Red Hat Trusted Application Pipeline 1.0

Red Hat Trusted Application Pipeline 1.0 发行注记

在此发行版本中探索新功能，并了解已知的问题。

Last Updated: 2024-07-02

Red Hat Trusted Application Pipeline 1.0 Red Hat Trusted Application Pipeline 1.0 发行注记

在此发行版本中探索新功能，并了解已知的问题。

法律通告

摘要

本文档提供有关 Red Hat Trusted Application Pipeline 1.0 中的最新功能和已知问题的信息。

目录

前言

Red Hat Trusted Application Pipeline 发行注记总结了新功能、功能增强、重要的技术更改、技术预览、错误修复、已知问题和其他相关公告或信息。

第 1 章 关于红帽受信任的应用程序管道

复杂的应用程序具有复杂的软件供应链，而较长的软件供应链是其受到各种攻击的安全漏洞。使用红帽受信任的应用程序 Pipeline (RHTAP)保护您的软件开发生命周期的每个阶段。RHTAP 可以通过安全 CI/CD 构建、测试、部署和监控源代码，并且其全面的安全工具可保护您的完整的软件供应链。

关键的 RHTAP 功能

- 从 Git 源代码持续构建、测试和部署容器镜像到内置开发环境。
- 随时可用的模板来开始学习和自定义。
- 将 Java、Python、Node、Go 或 npm 的应用构建到容器镜像中。
- 以您的自助服务开发人员门户身份访问 Red Hat Developer Hub。
- 生成、检查和管理您的软件资料清单(SBOM)。
- 使用 Tekton 链加密签名和 attest 容器镜像。
- 根据 40 多个规则，验证容器镜像 SLSA 合规性直到 3 级。
- 使用每个合并请求进行漏洞扫描，以识别和解决最早阶段的安全威胁。

谁是目标用户？

如果您是平台工程师、应用程序开发人员或安全团队成员，您将处于正确的位置。在 Red Hat Trusted Application Pipeline 中，您将找到安装、配置和自定义内部开发人员门户所需的一切内容，以便在开发生命周期中保护您的软件供应链。

它如何工作？

红帽受信任的应用程序管道(RHTAP)使您能够简化和保护整个 DevSecOps CI/CD 流程。

保护来自 onset 的开发

在 Red Hat Developer Hub 中安装并配置 RHTAP 后，访问预先构建的安全模板。只需选择适当的可用的软件模板，填写所需详情并创建新应用。这会创建一个专用的开发环境，其中包含您需要的所有内容：代码存储库和 GitOps 存储库、技术文档和持续集成/持续交付(CI/CD)管道。

整个开发生命周期的安全扫描

编辑源代码会触发应用程序中运行的管道运行。此管道确保每个构建工件都被签名，并进行测试以真实性。它还会扫描代码中的漏洞，并自动生成软件 Bills Materials (SBOMs)。这些 SBOM 详细介绍了容器镜像中包含的所有组件、库和依赖项，从而为您的应用程序提供完全透明的透明性。

review、Refine 和 Release

管道显示您检查和修复的任何识别的漏洞。您还可以查看 SBOM 以深入了解应用程序的组件。根据您的促销工作流，您可以通过开发、暂存和最终投入生产来推进应用程序。每个提升都会触发另一个管道运行，扫描漏洞并强制实施您的企业合同(EC)。EC 确保容器镜像在发布前满足预定义的质量和安全标准。如果镜像无法满足这些条件，则 EC 会发出确定所需更正的详细报告。

