Red Hat Insights 2023

评估和监控 RHEL 系统的安全策略合规性

了解 Red Hat Enterprise Linux 基础架构的安全合规状态

Last Updated: 2023-05-30

Red Hat Insights 2023 评估和监控 RHEL 系统的安全策略合规性

了解 Red Hat Enterprise Linux 基础架构的安全合规状态

法律通告

摘要

评估和跟踪 RHEL 环境的安全策略合规状态，以确定合规性级别并规划一系列操作来解决合规性问题。 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 RED HAT INSIGHTS 合规服务概述 3
1.1. 要求和先决条件 3
1.2. 支持的配置 3
1.3. 最佳实践 4
1.4. 用户访问注意事项 4

第 2 章 使用合规服务入门 6

第 3 章 在 INSIGHTS FOR RHEL 合规服务中管理 SCAP 安全策略 8
3.1. 创建新的 SCAP 策略 8
3.2. 编辑现有策略 10

第 4 章 分析并检索您的合规性报告 12
4.1. 合规性报告 12
4.2. SCAP 策略 12
4.3. 系统 12
4.4. 搜索 13

第 5 章 系统标签和组群 14
5.1. COMPLIANCE 服务中的组和标签过滤器 14
5.2. SAP 工作负载 14
5.3. SATELLITE 主机组 15
5.4. MICROSOFT SQL SERVER 工作负载 15
5.5. 自定义系统标记 17

第 6 章 参考资料 22

对红帽文档提供反馈 23

第 1 章 RED HAT INSIGHTS 合规服务概述

Red Hat Enterprise Linux 合规服务的 Red Hat Insights 可让 IT 安全和合规性管理员评估、监控和报告 RHEL 系统安全策略合规性。

合规性服务提供了一个简单而强大的用户界面，支持创建、配置和管理 SCAP 安全策略。通过构建过滤和上下文添加功能，IT 安全管理员可以轻松识别和管理 RHEL 基础架构中安全合规问题。

本文档描述了合规服务的一些功能，以帮助用户了解报告、管理问题并从服务获得最大值。

您还可以创建 Ansible Playbook 以解决安全合规问题，并与利益相关者共享报告以沟通合规状态。

其它资源

- *生成合规服务报告*

1.1. 要求和先决条件

合规服务是 Red Hat Enterprise Linux for Red Hat Enterprise Linux 的一部分，它包含在 Red Hat Enterprise Linux (RHEL)订阅中，并可与当前红帽支持的所有 RHEL 版本一起使用。您不需要额外的红帽订阅来使用 Insights for Red Hat Enterprise Linux 和合规性服务。

1.2. 支持的配置

红帽为每个 Red Hat Enterprise Linux (RHEL)的次要版本支持 SCAP 安全指南(SSG)的特定版本。SSG 版本中的规则和策略只对一个 RHEL 次版本准确。为了获得准确的合规性报告，系统必须安装有受支持的 SSG 版本。

Red Hat Enterprise Linux 次版本包括了并升级支持的 SSG 版本。但是，一些机构可能会决定在升级前临时使用较早的版本。

如果策略包括使用不被支持的 SSG 版本的系统，在 Red Hat Enterprise Linux > Compliance > Reports 中的策略的旁边带有 **unsupported** 警告以及受影响系统的数量。

注意

有关 RHEL 中支持哪些 SCAP 安全指南版本的更多信息，请参阅 Insights Compliance - 支持的配置。

带有运行不支持的 SSG 版本的系统的合规策略示例

1.2.1. 有关合规性服务的常见问题

如何解释 SSG 软件包名称？

软件包名称类似如下： **scap-security-guide-0.1.43-13.el7**。本例中的 SSG 版本为 0.1.43；版本为 13，构架为 el7。发行号可能与表中显示的版本号不同，但是，版本号必须与以下版本匹配，以便它是一个支持的配置。

