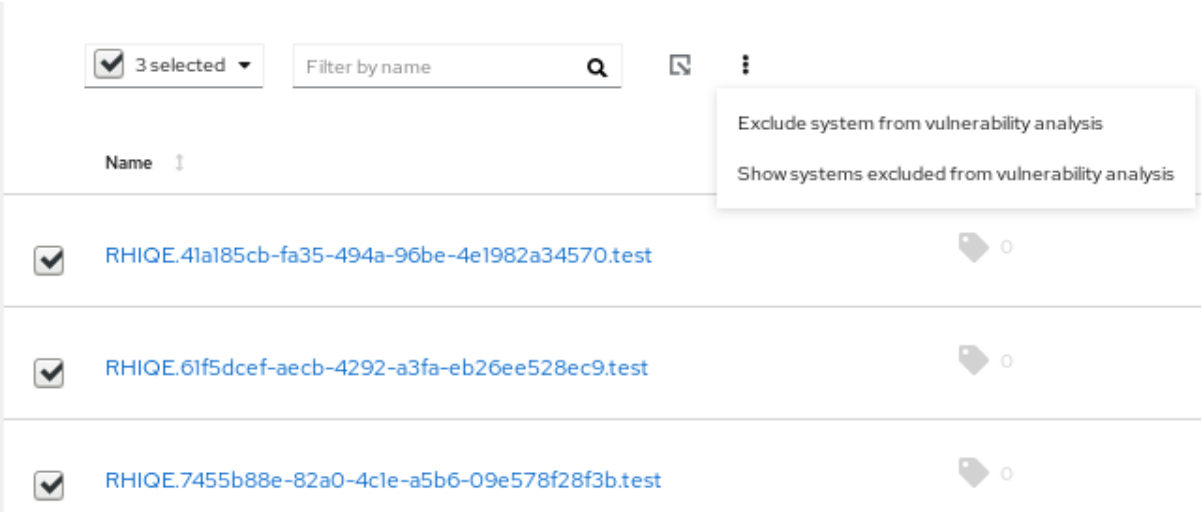
例如，如果您有以下类型的服务器： QA、Dev Dev 和 Production，您可能不负责检查 QA 服务器的漏洞，因此希望将这些系统排除在由漏洞服务执行的分析中。

当您从漏洞分析中排除系统时，Insights 客户端仍然会根据系统调度运行，但系统的结果在漏洞服务中不可见。客户端的继续操作可确保其他 Red Hat Insights for Red Hat Enterprise Linux 服务仍然可以上传所需的数据。这也意味着您仍然可以使用过滤查看这些系统的结果。

完成以下步骤，将所选 RHEL 系统从漏洞服务分析中排除：

流程

1. 进入 Security > Vulnerability > Systems 选项卡，并在需要时登录。
2. 选中您要从漏洞分析中排除的每个系统的复选框。
3. 点击工具栏中的 **more-actions** 图标，在系统的顶部，然后选择 **Exclude systems from vulnerability analysis**。



4. 另外，您可以通过点系统行中的 **more-actions** 图标并选择 **Exclude system from vulnerability analysis** 来排除一个 *特定*系统。

4.9. 显示之前排除的系统

完成以下步骤以显示之前排除的系统：

流程

1. 进入 Security > Vulnerability > Systems 选项卡，并在需要时登录。
2. 点工具栏中的 **more-actions** 图标，在系统列表的顶部，然后选择 **Show systems excluded from analysis** from。
3. 请参阅 漏洞分析中排除的系统。这可以通过 **Applicable CVEs** 列中的 **Excluded** 值进行验证。

4.10. 恢复系统漏洞分析

完成以下步骤，恢复系统的漏洞分析：

流程

1. 进入 Security > Vulnerability > Systems 选项卡，并在需要时登录。
2. 点工具栏中的 **more-actions** 图标，在系统列表的顶部，然后选择 **Show systems excluded from analysis** from。
3. 在结果列表中，选中您要恢复漏洞分析的每个系统的方框。
4. 再次点 **more-actions** 图标，选择 **Resume analysis for system**。

