Red Hat Insights 1-latest

使用 FedRAMP 的策略监控和对配置更改进行监控

如何创建策略来检测清单配置更改并发送电子邮件通知

Last Updated: 2024-10-16

Red Hat Insights 1-latest 使用 FedRAMP 的策略监控和对配置更改进行监控

如何创建策略来检测清单配置更改并发送电子邮件通知

Red Hat Customer Content Services

法律通告

摘要

本文档概述了 FedRAMP® 的策略服务，并解释了如何创建策略来检测系统配置更改以及电子邮件通知。 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 RED HAT INSIGHTS 策略服务概述

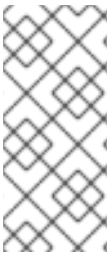
策略会评估环境中的系统配置，并在发生更改时发送通知。您创建的策略适用于 Insights 清单中所有系统。您可以使用 Red Hat Hybrid Cloud Console 中的 Red Hat Enterprise Linux 用户界面或使用 Insights API 创建和管理策略。

策略可以通过管理以下任务来帮助您：

- 当您的系统配置中特定条件发生时，会增加警报。
- 当安全软件包系统上已过时时，请发送电子邮件给团队。

使用策略监控清单中的配置更改，并通过电子邮件通知需要：

- 设置用户电子邮件首选项（如果尚未设置）。
- 创建用于检测配置更改作为触发器的策略，并选择电子邮件作为触发器操作。



注意

- 在 Red Hat Hybrid Cloud Console > **Settings** 图标(HBAC)> Identity & Access Management > User Access > Users 中配置 User Access。
- 有关此功能和示例用例的更多信息，*请参阅使用 FedRAMP 的基于角色的访问控制(RBAC)的用户访问配置指南*。

1.1. 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。

1.1.1. 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。

1.1.1.1. 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。

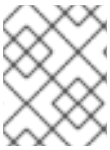
Default admin access 组仅包含具有机构管理员权限的用户。这个组会自动维护，且无法更改此组中的用户和角色。

1.1.2. 策略服务的用户访问角色

Red Hat Hybrid Cloud Console 上的以下预定义角色可以访问 Insights for Red Hat Enterprise Linux 中的策略功能：

- **策略管理员角色.**策略管理员角色提供读写访问权限，允许这些用户对策略资源执行任何可用的操作。此预定义角色位于 **Default admin access group** 中。

- **policies viewer 角色。**Policies viewer 角色提供只读访问。（如果您的组织决定策略查看器角色的默认配置不准确，则 **用户访问权限管理员可以创建** 具有您所需的特定权限的自定义角色。）此预定义角色位于 **Default 访问组** 中。



注意

如果您在 2023 年 4 月之前配置了组，则任何不是机构管理员的用户都会使用 Policies viewer 角色替代。在 4 月之前，对 Default access 组进行的修改不会被更改。

其它资源

- 如何在基于角色的访问控制(RBAC)中使用用户访问权限。
- 预定义的用户访问角色

第 2 章 设置通知和电子邮件首选项

通过在 Red Hat Hybrid Cloud Console 中配置通知和用户首选项设置，Red Hat Insights 将通知您对 Red Hat Enterprise Linux 系统的策略更改。

2.1. 为策略服务启用通知和集成

您可以在 Red Hat Hybrid Cloud Console 上启用通知服务，以便在策略服务检测到问题并生成警报时发送通知。使用通知服务可自由地检查 Red Hat Insights Dashboard 中的警报。

例如，您可以将通知服务配置为在策略服务检测到服务器安全软件过期时自动发送电子邮件消息，或者发送策略服务每天生成的所有警报的电子邮件摘要。

除了发送电子邮件信息外，您还可以将通知服务配置为发送策略事件数据：

- 使用经过身份验证的客户端查询 Red Hat Insights API 获取事件数据
- 使用 Webhook 将事件发送到接受入站请求的第三方应用程序
- 将通知与 Splunk 等应用程序集成，以将策略事件路由到应用程序仪表板