如果红帽对 RHEL 次版本支持多个 SSG？

当 RHELminor 版本支持多个 SSG 版本时，如 RHEL 7.9 和 RHEL 8.1，合规服务将使用最新的可用版本。

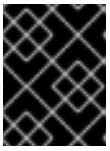
为什么我的旧策略不再被 SSG 支持？

因为 RHEL 次版本存在旧的，所以支持较少的 SCAP 配置集。要查看支持哪些 SCAP 配置集，请参阅 Insights Compliance - 支持的配置 。

有关不支持的配置的限制

以下条件适用于不支持的配置的结果：

- 这些结果是一个"最佳保证"的工作，因为使用红帽支持的任何 SSG 版本都可能会导致结果不准确。



重要

虽然您仍然可以看到安装了不支持的 SSG 版本的系统的结果，但这些结果可能会被视为不准确进行合规性报告目的。

- 使用不支持的 SSG 版本的系统 *的结果不包括在* 策略的整体合规评估中。
- 对于安装了不支持的 SSG 版本的系统上的规则，不提供补救。

1.3. 最佳实践

要获得最佳用户体验并获得合规服务中最准确的结果，红帽建议您遵循一些最佳实践。

确保 RHEL OS 系统次版本对 Insights 客户端可见

如果合规服务无法看到 RHEL OS 次版本，则无法验证支持的 SCAP 安全指南版本，且您的报告可能并不准确。Insights 客户端允许用户从上传到 Red Hat Enterprise Linux for Red Hat Insights for Red Hat Enterprise Linux 的数据有效负载中删除某些数据，包括 Red Hat Enterprise Linux OS 次版本。这将禁止准确的合规性服务报告。

要了解更多有关数据红色操作的信息，请参阅以下文档： Red Hat Insights 客户端数据红色操作 。

在合规服务中创建安全策略

在合规服务中创建组织的安全策略，允许您将多个系统与策略关联，保证根据您的 RHEL 次版本使用支持的 SCAP 安全指南，并根据机构的要求编辑包含哪些规则。

1.4. 用户访问注意事项

访问 Red Hat Enterprise Linux 的 Red Hat Enterprise Linux 功能是由您帐户中机构管理员在 User Access 中配置的设置控制。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。但是，有一些操作需要用户具有提升的访问权限。

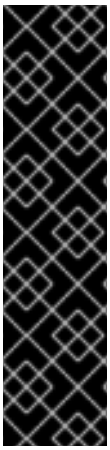
重要

在本文档中，声明是否必须有升级的访问权限才能执行此流程。

以下预定义角色与访问特别相关：

- **默认访问组。**帐户中的所有人都是 Default 访问组的成员。作为 Default 访问组的成员，您可以在 Insights for Red Hat Enterprise Linux 中查看大多数信息。

- **机构管理员。**帐户的机构管理员可以创建和修改用户访问组，并授予其他帐户用户的访问权限。您可以通过单击屏幕右上角的 Red Hat Hybrid Cloud Console 标头中的名称来确定是否是机构管理员。管理员"位于您的用户名下。



重要

如果您无法访问您需要的功能，请**求增强的访问**，您可能需要

- 联系客户服务 以获取机构管理员的详细信息。
  - 发送请求时提供您的帐户号。
- 联系该个人并询问访问权限，提供以下信息：
  - 您需要访问的角色的名称，例如 Remediations 管理员
  - 链接到完整的 用户访问文档，以帮助告知机构管理员如何提供访问权限。

1.4.1. compliance-service 用户的用户访问角色

以下角色启用对 Red Hat Enterprise Linux 的 Insights 中补救功能的标准或增强的访问：

- **合规性视图.**授予对任何合规资源的读取访问权限的 compliance-service 角色。
- **合规管理员。**一个 compliance-service 角色，授予任何合规资源的完整访问权限。

第 2 章 使用合规服务入门

这部分论述了如何配置 RHEL 系统，将合规性数据报告到 Insights for RHEL 应用程序。这会安装必要的其他组件，如 SCAP 安全指南(SSG)，用于执行合规性扫描。

