



Red Hat Insights 1-latest

使用 FedRAMP 的 Red Hat Insights 修复指南

使用补救 playbook 修复 RHEL 系统上的问题

Red Hat Insights 1-latest 使用 FedRAMP 的 Red Hat Insights 修复指南

使用补救 playbook 修复 RHEL 系统上的问题

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

在通过 FedRAMP[®] 注册了 Insights 的任何系统上创建 playbook 以修复问题。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 补救概述	3
1.1. RED HAT HYBRID CLOUD 控制台中的用户访问设置	3
第 2 章 在 INSIGHTS 中创建和管理补救 PLAYBOOK	4
2.1. 创建 PLAYBOOK 以修复 RHEL 系统上的 CVE 漏洞	4
2.2. 在 INSIGHTS FOR RED HAT ENTERPRISE LINUX 中管理补救 PLAYBOOK	8
第 3 章 使用补丁模板进行补救	11
3.1. 使用带有补救的补丁模板	11
对红帽文档提供反馈	12

第 1 章 补救概述

在 Red Hat Enterprise Linux (RHEL) 基础架构中识别最高补救优先级后，您可以创建修复 playbook 来解决这些问题。

订阅要求

- Red Hat Insights for Red Hat Enterprise Linux 都包括在每个 RHEL 订阅中。使用 Insights 修复功能不需要额外的订阅。

用户要求

- 所有 Insights 用户都会自动具有读取、创建和管理修复 playbook 的访问权限。

1.1. RED HAT HYBRID CLOUD 控制台中的用户访问设置

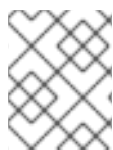
您的帐户中的所有用户都可以访问 Insights for Red Hat Enterprise Linux 中的大多数数据。

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. 补救用户的用户访问角色

Remediations Viewer 角色启用对 Insights for Red Hat Enterprise Linux 中的补救功能的标准或增强的访问。Remediations viewer 角色包含在 Default access 组中。Remediation viewer 角色允许访问查看帐户的现有 playbook 并创建新的 playbook。补救查看器无法在系统中执行 playbook。

第 2 章 在 INSIGHTS 中创建和管理补救 PLAYBOOK

创建 playbook 的工作流在 Insights for Red Hat Enterprise Linux 中的每个服务中类似。通常，您将修复系统或一组系统中的一个或多个问题。

Playbook 侧重于由 Insights 服务识别的问题。playbook 的建议做法是包括同一 RHEL 主/次版本的系统，因为解析将兼容。

2.1. 创建 PLAYBOOK 以修复 RHEL 系统上的 CVE 漏洞

在 Red Hat Insights 漏洞服务中创建补救 playbook。创建 playbook 的工作流与 Insights for Red Hat Enterprise Linux 中的其他服务类似。

先决条件

- 登录到 Red Hat Hybrid Cloud 控制台。



注意

创建修复 playbook 不需要增强的用户访问权限。

流程

1. 进入 [Security > Vulnerability > CVEs](#) 页面。
2. 根据需要设置过滤器并点击 CVE。
3. 向下滚动以查看受影响的系统。
4. 点击系统 ID 左侧的框选择要包含在修复 playbook 中的系统。



注意

包括同一 RHEL 主/次版本的系统，您可以通过过滤受影响系统列表来实现。

5. 点 **Remediate** 按钮。
6. 选择是否将补救 *添加到现有* 或 *新* playbook 中，并执行以下操作：
 - a. 单击 **Add to existing playbook**，然后从下拉列表中选择所需的 playbook，OR
 - b. 点 **Create new playbook** 并添加 playbook 名称。
 - c. 点 **Next**。
7. 检查 playbook 中包含的系统，然后单击 **Next**。
8. 查看 Remediation review summary 中的信息。
 - a. 默认情况下启用 **自动重新引导**。您可以通过单击 **关闭自动重新引导** 来禁用此选项。
 - b. 点 **Submit**。

验证步骤

1. 进入 [Automation Toolkit > Remediations](#)。
2. 搜索您的 playbook。您应看到您的 playbook。

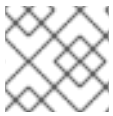
2.1.1. 当建议和备用解析选项存在时，创建 playbook 以修复带有安全规则的 CVE

Red Hat Insights for RHEL 中的大多数 CVE 都有一个补救选项，供您用来解决问题。使用安全规则修复 CVE 可能会包括推荐的多个解决方案，以及一个或多个备用解决方案。为具有一个或多个解析选项的 CVE 创建 playbook 的工作流与公告服务中的补救步骤类似。

