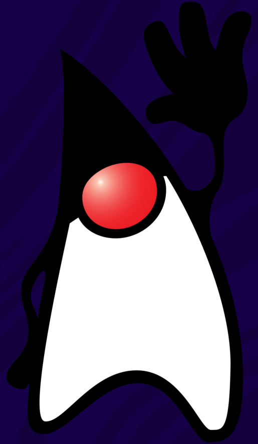
chainguard

Learning Lab:



Chainguard Libraries

Fundamentals, introduction, and getting started with Java

Meet Your Trainer

- Open source hacker and advocate
- Book author, teacher, presenter, and host
- Trino, Maven, Nexus, and more
- Dad, builder, biker, boarder, yogi, gardener, ...
- Victoria, BC, Canada

- manfred.moser@chainguard.dev

Manfred Moser

Agenda

- Introduction
- Fundamental concepts and Chainguard context
- Specifics for Chainguard Libraries for Java
- Demo with Apache Maven and Sonatype Nexus
- Q&A

We are the safe source for open source.

Built by the people behind widely adopted open source projects like Kubernetes, Sigstore, SLSA, and Google Distroless.

Chainguard enables companies to build software efficiently and securely from the start.

chainguard

Customers across industries

Software

appian Canva
CLOUDERA GitLab
CONFLUENT Figma
DELL Technologies elastic
Hewlett Packard Enterprise Logic Monitor
Palantir precisely
snowflake GONG

Health & Bio

AETION
Dexcom
GoHealth
lifebit
Optum

Security

okta WIZ
zscaler cyera
GitGuardian jamf
RELIAQUEST
1KOSMOS Checkmarx
Abnormal

FinServ

ADP
ANZ ABSA
FIDELITY NATIONAL FINANCIAL VPBank
BNP PARIBAS
Thomson Reuters

Public Sector

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
TEST RESOURCE MANAGEMENT CENTER DEPARTMENT OF DEFENSE
CDC
NASA
UNITED STATES NAVY
UNITED STATES ARMY

Defense / Safety

ANDURIL
ASI AIR SPACE INTELLIGENCE
Booz | Allen | Hamilton
Defense Unicorns 2F
AXON
SHIFT5

