Red Hat Trusted Application Pipeline 1.0

Release notes for Red Hat Trusted Application Pipeline 1.0

Explore new features in this release and learn about known issues.

Last Updated: 2024-07-01

Red Hat Trusted Application Pipeline 1.0 Release notes for Red Hat Trusted Application Pipeline 1.0

Explore new features in this release and learn about known issues.

Legal Notice

Abstract

This document provides information about the latest features and known issues in Red Hat Trusted Application Pipeline 1.0.

Table of Contents

PREFACE

The release notes for Red Hat Trusted Application Pipeline summarize new features and enhancements, notable technical changes, features in Technology Preview, bug fixes, known issues, and other related advisories or information.

CHAPTER 1. ABOUT RED HAT TRUSTED APPLICATION PIPELINE

Sophisticated applications have complex software supply chains, and the longer a software supply chain is, the more vulnerable it is to attacks of all kinds. Secure every phase of your software development lifecycle with Red Hat Trusted Application Pipeline (RHTAP). RHTAP can build, test, deploy, and monitor your source code with secure CI/CD, and its comprehensive set of security tools protects your complete software supply chain.

Key RHTAP features

- Continuously build, test, and deploy container images from your Git source code to a built-in development environment.
- Ready-to-use templates to start learning and customizing right away.
- Build Java, Python, Node, Go, or npm-based apps into container images.
- Access to Red Hat Developer Hub as your self-serve developer portal.
- Generate, check, and manage your software bill of materials (SBOM).
- Cryptographically sign and attest container image provenance with Tekton chains.
- Verify container image SLSA compliance up to level 3, against more than 40 rules.
- Vulnerabilities scanning with each merge request to identify and address any security threats at the earliest stage possible.

Who's the target user?

If you're a platform engineer, application developer, or security team member, you're in the right place. In Red Hat Trusted Application Pipeline, you'll find everything you need to install, configure, and customize the internal developer portal to secure your software supply chain across the development lifecycle.

How does it work?

Red Hat Trusted Application Pipeline (RHTAP) empowers you to streamline and secure your entire DevSecOps CI/CD process.

Secure development from the onset

Once RHTAP is installed and configured, access pre-built, secure templates within Red Hat Developer Hub. Simply select the appropriate ready-to-use software template, fill in the necessary details, and create a new application. This creates a dedicated development environment that includes everything you need: a code repository (source code and GitOps repositories), technical documentation, and a continuous integration/continuous delivery (CI/CD) pipeline.

Security scans throughout the development lifecycle

Editing the source code triggers a pipeline run within your application. This pipeline ensures every build artifact is signed and attested for authenticity. It also scans for vulnerabilities in your code and automatically generates Software Bills of Materials (SBOMs). These SBOMs detail all components, libraries, and dependencies included in the container image, providing complete transparency into your application's makeup.

Review, Refine, and Release

The pipeline presents any identified vulnerabilities for your review and remediation. You can also review the SBOM to gain a deeper understanding of your application's components. Depending on your promotional workflow, you might advance your application through development, staging, and finally to production. Each promotion triggers another pipeline run, scanning for vulnerabilities and enforcing your Enterprise Contract (EC). The EC ensures that container images meet predefined quality and security standards before release. Should an image fail to meet these criteria, the EC issues a detailed report identifying the necessary corrections.

This streamlined approach with RHTAP allows developers to focus on innovation while upholding the highest security standards throughout the development lifecycle.

To better understand how RHTAP works, take a look at the following descriptive list of the various components and technologies that support and are supported by RHTAP.

