Red Hat Insights 1-latest

使用 FedRAMP 在 RHEL 系统上评估和监控安全漏洞

了解您的环境以Potential Security Threats

Last Updated: 2024-06-28

Red Hat Insights 1-latest 使用 FedRAMP 在 RHEL 系统上评估和监控安全漏洞

了解您的环境以Potential Security Threats

法律通告

摘要

将漏洞服务与 FedRAMP® 搭配使用，评估和监控 RHEL 系统上安全漏洞的状态，了解基础架构的风险，并规划一系列行动。 红帽承诺替换我们的代码、文档和网页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 INSIGHTS FOR RHEL 漏洞服务概述

漏洞服务可以快速评估和全面监控 RHEL 基础架构对常见漏洞和风险(CVE)的公开，以便您更好地了解您的最关键问题和系统，并有效地管理补救。

通过上传到漏洞服务的数据，您可以过滤和排序系统和 CVE 组，以优化和优化您的视图。当上下文给系统造成额外的风险时，您还可以向单个 CVE 添加上下文。了解风险风险后，将 CVE 的状态报告给适当的利益相关者，然后创建 Ansible Playbook 来修复问题，以保护您的组织的安全。

先决条件

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

- **每个系统都安装了 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 入门说明 来安装客户端并注册您的系统。
- **由 Red Hat Subscription Management (RHSM)和 Satellite 6 及之后的版本管理的 RHEL 系统完全支持这个漏洞服务。**使用任何其他方法获取软件包更新，除带有 RHSM 的 RHSM 或使用 subscription.redhat.com （客户门户网站）注册的 RHSM 之外，可能会导致误导结果。
- **漏洞服务补救并不被完全支持，且可能无法在 Satellite 5 和 Spacewalk 的 RHEL 系统中正常工作。**
- **有些功能需要您的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)，以及查看和修补 Red Hat Insights for Red Hat Enterprise Linux 补丁服务中的漏洞，需要通过用户访问授予权限。

其他资源

- *生成安全漏洞服务报告*

1.1. 漏洞服务如何工作

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，漏洞服务会根据 Red Hat CVE 数据库和安全通知评估数据，以确定是否存在任何有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，您可以查看和排序显示的结果，评估漏洞的风险和优先级，报告其状态，并创建并部署 Ansible Playbook 以修复它们。漏洞服务的目标是启用防止 RHEL 基础架构中安全弱点的可重复流程。

1.2. RED HAT HYBRID CLOUD 控制台中的用户访问设置

您的帐户中的所有用户都可以访问 Insights for Red Hat Enterprise Linux 中的大多数数据。

1.2.1. 预定义的用户访问组和角色

为了便于管理组和角色，红帽提供了两个预定义的组和一组预定义的角色。

1.2.1.1. 预定义的组

Default access 组包含 您机构中的所有用户。很多预定义角色被分配给此组。红帽会自动更新。

注意

如果机构管理员对 **Default access** 组进行了更改，则其名称会更改为 **Custom default access** 组，且不再由红帽更新。

Default admin access 组仅包含具有机构管理员权限的用户。这个组会自动维护，且无法更改此组中的用户和角色。

1.2.2. 漏洞服务用户的用户访问角色

以下角色启用了 Red Hat Enterprise Linux 中对 Insights 中漏洞服务功能的标准或增强的访问：

- **漏洞查看器.**阅读任何 vulnerability-service 资源。
- **漏洞管理员.**对任何 vulnerability-service 资源执行任何可用的操作。

第 2 章 常见的漏洞和风险(CVE)

常见的漏洞和暴露(CVE)是在公开发布的软件包中标识的安全漏洞。CVE 由国家 Cybersecurity FFRDC (NCF)标识和列出，其联邦资金研究和开发中心由 Mitre 公司（位于美国家庭安全部的国家 Cyber Security 部门）的资金提供资金。CVE 的完整列表请参考 https://cve.mitre.org。

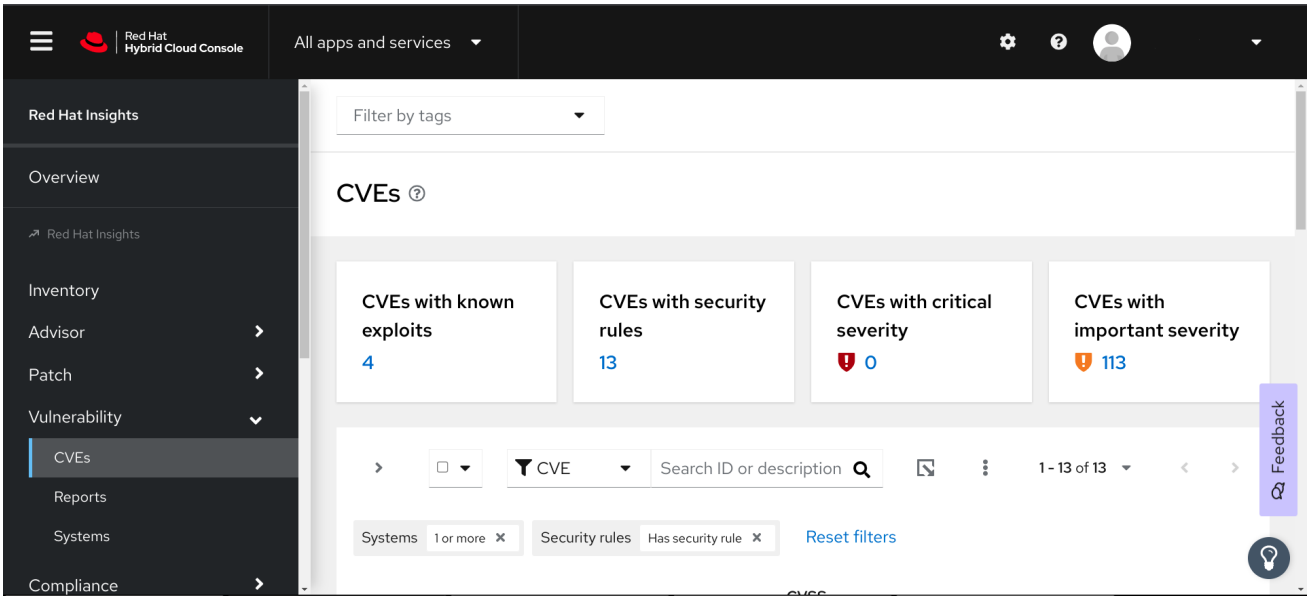
通过突出显示与 CVE 相关的公开已知漏洞和安全规则的 CVE，漏洞服务会增强威胁智能，以帮助确定哪些 CVE 对 RHEL 环境带来最大潜在风险，使用户能够有效地确定其最关键的问题，并首先解决其最重要的问题。