先决条件

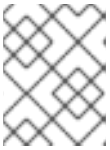
- Insights 客户端已在系统上部署。
- 必须具有系统上的 root 权限。

流程

1. 检查系统中的 RHEL 版本：

```
[user@insights]$ cat /etc/redhat-release
```

2. 查看 Insights Compliance - 支持的配置 文章，并记录系统中 RHEL 次版本支持的 SSG 版本。



注意

RHEL 的一些次要版本支持多个 SSG 版本。Insights 合规服务将始终显示最新支持版本的结果。

3. 检查系统上是否安装了 SSG 软件包的支持版本：
示例 - 对于 RHEL 8.4 运行：

```
[root@insights]# dnf info scap-security-guide-0.1.57-3.el8_4
```

4. 如果还没有安装，请在系统上安装受支持的 SSG 版本。
示例 - 对于 RHEL 8.4 运行：

```
[root@insights]# dnf install scap-security-guide-0.1.57-3.el8_4
```

5. 在合规服务 UI 中，Red Hat Enterprise Linux > Compliance > SCAP 策略 将系统添加到策略中。
   a. 点 **Create new policy** 将系统添加到新的安全策略中。
   b. 或者，选择一个现有策略并点击 **Edit policy** 将系统添加到其中。
6. 将每个系统添加到所需的安全策略后，返回到系统并运行合规性扫描：

```
[root@insights]# insights-client --compliance
```

注意

扫描可能需要 1 到 5 分钟才能完成。

7. 导航到 *生成 Compliance Service Reports* 以查看结果。
8. （可选） 使用 cron 调度合规作业。

其它资源

要了解 Red Hat Enterprise Linux 次版本支持哪些 SCAP 安全指南版本，请参阅 Insights Compliance - 支持的配置。

第 3 章 在 INSIGHTS FOR RHEL 合规服务中管理 SCAP 安全策略

在合规服务 UI 中完全创建和管理您的 SCAP 安全策略。定义新策略并选择您要与其关联的规则和系统，并根据您的要求更改编辑现有策略。

重要

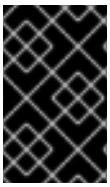
与 Red Hat Enterprise Linux 服务的其他 Red Hat Insights 不同，合规服务不会按默认计划自动运行。要将 OpenSCAP 数据上传到 Red Hat Enterprise Linux 应用程序的 Insights 中，您必须运行 **insights-client --compliance**，也可以是您设置的调度作业。

其他资源

如何为 Insights 服务设置周期性上传？

3.1. 创建新的 SCAP 策略

在执行扫描或查看合规服务 UI 中扫描前，您必须将 Red Hat Enterprise Linux 注册的系统的每个 Insights 添加到一个或多个安全策略中。要创建新策略，并包含特定的系统和规则，请完成以下步骤：