启用通知服务需要三个主要步骤：

- 首先，机构管理员会创建一个具有 Notifications 管理员角色的用户访问权限组，然后将帐户成员添加到组中。
- 接下来，通知管理员为通知服务中的事件设置行为组。行为组指定每个通知的交付方法。例如，行为组可以指定电子邮件通知是否发送到所有用户，或者只向机构管理员发送。
- 最后，从事件接收电子邮件通知的用户必须设置其用户首选项，以便他们为每个事件接收单独的电子邮件。

其他资源

- 有关配置 Hybrid Cloud Console 通知以了解已发生的识别事件并可能会影响您的机构的更多信息，*请参阅使用 FedRAMP 在 Red Hat Hybrid Cloud Console 中配置通知* 。
- 有关配置与第三方应用程序集成的混合云控制台通知的更多信息，*请参阅将 Red Hat Hybrid Cloud Console 与第三方应用程序集成*。

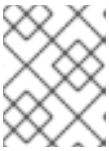
2.2. 设置用户首选项

要接收电子邮件通知，您可以按照以下流程设置或更新您的电子邮件首选项。

流程

1. 进入 **Operations > Policies**。
2. 点 **Open user preference**。此时会出现 My Notifications 页面。
3. 从左侧菜单中选择 **Red Hat Enterprise Linux > Policies**。
4. 选中适当的框以定义您的策略通知首选项。

5. 根据您的电子邮件通知首选项，您可以为每个具有触发策略的系统订阅 **Instant** 通知电子邮件，或者在 24 小时时间段内对触发的应用程序事件的**每日汇总**。要取消订阅所有通知，请从所有通知中选择 **Unsubscribe**。



注意

订阅即时通知可能会导致在大型清单中接收多个电子邮件。要减少电子邮件卷，请考虑选择 Daily 摘要选项。

6. 点 **Submit**。

第 3 章 创建策略

以下工作流示例解释了如何创建多种类型的策略，以检测系统配置更改并通过电子邮件发送通知更改。

注意

在创建策略时，如果您看到一条未选择的电子邮件警报的警告信息，请将您的用户首选项设置为从您的策略接收电子邮件。

3.1. 创建一个策略，以确保不会过度置备公有云供应商

使用以下步骤创建策略。

流程

1. 在 Red Hat Hybrid Cloud Console 中，进入 Operations > Policies。
2. 点击 **Create policy**。
3. 在 Create a policy 页面上，根据需要单击 **From scratch** 或 **As a existing Policy 的副本**。请注意，**作为现有 Policy 选项的副本** 将提示您从现有策略列表中选择策略，以用作起点。
4. 点击 **Next**。
5. 输入 **条件**。在本例中，输入：**facts.cloud_provider in ['alibaba', 'aws', 'azure', 'google'] and (facts.number_of_cpus >= 8 or facts.number_of_sockets >=2)**。此条件将检测指定公共云提供商上运行的实例是否使用高于允许限制的 CPU 硬件运行。

注意

您可以扩展 **什么条件，我定义了什么条件？** 和/或 **Review 可用系统事实** 来查看您可以使用的条件，并分别查看可用的系统事实。在本节中，您可以使用的语法示例。

6. 单击 **Validate condition**。
7. 验证条件后，单击 **下一步**。
8. 在 Trigger 操作页面中，点 **Add trigger actions**。如果通知被问候，请在通知框中选择 **Notification settings**。您可以在此处自定义通知及其行为。
9. 点击 **Next**。