重要

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

漏洞服务识别了影响您的 RHEL 系统的 CVE，表示严重性并可让您有效地利用最关键的暴露。dashbar 将提醒您以下 CVE 类型：

- 已知的漏洞利用
- 安全规则
- 严重严重性
- 重要严重性

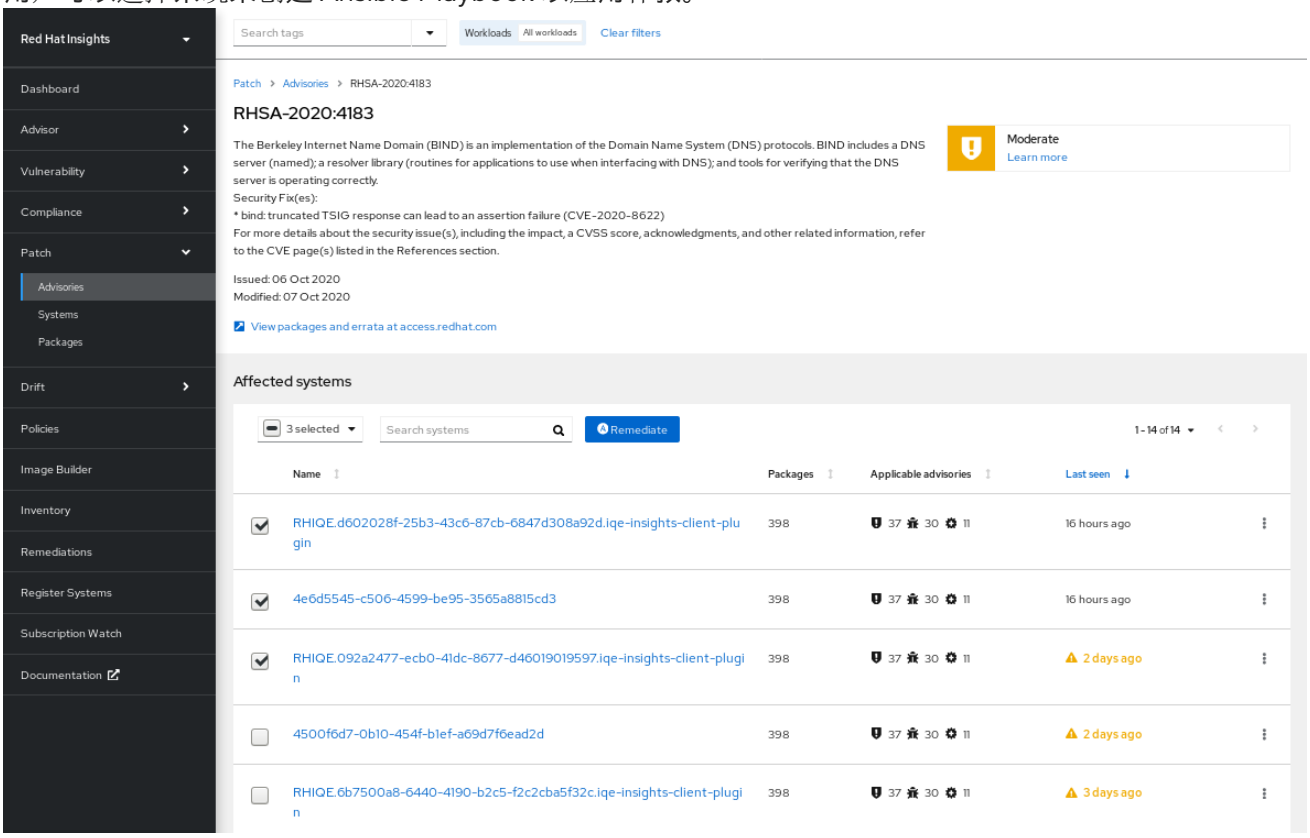


2.1. 红帽安全公告(RHSA)

红帽安全公告(RHSA)勘误记录了红帽产品中的安全漏洞，这些安全漏洞已提供补救或缓解措施。Red Hat Insights for Red Hat Enterprise Linux 漏洞服务显示与公开给一个 CVE 的每个系统关联的公告标识符。

选择 CVE 并选择 **Filter by affected systems** 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，公告列不可见，或者将显示"不可用"。

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。



2.2. 安全规则

安全规则的 CVE 带来了额外的可见性，因为风险提高并暴露与其相关联。这些是安全漏洞，可能会收到大量介质，并被红帽产品安全团队提供，使用产品安全 事件响应计划 工作流来帮助您确定您的 RHEL 环境风险。这些安全规则允许您采取适当的操作来保护您的机构。

安全规则在分析系统上运行的 RHEL 版本之外，提供深度威胁智能。手动策展安全规则，通过分析 Insights 客户端收集的系统元数据来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标识为向安全规则公开的系统，则可能会提高安全风险，问题应该与紧急情况解决。

重要

解决公开系统上的安全规则应该是您的最高优先级。

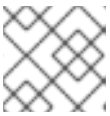
最后，并非所有公开给 CVE 的系统也公开给与该 CVE 相关的安全规则。虽然您可能正在运行存在安全漏洞的软件版本，但其他环境条件可能会降低威胁；例如，特定端口已关闭，或者您正在运行 SELinux。

2.2.1. 在 Insights for RHEL 仪表板中识别安全规则

使用以下步骤查看您的基础架构暴露的安全规则。

流程

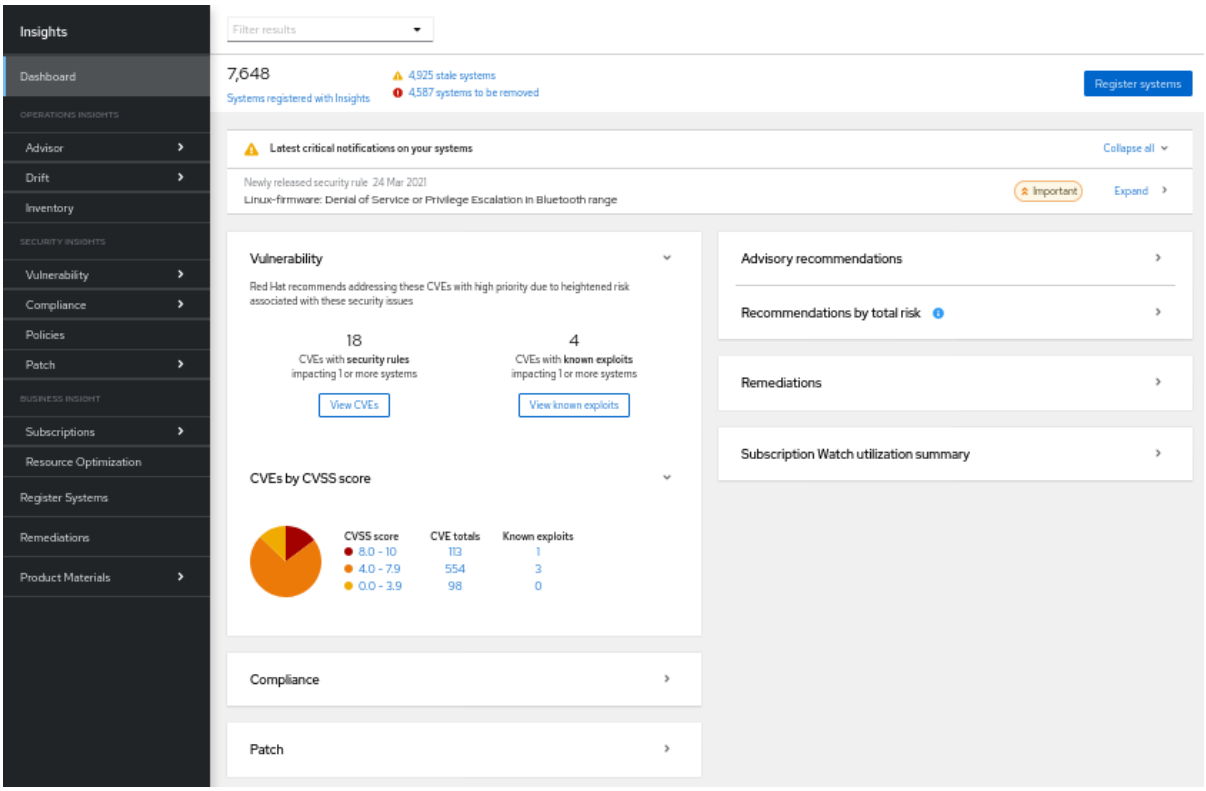
1. 导航到 Red Hat Insights for Red Hat Enterprise Linux 仪表板 。



注意

为了简单起见，以下屏幕截图中最小化与安全漏洞评估相关的服务面板。

:



2. 查看您的系统面板中的**最新的关键通知**。这些是安全性规则，其严重性评级为 "Important" 或 "Critical"。这些可能是您最关键的问题，应该优先考虑进行补救。

   a. 在每个通知的右侧，点 **Expand** 按钮查看相关的 CVE 以及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，即使您的基础架构中存在 CVE，但安全规则条件可能不存在。

   b. 在安全规则的名称下，在相关的 CVE 下点 CVE ID 链接。

   c. 查看您的系统哪些受安全规则 CVE 的影响，并选择性地选择公开的系统来创建 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。这个数字包括影响至少一个系统的严重性的安全规则。

      i. 点 **View CVEs**。按照高严重性安全规则，考虑更小的安全规则，您的第二个最高优先级进行补救。

2.3. 已知的漏洞利用

红帽分析了 Metasploit 数据，以确定代码是否公开利用 CVE，或一个 CVE 已经被公开利用。漏洞服务将"已知漏洞"标签应用到符合该条件的 CVE。

这种增强的威胁评估可帮助用户识别并解决首先存在关键风险的 CVE。红帽建议用户使用具有高优先级的"已知漏洞"标签来查看任何 CVE，并修复这些问题。

重要

通过这个漏洞服务，您的基础架构中的系统中存在已知的浏览 CVE。"已知漏洞"标签并不表示这个漏洞已在您的 RHEL 系统中被利用；漏洞服务不会做出该决定。

2.4. 常见的漏洞和风险通过分类功能提供深入威胁智能

漏洞服务为您提供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，但不受到安全漏洞的影响。**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。

这增加了威胁智能功能，使您能够首先分解问题并解决最紧急的问题。在管理大量服务器时，这会转化为加快的保护和显著的效率。

受影响但不易受攻击的 CVE 状态表示您正在运行软件，但目前还没有被利用的漏洞。这个系统需要补救，但不需要立即关注。

一个 **存在安全漏洞的** CVE 状态表示有漏洞的代码，它带有一个开放的路径才可以被利用。开放路径可以是允许以下之一的端口或操作系统版本：可能会泄漏机密信息，系统的完整性会被破坏或系统可用性被妨碍。

让我们来看一个 **存在安全漏洞的** 服务器示例，而不是 **受影响的服务器，但没有易受攻击的** 服务器：

假设 **服务器 A** 正在运行易受攻击的软件，允许对系统的 root 访问。 **服务器 A** 被视为存在安全漏洞，需要立即修复。

相反，假设 **Server B** 的当前配置会阻止漏洞清单，即使受影响的代码中存在也是如此。**服务器 B** 将被视为 **受影响，但不受到这个安全漏洞的影响**。这意味着，**Server B** 可以重新委派到待办列表，以便可以修复更即时的威胁，因此 **服务器 A** 可以修复。

重要

您应该会在 **Server A** 被解决后对 **Server B** 进行补丁，因为它正在运行潜在的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。

2.4.1. 在 Red Hat Insights for RHEL 仪表板中识别已知相关的 CVE

使用以下步骤为 Red Hat Enterprise Linux 仪表板漏洞卡识别 Insights 中的已知浏览 CVE。

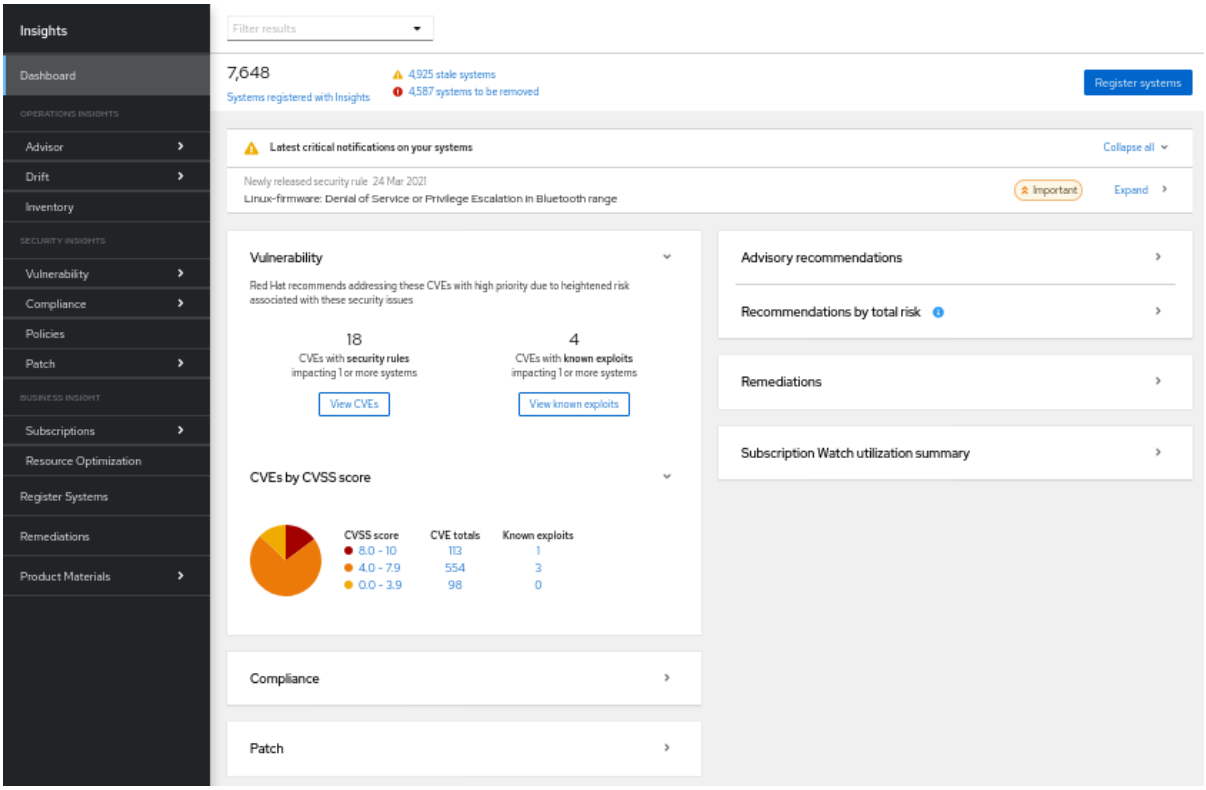
流程

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

注意

为了简单起见，以下屏幕截图中最小化与安全漏洞评估相关的服务面板。

:



2. 在 **漏洞** 卡中，请注意 **带有已知漏洞的 CVE 会影响 1 个或更多个系统，以及显示的数量。**
3. 点 **View Known exploits。**
4. 查看 CVE 中已过滤的 Known-exploit CVE 列表。

第 3 章 拒绝漏洞服务结果

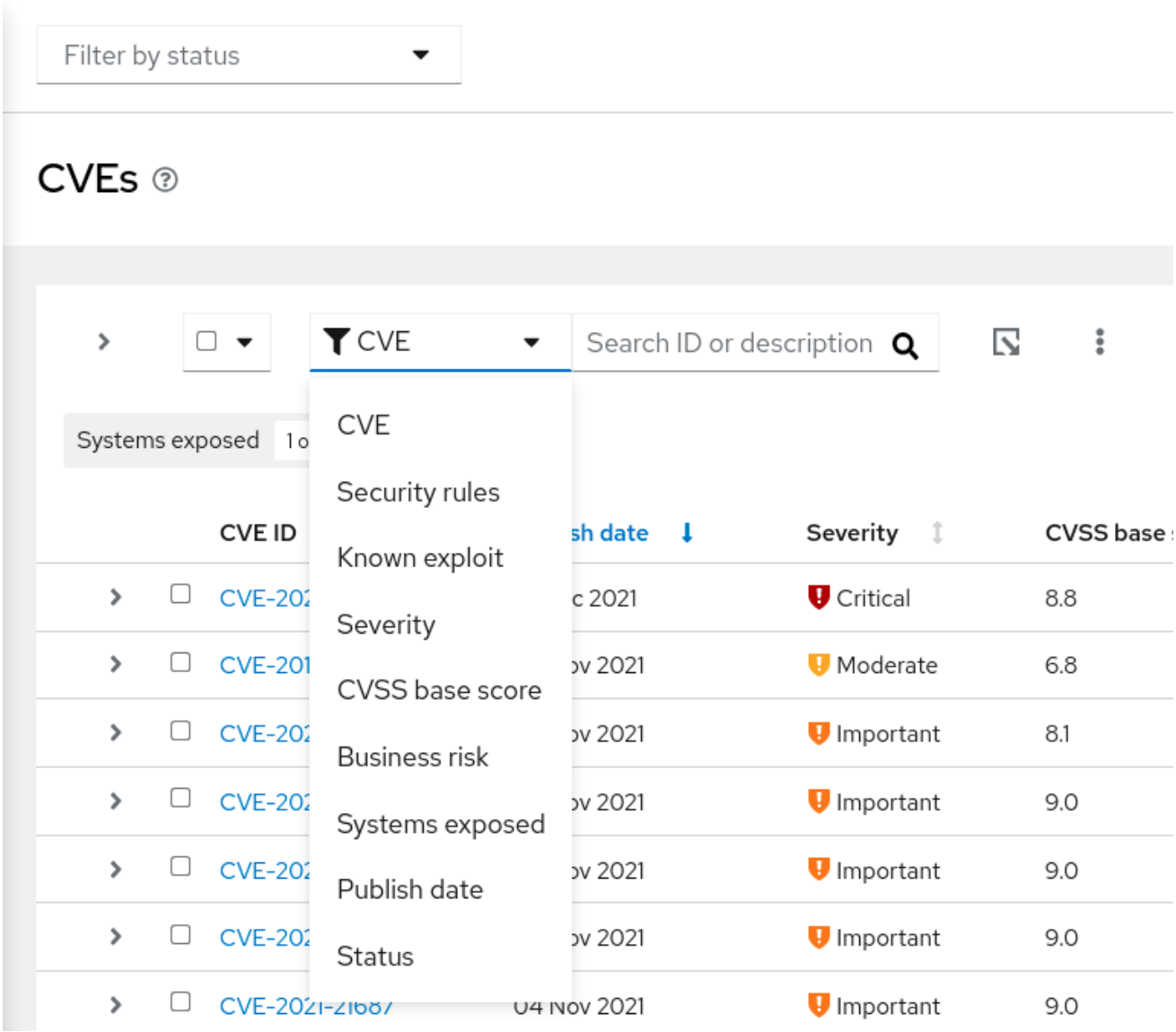
无论是向利益相关者或系统优先级进行补救报告结果，漏洞服务都允许许多方法来优化数据的视图，帮助您和其他注重关键系统、工作负载或问题。以下小节描述了您的数据组织以及可用于优化和增强结果的排序、过滤和上下文功能。