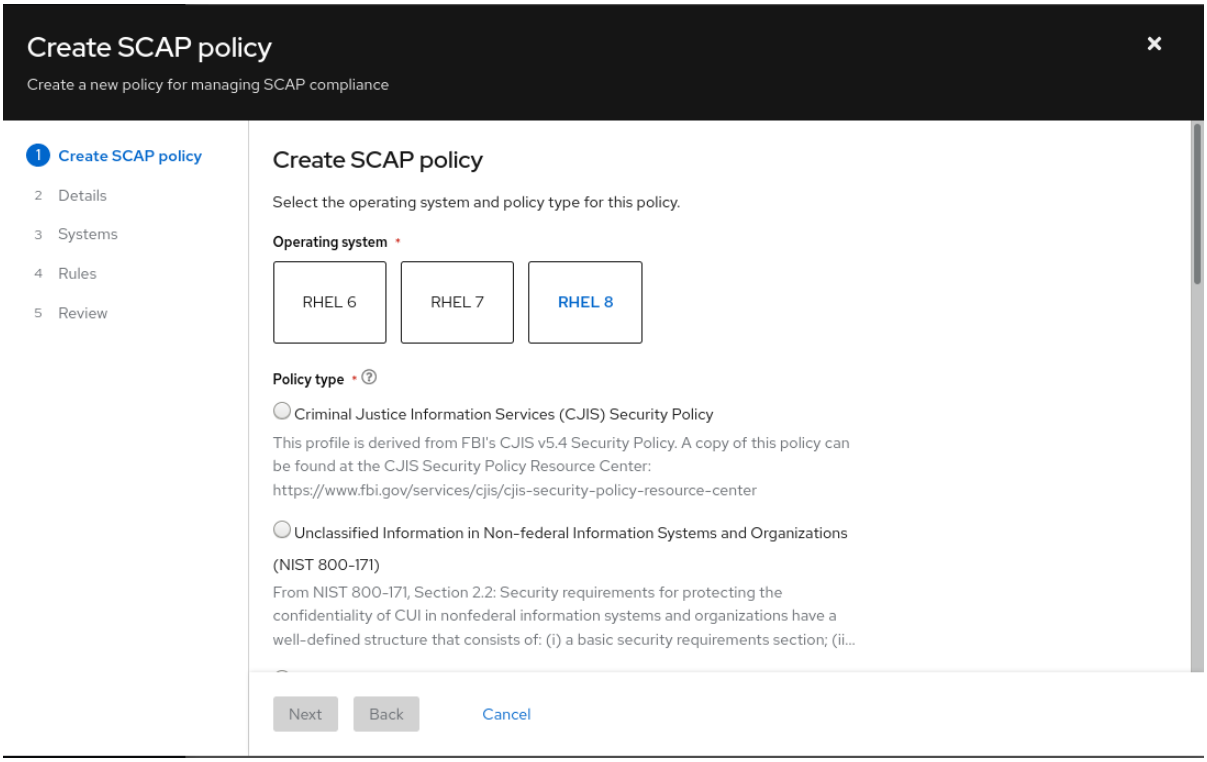


重要

如果您的 RHEL 服务器跨越多个 RHEL 主版本，您必须为每个主版本创建单独的策略。例如，所有 RHEL 7 服务器都将位于 RHEL 策略的一个 *标准系统安全配置文件中，所有 RHEL 8* 服务器都将位于另一个标准系统安全配置文件中。

流程

1. 登录到 Red Hat Hybrid Cloud Console 并进入 Red Hat Enterprise Linux > Compliance > SCAP policies 页面。
2. 点 **Create new policy** 按钮。
3. 在 **向导的 Create SCAP 策略** 页面中，选择策略中包含的系统的 **RHEL 主版本**。



4. 选择可用于该 RHEL 主版本 **的策略类型之一**，然后单击 **Next**。

5. 在 **Details** 页面中，接受已提供的名称和描述，或者提供您自己的更有意义的条目。

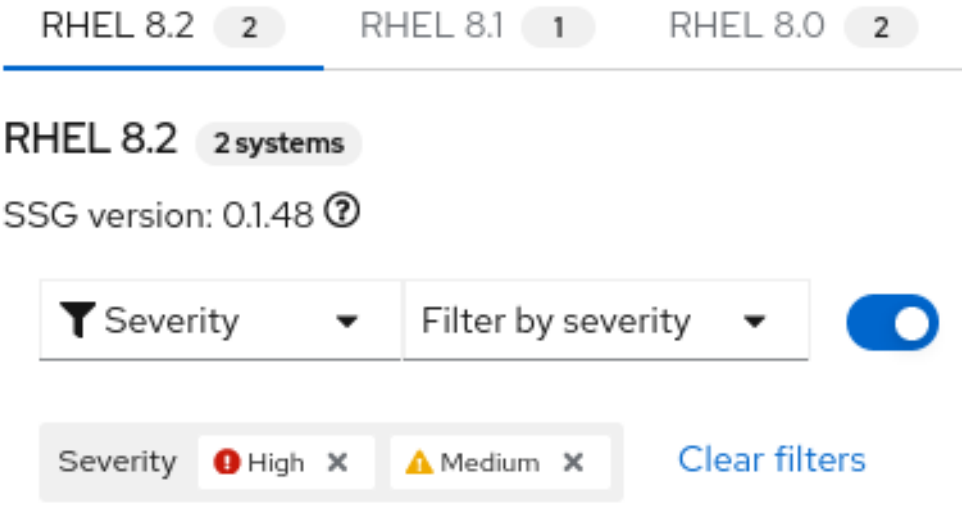
6. （可选）添加一个 **业务目标** 以提供上下文，例如 "CISO mandate"。

