Red Hat Insights 2023

使用策略监控和响应配置更改

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: 2023-05-31

Red Hat Insights 2023 使用策略监控和响应配置更改

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

本文档概述了策略服务，并解释了如何创建策略来检测系统配置更改并通过电子邮件通知。 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 策略服务概述 3
1.1. 用户访问注意事项 3

第 2 章 设置通知和电子邮件首选项 5
2.1. 为策略服务启用通知和集成 5
2.2. 设置用户首选项 5

第 3 章 创建策略 7
3.1. 创建一个策略，以确保不会过度置备公有云供应商 7
3.2. 创建策略来检测系统是否在运行过时的 RHEL 版本 8
3.3. 创建根据最新 CVE 检测存在安全漏洞的软件包版本的策略 8

第 4 章 检查和管理策略 10

第 5 章 附录 11
5.1. 系统事实 11
5.2. OPERATOR 13

对红帽文档提供反馈 15

第 1 章 RED HAT INSIGHTS 策略服务概述

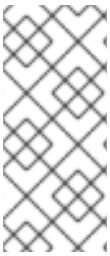
策略会评估环境中的系统配置，并可在更改时发送通知。您创建的策略适用于 Insights 清单中的所有系统。您可以使用 Red Hat Hybrid Cloud Console 中的 Red Hat Enterprise Linux 用户界面或使用 Insights API 创建和管理策略。

策略可通过管理以下任务来协助：

- 当您的系统配置中发生特定条件时，会引发警报。
- 当安全软件包在系统中过期时，发送电子邮件。

使用策略监控清单中的配置更改，并通过电子邮件通知：

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



注意

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

1.1. 用户访问注意事项

帐户上的机构管理员配置 User Access 中的设置，以控制对 Red Hat Insights for Red Hat Enterprise Linux 功能的访问。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，执行一些操作需要用户具有升级访问权限。

在 Red Hat Hybrid Cloud Console 中的 User Access 中授予访问权限。要授予或更改访问权限，机构管理员或用户访问权限管理员必须把具有 Red Hat Hybrid Cloud Console > Settings 菜单(gear icon)> Identity & Access Management > User Access 的所需角色的 User Access 组添加到 User Access 组中。

重要

在本文档中，对流程的先决条件声明是否需要提高访问权限来执行此流程。

与了解用户访问有关的重要预定义组和角色是：

- **默认访问组**
- **默认 admin 组**
- **机构管理员角色**

有关某些预定义组和角色的简要概述

以下预定义的组和角色与访问权限相关：

- **默认访问组。**帐户上的所有用户都是 Default access 组的成员。Default access 组的成员具有只读访问权限，供您在 Insights for Red Hat Enterprise Linux 中查看大多数信息。

- **默认 admin 访问组。**作为机构管理员的账户中的所有用户都是这个组的成员。用户不能修改红帽管理的 Default admin access 组中的角色。Default admin access 组的成员具有读写访问权限，允许您查看和执行 Insights for Red Hat Enterprise Linux 中的其他操作。

- **组织管理员角色.**机构管理员的所有用户都可以创建和修改 User Access 组，并授予对其他帐户用户的访问权限。要找出您是否是机构管理员，请在屏幕右上角点 Red Hat Hybrid Cloud Console 标头中的名称，并查看词语"Org"。管理员"在您的用户名下显示。

重要

如果无法访问 您需要的功能，您可以：

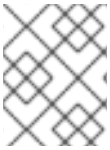
- 联系客户服务 以获取您帐户的机构管理员详情。
  - 发送请求时提供您的帐户号。
- 联系机构管理员并要求访问，提供以下信息：
  - 您需要访问权限的角色名称，例如 Remediations 管理员
  - 一个到 完整用户访问文档的链接，以帮助告知机构管理员如何为您提供访问权限。

1.1.1. 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 User Access Configuration Guide 中使用 User Access Configuration for Role-based Access Control (RBAC)。