3.1. CVE-LIST 和 SYSTEM-LIST 过滤器

过滤会缩小 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 CVE 列表，以根据严重程度或商业风险专注于 CVE，例如：选择单个 CVE 后，将过滤器应用到生成的受影响的系统列表，以便专注于特定 RHEL 主版本或次版本。

通过从左侧的过滤器下拉列表中选择一个主过滤器来激活过滤器，然后从右侧的过滤器选项下拉列表中选择二级子过滤器。所选过滤器在 Filters 菜单下显示，可通过单击每个过滤器旁边的 X 来停用。

CVEs 列表过滤器

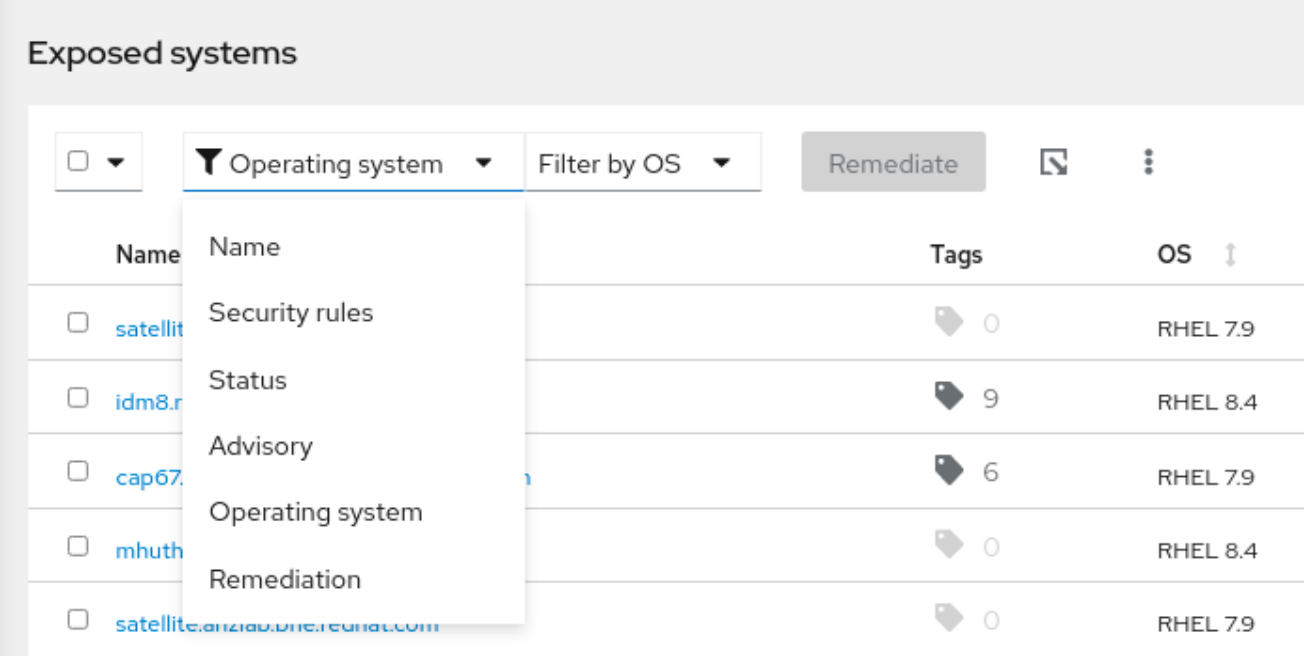


以下主要过滤器可从 CVEs 页面访问。选择主过滤器，然后在 subfilter 中定义参数：

- **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）
- **商业风险.**选择一个或多个值： High, Medium, Low, Not defined。
- **Systems exposed .**选择只显示带有当前受影响系统的 CVE，或者没有影响系统的系统。
- **发布日期.**从 All, Last 7 days, Last 30 天, Last 90 days, Last 90 days, Last year, 或 1 年以前选择。
- **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 via mitigation.

系统列表过滤器



以下主要过滤器可从 CVE 详情页面中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 有一个与它关联的安全规则，则根据其他系统过滤易受同一安全规则的影响，或者显示不受安全规则影响的系统。
- **状态。**显示特定状态或工作流类别中的系统。
- **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 中包含的系统、手动修复或未包含在当前补救计划中的系统。

3.1.1. 过滤 security-rule CVE

安全规则，特别是高严重性安全规则，为您的基础架构带来最大潜在威胁，并应考虑最高优先级进行识别和补救。使用以下步骤只查看 CVE 列表中的高严重性安全规则 CVE 并确定受影响的系统。

注意

并非所有公开给 CVE 的系统也公开给与该 CVE 相关的安全规则。虽然您可能正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，特定端口已关闭或者启用了 SELinux。

流程

1. 进入 Red Hat Insights for Red Hat Enterprise Linux 中的 Security > Vulnerability > CVEs。
2. 单击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。

3.1.2. 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*。

3.1.3. 过滤已知发现的 CVE

带有 "Known exploit" 标签的 CVE 由红帽决定漏洞利用这个漏洞，利用这个漏洞，代码可以被公开利用 CVE，或者已知可被公开利用 CVE。因此，应该优先考虑已知相关 CVE 进行识别和补救。

重要

红帽不决定您的注册的系统是否已被利用。我们只是识别可能构成额外风险的 CVE。

使用以下步骤过滤 CVE 列表中的已知扩展 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。

3.1.4. 过滤没有相关公告的 CVE

有些 CVE 没有相关的公告，也称为 *勘误*。这可能是因为以下任何原因发生：

- CVE 没有可用的修复
- 产品安全分析决定 CVE 影响您的环境，但没有可用于您的环境的勘误（虽然其他环境中相同的 CVE 可以在其他环境中有勘误）
- 您的系统不再处于支持状态

