



Red Hat Trusted Artifact Signer 1.0

发行注记

Red Hat 的 Trusted Artifact Signer 1.0.2 发行注记

Red Hat Trusted Artifact Signer 1.0 发行注记

Red Hat 的 Trusted Artifact Signer 1.0.2 发行注记

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

欢迎使用 Red Hat Trusted Artifact Signer's official release notes for version 1.0.2!本发行注记介绍了为 Red Hat Trusted Artifact Signer 1.0.2 软件发行版本实现的新功能、增强功能、已知问题、错误修复和弃用。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 简介	3
第2章 新功能及功能增强	4
第3章 程序错误修复	6
第4章 已知问题	8
第5章 过时的功能	9

第 1 章 简介

红帽的可信工件签名(RHTAS)服务通过简化加密签名和验证软件工件（如容器镜像、二进制文件和 Git 提交）来提高软件供应链安全性。受信任的 Artifact Signer 提供 [SecureSign 社区项目](#) 的生产就绪部署。

Trusted Artifact Signer 软件发行注记记录了最新版本的 1.0.2 的新功能、功能增强、错误修复和已知问题。我们将最新的项目添加到各章节的顶端，因为我们在主要版本和次要版本的生命周期上建立官方发行说明。

Red Hat Trusted Artifact Signer 文档位于 https://access.redhat.com/documentation/zh-cn/red_hat_trusted_artifact_signer/1。

第 2 章 新功能及功能增强

此 Red Hat Trusted Artifact Signer (RHTAS) 发行版本中引入的所有主要改进和新功能的列表。

这个版本添加的功能和增强有：

企业合同支持检查容器镜像的多个架构类型

在这个版本中，企业合同(EC)现在支持工件验证，以及对容器镜像的多个架构类型的策略强制。**ec validate image** 命令可以检查各个来自镜像索引的系统架构的容器镜像。

使用命令行参数添加规则数据

在这个版本中，您可以使用 **-- extra-rule-data** 参数在命令行中为 **ec validate image** 命令注入额外的规则数据。例如，您可以使用它来影响策略，以便发行版本管道的行为可能与持续集成和持续交付(CICD)管道中的行为不同。

验证容器镜像时企业合同的新报告格式

在这个版本中，**ec validate image** 命令可以生成新的报告格式。您可以将 **-- output 文本** 参数与 **ec validate image** 命令一起使用，以生成新的用户友好的输出格式。这个新报告格式只提供有关违反情况和警告的详情。要查看其他详情，请使用 JSON 或 YAML 格式。

支持 OpenShift 4.16 和 4.17

在这个版本中，我们添加了对在 OpenShift Container Platform 4.16 和 4.17 上运行的 Trusted Artifact Signer 服务的支持。客户可以在当前支持的 OpenShift Container Platform 版本中从 OperatorHub 安装 RHTAS Operator。

确认页面的 auto-closing

在这个版本中，我们将 **gitsign** 二进制文件更新至 0.10.2 版本。此版本为 Sigstore 确认页面启用 auto-closing 功能。身份验证成功后，确认页面将在 10 秒内关闭。

将 Trusted Artifact Signer 安装到同一 OpenShift 集群中的不同命名空间

在这个版本中，您可以在同一 OpenShift 集群中的不同命名空间中安装 RHTAS 服务。

升级的新发行频道

在这个版本中，我们添加了用户可以订阅的 **stable-v1.0** 频道。订阅此频道会让用户自动升级到 1.0.x 发行行。要接收所有即将发布的次发行版本的最新更新，然后订阅 **stable** 频道。另外，在这个版本中，我们删除了 **alpha** 频道。

Trillian 监控

在这个版本中，您可以为 Trillian 服务器启用监控。要启用监控，请在 **trillian** 小节下添加 **monitoring** 小节，并将 **Securesign** 实例的 **enabled** 设置为 **true**。例如：

```
...
  trillian:
    monitoring:
      enabled: true
  ...
```