注意

在 Trigger 操作页面中，您还可以启用电子邮件警报并设置其他可用的电子邮件首选项。

10. 在 Review and enable 页面中，点切换开关来激活策略并查看其详情。
11. 点 **Finish**。

您的新策略已创建。当策略在系统检查上评估时，如果满足策略中的条件，策略会自动向有权访问策略的帐户上的所有用户发送电子邮件，具体取决于他们的电子邮件首选项。

3.2. 创建策略来检测系统是否在运行过时的 RHEL 版本

您可以创建一个策略来检测系统是否运行过时的 RHEL 版本，并通过电子邮件通知您。

流程

1. 在 Red Hat Hybrid Cloud Console 中，进入 Operations > Policies。
2. 点击 **Create policy**。
3. 在 Create policy 页面上，根据需要单击 **From scratch** 或 **As a copy of existing Policy**。请注意，**作为现有 Policy 选项的副本** 会提示您从现有策略列表中选择策略，以用作起点。
4. 点击 **Next**。
5. 为策略输入**名称**和**描述**。
6. 点击 **Next**。
7. 输入 **条件**。在这种情况下，输入 **facts.os_release < 8.1**。此条件将检测系统是否仍然基于 RHEL 8.1 运行我们操作系统的过时的版本。
8. 单击 **Validate condition**，然后单击 **Next**。
9. 在 Trigger 操作页面中，单击 **Add trigger actions** 并选择 **Email**。
10. 点击 **Next**。
11. 在 Review and activate 页面中，点切换开关来激活策略并查看其详情。
12. 点 **Finish**。

您的新策略已创建。当在系统检查上评估策略时，如果触发策略中的条件，策略服务会自动向具有策略访问权限的帐户上的所有用户发送电子邮件，具体取决于其电子邮件首选项。

3.3. 创建策略以根据最新的 CVE 检测存在安全漏洞的软件包版本

您可以创建一个策略，它根据最新的 CVE 检测到存在安全漏洞的软件包版本，并通过电子邮件通知您它发现的内容。

流程

1. 在 Red Hat Hybrid Cloud Console 中，进入 Operations > Policies。
2. 点击 **Create policy**。
3. 在 Create Policy 页面上，根据需要单击 **From scratch** 或 **As a copy of existing Policy**。请注意，**作为现有 Policy 选项的副本** 将提示您从现有策略列表中选择策略，以用作起点。
4. 点击 **Next**。
5. 为策略输入**名称**和**描述**。
6. 点击 **Next**。

7. 输入 **条件**。在这种情况下，输入 **facts.installed_packages contains ['openssh-4.5']**。此条件将检测系统是否仍然根据最新的 CVE 运行 **openssh** 软件包的存在安全漏洞版本。
8. 单击 **Validate condition**，然后单击 **Next**。
9. 在 Trigger 操作页面中，单击 **Add trigger actions** 并选择 **Email**。
10. 点击 **Next**。
11. 在 Review and activate 页面中，点切换开关来激活策略并查看其详情。
12. 点 **Finish**。

您的新策略已创建。当策略在系统检查上评估时，如果满足策略中的条件，策略会自动向有权访问策略的帐户上的所有用户发送电子邮件，具体取决于他们的电子邮件首选项。

第 4 章 检查和管理策略

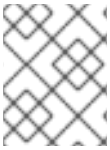
您可以通过进入到 Operations > Policies 来查看和管理所有创建的策略（启用和禁用）。

您可以根据名称和活跃状态过滤策略列表。您可以点击策略旁边的选项菜单来执行以下操作：

- 启用和禁用
- 编辑
- 重复
- 删除

另外，您可以通过从策略列表中选择多个策略并点击顶部的 **Create policy** 按钮旁的选项菜单 来批量执行以下操作：

- 删除策略
- 启用策略
- 禁用策略



注意

如果您看到有关电子邮件警报的警告信息，请将您的用户首选项设置为从您的策略中接收电子邮件。

第 5 章 附录

本附录包含以下参考资料：

- 系统事实
- Operator

5.1. 系统事实

下表定义了用于系统比较的系统事实。

表 5.1. 系统事实及其功能

事实名称	描述	示例值
Ansible	带有 Ansible 相关事实列表的 flavor	**controller_version**，值为 4.0.0
arch	系统架构	**x86_64**
bios_release_date	BIOS 发行日期；通常为 **MM/DD/YYYY** 的格式	01/01/2011
bios_vendor	BIOS 供应商名称	LENOVO
bios_version	BIOS 版本	1.17.0
cloud_provider	云供应商。值为 **google**,**azure**,**aws**,**alibaba**, 或 empty	**google**
cores_per_socket	每个插槽的 CPU 内核数	2
cpu_flags	带有 CPU 标记列表的 category。每个名称都是 CPU 标记（例如： **vmx**），并且该值始终被 **启用**。	**vmx**，值为 **enabled**
enabled_services	带有启用的服务列表的 flavor。类别中的每个名称都是服务名称（例如： **crond**），且该值始终被 **启用**。	**crond**，值为 **enabled**
fqdn	系统的完全限定域名(FQDN)	**system1.example.com**
infrastructure_type	系统基础架构；常见的值是 **virtual** 或 **physical**	**virtual**
infrastructure_vendor	基础架构厂商；常见值为 **kvm**、**VMware**、**baremetal** 等。	**kvm**