重要

CVE 信息目前可用于 RHEL 6、7、8 和 9。RHEL 5 系统不提供任何信息。

在没有公告的情况下可以识别 CVE 可让您采取措施来保护您的机构暴露这些漏洞，以便您可以执行必要的步骤来解决这个问题。

如果您的 RHEL 版本没有可用的修复，并被列为" will not fix"，请考虑以下条件：

- 漏洞的影响（严重性）
- RHEL 版本的生命周期阶段

如果您决定在没有相关公告的情况下对 CVE 需要修复，可以使用以下选项：

- 接受风险
- 升级至包括此漏洞的修复（如果可用）的受支持产品版本（推荐）
- 应用一个缓解方案（如果存在）

其他资源

有关 CVE 的更多信息，请参阅 常见漏洞和风险

有关漏洞的严重性评级的更多信息，请参阅了解严重性评级。

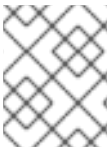
有关产品生命周期的更多信息，请参阅 生命周期和更新策略。

要在客户门户网站中创建一个支持问题单，请参阅 客户支持。

3.1.4.1. 启用没有公告的 CVE

启用没有公告的 CVE 可让您访问受 CVE 影响的系统，而无需在 Insights 中公告。

这个功能会被默认启用，但没有公告的 CVE 在主视图中会被默认隐藏。这意味着，您必须使用过滤器来显示并查看没有公告的 CVE。



注意

红帽的策略要求 Insights for Red Hat Enterprise Linux 显示所有高优先级、关键和重要的 CVE，无论这些 CVE 是否有相关的公告。

先决条件

- 在 Red Hat Insights 中对您的环境进行漏洞管理员访问

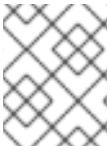
流程

1. 在 Red Hat Insights for RHEL 仪表板中，进入到 **Security > Vulnerability > CVEs**。
2. 点击 **More options** 图标（需要），然后选择 **Show CVEs without Advisories**。公告列表包括没有公告的 CVE。

3.1.4.2. 禁用没有公告的 CVE

要禁用没有公告功能的 CVE，取消选择 **Show CVEs without Advisories** 选项。

默认启用了没有公告选项的 CVE，但默认视图会隐藏 CVEs 没有公告。



注意

红帽的策略要求 Insights for Red Hat Enterprise Linux 显示所有高优先级、关键和重要的 CVE，无论这些 CVE 是否有相关的公告。

先决条件

- 在 Red Hat Insights 中对您的环境进行漏洞管理员访问
- 公告列表包括没有公告的 CVE

流程

1. 在 Red Hat Insights for RHEL 仪表板中，进入到 **Security > Vulnerability > CVEs**。
2. 点击 **More options** 图标（需要），然后选择 **Hide CVEs without Advisories**。

3.1.4.3. 查看没有公告的 CVE

在没有 Advisories 选项的情况下显示 CVE 可启用或禁用 CVE 没有公告。要查看没有公告的 CVE，必须启用 Show CVEs without Advisories 选项。

先决条件

- 机构管理员在没有公告选项的情况下启用了 CVE。

流程

1. 在 Red Hat Insights for RHEL 仪表板中，进入到 **Security > Vulnerability > CVEs**。
2. 从过滤器下拉菜单中，选择 **Advisory**。
3. 在 **Filter by Advisory** 下拉菜单中选择 **Not Available**。公告列表显示所有没有公告的 CVE。

3.1.4.4. 识别受 CVE 影响的系统没有公告

CVE 详情页面会显示受所选 CVE 影响的所有系统的列表。您可以过滤系统列表，以显示受 CVE 影响的系统（其中没有公告）。

先决条件

- 机构管理员在没有公告选项的情况下启用了 CVE。

流程

1. 找到没有公告的 CVE，您可以看到它会影响的系统。有关在没有公告的情况下识别 CVE 的更多信息，请参阅在没有公告的情况下识别带有 CVE 的系统。
2. 选择要导航到 CVE 详情页面的 CVE。显示 CVE 的 CVE 详情页面。该页列出了受该 CVE 影响的所有系统。
   a. 如果您在选择 CVE 时应用 **Filter by Advisory** filter and **Not Available** 选项，则这些过滤器会保留到 CVE 详情页面。
   b. 否则，当您导航到 CVE 详情页面时，从页面顶部的过滤器中选择 **Advisory**，然后选择 Select **Filter by Advisory**，然后单击 **Not Available** 复选框。系统更新列表，仅显示受该 CVE 影响的系统，而无需公告。**Advisory 列显示列表中的每个** 系统都不可用。
3. **可选：** 要查看系统的详情，请选择您要查看的系统名称。系统详情页面会显示。

3.1.4.5. 查看系统详情中没有公告的 CVE

系统详情页面会显示影响所选系统的所有 CVE 列表。您可以过滤 CVE 列表来显示没有公告的 CVE。

先决条件

- 机构管理员在没有公告选项的情况下启用了 CVE。

流程

1. 在 Red Hat Insights for RHEL 仪表板中进入 **Security > Vulnerability > Systems**。此时将显示 Vulnerability systems 页面。
2. 从列表中选择系统 ID。显示该系统的系统详情页面。该页列出了影响所选系统的所有 CVE。
3. 从页面顶部的过滤器中选择 **Advisory**。
4. 选中 **Filter by Advisory**，然后选择 **Not Available** 复选框。CVE 更新列表，仅显示没有公告的 CVE。Advisory 列显示列表中每个 CVE 的 **Not Available**。
5. **可选：** 要查看 CVE 的详情，请为您要查看的 CVE 选择 CVE ID。显示 CVE 的详细信息页面。

3.2. 过滤公开给安全规则的系统列表

过滤 CVE 列表以只查看您最关键的潜在威胁后，选择单个 CVE 来查看公开系统列表并将过滤器应用到列表。

流程

1. 选择安全规则 CVE 后，向下滚动到 **公开的系统列表**。并不是列表中的每个系统都有存在 CVE 的安全规则条件。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. 在二级子过滤器下拉列表中，选中 **Has security rule** 框。

4. 查看暴露于 CVE 的系统，这些 CVE 也存在安全规则的条件。

3.3. INSIGHTS FOR RHEL 组过滤器

通过按一组系统或工作负载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那些系统。它们可以是运行 SAP 工作负载（或通过 SAP ID）、Satellite 主机组或添加到 Insights 客户端配置文件中的自定义标签的系统。

可以使用位于 Insights for Red Hat Enterprise Linux 的 Insights 应用程序顶部的 **Filter 结果** 框在 Insights for Red Hat Enterprise Linux 中全局设置组过滤。从服务更改为 service 时，组选择会保留，页面到页面。但是，该功能因 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。

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

3.3.1. 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 Insights for Red Hat Enterprise Linux 应用程序。
3. 点位于 Insights 应用程序的任何页面顶部的 **Filter 结果** 框中的下箭头。
4. 选择要过滤您的系统的组。
   搜索或滚动以查看可用标签。要浏览可用标签的完整列表，滚动到列表的底部，再单击 **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 主机集合。

   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，并只查看属于您选择的组或组群的系统或 CVE。

3.4. 为 CVE 定义业务风险

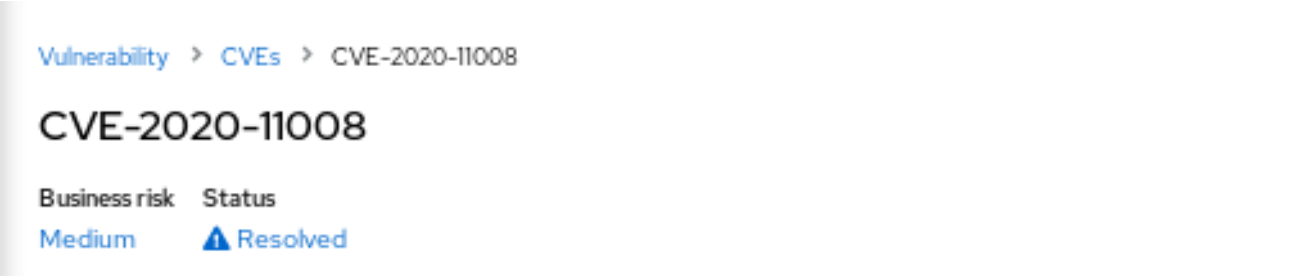
通过这个漏洞服务，您可以使用以下选项定义 CVE 的商业风险： High, Medium, Low, 或 Not Defined (default)。

