



# Red Hat Trusted Application Pipeline 1.0

## 使用红帽受信任的配置文件分析器检查 SBOM

了解如何扫描 SBOM，以获取有关应用程序安全状态的可操作信息。



## Red Hat Trusted Application Pipeline 1.0 使用红帽受信任的配置文件分析器 检查 SBOM

---

了解如何扫描 SBOM，以获取有关应用程序安全状态的可操作信息。

## 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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

本文档提供有关如何查看 SBOM 以获取有关应用程序安全状态的可操作信息。

## 目录

前言 .....	3
第1章 下载、转换和分析 SBOM .....	4



---

## 前言

当红帽受信任的应用程序管道构建应用程序镜像时，它还提供软件材料清单(SBOM)。SBOM 列出镜像使用的所有软件库。您可以使用 SBOM 来识别安全漏洞。

但是，SBOM 较长且难以阅读。要将原始 SBOM 转换为可操作的信息，您可以使用受信任的配置文件分析器(TPA)。例如，TPA 可以识别您的镜像中的依赖项，这些依赖项是已知常见漏洞和漏洞(CVE)的目标。

## 第 1 章 下载、转换和分析 SBOM

以下流程解释了如何使用 TPA 检查 SBOM。具体来说，它概述了如何下载 SBOM，将 SBOM 转换为兼容格式，并使用 TPA 分析 SBOM。

### 先决条件

- [Cosign](#)
- [Syft](#)
- [jq](#)

### 流程

1. 在容器 registry 中，找到要检查的 SBOM 容器镜像的完整地址。该地址的格式是 registry/namespace/image:tag。例如：quay.io/app/app-image:ff59e21cc...



#### 注意

不要使用 SBOM 镜像的地址，该镜像以 **.sbom** 结尾。将镜像的地址用于实际应用。

2. 在 CLI 中，使用 cosign 下载 SBOM。将输出重定向到您可以稍后参考的文件。确保新文件名以 **.json** 结尾。

```
cosign download sbom quay.io/redhat/rhtap-
app:8d34c03188cf294a77339b2a733b1f6811263a369b309e6b170d9b489abc0334 >
/tmp/sbom.json
```

3. (可选) 您的 SBOM 最终会出现在 TPA UI 中，并在此 .json 文件中列出的名称。默认情况下，Syft 根据 SBOM 的文件路径创建该名称。如果您希望 SBOM 出现在 TPA UI 中，且具有更有意义的名称，则必须在您刚刚下载的 .json 文件中手动更改它。具体来说，您必须替换 **.metadata.component** 对象中的名称。如果需要，您可以选择在此处添加 **version** 字段。

```
$ vim /tmp/sbom.json
"component": {
  "bom-ref": "fdef64df97f1d419",
  "type": "file",
  "name":
"/var/lib/containers/storage/vfs/dir/3b3009adcd335d2b3902c5a7014d22b2beb6392b1958f1d9c
7aabe24acab2deb" #Replace this with a meaningful name
}
```

4. 运行以下命令，将 Bombastic API URL 存储为环境变量。

```
$ bombastic_api_url="https://$(oc -n rhtap get route --selector
app.kubernetes.io/name=bombastic-api -o jsonpath='{.items[].spec.host}')
```



#### 注意

在此命令和下一个命令（在 **-n** 之后），请务必输入安装 RHTAP 的命名空间。示例假设您使用了名为 **rhtap** 的命名空间。



5. 在 CLI 中，使用以下值创建新的 `token_issuer_url` 环境变量：

```
$ token_issuer_url=https://$(oc -n rhtap get route --selector
app.kubernetes.io/name=keycloak -o
jsonpath='{.items[].spec.host}')/realms/chicken/protocol/openid-connect/token
```

6. 接下来，您需要设置 `TPA__OIDC__WALKER_CLIENT_SECRET` 环境变量。如果您在安装 RHTAP 时可以访问您机构生成的 `private.env` 文件，则只需提供该文件即可。如果您无法访问该文件，请咨询谁安装了 RHTAP，以为您提供 TPA OIDC Walker 客户端 secret。
- a. 如果可以访问 `private.env` 文件：

```
$ source private.env
```

- b. 或者，一旦从其安装了 RHTAP 中获取了 secret：

```
$ TPA__OIDC__WALKER_CLIENT_SECRET=<secret value>
```

7. 运行以下命令，以获取 BOMBastic API 的令牌。令牌允许您上传 SBOM。

```
$ tpa_token=$(curl \
-d 'client_id=walker' \
-d "client_secret=$TPA__OIDC__WALKER_CLIENT_SECRET" \
-d 'grant_type=client_credentials' \
"$token_issuer_url" \
| jq -r .access_token)
```

8. 尝试上传 SBOM。

```
curl \
-H "authorization: Bearer $tpa_token" \
-H "transfer-encoding: chunked" \
-H "content-type: application/json" \
--data @/tmp/sbom.json \
"$bombastic_api_url/api/v1/sbom?id=my-sbom"
```

- a. 如果您收到 **错误消息存储错误：无效的存储内容**，请使用 Syft 将 SBOM 转换为早期 CycloneDX 1.4。您可以忽略有关将软件包与不同 pURL 合并的警告；它们表示 Syft 可能会丢失原始 SBOM 中的一些数据，但这些数据并不重要。

```
$ syft convert /tmp/sbom.json -o cyclonedx-json@1.4=/tmp/sbom-1-4.json
```

- b. 然后尝试再次上传 SBOM：

```
$ curl \
-H "authorization: Bearer $tpa_token" \
-H "transfer-encoding: chunked" \
-H "content-type: application/json" \
--data @/tmp/sbom-1-4.json \
"$bombastic_api_url/api/v1/sbom?id=my-sbom"
```

9. 通过 OpenShift 控制台访问运行 RHTAP 的集群。

10. 在 `rhtap` 项目中，进入到 `Networking > Routes`。打开与 `spog-ui` 服务相同的行中列出的 URL。

11. 使用 Register 按钮创建新帐户并向 TPA 进行身份验证。
12. 选择 SBOM（最新的上传），并根据 SBOM 查看有关您的应用程序提供的 insights TPA。
  - a. 进入 Dependency Analytics Report 选项卡，以查看漏洞和补救。

#### 其他资源

- 本文档的部分内容基于 [SBOM 的信任文档](#)。

更新于 2024-07-02