AI

scale
C3.ai
fiddler securiti
HIDDENLAYER
yurts

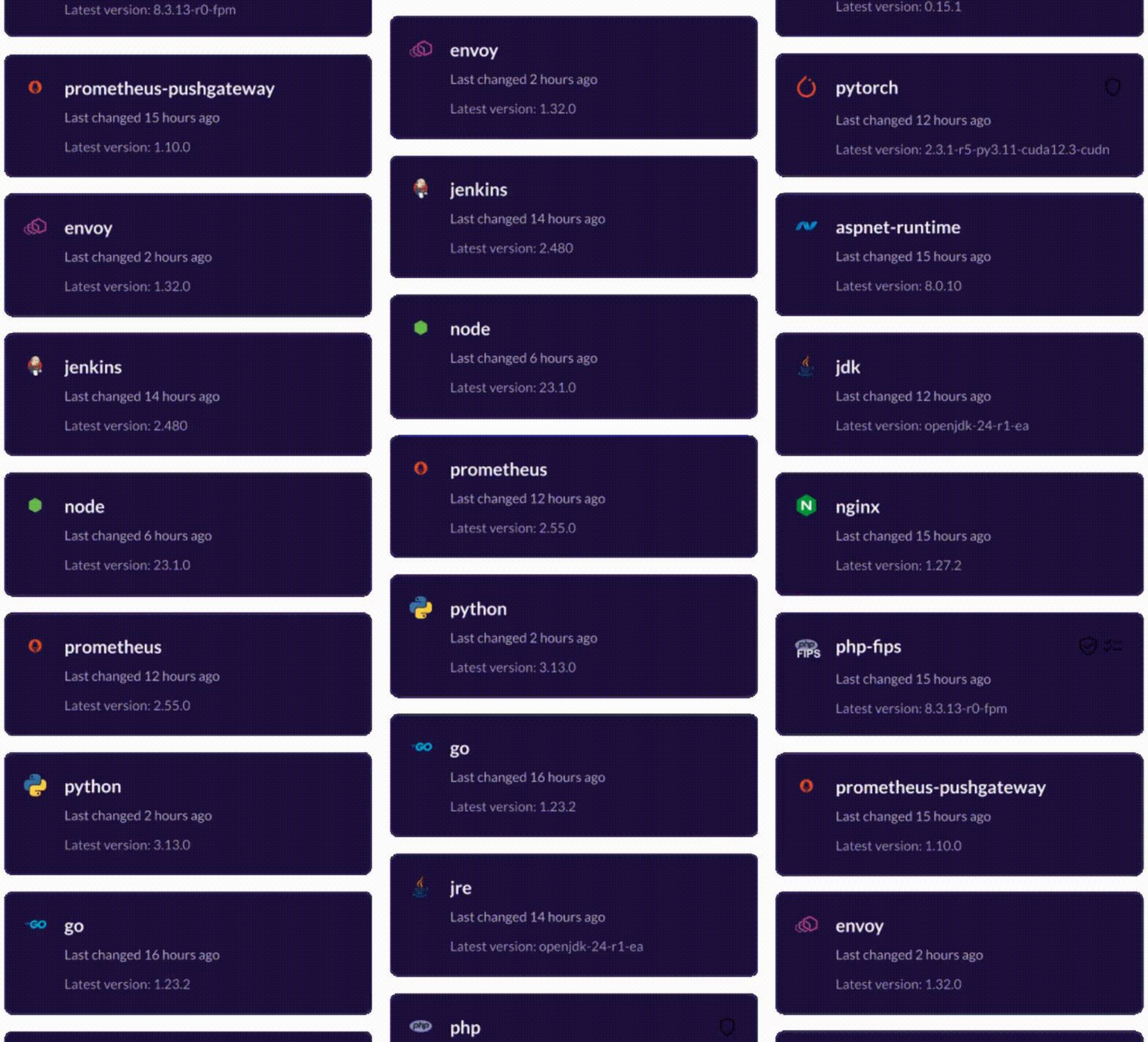
F500

American Airlines
CISCO
TESLA
THE HOME DEPOT Ford
coupang

Chainguard Containers

- ✅Over 1300 different containers
- ✅ Built in Chainguard Factory
- ✅Minimal attack surface
- ✅All maintained versions
- ✅Zero CVEs
- ✅SLAs for CVE remediation
- ✅Dedicated OS-level STIG
- ✅Kernel-independent FIPS
- ✅HTML OSCAP scan reports
- ✅SBOMs and attestation