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他们对您的机构的影响对 CVE 进行评级。这样，您可以在大型环境中高效管理风险，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。

CVE ID	Publish date	Severity	CVSS base score	Systems exposed	Business risk	Status
CVE-2020-11008	20 Apr 2020	Important	7.5	260	Medium	Resolved

每个 CVE 的详情卡中也会看到业务风险，其中显示了更多信息并列出受影响的系统。



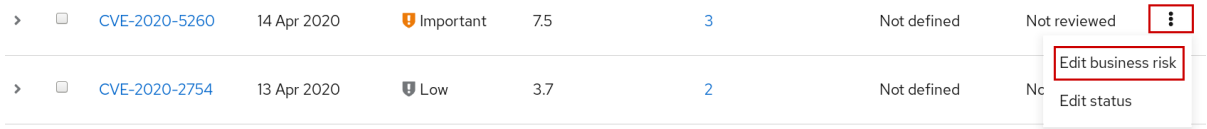
3.4.1. 为单个 CVE 设置业务风险

完成以下步骤，为单个 CVE 设置业务风险：

注意

该 CVE 的业务风险在受到影响 *的所有* 系统上都是一样的。

1. 进入 Security > Vulnerability > CVEs 页面，并在需要时登录。
2. 确定设定业务风险的 CVE。
3. 点 CVE 行右侧的 **more-actions** 图标（三个垂直点），然后点 **Edit business risk**。



4. 为适当的级别设定业务风险值，并选择性地为您的风险评估添加合理性。
5. 点击 **Save**。

3.4.2. 为多个 CVE 设置业务风险

完成以下步骤，在您选择的多个 CVE 中设置相同的商业风险：

1. 进入 Security > Vulnerability > CVEs 并在需要时登录。
2. 选中您要为其设置商业风险的 CVE 的框。
3. 执行以下步骤设定业务风险：
   a. 单击工具栏中过滤器下拉菜单右侧的 **更多操作** 图标（三个垂直排列点），然后单击 **Edit Business risk**。
   b. 设置适当的商业风险值，并选择性地为您的风险评估添加合理性。
   c. 点击 **Save**。

3.5. 从漏洞服务分析中排除系统

漏洞服务允许您从漏洞分析中排除特定的系统。这可节省时间，并注意与您的组织目标无关的系统上审核和重新检查问题。

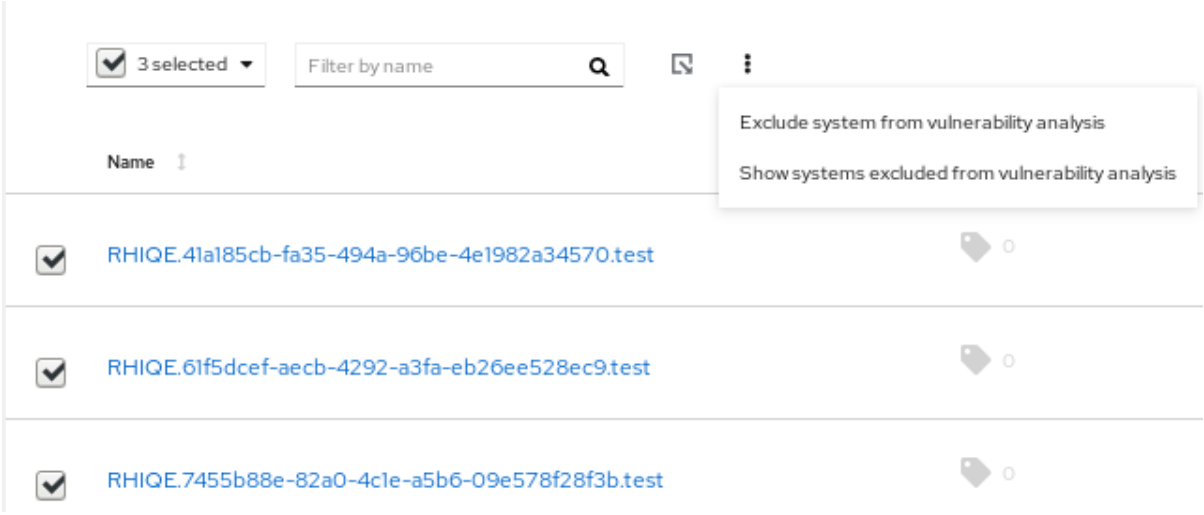
例如，如果您有以下服务器类别：QA、Dev Dev 和 Production，您可能不关心检查 QA 服务器的漏洞，因此想将这些系统排除在漏洞服务执行的分析中。

当您排除系统漏洞分析时，Insights 客户端仍然会在系统上按调度运行，但系统的结果在漏洞服务中不可见。客户端的持续操作可确保其他 Red Hat Insights for Red Hat Enterprise Linux 服务仍然可以上传它们所需的数据。它还意味着您仍然可以使用过滤来查看这些系统的结果。

完成以下步骤，将所选的 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. 在系统列表的顶部点工具栏中的 **more-actions** 图标，**然后从漏洞分析中选择 Exclude systems**。



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。

3.6. 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. 在系统列表的顶部，单击工具栏中的 **more-actions** 图标，然后选择 **Show systems excluded from analysis**。
3. 请参阅漏洞分析中排除的系统。这可以通过 **Applicable CVEs** 列中 **Excluded** 的值进行验证。

3.7. 为系统恢复漏洞分析

完成以下步骤以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. 在系统列表的顶部，单击工具栏中的 **more-actions** 图标，然后选择 **Show systems excluded from analysis**。
3. 在结果列表中，选中您要恢复漏洞分析的每个系统的复选框。
4. 再次点 **more-actions** 图标，选择 **Resume analysis for system**。

3.8. CVE 状态

管理影响您系统的 CVE 的另一种方法是通过设置 CVE 的状态。漏洞服务启用以下为 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。

状态值是 preset，并包括以下选项：

- 未检查（默认）
- in-review
- on-hold
- 为补丁调度
- 已解决
- 无操作 - 风险接受
- 通过缓解方案解决

为 CVE 设置状态有助于通过其生命周期更好地检索到它，以便修复它。通过定义状态，您的组织可以保持更好的标签页，其中最关键的 CVE 在其生命周期中，您应该专注于努力解决每个业务需求的最关键问题。CVE 的状态可在漏洞服务和单个 CVE 视图中的所有 CVE 表中可见。

3.8.1. 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，并将该状态应用到其影响的所有系统上的 CVE：

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，然后选择 **Edit status**。
3. 选择适当的状态，并选择性地在 **Justification** 文本框中为您的决策输入一个比例。

4. 如果在单个系统中为这个 CVE 设定了状态且您要保留，则检查 **Do not overwrite individual system status**。否则，保留未选中框，以将此状态应用到它影响的所有系统。

5. 点击 **Save**。

3.8.2. 为 CVE 和系统对设置状态

完成以下步骤，在 CVE 和系统对中设置状态：

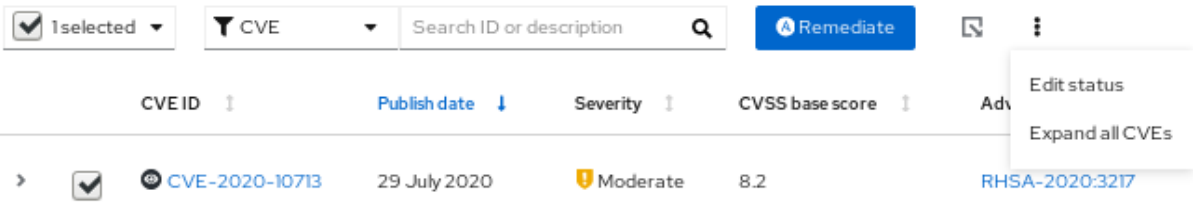
流程

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

   如果选中了 **使用整个 CVE 状态** 的框，则无法为对设置状态。

   b. （可选）为您的状态确定输入一个合理信息。

   c. 点击 **Save**。

6. 在列表中找到 CVE，并验证是否设置了状态。

3.9. 使用搜索框

漏洞服务的搜索功能适用于您要查看的页面的上下文。

- **CVEs 页面.**搜索框位于 CVEs 列表顶部的工具栏中。在设置了 CVE 过滤器时，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。