启用监控后，您可以通过展开导航菜单中的 **Observe** 来查看和查询从 OpenShift Web 控制台收集的指标，然后点 **Metrics**。

监控证书转换日志

在这个版本中，您可以为证书转换日志(CTlog)服务器启用监控。要启用监控，请在 **ctlog** 小节下添加 **monitoring** 小节，并将 *Securesign* 实例的 **enabled** 设置为 **true**。例如：

```
...
  ctlog:
    monitoring:
      enabled: true
...
```

启用监控后，您可以通过展开导航菜单中的 **Observe** 来查看和查询从 OpenShift Web 控制台收集的指标，然后点 **Metrics**。

对片段备份作业的改进

在这个版本中，Trusted Artifact Signer 服务对片段备份作业有几个改进。由于现有漏洞，片段备份作业已在 Python 中重写，并验证集群级别的指标是否被允许。

第 3 章 程序错误修复

在此 Red Hat Trusted Artifact Signer (RHTAS) 发行版本中，我们修复了以下错误：除了这些修复外，我们列出了之前在我们修复的早期版本中发现的问题的描述。

检测 OpenShift 环境时对 operator 逻辑的更新

在 OpenShift 集群重启期间，T RHTAS 操作器逻辑用于检测 OpenShift 环境是不可靠的。Operator 会错误地认为它在非 OpenShift 环境中运行，并错误地配置了系统。这会导致 API 不可用，Trillian 数据库 pod 无法启动。这也会导致 OpenShift 安全性上下文约束(SCC)违反。

在这个版本中，我们删除了 RHTAS 操作器中的 OpenShift 环境的动态检测。在安装 RHTAS operator 期间，必须使用新的 **OPENSHIFT** 环境变量明确配置目标环境。这样做可确保 RHTAS 操作器一致应用于部署的正确配置。使用 Operator Lifecycle Manager (OLM) 部署 RHTAS 操作器，默认情况下将 **OPENSHIFT** 环境变量设置为 **true**。因此，RHTAS 操作器一致配置系统，从而防止重新启动服务启动问题，不再违反 OpenShift SCC。

企业合同速度更快且效率更高

在此次更新之前，企业合同(EC)将从配置的源下载策略和策略数据，以验证每个组件。这会导致 **ec validate image** 命令通过下载超过所需数据来运行更长。在本发行版本中，当 **ec validate image** 命令检测到相同的策略源来验证不同的容器镜像时，它不再会多次下载策略数据。

Operator 在 nil pointer 异常上终止

当 **fulcio.spec.privateKeyPasswordRef** 的 Certificate Transparency 日志'(CTlog)密码被错误设置时，RH RHTAS operator 会终止且没有有意义的错误消息。在这个版本中，我们为此场景添加了更强大的错误处理，并在未正确设置 CTlog 时更有意义的 operator 错误消息。

Fulcio 证书的常见名称错误

sigstore.issuer 字段被硬编码为使用 **spec.certificate.commonName** 中指定的通用 name 值用于 Fulcio 证书。在这个版本中，我们添加了相应的逻辑来正确设置 **sigstore.issuer** 字段。如果 **spec.certificate.commonName** 为空，则我们根据 **spec.externalAccess.host** 值设置 **sigstore.issuer**。如果 **spec.certificate.commonName** 和 **spec.externalAccess.host** 为空，则将 **sigstore.issuer** 设置为 OpenShift 集群的域名。因此，我们为 Fulcio 证书正确设置了通用名称。

从 Operator 中删除了 kube-rbac-proxy

弃用了 **kube-rbac-proxy** 的 **--tls-cert-file** 和 **--tls-private-key-file** 标志后，我们在安装 RHTAS operator 时删除了基于角色的访问控制(RBAC) HTTP 代理资源。因此，您需要在 Operator 命名空间中有一个预定义的证书和私钥。默认 operator 命名空间为 **openshift-operators**。因此，我们不再使用此 RBAC HTTP 代理资源来保护 Operator 控制器的 **/metrics** API 端点。