7. 定义一个 **符合您的要求的合规性阈值**，然后单击 **Next**。

8. 选择要包含在 **此策略** 中的系统，然后单击 **Next**。您选择第一步中的 RHEL 主版本会自动决定可以添加到此策略中哪些系统。

9. 选择要包含在每个策略中的规则。因为 RHEL 的每个次要版本都支持使用特定的 SCAP 安全指南 (SSG)版本（有时称为多个版本，在这种情况下，我们使用最新的），每个 RHEL 次版本设置的规则略有不同，且必须单独选择。

   a. （可选）使用过滤和搜索功能来重新定义规则列表。
   例如，若要只显示最高严重性规则，请单击主过滤器下拉菜单并选择 **严重性**。在二级过滤器中，选中 **High** 和 **Medium** 的复选框。



b. 默认显示的规则是为该策略类型和 SSG 版本指定的规则。默认情况下启用过滤器框旁边的 **Selected only** 切换。如果需要，您可以删除此切换。

c. 根据需要 *为每个* **RHEL 次版本**选项卡 重复此过程。

d. 为每个 Red Hat Enterprise Linux 次版本 SSG 选择规则后，点 **Next**。

10. 在 **Review** 页面中，验证显示的信息是否正确，然后单击 **Finish**。

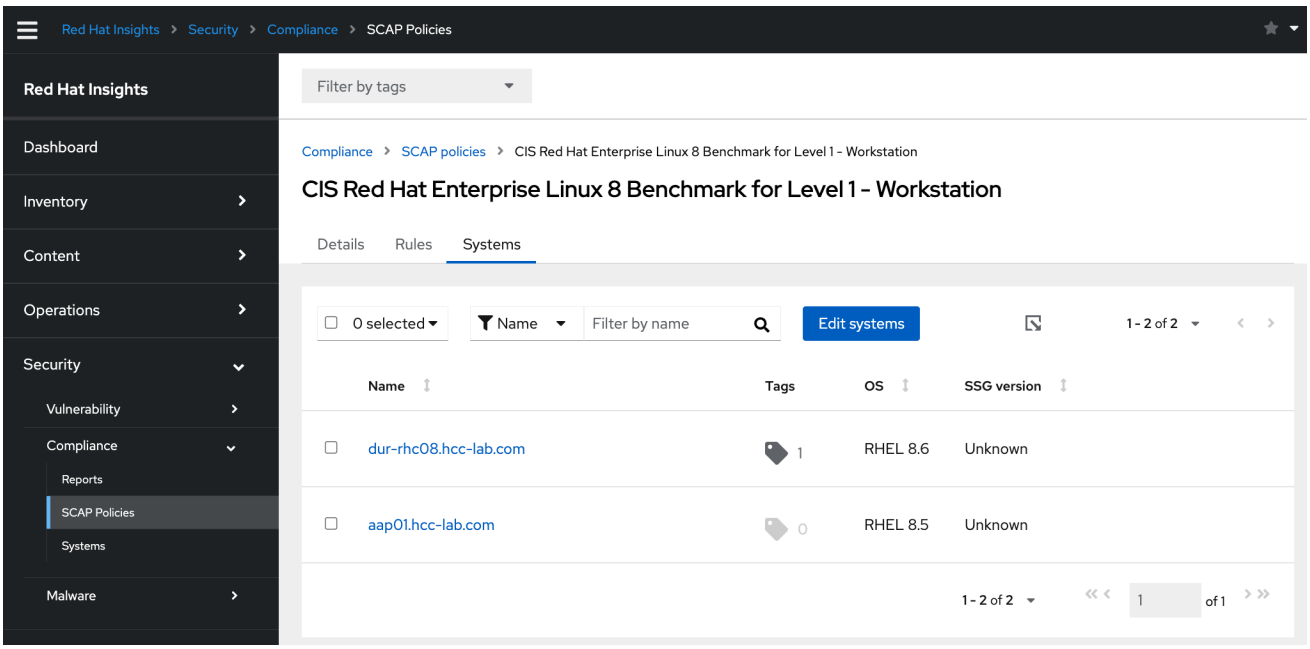
11. 给应用程序提供一分钟来创建策略，然后单击返回至 **应用程序** 按钮，以查看您的新策略。