3.10. 排序 CVE 列表数据

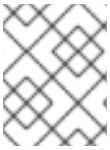
漏洞服务的排序功能因您正在查看的页面上下文而异。

流程

1. 在 **CVEs** 选项卡中，您可以将排序应用到以下列：
   - CVE ID
   - 发布日期
   - 重要性
   - CVSS 基本分数
   - 公开的系统
   - 商业风险
   - 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
   - 商业风险
   - 状态

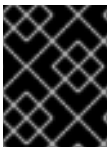
第 4 章 系统标签和组

Red Hat Insights for Red Hat Enterprise Linux 使管理员能够使用组标签过滤清单中的系统组以及单个服务中的系统组。组通过到 Insights for Red Hat Enterprise Linux 的系统数据识别的方法。Insights for Red Hat Enterprise Linux 支持根据运行 SAP 工作负载、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来过滤系统组。



注意

从 Spring 2022 开始，清单、公告、合规性、漏洞、补丁、偏移和策略根据组和标签进行过滤。其他服务将遵循。



重要

与启用标记的其他服务不同，合规性服务在合规服务 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 中的以下部分组和* 标签过滤器。

使用 global, **Filter 结果** 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过滤。

先决条件

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

- 每个系统中已安装并注册了 Red Hat Insights 客户端。
- 您必须具有 root 权限或对应的权限，才能创建自定义标签或更改 **/etc/insights-client/tags.yaml** 文件。

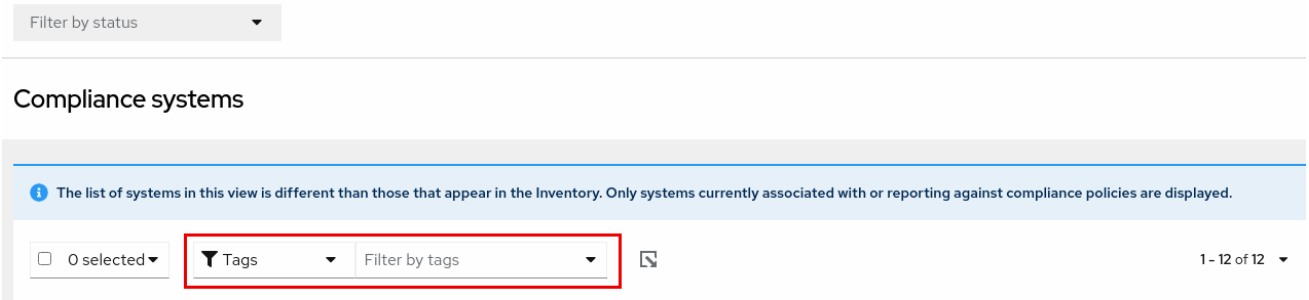
4.1. 合规服务中的组和标签过滤器

合规服务允许用户将标签和组过滤器应用到系统报告合规性数据，但它们没有使用 **Filter by status** 下拉菜单设置。与 Insights for Red Hat Enterprise Linux 应用程序中的大多数其他服务不同，合规服务只在以下情况下显示系统的数据：

- 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。

由于这些条件，compliance-service 用户必须使用位于合规性服务 UI 中的系统列表的主和次要过滤器来设置标签和组过滤器。

在合规服务中标记和组过滤以上系统列表



4.2. SAP 工作负载

由于 Linux 在 2025 年成为 SAP deployments 工作负载的强制操作系统，Red Hat Enterprise Linux 和 Red Hat Insights for Red Hat Enterprise Linux 致力于使 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 工作负载和 SAP ID (SID)的系统，而无需管理员进行任何自定义。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。

4.3. 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。

4.4. 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。这些规则向管理员发出没有遵守 Microsoft 和 Red Hat 记录的建议的操作系统级别配置。

这些规则的一个限制是，它们主要分析操作系统，而不是数据库本身。最新版本的 Insights for Red Hat Enterprise Linux 和 RHEL 8.5 引入了 Microsoft SQL assessment API。SQL 评估 API 提供了一种机制来评估 MS SQL Server 的数据库配置以了解最佳实践。API 提供了一个规则集，其中包含 Microsoft SQL Server 团队推荐的最佳实践规则。虽然此规则集通过新版本改进，但 API 构建旨在提供高度可自定义的可扩展解决方案，让用户能够自行调优默认规则并自行创建。

SQL 评估 API 由 Linux 的 PowerShell 支持（可从 Microsoft 使用），Microsoft 开发了可用于调用 API 的 PowerShell 脚本，并将其结果存储为 JSON 格式的文件。在 RHEL 8.5 中，Insights 客户端现在上传此 JSON 文件，并在 Insights for Red Hat Enterprise Linux UI 中以易于理解的格式显示结果。

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

4.4.1. 设置 SQL Server 评估

要将 Microsoft SQL 评估 API 配置为向 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 Authentication 为 SQL Server 创建登录评估。以下 Transact-SQL 创建一个登录。将 **<*PASSWORD*&** gt; 替换为强密码：

```
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 <*PASSWORD*> 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。这与您在安装 **mssql-tools** 和 **mssqlodbc17** 软件包作为 SQL Server 安装的一部分时配置的存储库相同。

```
# 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 runassessment 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，但请务必以 mssql 用户身份这样做，以便后续评估可以作为 mssql 用户更加安全地通过 cron 或 systemd 自动运行。

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

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

```
# insights-client
```

4.4.1.1. 在计时器上设置 SQL 评估

由于 SQL Server 评估可能需要 10 分钟或更长时间来完成，所以您可以每天自动运行评估过程，也可能不意义。如果要自动运行它们，Red Hat SQL Server 社区已创建了 systemd 服务和计时器文件，以用于评估工具。

流程

1. 从红帽公共 SQL Server 社区下载以下文件，以实践 GitHub 站点。
   - **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/
```

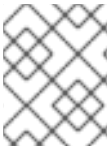
3. 启用计时器：

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

4.5. 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，您可以将上下文标记添加到各个系统，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。在大规模部署 Insights for Red Hat Enterprise Linux 时，此功能特别有价值，管理有大量数百个或数千个系统。

除了将自定义标签添加到多个 Insights for Red Hat Enterprise Linux 服务外，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，这些系统可能需要更多关注，比如那些需要较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 权限或等效的权限，才能添加到或更改 **/etc/insights-client/tags.yaml** 文件。

4.5.1. 标签结构

标签使用 **namespace/key=value** 对的结构。

- **namespace。**命名空间是 ingestion 点(*insights-client*)的名称，且无法更改。**tags.yaml** 文件从命名空间中提取，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，也可以是系统中的预定义密钥。您可以使用大写、字母、数字、符号和空格的组合。
- **值。**定义您自己的描述性字符串值。您可以使用大写、字母、数字、符号和空格的组合。

注意

顾问服务包括红帽支持的预定义标签。

4.5.2. 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=** 键和 &lt **;name-you-choose&gt**; 值添加到 **tags.yaml**
- 将系统的新存档上传到 Insights for Red Hat Enterprise Linux 应用程序，以便立即看到新标签以及最新的结果

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 清单中是否存在该标签。

创建新组的步骤

1. 以 root 用户身份运行以下命令，在 **--group=** 后添加自定义组名称：

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

tags.yaml 格式示例

以下 **tags.yaml** 文件示例显示了一个文件格式示例，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
```

验证是否已创建自定义组的步骤

1. 导航到 Red Hat Insights > RHEL > Inventory，并根据需要登录。
2. 单击 **Filter 结果** 下拉菜单。
3. 滚动浏览列表或使用搜索功能来定位标签。
4. 单击标签以对其进行过滤。
5. 验证您的系统是否在公告系统列表中的结果。

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，直到您看到您的系统，然后选择它。
3. 验证系统名称旁边，标签符号为 darkened，并显示代表所应用正确标签数的数字。