有关安全规则的更多信息，请参阅 [安全规则](#)，并在 [RHEL 系统中评估和监控安全漏洞](#) 中的 [过滤公开给安全规则的系统列表](#)。

先决条件

- 登录到 Red Hat Hybrid Cloud 控制台。



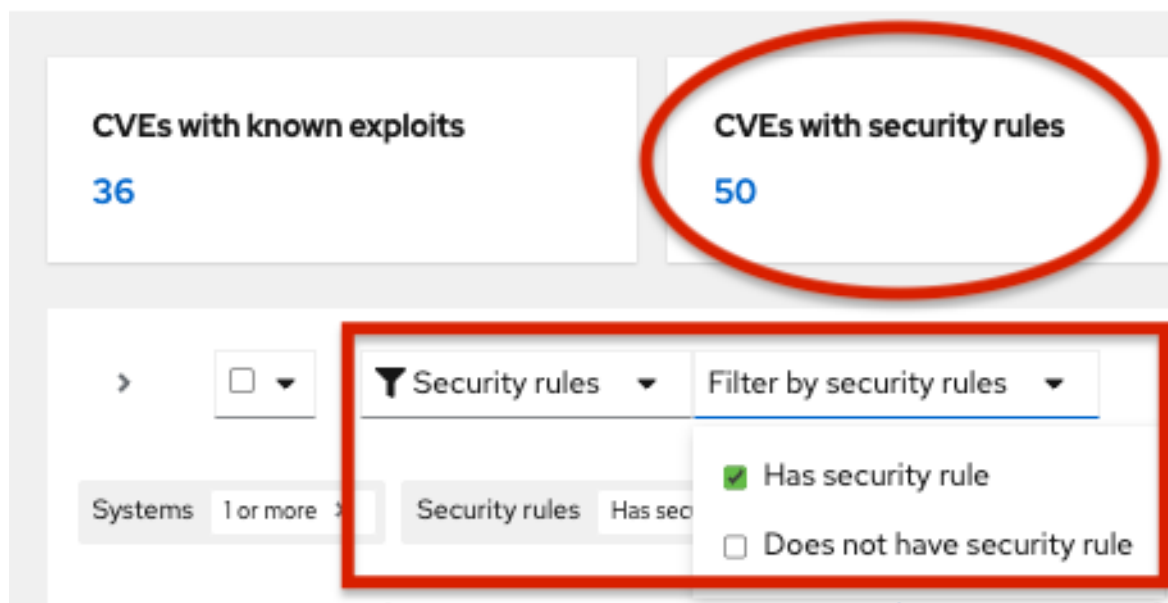
注意

您不需要增强用户访问权限来创建修复 playbook。

流程

1. 导航到 [Security > Vulnerability > CVEs](#)
2. 如果需要，设置过滤器（例如，过滤 [以查看带有安全规则的 CVE](#)），以专注于与其相关的风险的问题。或者，点带有横线上安全规则标题的 CVE。两个选项都显示在示例镜像中。

CVEs ?



3. 点列表中的 CVE。



- 滚动以查看受影响的系统，并通过点击 **Review systems** 页面上的系统 ID 左侧的框来选择您要包含在修复 playbook 中的系统 ID。（选择一个或多个系统可激活 Remediate 按钮。）



注意

推荐的： 通过过滤受影响系统列表来包括同一 RHEL 主版本或次版本的系统。

- 点 **Remediate**。
- 通过执行以下操作之一决定是否将补救添加到现有或新 playbook 中：
 - 选择 **Add to existing playbook**，然后从下拉列表中选择所需的 playbook，或者
 - 选择 **Create new playbook**，再添加一个 playbook 名称。在本例中，HCCDOC-392。
- 点击 **Next**。系统列表显示在屏幕上。
- 检查 playbook 中包含的系统（选择您不想包含的任何系统）。
- 点 **Next** 查看 **Review and edit actions** 页面，它显示了您修复 CVE 的选项。要修复的项目数量可能会有所不同。您还会看到有关 CVE 的额外信息（您可以扩展和折叠），例如：
 - action**：显示 CVE ID。
 - 解决方案**：显示 CVE 的推荐解决方案。显示您是否有备用解析选项。
 - 需要重启**：显示您必须重启您的系统。
 - 系统**：显示您要修复的系统数量。
- 在 **Review and edit actions** 页面中，选择以下两个选项之一来完成创建 playbook：
 - 选项 1：查看所有可用推荐和备用补救选项（并选择其中一个选项）：
 - 选择 **Review and/or 更改此 1 操作的解析步骤**，或根据您的实际选项类似。

Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 **Review and edit actions**
4 Remediation review

Review and edit actions

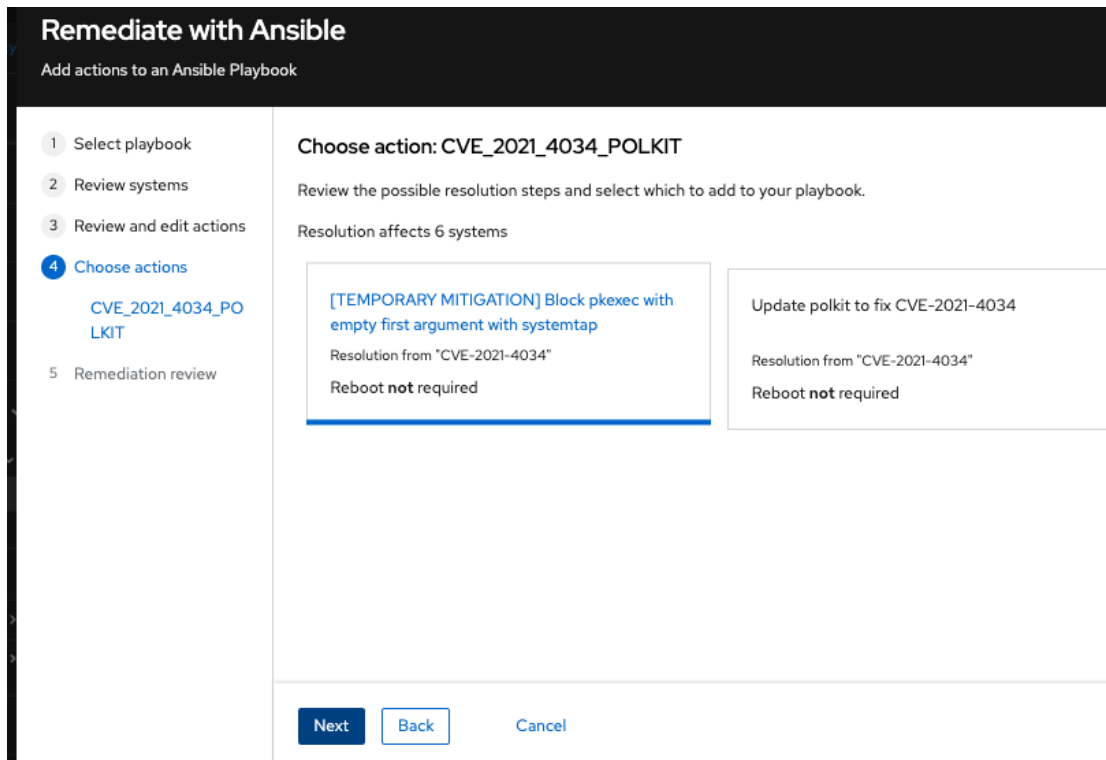
You have selected 1 item to remediate. 1 of 1 item allows for you to chose from multiple resolution steps.

Review and/or change the resolution steps for this 1 action.

Action	Resolution	Reboot required	Systems
> CVE-2021-4034	[TEMPORARY MITIGATION] Block pkexec with empty first argument with systemtap 1 alternate resolution	Not required	6

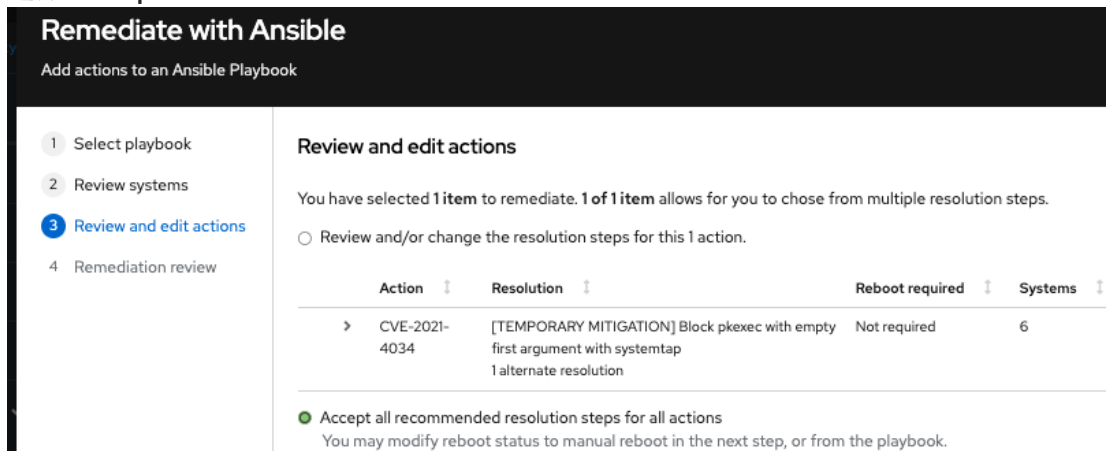
Accept all recommended resolution steps for all actions
You may modify reboot status to manual reboot in the next step, or from the playbook.