chainguard



Latest version: 8.3.13-r0-fpm

prometheus-pushgateway
Last changed 15 hours ago
Latest version: 1.10.0

envoy
Last changed 2 hours ago
Latest version: 1.32.0

jenkins
Last changed 14 hours ago
Latest version: 2.480

node
Last changed 6 hours ago
Latest version: 23.1.0

prometheus
Last changed 12 hours ago
Latest version: 2.55.0

python
Last changed 2 hours ago
Latest version: 3.13.0

go
Last changed 16 hours ago
Latest version: 1.23.2

envoy
Last changed 2 hours ago
Latest version: 1.32.0

jenkins
Last changed 14 hours ago
Latest version: 2.480

node
Last changed 6 hours ago
Latest version: 23.1.0

prometheus
Last changed 12 hours ago
Latest version: 2.55.0

python
Last changed 2 hours ago
Latest version: 3.13.0

go
Last changed 16 hours ago
Latest version: 1.23.2

jre
Last changed 14 hours ago
Latest version: openjdk-24-r1-ea

php

Latest version: 0.15.1

pytorch
Last changed 12 hours ago
Latest version: 2.3.1-r5-py3.11-cuda12.3-cudn

aspnet-runtime
Last changed 15 hours ago
Latest version: 8.0.10

jdk
Last changed 12 hours ago
Latest version: openjdk-24-r1-ea

nginx
Last changed 15 hours ago
Latest version: 1.27.2

php-fips
Last changed 15 hours ago
Latest version: 8.3.13-r0-fpm

prometheus-pushgateway
Last changed 15 hours ago
Latest version: 1.10.0

envoy
Last changed 2 hours ago
Latest version: 1.32.0

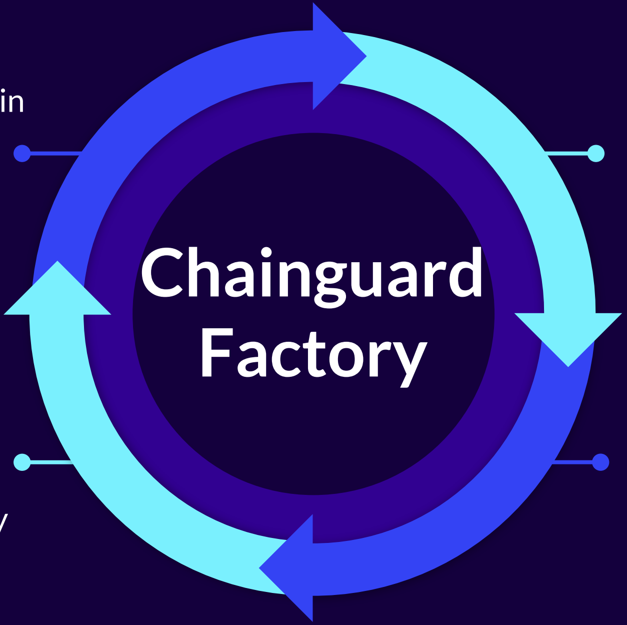
The Harder But Better Path to Delivering Secure and Effective Software

Builds from source

Compile upstream code from scratch in SLSA infrastructure and include updated dependencies

SLA for security patches

Continuously scan software and apply patches faster than alternative distributions



Minimal containers

Include only the packages and dependencies required to run your applications

Consistency

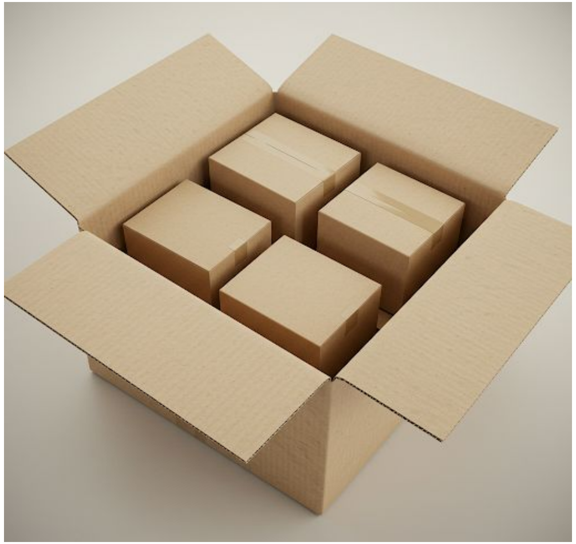
Ensure stable builds, consistent functionality, and trust delivery to the registry of your choice

Secure containers are great ….

But what’s inside?

Applications

Containers run your applications



... with lots of libraries inside.

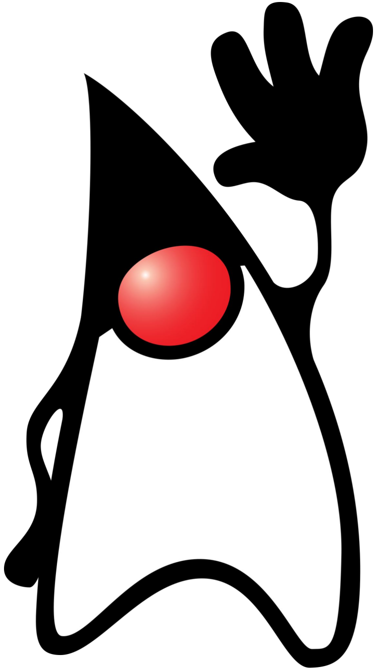
Outside containers

Even outside containers - your application is built from (open source) components.

So what is a library?