- 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 仪表板是否有警报。

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

除了发送电子邮件消息外，您还可以将通知服务配置为以其他方式发送策略事件数据：

- 使用经过身份验证的客户端查询 Red Hat Insights API 以了解事件数据
- 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，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，机构管理员创建一个带有 Notifications administrator 角色的用户访问组，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，行为组可以指定是否向所有用户发送电子邮件通知，还是只发送给机构管理员。
- 最后，从事件接收电子邮件通知用户必须设置其用户首选项，以便接收每个事件的独立电子邮件。

其他资源

- 有关配置混合云控制台通知以了解已发生并可能会影响您的机构的事件的更多信息，请参阅 在 *Red Hat Hybrid Cloud Console 上配置通知* 和集成。
- 有关配置混合云控制台通知以与第三方应用程序集成的更多信息，请参阅 在 *Red Hat Hybrid Cloud Console 中配置集成和事件*。

2.2. 设置用户首选项

要接收电子邮件通知，您可以使用以下步骤设置或更新您的电子邮件首选项。

流程

1. 点击右上角的用户菜单，然后进入：用户首选项 > Notifications > Red Hat Enterprise Linux https://console.redhat.com/user-preferences/email。选中适当的复选框以定义您的策略通知首选项。
2. 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**。

注意

订阅即时通知可能会导致大型清单收到许多电子邮件，即每个系统检查一个电子邮件。

3. 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来检测系统配置更改，并通过电子邮件发送更改通知。

注意

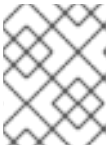
在创建策略时，如果您看到您没有选择电子邮件警报的警告信息，请将您的用户首选项设置为从您的策略接收电子邮件。

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 Red Hat Enterprise Linux > Policies 。
2. 点击 **Create policy**。
3. 在 Create a policy 页面中，根据需要点 **From scratch** 或 **As an existing Policy 副本**。请注意，**作为现有 Policy 选项的复制** 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. 输入 **Condition**。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)**。此条件将检测在指定公有云供应商上运行的实例是否使用超过允许的限制的 CPU 硬件运行。



注意

您可以扩展 **哪些条件，可以定义？** 和/或 **查看可用的系统事实** 来查看您可以使用的条件说明，并查看可用的系统事实。本节是您可以使用的语法示例。

6. 单击 **Validate 条件**。
7. 验证条件后，点 **Next**。
8. 在 Trigger 操作页面中，点 **Add trigger action**。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以及打开电子邮件首选项。

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

您的新策略已创建。在系统检查中评估策略时，如果满足策略中的条件，策略会自动向帐户中的所有用户发送电子邮件，具体取决于其电子邮件首选项。

3.2. 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在运行过时的 RHEL 版本，并通知您它找到的内容。

流程

1. 在 Red Hat Hybrid Cloud Console 中，进入 Red Hat Enterprise Linux > Policies 。
2. 点击 **Create policy**。
3. 在 Create policy 页面中，根据需要点 **From scratch** 或 **As an existing Policy 副本**。请注意，**作为现有 Policy 选项的复制** 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 **Condition**。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会根据 RHEL 8.1 运行过时的操作系统版本。
8. 单击 **Validate 条件**，然后单击 **Next**。
9. 在 Trigger actions 页面中，点 **Add trigger actions** 并选择 **Email**。
10. 点击 **Next**。
11. 在 Review and activate 页面中，点切换开关激活策略并查看其详情。
12. 点 **Finish**。