注意

您必须进入系统并运行合规性扫描，然后才能在合规服务 UI 中显示结果。

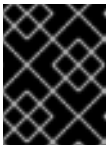
3.2. 编辑现有策略

创建合规策略后，您可以编辑策略以更改包含哪些规则或系统。使用以下步骤编辑现有策略以添加或删除特定规则或系统。在 Red Hat Hybrid Cloud Console 中，在合规服务策略页面中编辑合规策略。在策略详情视图中，您可以编辑 Rules 选项卡中包含的规则，并在 Systems 选项卡中编辑包含的系统。



流程

1. 登录到 Red Hat Hybrid Cloud Console 并进入 Red Hat Enterprise Linux > Compliance > SCAP policies 页面。
2. 找到要编辑的策略。
3. 在策略行的右侧，点 More Actions 图标 ，然后点 **Edit policy**。
4. 在 **Edit <Policy name>** 卡中，点 **Rules** 选项卡。
   a. 使用过滤器或搜索功能查找要删除的规则。

   重要

   默认情况下启用 **Selected only** to the search 右侧。您可以根据需要删除切换。

   b. 取消选中您要删除的任何规则旁边的复选框。
   c. 根据需要为每个 RHEL 次版本 SSG 选项卡重复此步骤。
5. 点击 **Save**。

验证

1. 进入 Red Hat Enterprise Linux > Compliance > SCAP policies 页面，找到编辑的策略。
2. 点策略，并验证包含的规则是否与您所做的编辑一致。

第 4 章 分析并检索您的合规性报告

合规性服务向服务显示每个策略和系统注册（和报告数据）的数据。这可以是一个大量数据，其中大多数数据可能不与您的即时目标相关。

以下小节讨论了在报告、SCAP 策略和系统 - 中调整合规性服务数据的批量方法，专注于与您最相关的系统或策略。

合规服务允许用户在系统、规则和策略列表中设置过滤器。与 Red Hat Enterprise Linux 服务的其他 Insights 一样，合规服务还可根据 system-group 标签进行过滤。但是，由于合规性注册的系统使用不同的报告机制，所以标签过滤器必须直接在合规性 UI 视图中的系统列表中设置，而不是从全局设置，而 **Filter by status** 下拉菜单在 Insights 应用程序其他位置使用。

重要

要查看您的系统准确数据，请在在 UI 中查看结果前在每个系统上运行 **insights-client --compliance**。

4.1. 合规性报告

在 Red Hat Enterprise Linux > Compliance > Reports 中，使用以下主过滤器和次要过滤器来专注于特定的或缩小报告集合：

- **策略名称。**按名称搜索策略。
- **策略类型。**从为基础架构在合规服务中配置的策略类型中选择。
- **操作系统。**选择一个或多个 RHEL OS 主版本。
- **系统满足合规性。**显示包含系统百分比（范围）的策略。

4.2. SCAP 策略

在 Red Hat Enterprise Linux > Compliance > SCAP policies 中，使用 **Filter by name** 搜索框按名称查找特定的策略。然后点击策略名称查看策略卡，其中包括以下信息：

