SBOM mit dem Open Build Service

und dann?

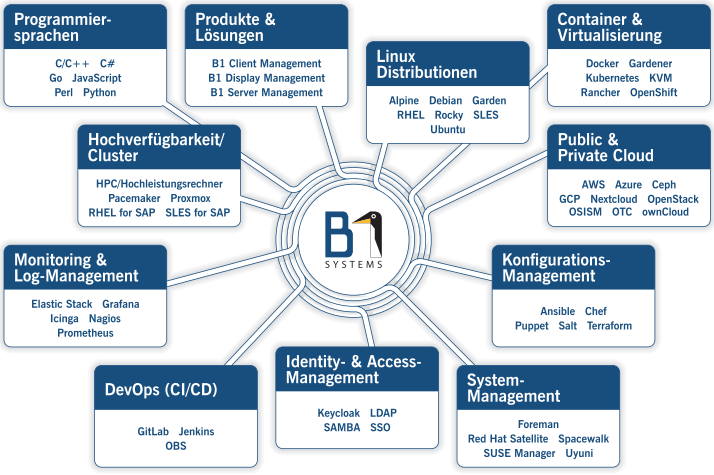
17. August 2024

Christian Schneemann
Senior Consultant
B1 Systems GmbH
schneemann@b1-systems.de

Vorstellung B1 Systems

- gegründet 2004
- spezialisiert auf Linux/Open Source-Themen
- national & international tätig
- ca. 150 Mitarbeiter:innen
- unabhängig von Soft- & Hardware-Herstellern
- Leistungsangebot:
  - Managed Service & Betrieb
  - Beratung & Consulting
  - Support
  - Training
  - Lösungen & Entwicklung
- Standorte in Rockolding, Köln, Berlin, Dresden & Jena

Schwerpunkte



Software Bill of Materials

Allgemein

- "Inventarisierung“ von Softwarebestandteilen
- macht Softwareprodukte vergleichbar
- Lizensierungsfragen
- Risikobewertung/Schwachstellensuche
- Sicherstellung der Lieferkette

Beispiele

Mit Unterstützung im Open Build Service[1]

- SPDX
- CycloneDX

[1] `https://open-build-service.org`

SPDX - Software Package Data Exchange

"Standardformat, das den Umgang mit Freier Software bzw. Open-Source-Software vor allem in Unternehmen und Kommunen erleichtern soll." [2]

[2] https://de.wikipedia.org/wiki/Software_Package_Data_Exchange Abruf 16.08.2024

Software Package Data Exchange

- Entwicklung innerhalb der SPDX-Workgroup[3] (Projekt der Linux Foundation[4])
- SPDX 1.0 veröffentlicht im August 2011
- SPDX 2.3 veröffentlicht im August 2022
- SPDX 3.0 veröffentlicht im April 2024
- Open Build Service unterstützt derzeit SPDX 2.3

[3] https://spdx.dev
[4] https://www.linux-foundation.org

SPDX - Format - JSON 1/4

```
"spdxVersion" : "SPDX-2.3",
"dataLicense" : "CC0-1.0",
"SPDXID" : "SPDXRef-DOCUMENT",
"name" : "KIWIROOT-vmx",
"documentNamespace" : "http://open-build-service.org/spdx/KIWIROOT-vmx-53
    c64ffe-db06-5af4-aa4f-2344341cce04",
"creationInfo" : {
   "created" : "2024-08-16T08:54:06Z",
   "creators" : [
      "Tool: obs_build_generate_sbom-1.1"
   ],
   "licenseListVersion" : "3.24"
},
"packages" : [ ],
"files": [ ],
```

SPDX - Format - JSON - Package 2/4

```
"name": "aaa_base",
"SPDXID": "SPDXRef-Package-rpm-aaa-base-2a3c24c0b344e33f699a5bac55fce4fb
    ",
"versionInfo": "84.87+git20180409.04c9dae-150300.10.20.1",
"supplier": "NOASSERTION",
"originator": "Organization: SUSE LLC <...>",
"downloadLocation": "NOASSERTION",
"sourceInfo": "acquired package info from RPM DB",
"homepage": "https://github.com/openSUSE/aaa_base",
"licenseConcluded": "GPL-2.0+",
"licenseDeclared": "GPL-2.0+",
"copyrightText": "NOASSERTION",
"externalRefs": [ ]
```

