Special Interest Group Software Supply Chain

Supply Chain Security Journey for Jenkins X - Now and Beyond

JENKINS X

CD.FOUNDATION

25th Aug 2022

Topics

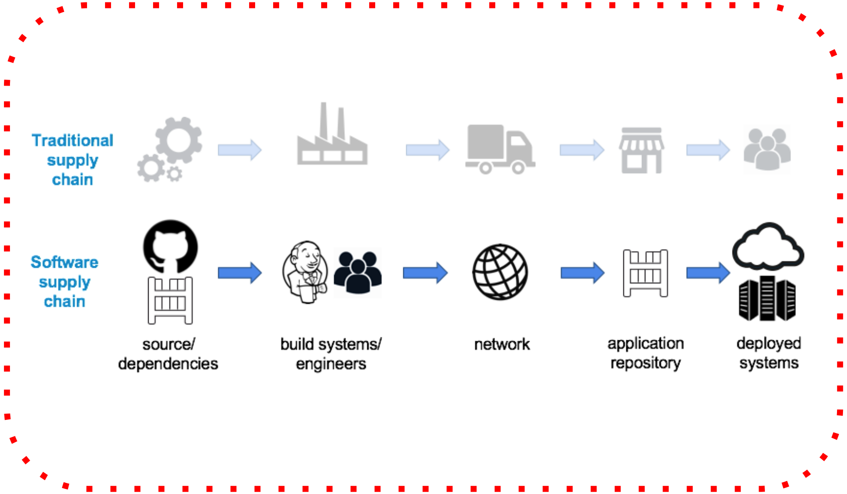
- What is Jenkins X
- What is the Goal of Supply Chain Security in Jenkins X
- What is SBOM and its use in Supply Chain Security
- SBOM different standards and formats
- SBOM generation tools
- Jenkins X approach to generate SBOMs
- Future Work
- Discussion

What is Jenkins X?

- Jenkins X is an all-in-one CI/CD solution for Kubernetes. We aim to provide our users with the ability to build a complete robust secure pipelines to ship their deployment with ease.
- This includes support for different features such as multi-cluster GitOps, Secrets management, ChatOps and preview environments. All of this is integrated natively inside the Kubernetes cluster you use.
- Jenkins X is built on top of Tekton pipeline which is a cloud-native pipeline orchestration tool but JX aims to extend the readability and ease of use for users even more.
- One of our main goals is to provide enough ease of use to allow for non-specialized engineers to automate their processes.
- You focus on writing great code, we build and ship it for you!!.

Supply chain security with Jenkins X

- As an all-in-one and end-to-end solution, we realize the importance of supply chain security in Jenkins X
- Not only to secure Jenkins X artifacts but as a CI/CD platform we aim to enable adding supply chain security in the users' pipelines
- The current agenda for the Project includes adding those features to Jenkins X:
  - SBOM (Software Bill of Materials) generation support
  - Integrate with Tekton Chains
- The current stable finished state is SBOM generation support.
- We will go explaining about the investigation made and how we implement it in Jenkins X



What is SBOM?

- Software Bill of Materials is a formally structured list of the components used to build a certain software artifact.

- Components of an SBoM document should mainly have information about the license compliance of the software, the source code it originated from, and many other details about the build process.

- It should ensure the authenticity of the software and the validity of the document itself

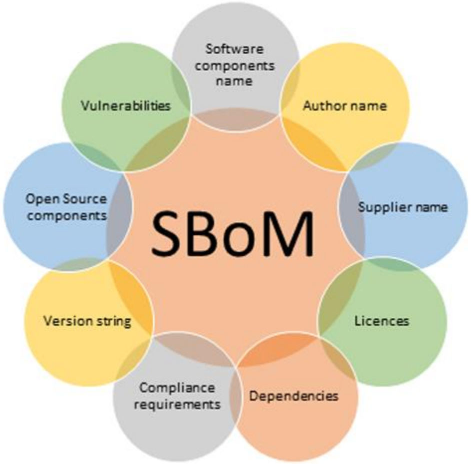
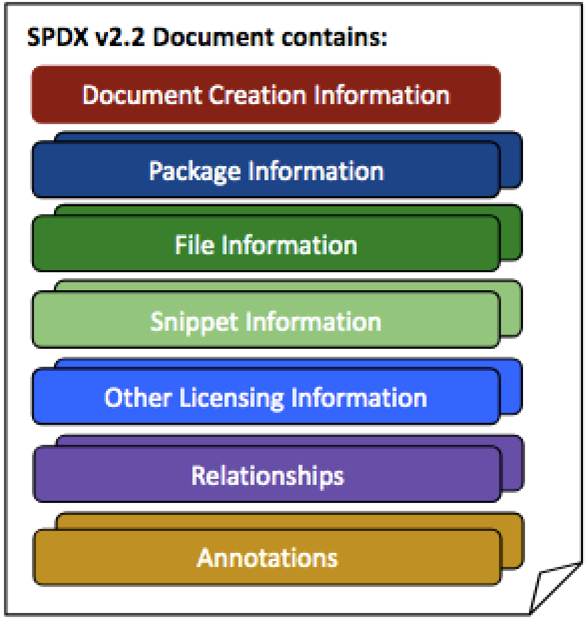