4.11. CVE 状态

管理影响您的系统的 CVE 的另一种方法是通过为 CVE 设置状态。漏洞服务启用了以下为 CVE 设置状态的方法：

- 为*所有*系统的一个 CVE 设置一个状态。
- *为特定 CVE + 系统对* 设置状态。

状态值为 preset，并包含以下选项：

- 未审核（默认）
- in-review
- on-hold
- 调度补丁
- 已解决
- 无操作 - 接受的风险

- 通过缓解措施解决

为 CVE 设置状态有助于更好地分类其生命周期。通过定义状态，您的机构可以保持更好的标签页，其中最重要的 CVE 处于其生命周期，您应该专注于解决每个业务需求最重要的问题。CVE 的状态在漏洞服务和单个 CVE 视图中的所有 CVE 表中可见。

4.11.1. 在所有受影响的系统中为 CVE 设置状态

完成以下步骤，为 CVE 设置状态，并将该状态应用到它影响的所有系统中：

流程

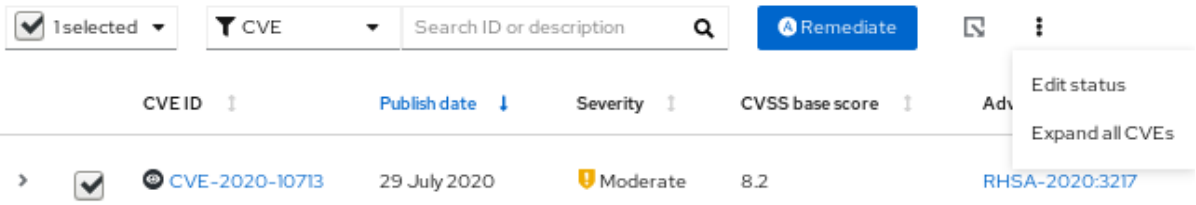
1. 进入 Security > Vulnerability > CVEs 选项卡，并在需要时登录。
2. 点击 CVE 行右侧的 **more-actions** 图标并选择 **Edit status**。
3. 选择适当的状态，并选择性地在 **Justification** 文本框中输入您的决策的比例。
4. 如果在 **独立系统中为这个 CVE 设置了状态且希望保留，请检查 不要覆盖** 单独的系统状态。否则，不选中复选框，将这个状态应用到它影响的所有系统中。
5. 点击 **Save**。

4.11.2. 为 CVE 和系统对设置状态

完成以下步骤以在 CVE 和系统对中设置状态：

流程

1. 进入 Security > Vulnerability > Systems 选项卡，并在需要时登录。
2. 确定系统并点击系统名称来打开它。
3. 从列表中选择一个 CVE，并选中 CVE ID 旁边的框。
4. 单击工具栏中的 **more-options** 图标，然后选择 **Edit status**。



5. 在弹出卡中执行以下操作：
   a. 为 CVE 和系统对设置状态。

注意

如果选中 **使用总体 CVE 状态** 的复选框，则无法为这个对设置状态。

   b. （可选）为您的状态确定输入说明。
   c. 点击 **Save**。

6. 在列表中找到 CVE，并验证是否已设置状态。

4.12. 使用搜索框

漏洞服务的搜索功能可在您要查看的页面上下文中工作。

- **CVE 页面。**搜索框位于 CVE 列表顶部的工具栏中。设置 CVE 过滤器后，搜索 CVE ID 和描述。

- **系统页面。**搜索框位于列表顶部的工具栏中。搜索系统名称或 UUID。

4.13. 排序 CVE 列表数据

漏洞服务中的排序功能因您要查看页面的上下文而异。

流程

1. 在 **CVEs 选项卡中**，您可以应用以下列排序：
   - CVE ID
   - 发布日期
   - 重要性
   - CVSS 基本分数
   - 已公开的系统
   - 业务风险
   - 状态
2. 在 **Systems 选项卡中**，可以排序以下列：
   - Name
   - 适用的 CVE
   - 最后看到
3. 在 Systems 选项卡中选择系统后，特定于系统的 CVE 列表允许以下排序选项：
   - CVE ID
   - 发布日期
   - 影响
   - CVSS 基本分数