这种通过 RHTAP 的简化方法使开发人员能够专注于创新，同时在开发生命周期中占据最高安全标准。

要更好地了解 RHTAP 的工作原理，请查看以下关于支持以及 RHTAP 支持的各种组件和技术的描述性列表。

表 1.1. RHTAP 技术和组件

组件和技术	描述
Red Hat Developer Hub	RHDH 可让您访问用于安全软件开发的无数资源和工具，因此，使用 RHTAP 入门非常精简且简单。RHDH 鼓励最佳实践，并促进从开发流程非常开始的安全措施集成。
Red Hat Trusted Artifact Signer	RHTAS 通过确保您的每个代码和所有工件都已签名并进行测试，从而增强了软件的完整性。RHTAS 提供可验证的信任链，以确认您的所有软件组件都已保护和身份验证。
Red Hat Trusted Profile Analyzer	RHTPA 自动创建您的软件清单(SBOM)。SBOM 对于维护软件供应链透明性和合规性至关重要，因为它们提供了软件产品中包含的所有组件、库和依赖项的详细列表。当您使用 RHTPA 生成和管理 SBOM 时，您确保所有利益相关者都有有关软件构成的准确和当前信息。
OpenShift	RHTAP 将 OpenShift Container Platform (OCP)集群用于计算资源。OCP 还包括一个控制台，它提供各种服务来标准化工作流，并更容易安全地管理整个开发生命周期。
GitHub	RHTAP 会根据拉取请求(PR)中的管道定义自动启动构建。您还可以根据检查 API 查看 PR 测试反馈，并在成功测试后，您可以将 PRs 设置为 automerge。
Argo CD	GitOps 中的 Argo CD 声明和控制应用程序定义、配置和环境的版本，并自动化和跟踪应用程序部署和生命周期管理。
Tekton 构建管道	使用 RHTAP 构建时，您可以将完整的 Tekton 构建管道存储在存储库中。
Tekton Chains	RHTAP 可以使用 Tekton Chains 在测试时生成签名的构建管道。

其他资源

- 有关 RHTAP 入门的更多信息，请参阅开始使用 Red Hat Trusted Application Pipeline。
- 有关 Red Hat Developer Hub 的更多信息，请参阅 Red Hat Developer Hub 1.1 的产品文档 。
- 有关红帽受信任的工件签名程序的更多信息，请参阅 Red Hat Trusted Artifact Signer Deployment 指南。
- 有关红帽受信任的配置文件分析器的更多信息，请参阅 Red Hat Trusted Profile Analyzer 的产品文档。
- 如需有关 OpenShift 的更多信息，请参阅 OpenShift。

- 有关 Argo CD 的更多信息，请参阅 Argo CD。
- 有关 Tekton 构建管道的更多信息，请参阅 Tekton 构建管道。
- 有关 Tekton 链的更多信息，请参阅 Tekton 链。

第 2 章 兼容性和支持列表

Red Hat Trusted Application Pipeline 或 RHTAP 在 OpenShift Container Platform 上安装。

产品	Version
OpenShift Container Platform	4.15, 4.14, 4.13

RHTAP 在安装过程中安装以下产品和组件：

安装了 RHTAP 的产品	Version
Red Hat Developer Hub	1.1.x
Red Hat Trusted Artifact Signer	1.0.x
Red Hat Trusted Profile Analyzer	1.0.0
OpenShift Pipelines	1.14.x
OpenShift GitOps	1.12.x

RHTAP 也与以下产品或组件集成，以帮助保护您的软件供应链：

产品	Version
Red Hat Advanced Cluster Security	4.3
Quy	3.10

第 3 章 已知问题

- 由于 RHTAP SecureSign 的已知问题，安装可能会失败。要恢复，只需删除已将 RHTAP （默认为**rhtap**）部署到的命名空间，然后重新运行安装程序。在第二次运行时，安装应该可以成功。

- 您可以在您为安装的 **private-values.yaml** 文件中将 GitLab 配置为身份验证供应商。但是，配置了 GitLab 后，它仍然不会显示为登录选项。GitLab 的登录可在设置页面 < **host>/settings/auth-providers** 中访问，但需要登录到 GitHub 以访问该页面。

- **pull-request** 管道通常会失败并显示 **build-container** 任务，并显示以下出错信息： **Access to the requested resource is not authorized**。要解决这个问题，将容器镜像推送到 Quay.io，然后再次运行管道。

- 在提升应用程序时，**verify-enterprise-contract** 任务当前失败。但是，要解决这个问题，您只需要删除 Rekor 自定义资源(CR)。然后，启动一个新的 Rekor CR，但任务不再会失败。使用以下方法之一删除 CR：

  - 在命令行中删除 Rekor CR。
    oc delete rekor -n $<namespace where rhtap is installed> rhtap-securesign

  - 在 OCP 控制台中，在 **Admin** 视图中，单击 **Home** 选项卡下的 **Search**。在 **rhtap** 命名空间中搜索 "Rekor"，并删除找到的 CR 实例。

- 当您从 Go 或 Python 软件模板将新容器镜像提升到 RHTAP 阶段环境时，您将运行 **verify-enterprise-contract** 步骤。此步骤可能会导致以下错误： **不测试与给定公钥匹配的镜像。**您必须手动更新镜像存储库，使其变为公共存储库。

- RHTAP 1.0 不支持以下环境：任何 air-gapped 环境、IBM Power Platform、IBM Z Platform、ARM64 和联邦信息处理标准(FIPS)模式 OCP。

- 目前不支持卸载 RHTAP，但可以通过从集群中删除所有 RHTAP 命名空间来完成。

更新于 2024-07-02