- 点击 **Next**。
- 在 **Choose action: <CVE information>** 页面中，点标题来选择您首选的补救选项。选择时标题的底部边缘。默认突出显示推荐的解决方案。



d. 点击 **Next**。

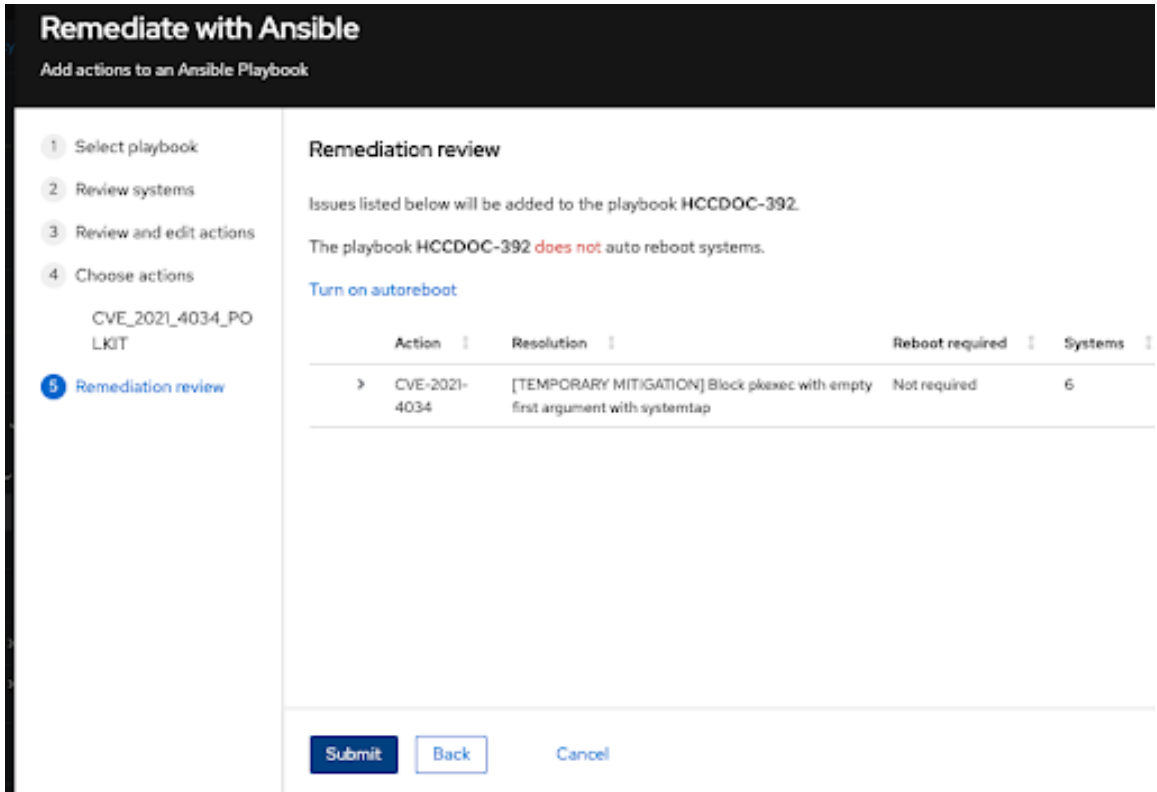
- 选项 2：接受所有推荐的补救：
 - 选择 **Accept all recommended resolutions all actions**。



11. 在 **Remediations 查看** 页面中查看有关自动重新引导系统的选择和更改选项的信息。该页面显示：

- 您添加到 playbook 的问题。
- 更改系统自动引导过程要求的选项。

- 有关修复它们的 CVE 和解决方案选项的摘要。



Remediate with Ansible
Add actions to an Ansible Playbook

1 Select playbook
2 Review systems
3 Review and edit actions
4 Choose actions
5 Remediation review

CVE_2021_4034_PO LKIT

Remediation review

Issues listed below will be added to the playbook HCCDOC-392.
The playbook HCCDOC-392 **does not** auto reboot systems.