- 业务风险
- 状态

第 5 章 系统标签和组群

Red Hat Insights for Red Hat Enterprise Linux 可让管理员使用组标签过滤清单中的系统组以及各个服务。组通过针对 Red Hat Enterprise Linux 的 Insights 的系统数据查找方法来标识。Insights for Red Hat Enterprise Linux 允许根据运行 SAP 工作负载的系统组（由 Satellite 主机组）、Microsoft SQL Server 工作负载以及具有 root 访问权限的自定义标签过滤系统组，以便在系统中配置 Insights 客户端。

注意

自 Spring 2022 年，清单、公告、合规性、漏洞、补丁、偏移和策略启用按组和标签进行过滤。其他服务将遵循。

重要

与启用标记的其他服务不同，合规服务在合规服务 UI 中的系统列表中设置标签。如需更多信息，请参阅 *合规性服务中的以下章节组和标签过滤器*。

使用 global, **Filter results** 复选框，根据 SAP 工作负载、Satellite 主机组、MS SQL Server 工作负载或添加到 Insights 客户端配置文件中的自定义标签进行过滤。

先决条件

在 Red Hat Enterprise Linux 中使用 Red Hat Insights 中的标记功能，必须满足以下先决条件和条件：

- Red Hat Insights 客户端已安装并在每个系统中注册。
- 您必须具有 root 权限或等效权限才能创建自定义标签或更改 **/etc/insights-client/tags.yaml** 文件。

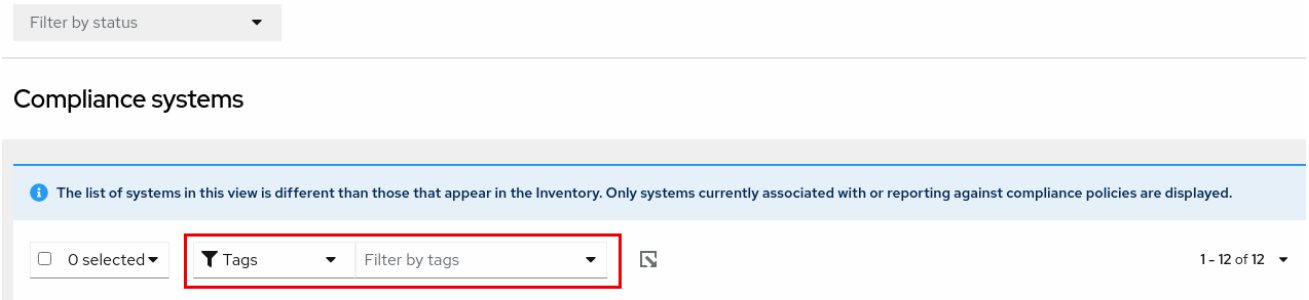
5.1. COMPLIANCE 服务中的组和标签过滤器

合规服务允许用户将标签和组过滤器应用到报告合规性数据的系统，但不使用 **Filter by status** 下拉菜单进行设置。与 Insights for Red Hat Enterprise Linux 应用程序的 Insights 中大多数其他服务不同，合规服务只显示以下条件的系统数据：

- 系统与合规服务安全策略关联。
- 系统使用 **insights-client --compliance** 命令报告合规数据以深入了解。

由于这些条件，compliance-service 用户必须使用符合合规服务 UI 中的系统列表和次过滤器来设置 tag 和 group 过滤器。

在合规服务中，标签和组过滤器上面的系统列表



5.2. SAP 工作负载

随着 Linux 成为 2025 年 SAP ERP 工作负载的强制操作系统，Red Hat Enterprise Linux 和 Red Hat Insights for Red Hat Enterprise Linux 正努力使 Insights for Red Hat Enterprise Linux 成为 SAP 管理员选择的管理工具。