事实名称	描述	示例值
installed_packages	安装的 RPM 软件包列表。这是一个类别。	**Bash**，值设为 **4.2.46-33.el7.x86_64**。
installed_services	带有已安装服务列表的 flavor。类别中的每个名称都是服务名称（例如： **crond**），并且该值始终被 **安装**。	**crond**，值为 **installed**。
kernel_modules	内核模块列表。类别中的每个名称都是内核模块（例如： **nfs**），其值 **已启用**。	**nfs**，值为 **enabled**.
last_boot_time	**YYYY-MM-DDTHH:MM:SS** 格式的引导时间。仅信息；我们不会跨系统比较引导时间。	**2019-09-18T16:54:56**
mssql	带有与 Microsoft SQL Server 相关的事实列表的类别	**mssql_version**，值为 15.0.4153.1
network_interfaces	与网络接口相关的事实列表。	
	每个接口都有六个事实：**ipv6_addresses**,**ipv4_addresses**,**mac_address**,**mtu**,**state** 和 **type**。两个地址字段是用逗号分开的 IP 地址列表。**state** 字段可以是 **UP** 或 **DOWN**。**type** 字段是接口类型（例如：**ether**、**loop**、**bridge** 等）。	
	每个接口都以事实名称作为前缀。例如，接口 **em1** 将具有 **mac_address** 系统事实值 **em1.mac_address**。	
	与大多数网络接口事实进行比较，以确保它们在系统间相等。但是，会检查 **ipv4_addresses**、**ipv6_addresses** 和 **mac_address**，以确保它们在系统中有所不同。**lo** 的子域必须始终在所有系统中具有相同的 IP 和 MAC 地址。	
number_of_cpus	CPU 总数	**1**
number_of_sockets	插槽总数	**1**
os_kernel_version	内核版本	**4.18.0**
os_release	内核版本	**8.1**

事实名称	描述	示例值
running_processes	正在运行的进程列表。事实名称是进程的名称，值是实例数。	**crond**，值设为 **1**。
sap_instance_number	SAP 实例号	**42**
sap_sids	SAP 系统 ID (SID)	**A42**
sap_system	指明系统上是否安装了 SAP 的布尔值字段	**True**
sap_version	SAP 版本号	**2.00.052.00.1599235305**
satellite_managed	指明系统是否注册到 Satellite 服务器的布尔值字段	**FALSE**
selinux_current_mode	当前 SELinux 模式	**enforcing**
selinux_config_file	在配置文件中设置的 SELinux 模式	**enforcing**
systemd	失败数量、已排队的当前作业数量以及 **systemd**的当前状态	**state**，值为 **degraded**
system_memory_bytes	系统内存总量（以字节为单位）	**8388608**
tuned_profile	来自命令 **tuned-adm active**的当前配置集	**desktop**
yum_repos	yum 存储库列表。存储库名称添加到事实的开头。每个存储库都关联有 **base_url**、**enabled** 和 **gpgcheck**。	**Red Hat Enterprise Linux 7 Server (RPMs)）.base_url** 的值为 **https://cdn.redhat.com/content/dist/rhel/server/7/$releasever/$basearch/os**

5.2. OPERATOR

表 5.2. 条件中的可用 Operator

Operator	值
逻辑 Operator	和
	或者

Operator	值
布尔值 Operator	非
	!
	=
	!=
数字比较 Operator	>
	>=
	<
	<=
字符串比较 Operator	CONTAINS
	MATCHES
数组 Operator	IN
	CONTAINS

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。