- Building blocks for your application
- Specific feature set and capabilities
  - Logging, telemetry, image generation, JSON handling, and many more
- Well beyond 70% of your application
- Typically open source, but also commercial
- Different names across language ecosystems
  - Library, component, package, framework (group of libraries), toolkit, dependency, artifact, module, …
- In all shapes and sizes

Java



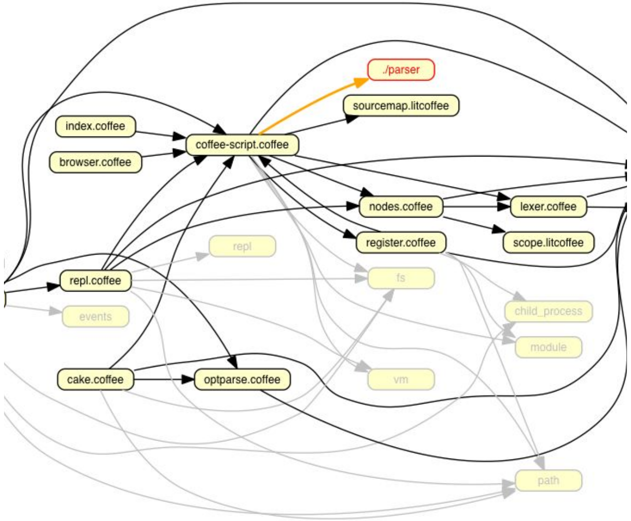
- Very widely used
- Language and runtime
- Java Development Kit JDK,
  Java Runtime Environment JRE,
  JVM Java Virtual Machine
- Java, Scala, Groovy, Kotlin, …
- Open source
- Many vendors
- Collection of vibrant open source communities

Java™

Libraries in Java

- Provide functionality beyond the built-in class libraries from Java itself (`java.lang`, `java.util`, …)
- Commonly as Java Archive (JAR) file
- Zip file with metadata, resources, and compiled class files
- Also other formats like WAR
- Build and also use with build tool or the `java` command