- **详情。**查看合规阈值、业务目标、操作系统和 SSG 版本等详情。
- **规则。**查看并过滤策略的特定 SSG 版本中包含的规则，按名称、严重性和修复提供。然后，按规则名称、严重性或 Ansible Playbook 支持对结果进行排序。
- **系统。**根据系统名称搜索以查找与策略关联的特定系统，然后单击系统名称以查看该系统以及可能会影响它的问题的更多信息。

4.3. 系统

Red Hat Enterprise Linux > Compliance > Systems 的默认功能是按系统名称搜索。

- **标签。**按系统组或标签名称搜索。
- **名称。**按系统名称搜索。
- **policy。**按策略名称搜索并查看该策略中包含的系统。
- **操作系统。**根据 RHEL OS 主版本搜索，仅查看 RHEL 7 或 RHEL 8 系统。

4.4. 搜索

合规服务的搜索功能可在您要查看的页面上下文中工作。

- **SCAP 策略。**按名称搜索特定策略。
- **系统。**根据系统名称、策略或 Red Hat Enterprise Linux 操作系统主版本进行搜索。
- **规则列表（单一系统）。**规则列表搜索功能允许您按规则名称或标识符进行搜索。标识符直接在规则名称下方显示。

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。

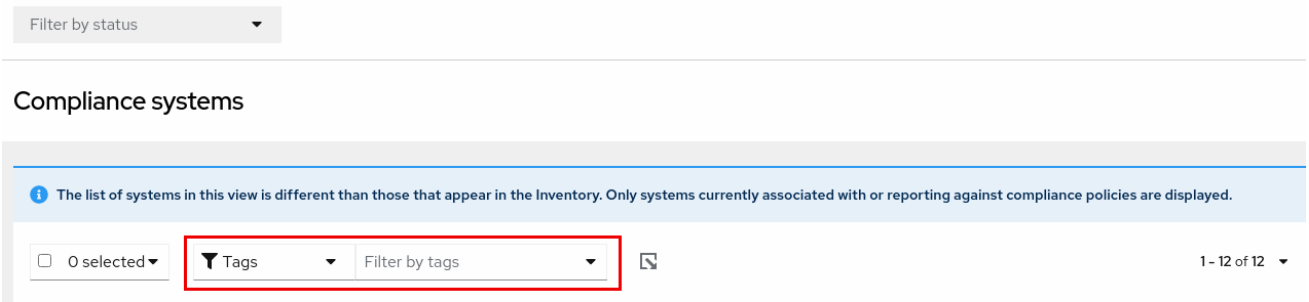
5.1. COMPLIANCE 服务中的组和标签过滤器

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/
```

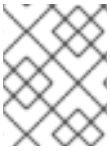
3. 使用以下方法启用计时器：

```
# 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. 进入 Red Hat Enterprise Linux > 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。
6. 验证系统是否已标记的流程
7. 进入 Red Hat Enterprise Linux > Inventory，并根据需要登录。
8. 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。
9. 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

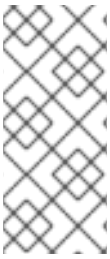
Red Hat Insights 顾问服务建议会平等地处理每个系统。但是，有些系统可能需要比其他系统更安全，或者需要不同的网络性能级别。除了添加自定义标签外，Red Hat Insights for Red Hat Enterprise Linux 还提供了预定义的标签，公告服务还可以为可能需要更多关注的系统创建目标建议。