SPDX - Format - JSON - externalRefs 3/4

```
{
"referenceCategory": "PACKAGE-MANAGER",
"referenceType": "purl",
"referenceLocator": "pkg:rpm/suse/aaa_base@"
}
```

SPDX - Format - JSON - Reflocator 4/4

```
"referenceLocator": "pkg:rpm/suse/aaa_base@84.87%2Bgit20180409.04c9dae
    -150300.10.20.1?arch=x86_64&upstream=aaa_base-84.87%2Bgit20180409.04
    c9dae-150300.10.20.1.src.rpm&distro=opensuse-leap-15.6"
```

Cyclone DX

Cyclone DX

- entwickelt innerhalb des `Open Worldwide Application Security Project` [5]
- bietet nicht nur SBOM
  - Hardware Bill of Materials (HBOM)
  - Operations Bill of Materials (OBOM)
  - Machine Learning Bill of Materials (ML-BOM)
- `https://cyclonedx.org`
- JSON oder XML Format
- erster Prototyp Mai 2017
- Version 1.6 April 2024
- Open Build Service unterstützt Version 1.15 (Juni 2023)

[5] `https://owasp.org`

CycloneDX - Format JSON 1/3

```
{
   "bomFormat" : "CycloneDX",
   "specVersion" : "1.5",
   "serialNumber" : "urn:uuid:66b64034",
   "version" : 1,
   "metadata" : {
      "timestamp" : "2024-08-16T08:54:02Z",
      "tools" : [
         {
            "name" : "obs_build_generate_sbom",
            "version" : "1.1"
         }
      ],
      "component" : {
         "bom-ref" : "root",
         "name" : "KIWIROOT-vmx",
         "type" : "application"
      }
   },
...
}
```

CycloneDX - Format JSON - Components 2/3

```
"bom-ref" : "pkg:rpm/aaa-base-2a3c24c0b344e33f699a5bac55fce4fb",
"type" : "library",
"name" : "aaa_base",
"version" : "84.87+git20180409.04c9dae-150300.10.20.1",
"purl" : "pkg:rpm/suse/aaa_base@84.87...",
"licenses" : [
 {
  "license" : {
     "id" : "GPL-2.0+"
  }
 }
],
"publisher" : "SUSE LLC <https://www.suse.com/>"
```

CycloneDX - Format JSON - purl[6] 3/3

```
"purl" : "pkg:rpm/suse/aaa_base@84.87%2Bgit20180409.04c9dae-150300.10.20.1?arch=x86_64&upstream=
    aaa_base-84.87%2Bgit20180409.04c9dae-150300.10.20.1.src.rpm&distro=opensuse-leap-15.6",
```

[6] Persistent Uniform Resource Locator

Open Build Service (OBS)

Allgemein

- von SUSE[7]/openSUSE[8] entwickelte Plattform für "Softwarepaketierung“
- 24.01.2006 unter GPL gestellt
- `https://www.open-build-service.org`
- `https://github.com/openSUSE/open-build-service`
- frei nutzbare Instanz `https://build.opensuse.org`

[7] `https://www.suse.com`
[8] `https://www.opensuse.org`

Features 1/2

- Bau von Installationspaketen (RPM, DEB, Arch, Windows)
- Erstellung von Medien
  - Installationsmedien
  - VM-Images
  - Container

Features 2/2

- Paket-/Imagebau in immer frischen Buildroot
- kein Netzwerkzugang während des Baus
- Sourcen von externen Quellen können per Services bezogen werden
- interne Revisionsverwaltung der Sourcen
- RPMlint mit erweiterten Checks sorgt für Paketqualität
- Unterstützung für collaboratives Arbeiten/Mehraugenprinzip
- Workflows zur SCM/CI Integration (github/gitlab)

Medienerstellung

Supportete Tools:

- KIWI[9]
- mkosi[10]
- livebuild[11]

[9] https://osinside.github.io/kiwi/
[10] https://mkosi.systemd.io
[11] https://www.debian.org/devel/debian-live/

SBOM Support

SBOM Support für mkosi und livebuild derzeit nur in eigener (gepatchter) Instanz (PRs sind offen).