[Turn on autoreboot](#)

Action	Resolution	Reboot required	Systems
> CVE-2021-4034	[TEMPORARY MITIGATION] Block plexec with empty first argument with systemtap	Not required	6

Submit Back Cancel

12. 可选。如果需要，在 **Remediation review** 页面中更改 autoreboot 选项。（默认启用自动重新引导，但根据您的补救选项，您的设置可能会有所不同。）
13. 点 **Submit**。显示通知显示添加到 playbook 中的补救操作数量，以及您的 playbook 的其他信息。

验证步骤

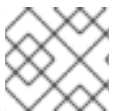
1. 进入 [Automation Toolkit > Remediations](#)。
2. 搜索您的 playbook。
3. 要运行（执行）您的 playbook，请参阅从 [Insights for Red Hat Enterprise Linux 执行修复 playbook](#)。

2.2. 在 INSIGHTS FOR RED HAT ENTERPRISE LINUX 中管理补救 PLAYBOOK

您可以为您的机构下载、归档和删除现有的修复 playbook。以下流程描述了如何执行常见的 playbook-management 任务。

先决条件

- 登录到 Red Hat Hybrid Cloud 控制台。



注意

无需查看、编辑或下载现有 playbook 的信息。

2.2.1. 下载补救 playbook

使用以下步骤从 Insights for Red Hat Enterprise Linux 应用程序下载修复 playbook。

流程

1. 进入 [Automation Toolkit > Remediations](#)。
2. 找到您要管理的 playbook，然后点 playbook 的名称。playbook 详情可见。
3. 点 **Download playbook** 按钮将 playbook YAML 文件下载到您的本地驱动器。

2.2.2. 归档补救 playbook

您可以归档不再需要的补救 playbook，但要保留的详情。


流程

1. 进入 [Automation Toolkit > Remediations](#)。
2. 找到您要归档的 playbook。
3. 点击选项图标（需要）并选择 **Archive playbook**。该 playbook 已存档。

2.2.3. 查看归档的补救 playbook

您可以在 Insights for Red Hat Enterprise Linux 中查看归档的补救 playbook。

流程

1. 进入 [Automation Toolkit > Remediations](#)。
2. 点击 Download playbook 按钮右侧的 **More options** 图标  并选择 Show archive playbook。

2.2.4. 删除补救 playbook

您可以删除不再需要的 playbook。

流程

1. 进入 [Automation Toolkit > Remediations](#)。
2. 找到并单击您要删除的 playbook 的名称。
3. 在 playbook 详情页面中，点 **More options** 图标  并选择 **Delete**。

2.2.5. 监控补救状态

您可以查看每个 playbook 的补救状态。状态信息告诉您最新活动的结果，并提供该 playbook 的所有活动的摘要。您还可以查看日志信息。

先决条件

- 登录到 Red Hat Hybrid Cloud 控制台。

流程

1. 进入 [Automation Toolkit > Remediations](#)。该页面显示补救 playbook 列表。
2. 点 playbook 的名称。
3. 在 **Actions** 选项卡中，单击 **Status** 列中的任何项目，以查看具有分辨率状态的弹出窗口。

要在 Satellite Web UI 中 [监控](#) playbook 的状态，请参阅 Red Hat Satellite [管理主机](#) 指南中的监控远程作业。

第 3 章 使用补丁模板进行补救

Red Hat Insights 补丁应用程序支持调度的补丁周期。

补丁模板不会影响主机上的 **yum/dnf** 操作，但它们允许您优化 Red Hat Insights 中的补丁状态报告。您可以使用模板为简单的补丁周期创建修复 playbook。

3.1. 使用带有补救的补丁模板

补丁模板可包含您要应用到多个系统的一个或多个补救方法。您可以创建一个补丁模板，在测试环境中更新一组系统，并使用同一补丁模板来更新生产环境中的系统。

有关创建和使用补救的补丁模板的更多信息，[请参阅使用修复 Playbook 的系统](#) 补丁。



注意

将补丁模板应用到您分配的系统后，您不会看到适用于这些系统的最近发布的公告。使用 Red Hat Hybrid Cloud Console 通知以确保您了解可能影响您基础架构的新发布的公告。

有关 Red Hat Hybrid Cloud Console 中的通知的更多信息，[请参阅使用 FedRAMP 在 Red Hat Hybrid Cloud Console 上配置通知](#)。

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。