4.5.3. 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，以添加或修改标签。

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、数字、符号和空格的组合。

3. 保存更改并关闭编辑器。

4. （可选）为 Red Hat Enterprise Linux 生成到 Insights 的上传。

```
# insights-client
```

4.5.4. 使用预定义的系统标签获得更准确的 Red Hat Insights 顾问服务建议并提高安全性

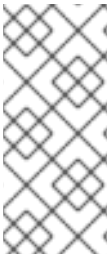
Red Hat Insights 顾问服务建议同样地处理每个系统。但是，有些系统可能需要比其他系统更安全，或者需要不同的网络性能级别。除了添加自定义标签的功能外，Red Hat Insights for Red Hat Enterprise Linux 提供了预定义的标签，公告服务还可用来为可能需要更多关注的系统创建目标建议。

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，公告服务会根据适用于您的系统的定制严重性级别和首选网络性能提供建议。

要配置标签，请使用 **/etc/insights-client/tags.yaml** 文件以类似的方式标记带有预定义标签的系统，您可能使用它来标记 inventory 服务中的系统。预定义的标签是使用用于创建自定义标签的相同 **key=value** 结构配置的。下表包括了 Red Hat-predefined tags 的详细信息。

表 4.1. 支持的预定义标签列表

键	值	备注
安全	**normal** （默认）/ **strict**	使用 **normal** （默认） 值，公告服务会将系统的风险配置集与从 RHEL 最新版本的默认配置以及经常使用的模式的默认配置进行比较。这会以数字为重点、可操作和低的建议。使用 **严格** 值时，公告服务将系统视为安全敏感，从而导致特定建议使用更严格的基线，甚至可能会在最新的 RHEL 安装中显示建议。
network_performance	**null** （默认）/ **延迟** / **吞吐量**	首选网络性能（根据您的业务要求的延迟或吞吐量）会影响到系统的公告服务推荐的严重性。



注意

预定义的标签键名称被保留。如果您已使用关键 **安全性**，且值与其中一个预定义值不同，您不会在您的建议中看到更改。如果您的现有 **key=value** 与其中一个预定义键相同，才会看到建议更改。例如，如果您有一个 **key=value** of **security: high**，您的建议不会因为红帽定义的标签而改变。如果您目前有一个 **key=value** 对 **security: strict**，则会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 建议更好地理解您的环境
- 自定义系统标记

4.5.5. 配置预定义的标签

您可以使用 Red Hat Insights for Red Hat Enterprise Linux 顾问服务的预定义标签来调整系统的建议行为，以便扩展安全强化和增强检测和修复功能。您可以按照这个流程配置预定义的标签。

先决条件

- 有对系统的 root 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** 命令生成到 Red Hat Insights for Red Hat Enterprise Linux 的上传，或等待下一个调度的 Red Hat Insights 上传。

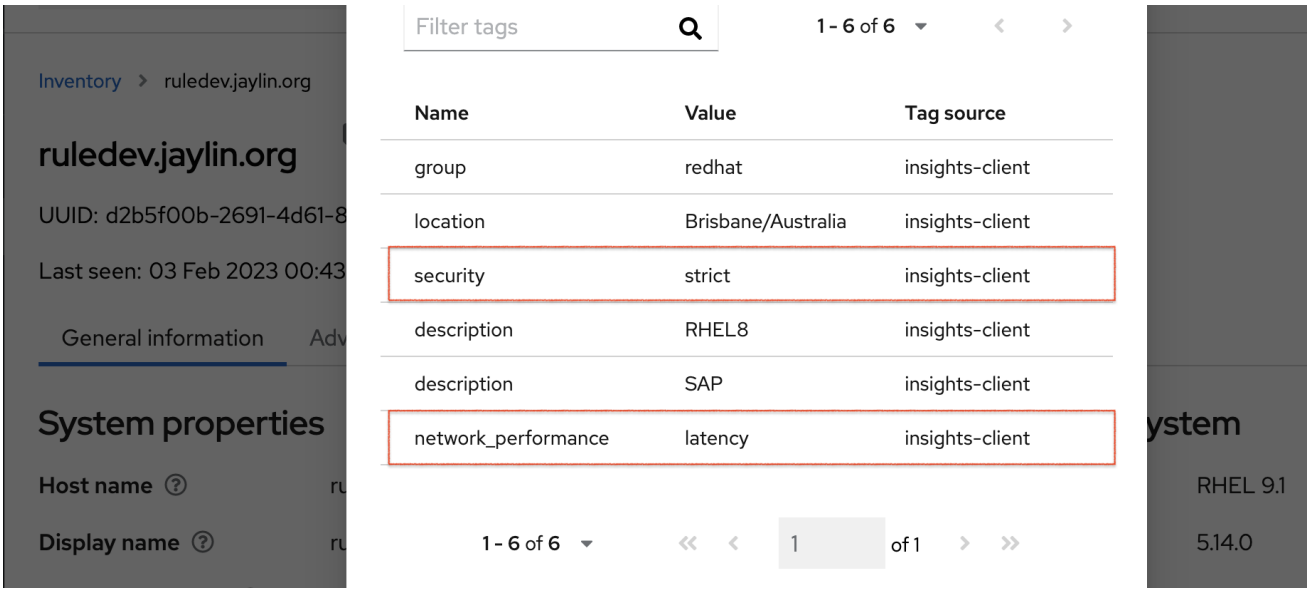
```
[root@server ~]# insights-client
```

确认预定义的标签在您的生产区中

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。您会看到一个显示的表：

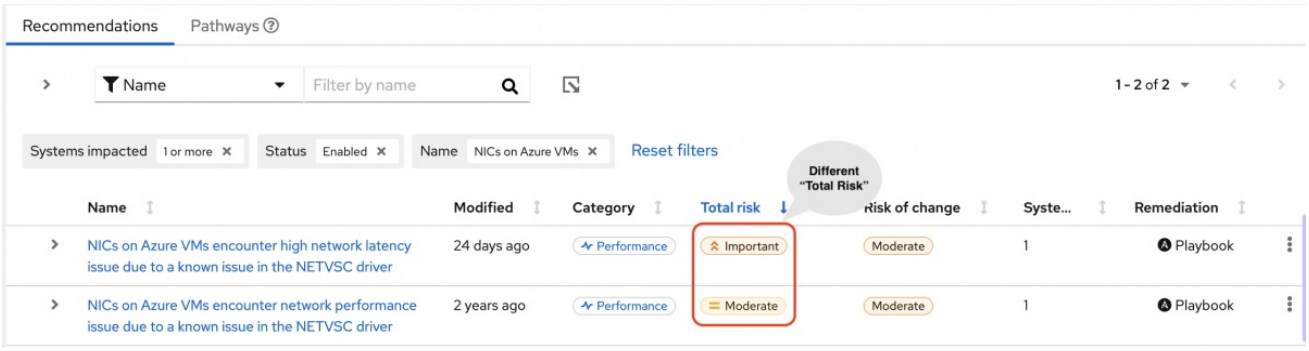
- Name
- 值
- 标签源（例如 insights-client）。

下图显示了您在创建标签后在清单中看到的示例。



应用预定义的标签后的建议示例

以下公告服务镜像显示了配置了 **network_performance: latency** 标签的系统。



系统显示具有较高的 Total Risk 级别 Important 的建议。没有 **network_performance: latency** 标签的系统具有中等总风险。您可以决定系统优先级更高的总风险。

第 5 章 参考

请参阅以下参考资料以了解更多信息。

5.1. 参考资料

要了解更多有关漏洞服务的信息，请参阅以下资源：

- *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 产品支持页面

对红帽文档提供反馈

我们非常感谢并对我们文档的反馈进行优先排序。提供尽可能多的详细信息，以便快速解决您的请求。

先决条件

- 已登陆到红帽客户门户网站。

流程

要提供反馈，请执行以下步骤：

1. 点击以下链接： Create Issue
2. 在 **Summary** 文本框中描述问题或功能增强。
3. 在 **Description** 文本框中提供有关问题或请求的增强的详细信息。
4. 在 **Reporter** 文本框中键入您的名称。
5. 点 **Create** 按钮。

此操作会创建一个文档票据，并将其路由到适当的文档团队。感谢您花时间来提供反馈。