RPM

Allgemein

- ursprüngliche Hauptnutzen des OBS
- OBS kümmert sich um Abhängigkeiten

Beispiel - SPEC

```
Name:           hallo-paket
Version:        1.0
Release:        1
Summary:        Ein einfaches Beispiel-Paket
License:        GPL2
BuildArch:      noarch

%description
%{summary}.

%prep

%build

%install
mkdir -p %{buildroot}/usr/local/bin

echo "echo Hallo" > %{buildroot}/usr/local/bin/hallo

%files
/usr/local/bin/hallo

%changelog
```

RPMlint

https://spdx.org/licenses/

```
RPMLINT report:
===============
hallo-paket.noarch: W: invalid-license GPL2
hallo-paket.src: W: invalid-license GPL2
The specified license string is not recognized. Please refer to
https://spdx.org/licenses/ for the list of known licenses and their exact
spelling.
```

weitere Paketformate

- Debian (DSC)
- Arch (Pkg)
- AppImage
- Flatpak

KIWI

Allgemein

- "command line utility to build Linux system appliances"[12]
- unterstützte Images
  - hybride Live Image
  - Virtual Disk Image
  - OEM expandable Disk Image
  - Docker Container Image
  - WSL Container Image
  - KIS[13] Root File System Image
- Beispiele: `https://github.com/OSInside/kiwi-descriptions`

[12] `https://osinside.github.io/kiwi/`
[13] Kernel, Initrd, System

Nutzung innerhalb des OBS

- Konfigurationsdatei (XML) als `<IMAGE>.kiwi` hinterlegen

`minimal.kiwi`

- Type in Project Config als `kiwi` hinterlegen

```
%if "%_repository" == "kiwi_images"
Type: kiwi
%endif
```

Beispiel XML

```
<?xml version="1.0" encoding="utf-8"?>
<image schemaversion="6.1" name="openSUSE-Leap-15.6-Minimal" displayname="openSUSE Leap 15.6">
  <description type="system">
    <author>openSUSE Project</author>
    <contact>crc@suse.com</contact>
    <specification>openSUSE Leap 15.6 Minimal</specification>
  </description>
  <preferences>
  <version>15.6.0</version>
  <packagemanager>zypper</packagemanager>
  <type image="vmx" filesystem="xfs" format="qcow2"/>
  </preferences>
  <repository type="rpm-md" >
      <source path='obsrepositories:/'/>
  </repository>
  <packages type="image">
      <package name="patterns-base-base"/>
      <package name="aaa_base-extras"/>
      <package name="acl"/>
      <package name="chrony"/>
...
```

Resultat

```
_buildenv
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.cdx.json
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.packages
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.qcow2
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.qcow2.sha256
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.qcow2.sha256.asc
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.report
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.spdx.json
openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.verified
_statistics
```

Livebuild

Allgemein

- Tool zur Erstellung von Debian Images (u.a. live)

Nutzung innerhalb des OBS

- Konfigurationsdateien als Archiv auf ".livebuild“ endend zu hinterlegen

```
minimal.livebuild
```

- Type in Project Config als `kiwi` hinterlegen

```
%if "%_repository" == "livebuild_images"
Type: livebuild
%endif
```

Resultat

```
standard_amd64_Build1.1.spdx.json.sha256
standard_20240816T1159_amd64_Build1.1.files
standard_amd64_Build1.1.cdx.json.sha256
standard_Build1.1.livebuild.tar
_statistics
standard_20240816T1159_amd64_Build1.1.contents.sha256
standard_20240816T1159_amd64_Build1.1.files.sha256
standard_amd64_Build1.1.spdx.json
standard_20240816T1159_amd64_Build1.1.hybrid.iso_ONIE.bin
standard_20240816T1159_amd64_Build1.1.hybrid.iso_ONIE.bin.sha256
standard_20240816T1159_amd64_Build1.1.packages
standard_20240816T1159_amd64_Build1.1.hybrid.iso
standard_20240816T1159_amd64_Build1.1.packages.sha256
standard_20240816T1159_amd64_Build1.1.hybrid.iso.zsync
standard_amd64_Build1.1.cdx.json
standard_20240816T1159_amd64_Build1.1.contents
standard_20240816T1159_amd64_Build1.1.hybrid.iso.sha256
standard_20240816T1159_amd64_Build1.1.hybrid.iso.zsync.sha256
```

MKosi

Allgemein

"A fancy wrapper around dnf –installroot, apt, pacman and zypper that generates customized disk images with a number of bells and whistles."[14]

- Entwicklung innerhalb des systemd[15] Projekts
- erstellt Images für verschiedene Linux Distributionen