作为这一持续工作的一部分，Red Hat Enterprise Linux 的 Insights 会自动标记运行 SAP 工作负载的系统，以及 SAP ID (SID)，而无需管理员所需的自定义。用户可以使用全局 **Filter by tags** 下拉菜单在 Insights for Red Hat Enterprise Linux 应用程序中轻松过滤这些工作负载。

5.3. SATELLITE 主机组

Satellite 主机组在 Satellite 中配置，并由 Insights for Red Hat Enterprise Linux 自动识别。

5.4. MICROSOFT SQL SERVER 工作负载

使用全局 **Filter by tags** 功能，Red Hat Insights for Red Hat Enterprise Linux 用户可以选择运行 Microsoft SQL Server 工作负载的系统组。

2019 年 5 月，Red Hat Insights 团队为在 Red Hat Enterprise Linux (RHEL)上运行的 Microsoft SQL Server 引进了一组新的 Insights for Red Hat Enterprise Linux 建议。这些规则提醒管理员迁移到不符合 Microsoft 和 Red Hat 文档的建议的操作系统级别配置。

这些规则的限制是它们主要分析操作系统而不是数据库本身。Insights for Red Hat Enterprise Linux 和 RHEL 8.5 的最新版本引入了 Microsoft SQL 评估 API。SQL 评估 API 提供了用于评估 MS SQL Server 的数据库配置的机制，以获得最佳性能。API 附带一个规则集，其中包含 Microsoft SQL Server 团队推荐的最佳实践规则。虽然此规则集随着新版本发布进行了增强，但 API 使用意图构建，以提供高度可定制且可扩展的解决方案，用户可以调整默认规则并自行创建。

Linux 的 PowerShell 支持 SQL 评估 API （可从 Microsoft 使用），Microsoft 定义了一个 PowerShell 脚本，可用于调用 API 并将其结果存储为 JSON 格式的文件。使用 RHEL 8.5 时，Insights 客户端现在上传此 JSON 文件，并在 Insights for Red Hat Enterprise Linux UI 中以易进的形式呈现结果。

有关 Insights for Red Hat Enterprise Linux 中的 SQL Server 评估的更多信息，请参阅通过 Red Hat Insights 提供 SQL Server 数据库最佳实践。

5.4.1. 设置 SQL Server 评估

要配置 Microsoft SQL 评估 API，以便为 Red Hat Insights 提供信息，数据库管理员需要执行以下步骤。

流程

1. 在您要评估的数据库中，使用 SQL 身份验证为 SQL Server 评估创建一个登录。以下 Transact-SQL 创建一个登录。使用强大的密码替换 **<rhacmPASSWORD** the> ：

```
USE [master]
GO
CREATE LOGIN [assessmentLogin] with PASSWORD= N'<*PASSWORD*>'
ALTER SERVER ROLE [sysadmin] ADD MEMBER [assessmentLogin]
GO
```

2. 按如下所示存储用于登录的凭证，再次将 < 过程PASSWORD the 替换为在第 1 步中使用的密码。

```
# echo "assessmentLogin" > /var/opt/mssql/secrets/assessment
# echo "<*PASSWORD*>" >> /var/opt/mssql/secrets/assessment
```

3. 通过确保只有 mssql 用户可以访问凭证，来保护评估工具所使用的凭证。

```
# chmod 0600 /var/opt/mssql/secrets/assessment
# chown mssql:mssql /var/opt/mssql/secrets/assessment
```

4. 从 microsoft-tools 存储库下载 PowerShell。这是安装 **mssql-tools** 和 **mssqlodbc17** 软件包时配置的仓库，作为 SQL Server 安装的一部分。

```
# yum -y  install powershell
```