Fig 1: SBoM contents

SBOM formats

The Software Package Data Exchange (SPDX)

- Adopted by the Linux Foundation as an industry standard
- It has improved continuously to meet the NTIA requirements, and specifications were updated till the latest SPDX v2.2.2
- A single SBOM of the SPDX v2.2 format contains different fields to be considered a valid document
- The only mandatory field is the “Document Creation Information”
- SPDX supports different file formats like JSON, YAML, and XML and we can view different examples from here.


SPDX v2.2 Document contains:
Document Creation Information
Package Information
File Information
Snippet Information
Other Licensing Information
Relationships
Annotations

More details and illustrations about other SBOM formats like CycloneDX and SWID tags are discussed in this Jenkins-X blog post.

SBOM generation tools

- SBOM should be machine-readable, following a standard format, and generated automatically.
- There are several open-source tools to generate SBOMs from different types of artifacts
- What makes a good SBOM generation tool?
  - Supports multiple standards and formats
  - Can take multiple types of resources
  - Ease of use for CI/CD systems

SBOM Tools

Anchore Syft

- Syft is a CLI tool developed by Anchore which can generate SBOMs from different artifacts such as container images, binaries, and filesystems.
- It supports the SPDX, Cyclone DX, and JSON formats.

Oras (OCI Registry As Storage)

- Oras, a CNCF sandbox project, is a CLI tool to store different file formats as OCI artifacts.
- It supports storing documents or non-binary files in the final layer of an OCI image
- It can be a great solution to store SBOMs generated from docker images to be stored in the same repository.

Grype

- A vulnerability scanner for SBOMs, container images, and filesystems.

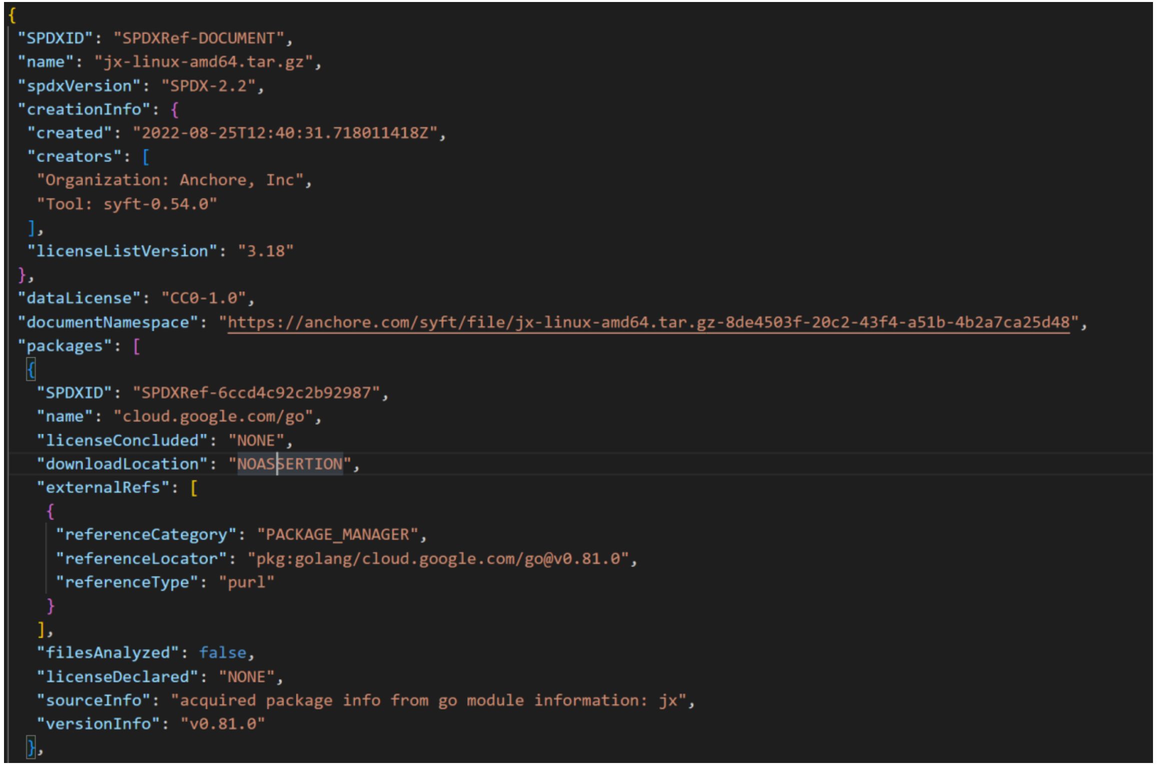
More generation tools are discussed in this Jenkins-X blog post.