[14] https://mkosi.systemd.io/
[15] https://systemd.io

Nutzung innerhalb des OBS

- Konfigurationsdatei auf ".mkosi“ endend zu hinterlegen

```
minimal.mkosi
```

- Type in Project Config als `kiwi` hinterlegen

```
%if "%_repository" == "mkosi_images"
Type: mkosi
%endif
```

Beispiel

```
[Distribution]
Distribution=debian
Release=testing

[Output]
Format=disk

[Partition]
Format=squashfs

[Content]
WithDocs=yes
RootPassword=linux
Autologin=no
Packages=
  debian-installer-launcher
  linux-image-amd64
  shim-signed
  grub2-common
  grub-efi-ia32-bin
  grub-pc-bin
  binutils
  task-english
  memtest86+
  task-ssh-server
  docker.io
```

Resultat

```
standard_amd64_Build1.1.spdx.json.sha256
standard_20240816T1159_amd64_Build1.1.files
standard_amd64_Build1.1.cdx.json.sha256
standard_Build1.1.livebuild.tar
_statistics
standard_20240816T1159_amd64_Build1.1.contents.sha256
standard_20240816T1159_amd64_Build1.1.files.sha256
standard_amd64_Build1.1.spdx.json
standard_20240816T1159_amd64_Build1.1.hybrid.iso_ONIE.bin
standard_20240816T1159_amd64_Build1.1.hybrid.iso_ONIE.bin.sha256
standard_20240816T1159_amd64_Build1.1.packages
standard_20240816T1159_amd64_Build1.1.hybrid.iso
standard_20240816T1159_amd64_Build1.1.packages.sha256
standard_20240816T1159_amd64_Build1.1.hybrid.iso.zsync
standard_amd64_Build1.1.cdx.json
standard_20240816T1159_amd64_Build1.1.contents
standard_20240816T1159_amd64_Build1.1.hybrid.iso.sha256
standard_20240816T1159_amd64_Build1.1.hybrid.iso.zsync.sha256
```

SBOM Tools

Validierung

- https://tools.spdx.org/app/validate/
- https://pypi.org/project/spdx-tools/

Vulnerability Scan

- https://github.com/devops-kung-fu/bomber
- https://github.com/intel/cve-bin-tool-action

bomber

```
bomber scan openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.spdx.json
```

```
DKFM - DevOps Kung Fu Mafia
https://github.com/devops-kung-fu/bomber
Version: 0.5.0

    Scanning Files:
  openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.spdx.json
    Ecosystems detected: rpm
    Scanning 376 packages for vulnerabilities...
    Vulnerability Provider: OSV Vulnerability Database (https://osv.dev)

    Files Scanned
    openSUSE-Leap-15.6-Minimal-VM.x86_64-15.6.0-Cloud-Build2.1.spdx.json

    No vulnerabilities found using the osv provider

    NOTE: Just because bomber didn't find any vulnerabilities using the osv provider does
    not mean that there are no vulnerabilities. Please try the other providers that bomber
    supports (osv, ossindex)
```

Intel - cve-bin-tool

```
cve-bin-tool --sbom spdx --sbom-file Cloud-Build2.1.spdx.json -f html
...
INFO cve_bin_tool.CVEScanner - 3 CVE(s) in npmjs.tar version 1.34-150000.3.34.1
INFO cve_bin_tool.CVEScanner - 1 CVE(s) in unknown.util-linux version 2.39.3-150600.4.9.4
INFO cve_bin_tool.CVEScanner - 2 CVE(s) in gnu.wget version 1.20.3-150600.19.3.1
INFO cve_bin_tool.CVEScanner - 1 CVE(s) in schneems.wicked version 0.6.76-150600.11.9.1
INFO cve_bin_tool.CVEScanner - 1 CVE(s) in unknown.wicked version 0.6.76-150600.11.9.1
INFO cve_bin_tool.CVEScanner - 1 CVE(s) in unknown.xz version 5.4.1-150600.1.2
INFO cve_bin_tool - Overall CVE summary:
INFO cve_bin_tool - There are 42 products with known CVEs detected
INFO cve_bin_tool.OutputEngine - HTML report stored at output.cve-bin-tool.2024-08-16.13-43-38.
     html
```

Fazit

Fazit

- einfache Dokumentation der Inhalte von Images
- Einfach weiterzugeben/archivieren
- Vielzahl an Analysetools

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de oder +49 (0)8457 - 931096