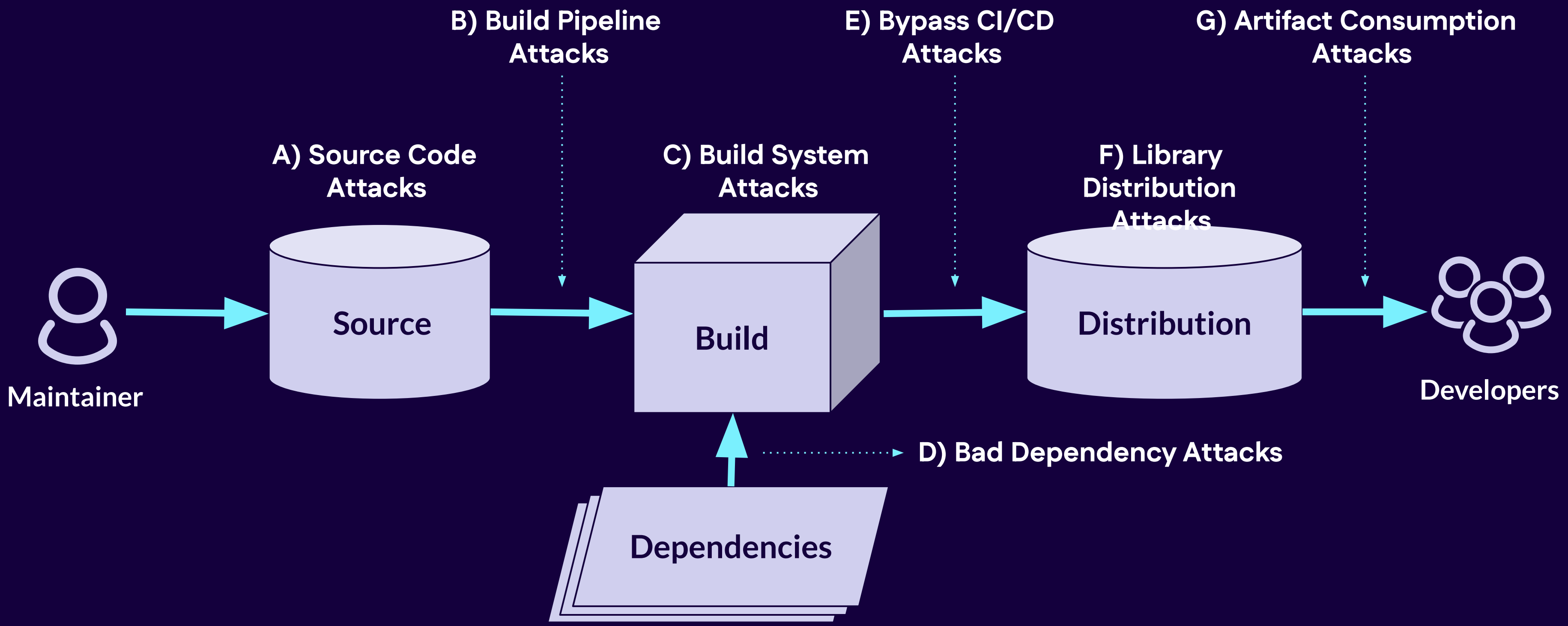
Software Supply Chain of Libraries



- Generated from source code
- Consumed as binaries
- Libraries are declared as dependencies
- Dependencies have dependencies - transitive dependencies
- Results in dependency tree or web or graph

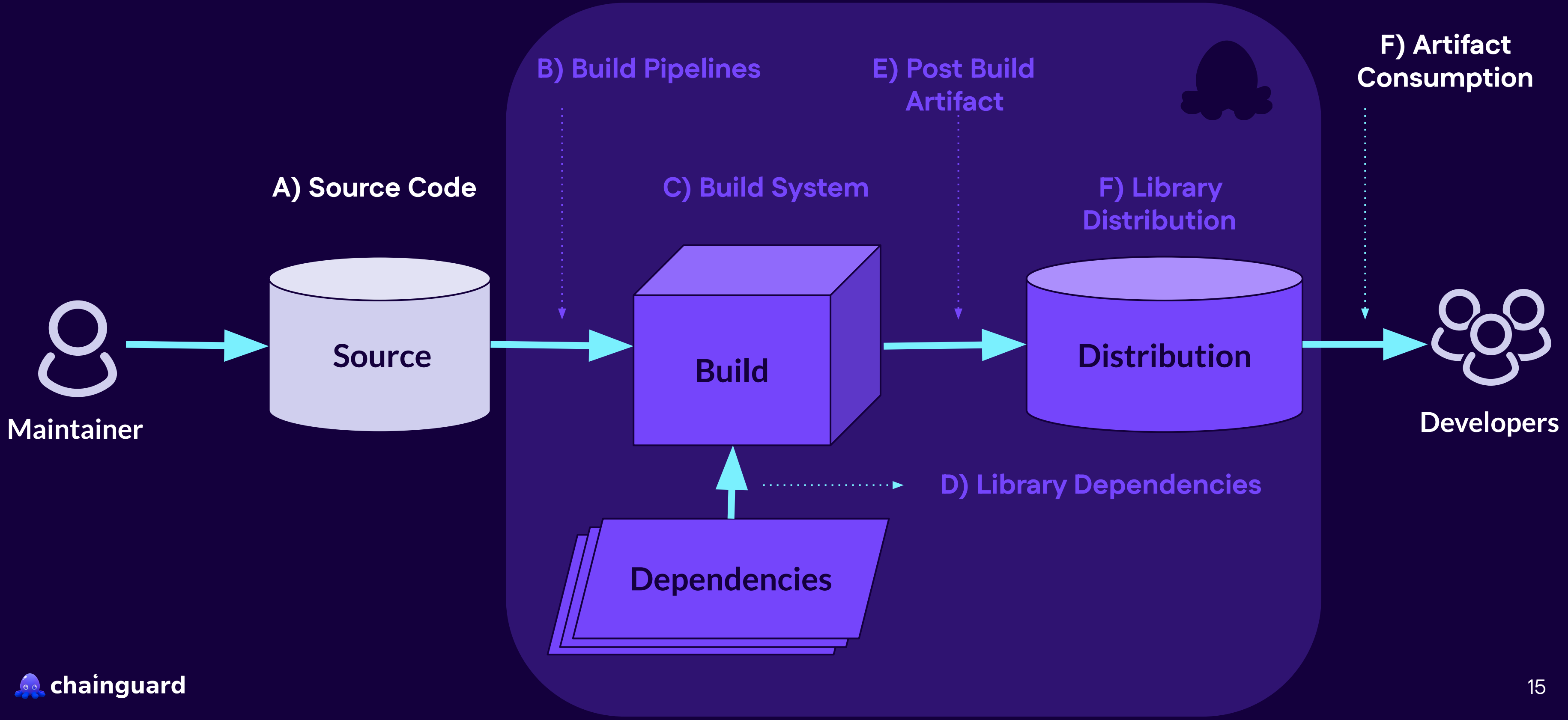
All dependencies need to be pulled in!