5. 为 PowerShell 安装 SQLServer 模块。此模块包括评估 API。

```
# su mssql -c "/usr/bin/pwsh -Command Install-Module SqlServer"
```

6. 从 Microsoft 示例 GitHub 存储库下载 run\":\" 脚本。确保它归 mssql 所有并由其执行。

```
# /bin/curl -LJ0 -o /opt/mssql/bin/runassessment.ps1
https://raw.githubusercontent.com/microsoft/sql-server-samples/master/samples/manage/sql-assessment-api/RHEL/runassessment.ps1
# chown mssql:mssql /opt/mssql/bin/runassessment.ps1
# chmod 0700 /opt/mssql/bin/runassessment.ps1
```

7. 创建用于存储 Red Hat Insights 使用的日志文件的目录。同样，请确保它归 mssql 所有并可执行。

```
# mkdir /var/opt/mssql/log/assessments/
# chown mssql:mssql /var/opt/mssql/log/assessments/
# chmod 0700 /var/opt/mssql/log/assessments/
```

8. 现在，您可以创建第一个评估，但请确保以用户 mssql 用户身份执行此操作，以便以 mssql 用户身份通过 cron 或 systemd 自动运行后续评估。

```
# su mssql -c "pwsh -File /opt/mssql/bin/runassessment.ps1"
```

9. Insights for Red Hat Enterprise Linux 将在下次运行时自动包含评估，或者您可以运行以下命令来启动 Insights 客户端：

```
# insights-client
```

5.4.1.1. 在计时器上设置 SQL 评估

由于 SQL Server 评估可能需要 10 分钟或更长时间完成，因此您可能并没有意义，以便每天自动运行评估过程。如果您希望自动运行它们，Red Hat SQL Server 社区创建了 systemd 服务和计时器文件，用于评估工具。

流程

1. 从 实践 GitHub 站点的红帽公共 SQL Server 社区 下载以下文件：
   - **mssql-runassessment.service**
   - **mssql-runassessment.timer**

2. 在 **/etc/systemd/system/** 目录中安装这两个文件：

```
# cp mssql-runassessment.service /etc/systemd/system/
# cp mssql-runassessment.timer /etc/systemd/system/
# chmod 644 /etc/systemd/system/
```

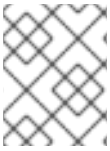
3. 使用以下方法启用计时器：

```
# systemctl enable --now mssql-runassessment.timer
```

5.5. 自定义系统标记

通过将自定义分组和标记应用到您的系统，您可以为各个系统添加上下文标记，根据 Insights for Red Hat Enterprise Linux 应用程序中的标签过滤，并更轻松地专注于相关系统。当大规模部署 Insights for Red Hat Enterprise Linux 时，此功能可能尤其重要，管理中有很多数百个或数千个系统。

除了向多个 Insights for Red Hat Enterprise Linux 服务的 Insights 中添加自定义标签外，您还可以添加预定义的标签。顾问服务可以使用这些标签为您的系统创建目标建议，比如那些需要更高级别的安全性的系统。



注意

要创建自定义和预定义的标签，您必须具有 root 权限或等效权限才能添加到或更改 **/etc/insights-client/tags.yaml** 文件。

5.5.1. 标签结构

标签使用 **namespace/key=value** 对结构。

- **命名空间。**namespace 是 ingestion point, *insights-client*,且不可更改。**tags.yaml** 文件从命名空间中提取，这在上传前由 Insights 客户端注入。
- **密钥。**密钥可以是用户选择的密钥，也可以是系统的预定义密钥。您可以使用大写、字母、数字、符号和空格混合。
- **value.**定义您自己的描述性字符串值。您可以使用大写、字母、数字、符号和空格混合。

注意

顾问服务包括红帽支持的预定义标签。

5.5.2. 创建 tags.yaml 文件并添加自定义组

使用 **insights-client --group=<name-you-choose>** 创建并为 **/etc/insights-client/tags.yaml** 添加标签，这会执行以下操作：