Table 1.1. RHTAP technologies and components

Components and technologies	Description
Red Hat Developer Hub	RHDH gives you access to countless resources and tools for secure software development, so getting started with RHTAP is streamlined and straightforward. RHDH encourages best practices and facilitates the integration of security measures from the very start of your development process.
Red Hat Trusted Artifact Signer	RHTAS enhances software integrity by making sure every piece of your code and all of your artifacts are signed and attested. RHTAS provides a verifiable trust chain to confirm that all of your software components are safeguarded and authentic.
Red Hat Trusted Profile Analyzer	RHTPA automates the creation of your software bill of materials (SBOM). SBOMs are critical for maintaining software supply chain transparency and compliance because they provide a detailed list of all components, libraries, and dependencies included in a software product. When you use RHTPA to generate and manage your SBOM, you're making sure that all of your stakeholders have accurate and current information about the composition of your software.
OpenShift	RHTAP uses an OpenShift Container Platform (OCP) cluster for compute resources. OCP also includes a console, which offers various services to standardize workflows and make it easier to securely manage the entire development lifecycle.
GitHub	RHTAP automatically starts a build according to the pipeline definition in your pull request (PR). You can also view PR test feedback according to the checks API, and after successful tests, you can set up your PRs to automerge.

Components and technologies	Description
Argo CD	Argo CD from GitOps declares and controls versions of your app definitions, configurations, and environments, and automates and tracks app deployment and lifecycle management.
Tekton build pipeline	When you build with RHTAP, you store a complete Tekton build pipeline in your repository.
Tekton Chains	RHTAP can use Tekton Chains to produce a signed build pipeline attestation.

Additional resources

- For more information about getting started with RHTAP, see Getting Started with Red Hat Trusted Application Pipeline.
- For more information about Red Hat Developer Hub, see Product Documentation for Red Hat Developer Hub 1.1.
- For more information about Red Hat Trusted Artifact Signer, see Red Hat Trusted Artifact Signer Deployment guide.
- For more information about Red Hat Trusted Profile Analyzer, see Product Documentation for Red Hat Trusted Profile Analyzer.
- For more information about OpenShift, see OpenShift.
- For more information about Argo CD, see Argo CD.
- For more information about Tekton build pipelines, see Tekton build pipeline.
- For more information about Tekton Chains, see Tekton Chains.

CHAPTER 2. COMPATIBILITY AND SUPPORT MATRIX

Red Hat Trusted Application Pipeline, or RHTAP, installs on OpenShift Container Platform.

Product	Version
OpenShift Container Platform	4.15, 4.14, 4.13

RHTAP installs the following products and components during installation:

Products installed with RHTAP	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 also integrates with the following products or components to help protect your software supply chain:

Product	Version
Red Hat Advanced Cluster Security	4.3
Quay	3.10

CHAPTER 3. KNOWN ISSUES

- Installation might fail due to a known issue with RHTAP SecureSign. To recover, simply delete the namespace into which you've deployed RHTAP (**rhtap** by default) and rerun the installer. On the second run, the installation should be successful.

- You can configure GitLab as an authentication provider in the **private-values.yaml** file you create for installation. However, once GitLab is configured, it still doesn't show up as a sign in option. The login for GitLab is accessible in the settings page, **<host>/settings/auth-providers**, but requires signing in to GitHub to access that page.

- The **pull-request** pipeline often fails with the **build-container** task and displays the following error message: **Access to the requested resource is not authorized**. To fix this, push your container image to Quay.io and run the pipeline again.

- When promoting applications, the **verify-enterprise-contract** task currently fails. However, to fix this issue, you simply need to remove the Rekor custom resource (CR). A new Rekor CR then starts up, but the task no longer fails. Remove the CR with one of the following methods:

    - Delete the Rekor CR in your command line.
      oc delete rekor -n $<namespace where rhtap is installed> rhtap-securesign

    - In the OCP console, in the **Admin** view, click on **Search** under the **Home** tab. Search for "Rekor" in the **rhtap** namespace, and delete the instance of the CR that you find.

- When you promote a new container image to the RHTAP stage environment from a Go or Python software template, you run the **verify-enterprise-contract** step. This step might cause the following error: **No image attestations found matching the given public key.** You must manually update the image repository so that it's public.

- RHTAP 1.0 does not support the following environments: any air-gapped environment, IBM Power Platform, IBM Z Platform, ARM64, and Federal Information Processing Standards (FIPS) mode OCP.

- Uninstallation of RHTAP is not currently supported, but it can be done by removing all RHTAP namespaces from the cluster.

Revised on 2024-07-01 13:32:22 UTC