您的新策略已创建。在系统检查中评估策略时，如果触发策略中的条件，策略服务会自动向帐户中的所有用户发送电子邮件，根据其电子邮件首选项。

3.3. 创建根据最新 CVE 检测存在安全漏洞的软件包版本的策略

您可以创建一个根据最新 CVE 检测到存在安全漏洞的软件包版本的策略，并通知您它找到的内容。

流程

1. 在 Red Hat Hybrid Cloud Console 中，进入 Red Hat Enterprise Linux > Policies 。
2. 点击 **Create policy**。
3. 在 Create Policy 页面中，根据需要点 **From scratch** 或 **As an existing Policy 副本**。请注意，**作为现有 Policy 选项的复制** 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 **Condition**。在这种情况下，输入 **facts.installed_packages 包含 ['openssh-4.5']**。此条件将检测系统是否仍然运行基于最新 CVE 的 **openssh** 软件包的漏洞版本。

8. 单击 **Validate 条件**，然后单击 **Next**。
9. 在 Trigger actions 页面中，点 **Add trigger actions** 并选择 **Email**。
10. 点击 **Next**。
11. 在 Review and activate 页面中，点切换开关激活策略并查看其详情。
12. 点 **Finish**。

您的新策略已创建。在系统检查中评估策略时，如果满足策略中的条件，策略会自动向帐户中的所有用户发送电子邮件，具体取决于其电子邮件首选项。

第 4 章 检查和管理策略

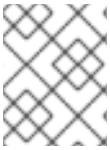
您可以通过导航到 Red Hat Enterprise Linux > Policies 来查看和管理所有创建的策略（启用和禁用）。

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

- 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，然后点击顶部的 **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

如果您看到有关未选择的电子邮件警报的警告消息，请将您的用户首选项设置为从您的策略接收电子邮件。

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

下表显示了在系统比较中使用的系统事实。

表 5.1. 系统事实和不功能

事实名称	描述	值示例
Ansible	带有 Ansible 相关事实列表的类别	controller_version 的值为 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。值包括 **google**、**azure**、**aws**、**alibaba** 或空	**google**
cores_per_socket	每个插槽的 CPU 内核数	2
cpu_flags	带有 CPU 标记列表的类别。每个名称都是 CPU 标记（例如： **vmx**），其值始终被 **启用**。	**vmx**，值为 **enabled**。
enabled_services	带有启用的服务列表的类别。类别中的每个名称是服务名称（例如： **crond**），其值始终被 **启用**。	**crond**，值为 **enabled**。
fqdn	系统完全限定域名	*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	值示例
installed_packages	已安装的 RPM 软件包列表。这是一个类别。	**Bash**，值为 **4.2.46-33.el7.x86_64**。
installed_services	带有已安装服务列表的类别。类别中的每个名称是服务名称（例如： **crond**），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；我们不比较系统间的引导时间。	**2019-09-18T16:54:56**
mssql	带有 MSSQL 相关事实列表的类别	mssql_version 的值为 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**、**状态 和类型**。两个地址字段是以逗号分隔的 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**、**loopback**、**bridge** 等等）。	
	每个接口（例如： **lo**、**em1** 等等）都作为事实名称作为前缀。例如，em1 的 mac 地址将是名为 **em1.mac_address** 的事实。	
	比较大多数网络接口事实以确保在系统间是相等的。但是，会检查 **ipv4_addresses**、**ipv6_addresses** 和 **mac_address**，以确保它们在系统之间有所不同。**lo** 的子接口应该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	内核发行版本	**8.1**
running_processes	运行的进程列表。事实名称是进程的名称，值为实例数。	**crond**，值为 **1**。

事实名称	描述	值示例
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	表示系统已注册到 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**
system_memory	以人类可读形式的系统内存总量	**3.45 GiB**
tuned_profile	当前从命令 **tuned-adm active**中生成的配置集	**desktop**
yum_repos	yum 软件仓库列表。存储库名称添加到事实的开头。每个存储库都有关联的 **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
布尔值 Operator	EQUAL
	注意QUAL

Operator	值
数字比较 Operator	GT
	GTE
	LT
	LTE
字符串 Compare Operator	CONTAINS
数组 Operator	IN
	CONTAINS
解析器 Operator	或者
	和
	非
	EQUAL
	注意QUAL
	CONTAINS
	NEG

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。