- 创建 **etc/insights-client/tags.yaml** 文件
- 将 **group=** key 和 &lt ;**name-you-choose&gt**; 值添加到 **tags.yaml**
- 将新存档从系统上传到 Insights for Red Hat Enterprise Linux 应用程序，以便新标签会立即看到

创建初始 组 标签后，通过编辑 **/etc/insights-client/tags.yaml** 文件根据需要添加额外的标签。

以下流程演示了如何创建 **/etc/insights-client/tags.yaml** 文件和初始组，然后验证 Insights for Red Hat Enterprise Linux 清单中存在该标签。

创建新组的步骤

1. 以 root 身份运行以下命令，在 **--group=** 之后添加您的自定义组名称：

```
[root@server ~]# insights-client --group=<name-you-choose>
```

tags.yaml 格式示例

以下 **tags.yaml** 文件示例显示了文件格式示例，并为新组添加其他标签：

```
# tags
---
group: eastern-sap
name: Jane Example
contact: jexample@corporate.com
Zone: eastern time zone
Location:
- gray_rack
- basement
Application: SAP
```

验证您的自定义组的步骤

1. 导航到 Red Hat Insights > RHEL > Inventory，并根据需要登录。
2. 点 **Filter results** 下拉菜单。
3. 滚动浏览列表，或使用搜索功能来定位标签。
4. 点标签来根据它过滤。
5. 验证您的系统是否在公告系统列表的结果中。

验证系统是否已标记的步骤

1. 导航到 Red Hat Insights > RHEL > Inventory，并根据需要登录。
2. 激活 **Name** 过滤器并开始输入系统名称，直到您看到系统，然后选择它。
3. 验证系统名称旁边，标签符号为 darkened，并显示代表应用正确标签数的数字。

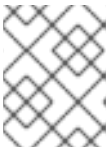
5.5.3. 编辑 tags.yaml 以添加或更改标签

创建组过滤器后，根据需要编辑 **/etc/insights-client/tags.yaml** 的内容来添加或修改标签。

流程

1. 使用命令行，打开标签配置文件进行编辑。
   [root@server ~]# vi /etc/insights-client/tags.yaml
2. 根据需要编辑内容或添加额外的值。以下示例演示了如何在向系统添加多个标签时组织 **tags.yaml**。

```
# tags
---
group: eastern-sap
location: Boston
description:
- RHEL8
- SAP
key 4: value
```



注意

根据需要添加任意数量的 key=value 对。使用大写字母、字母、数字、符号和空格的组合。

3. 保存更改并关闭编辑器。

4. 另外，还可为 Red Hat Enterprise Linux 生成 Insights 上传到 Insights。

```
# insights-client
```

5.5.4. 使用预定义的系统标签来获取更准确的 Red Hat Insights 顾问服务建议并增强安全性

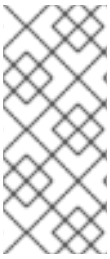
Red Hat Insights 顾问服务建议会平等地处理每个系统。但是，有些系统可能需要比其他系统更安全，或者需要不同的网络性能级别。除了添加自定义标签外，Red Hat Insights for Red Hat Enterprise Linux 还提供了预定义的标签，公告服务还可以为可能需要更多关注的系统创建目标建议。

要选择并获取预定义的标签提供的扩展安全强化和增强检测和修复功能，您需要配置标签。配置后，公告服务根据定制的严重性级别和适用于您的系统的首选网络性能提供建议。

要配置标签，请使用 **/etc/insights-client/tags.yaml** 文件，以类似方式标记具有预定义标签的系统，您可以将其用于标记清单服务中的系统。预定义的标签使用用于创建自定义标签的同一 **key=value** 结构进行配置。下表中提供了有关红帽预定义标签的详细信息。