Package Lifecycle and Types of Supply Chain Attacks



chainguard

Chainguard Libraries eliminate supply chain attacks at build and distribution



Dependencies from where?

- Declarative definition of dependencies
- Build tools retrieve from repositories
- Built-in public repositories of binaries
    - For Java - Maven Central
    - `https://repo1.maven.org/maven2/`
- Other repositories

Repository basics

- What is a repository?
  - A storage for libraries
  - Enables use in build and other tools
- Maven repository format
  - groupId, artifactId, version
  - Creates directory structure
- Registry = same idea different name
- Sometimes also “archive” .. think CPAN

How dependencies get into Maven Central

- Lots of maintainers
- Various build tools like Maven, Gradle, …
- Build on workstations, CI server, in cloud, ..
- Various rules and validation
- Closed source/no source also possible

Chainguard Libraries for Java

- Rebuild of most packages from Maven Central
- Completely from source
- Chainguard Factory - SLSA secure infrastructure
- Including new releases
- Only open source
    - no commercial code
- No malware since there is no source code

Repository manager

- Application to operate multiple repositories
- Best practice for any organization
- Maven repository format
- Proxy repo - cache for upstream repository
- Hosted repo - permanent storage
- Group/virtual - combination for ease of use

Repository managers

sonatype
nexus repository

JFrog
ARTIFACTORY

cloudsmith

Google Cloud
Artifact Registry

Developer tools

Maven™

Gradle

Others like sbt, Bazel, Ant, …

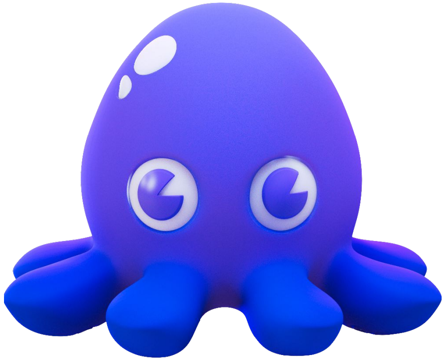
All understand Maven repo format and use it

Demo time

- Apache Maven
- Sonatype Nexus
- Chainctl

Maven™

sonatype
nexus repository



Get access

- Verify your account
  ```
  chainctl auth login
  ```
- Verify entitlement for your organization
  ```
  chainctl libraries entitlements list
  --parent=example
  ```
- Get access token
  ```
  chainctl auth pull-token
  --library-ecosystem=java --parent=example
  --ttl=8670h
  ```

Configure your repository manager

- Proxy repo for Chainguard Libraries for Java
  - `https://libraries.cgr.dev/java/`
- Proxy repo for Maven Central as backfill
- Ordered group repository

Configure build tools

- On workstations and CI servers
- `~/.m2/settings.xml`
- Pointing at the group repository
- Authentication if required

Let’s look at the whole file …

Prepare to build

- Wipe local repository
- Safe since it is just a cache
- Triggers new downloads of everything
- First and foremost Chainguard Libraries for Java artifacts
- `rm -rf ~/.m2/repository`

Maven project setup and use

- Build with `mvn install`
- Define dependency in `pom.xml`
- List all dependencies with
  `mvn dependency:list`
- Inspect dependency hierarchy
  `mvn dependency:tree`

Results

- Local repository with libraries
- Repositories in Nexus
    - What is and is not from Chainguard?
- Verification with `cosign`
- Libraries in use in your application artifacts

Summary and Wrapping Up

- Chainguard Libraries for Java is a trusted provider for open source library binaries.
- Avoid software supply chain issues and malware.
- Works seamlessly with your repo managers and build tools.

What's next?

- Build receipt
- Documentation updates
- Technical blog post about building Java libraries in Chainguard Factory
- Python and PyPI

Join us as early access or beta user!

Questions

?

Further Resources

- https://edu.chainguard.dev/chainguard/libraries/
- https://edu.chainguard.dev/chainguard/libraries/java/

Thank you!

chainguard