默认启用 Rekor 搜索 UI

在这个版本中，不再需要用户手动安装 Rekor 搜索用户界面(UI)。我们默认启用 Rekor 搜索 UI。

CreateTree 任务在安装失败后继续运行

删除然后重新安装 RHTAS 服务时，**CreateTree** 任务在某些情况下可能会持续运行，从而防止后续安装成功。在这个版本中，如果 RHTAS 安装过程检测到运行 **CreateTree** 任务，则它会清理该任务，而无需用户干预。如需了解更多详细信息，请参阅 [GitHub 问题 #230](#)。

将 kube-rbac-proxy 的上游版本替换为支持的版本

Red Hat Trusted Artifact Signer 1.0 附带的 Role-base 访问控制(RBAC)代理容器 **gcr.io/kubebuilder/kube-rbac-proxy**。在这个版本中，我们使用官方支持的红帽版本 **registry.redhat.io/openshift4/ose-kube-rbac-proxy** 替换上游版本。

当没有足够的内存可用时，可信 Artifact Signer operator 可能会崩溃

在安装 RHTAS 运算符期间，如果未分配足够的内存，这会导致 **CrashLoopBackoff** 状态。此崩溃会阻止 RHTAS 操作器正确安装。

在这个版本中，增加了 RHTAS 运算符的内存分配，允许它成功安装。

缺少企业合同二进制下载

当用户试图下载企业合同(EC)二进制文件时，他们会收到 404 页面。因为 Windows 的 EC 二进制文件的路径被错误设置，所以会生成 404 页面。在这个版本中，Windows 的 EC 二进制文件的路径被正确设置，不再提供 404 页面。

cosign Windows 可执行文件缺少 .exe 扩展

下载二进制文件时，Windows 的 **cosign** 二进制文件缺少 **.exe** 文件名扩展。缺少 **.exe** 文件扩展名不允许在 Windows 上运行 **cosign** 二进制文件。在这个版本中，**cosign** 二进制文件具有 **.exe** 文件名扩展名，并在 Windows 上按预期运行。

升级 Trusted Artifact Signer operator 的技术预览版本失败

在以前的版本中，RHTAS 运算符的技术预览版本(0.0.2)会自动升级到正式发布的版本(1.0.0)，从而导致升级失败。如果 *Securesign* 实例及其自定义资源(CR)已存在，则从技术预览版本升级不再会失败。

片段备份作业的集群权限

在以前的版本中，负责收集 Rekor 和 Fulcio 指标的片段备份服务帐户的基于角色的访问控制(RBAC)错误配置已提升了权限。启用片段备份作业时，这些升级的权限可能会读取集群范围的 `secret`。

在这个版本中，我们通过限制网段备份服务帐户的特权来解决错误配置。现在，我们默认启用这些指标的收集。

第 4 章 已知问题

以前已解决的已知问题：

- [片段备份作业的集群权限](#)
- [升级 Trusted Artifact Signer operator 的技术预览版本失败](#)

此 Red Hat Trusted Artifact Signer (RHTAS)中发现的已知问题列表：

Rekor Search UI 不会在升级后显示记录

将 RHTAS 运算符升级到最新版本(1.0.1)后，通过电子邮件地址搜索时不会发现现有的 Rekor 数据。**backfill-redis** CronJob，可确保 Rekor Search UI 在午夜仅查询透明度日志运行一次。要解决这个问题，您可以手动触发 **backfill-redis** 作业，而不是等到午夜为止。

要从命令行界面触发 **backfill-redis** 作业，请运行以下命令：

```
oc create job --from=cronjob/backfill-redis backfill-redis -n trusted-artifact-signer
```

这样做会将缺少的数据重新添加到 Rekor Search UI 中。

OpenShift 4.13 中会错误地报告版本号

在 OpenShift Container Platform 4.13 上安装 RHTAS Operator 会错误地显示 0.0.2 版本（当实际安装版本 1.0.1 时）。目前，还没有临时解决方案来解决这个问题。

第 5 章 过时的功能

有关此 Red Hat Trusted Artifact Signer 发行版本中已弃用功能的概述。

弃用 Red Hat Trusted Artifact Signer 软件堆栈的 Helm 部署

在这个版本中，红帽使用 Helm chart 弃用红帽受信任的工件签名产品的部署。不再支持使用 Helm 部署 Trusted Artifact Signer。