表 5.1. 支持的预定义的标签列表

键	值	备注
安全	**normal** （默认）/ **strict**	使用 **normal** （默认）值，Invisor 服务会将系统的风险配置集与从 RHEL 最新版本的默认配置派生的基准进行比较，以及通常使用的用法模式。这会专注于数字、可操作和低的建议。有了 **严格的** 值，公告服务认为系统具有安全敏感性，从而导致特定建议使用更严格的基准，也可以在全新最新的 RHEL 安装中显示建议。
network_performance	**null** （默认）/ **延迟** / **吞吐量**	首选网络性能（根据您的业务要求，延迟或吞吐量）会影响到系统的顾问服务建议的严重性。



注意

预定义的标签键名称会被保留。如果您已使用密钥 **安全**，其值与其中一个预定义值不同，您将无法在建议中看到更改。只有在现有 **key=value** 与预定义键之一相同时，才会看到对建议的更改。例如，如果您有一个 **key=value** 为 **security: high**，则建议不会因为红帽预定义的标签而改变。如果您目前具有 **security: strict** 的 **key=value** 对，您将在您的系统建议中看到更改。

其他资源

- 使用系统标签启用扩展安全强化建议
- 利用标签使 Red Hat Insights Advisor 建议更好地了解您的环境
- 自定义系统标记

5.5.5. 配置预定义的标签

您可以使用 Red Hat Enterprise Linux advisor 服务的预定义标签来调整系统的建议行为，以扩展安全强化和增强检测和修复功能。您可以按照以下步骤配置预定义的标签。

先决条件

- 有对系统的根级别访问权限
- 已安装 Insights 客户端
- 您已在 Insights 客户端中注册了系统
- 您已创建了 **tags.yaml** 文件。请参阅 创建 tags.yaml 文件并添加自定义组

流程

1. 使用命令行和您首选的编辑器，打开 **/etc/insights-client/tags.yaml**。（以下示例使用 Vim。）

```
[root@server ~]# vi /etc/insights-client/tags.yaml
```

2. 编辑 **/etc/insights-client/tags.yaml** 文件，为标签添加预定义的 **key=value** 对。本例演示了如何添加 **security: strict** 和 **network_performance: latency** 标签。

```
# cat /etc/insights-client/tags.yaml
group: redhat
location: Brisbane/Australia
description:
- RHEL8
- SAP
security: strict
network_performance: latency
```

3. 保存您的更改。
4. 关闭编辑器。
5. **可选：** 运行 **insights-client** 命令，以生成上传到 Red Hat Enterprise Linux 的 Red Hat Insights，或等到下一个调度的 Red Hat Insights 上传。

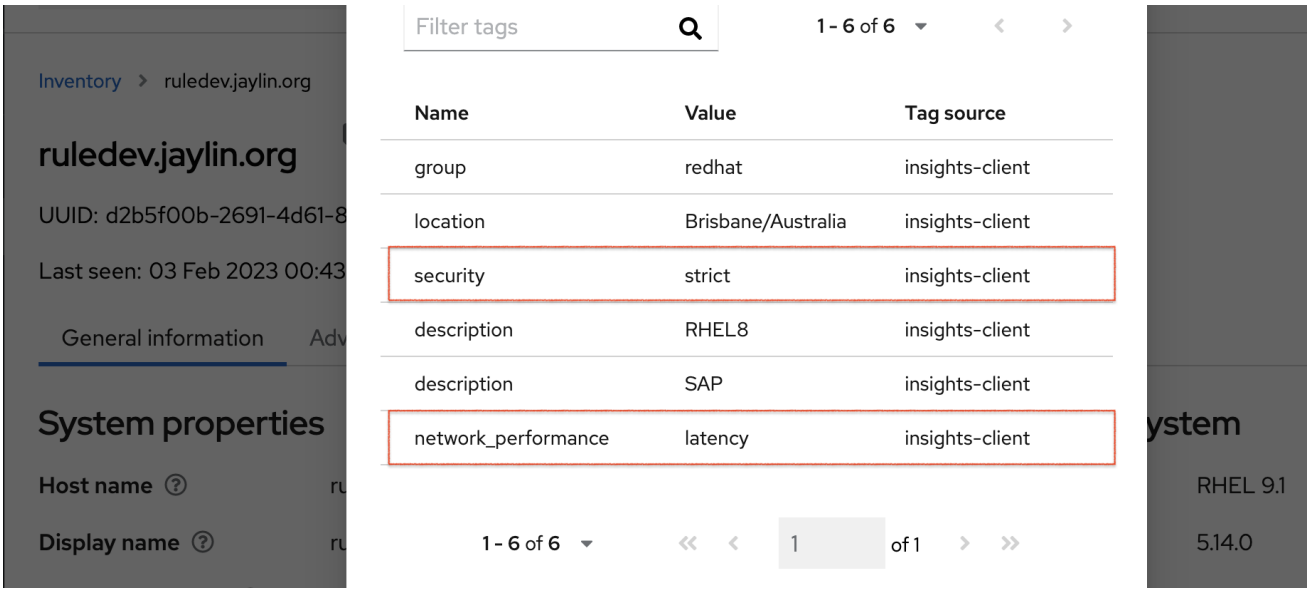
```
[root@server ~]# insights-client
```