How does Jenkins X generate SBOMs

- Jenkins X has a centralized repository (The pipeline catalog) where users can include steps in their pipeline.
- So, we added a step to install Anchore syft inside a Task running alpine docker image.
- On the user’s side, we can reference this step in the pipeline before generating the SBOM like here.
- In our own SBOM generation we use goreleaser which supports generating SBOMs but requires syft to be installed.
- For uploading the SBOM for docker images, it needs to be stored in the same container repository as an OCI artifact
- We added another step in the pipeline catalog to use the Oras project to push the generated SBOMs to the container repository if needed.
- We use Grype to scan the generated SBOMs to detect vulnerable dependencies [WIP].

Jenkins X SBOM example

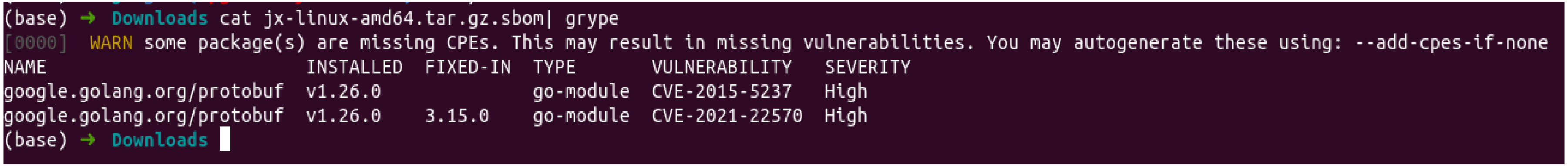
- Refer to this for the full SBOM generated for JX



```
{
 "SPDXID": "SPDXRef-DOCUMENT",
 "name": "jx-linux-amd64.tar.gz",
 "spdxVersion": "SPDX-2.2",
 "creationInfo": {
  "created": "2022-08-25T12:40:31.718011418Z",
  "creators": [
   "Organization: Anchore, Inc",
   "Tool: syft-0.54.0"
  ],
  "licenseListVersion": "3.18"
 },
 "dataLicense": "CC0-1.0",
 "documentNamespace": "https://anchore.com/syft/file/jx-linux-amd64.tar.gz-8de4503f-20c2-43f4-a51b-4b2a7ca25d48",
 "packages": [
  {
   "SPDXID": "SPDXRef-6ccd4c92c2b92987",
   "name": "cloud.google.com/go",
   "licenseConcluded": "NONE",
   "downloadLocation": "NOASSERTION",
   "externalRefs": [
    {
     "referenceCategory": "PACKAGE_MANAGER",
     "referenceLocator": "pkg:golang/cloud.google.com/go@v0.81.0",
     "referenceType": "purl"
    }
   ],
   "filesAnalyzed": false,
   "licenseDeclared": "NONE",
   "sourceInfo": "acquired package info from go module information: jx",
   "versionInfo": "v0.81.0"
  },
```

Scanning SBOMs

- Scanning SBOMs can help to detect vulnerable dependencies using vulnerability scanning tools like Grype
- Grype is a vulnerability scanning cli developed by anchor (the creator of syft).
- We have started scanning our SBOMs using Grype



```
(base) ➜ Downloads cat jx-linux-amd64.tar.gz.sbom| grype
[0000]  WARN some package(s) are missing CPEs. This may result in missing vulnerabilities. You may autogenerate these using: --add-cpes-if-none
NAME                         INSTALLED  FIXED-IN  TYPE       VULNERABILITY   SEVERITY
google.golang.org/protobuf  v1.26.0              go-module  CVE-2015-5237   High
google.golang.org/protobuf  v1.26.0    3.15.0    go-module  CVE-2021-22570  High
(base) ➜ Downloads
```

Note: the detected vulnerability is a false positive and not a real issue with protobuf go client.

- Apart from Grype, Jenkins X is using dependabot to detect vulnerabilities in its dependencies.

Future Work

- Pipeline catalog task to scan SBOMs with Grype
- Generate SBOMs for docker images and upload them using Oras
- For now, Jenkins X is in SLSA level 1and we hope to achieve SLSA level 2 by the end of this year.
  - Tekton Chains integration
- prototype implementation of the CNCF's Secure Software Factory Reference Architecture using Jenkins X.

Comments, Questions
Open Discussion

CD.FOUNDATION