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。

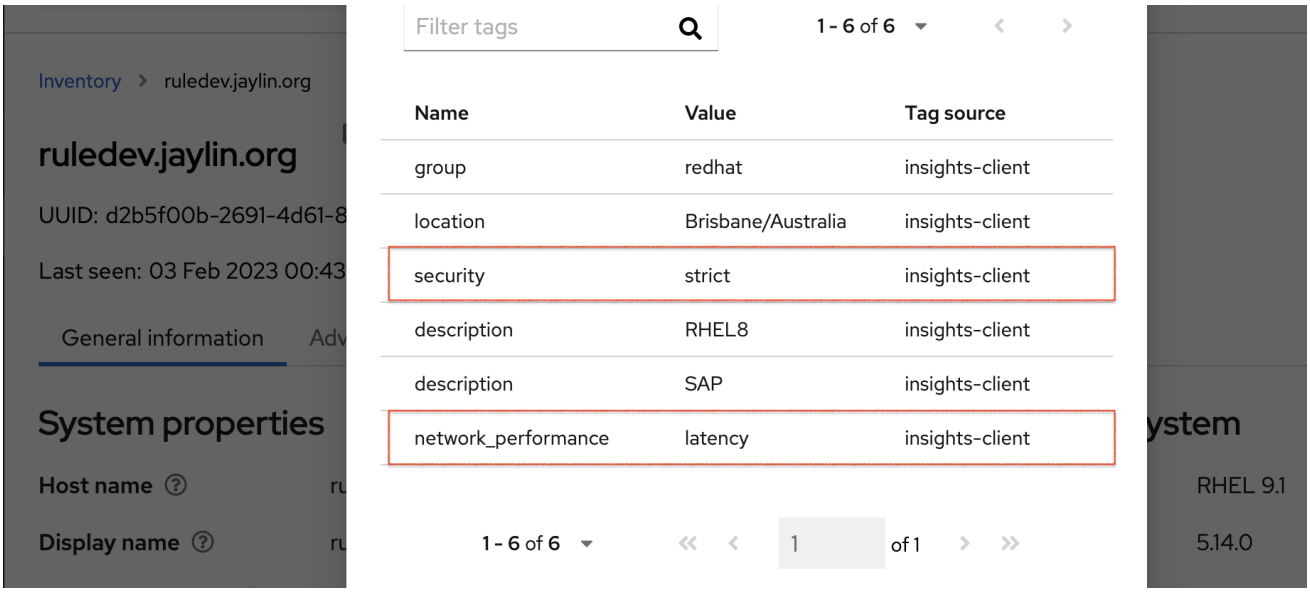
```
[root@server ~]# insights-client
```

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 Enterprise Linux > Inventory 找出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：

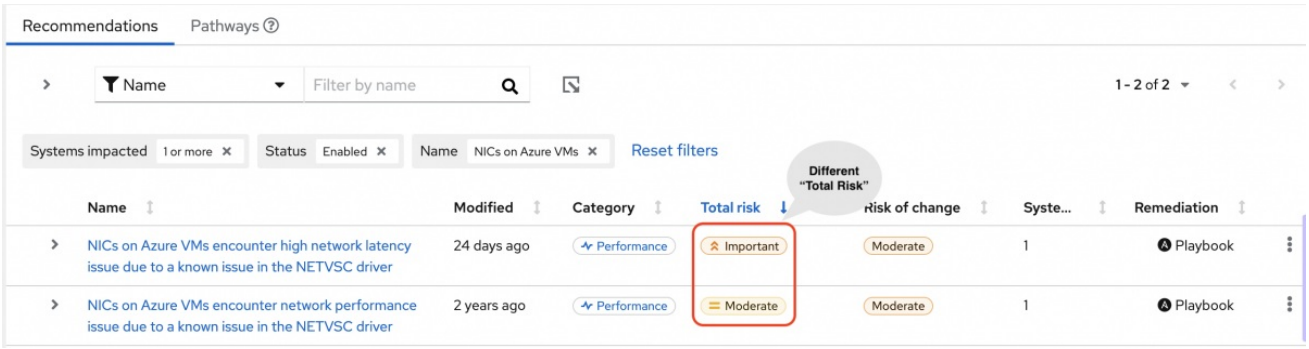
- Name
- 值
- 标签源（如 insights-client）。

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 参考资料

要了解更多有关合规服务的信息，请查看以下资源：

- *生成合规服务报告*
- 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。