确认预定义的标签位于您的生产区域中

在生成上传到 Red Hat Insights （或等待下一个调度的 Insights 上传）后，您可以通过访问 Red Hat Insights > RHEL > Inventory 来查找标签是否在生产环境中。查找您的系统并查找新创建的标签。您会看到显示以下内容的表：

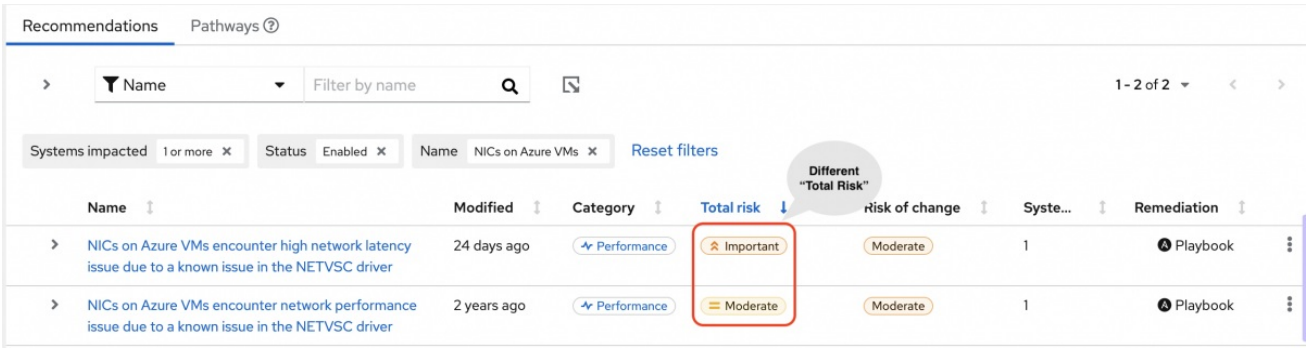
- Name
- 值
- 标签源（如 insights-client）。

下图显示了您在创建标签后清单中看到的示例。



应用预定义的标签后的建议示例

以下 advisor 服务镜像显示配置了 **network_performance: latency** 标签的系统。



系统显示较高的风险级别为 Important 的建议。没有 **network_performance: latency** 标签的系统的总风险为 Moderate （中度）。您可以决定系统优先级更高的总风险。

第 6 章 参考

请参阅以下参考资料以了解更多信息。

6.1. 参考资料

要了解更多有关漏洞服务的信息，请查看以下资源：

- *使用漏洞服务和 Ansible Playbook 修复安全风险*
- *生成安全漏洞服务报告*
- Red Hat Insights for Red Hat Enterprise Linux 文档
- Red Hat Insights for Red Hat Enterprise Linux 产品支持页

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。

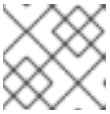
先决条件

- 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。