SBOM

WH Theme: SBOMs / Notifications

- Look at OpenSSF SLSA/SBOM work ([SLSA]). See also mail from GOSST
- Look at https://github.com/ossf/wg-security-tooling
- https://github.com/spdx/spdx-maven-plugin
- See security-discuss mailing list discussion

Other background:

- SBOM section at https://op ensf. org/oss-security-mobilization-plan/ based on WH and other meetings

Draft ASF Position:

- SBOMs need to be automatically generated for builds at build time
- SBOMs need to be signed with the same keys used for releases, in the same way (detached signature, detached hash)
- SBOMs are expected to be static to the given release, must never be changed after release
- SBOMs need to be useful (i.e. can be parsed, machine readable by current/future tools)

Questions

- What type of projects/builds should include SBOMs?
- What format should be used (e.g., SPDX, CycloneDX)
- What projects are interested in working on this?
  - Airflow (Python, CycloneDX, merged)
  - ARROW Java: Publish SBOM artifacts (Maven, CycloneDX, published)
  - AVRO-3700: Publish SBOM artifacts (Maven, CycloneDX)
  - Commons https://github.com/apache/commons-parent/pull/122 (Maven, CycloneDX, published for some)
  - DRUID: Publish SBOM artifacts (Maven, CycloneDX, merged)
  - FLINK-30578: Publish SBOM artifacts (Maven, CycloneDX, published)
  - HADOOP-18590: Publish SBOM artifacts (Maven, CycloneDX, published)
  - HIVE-26912: Publish SBOM artifacts (Maven, CycloneDX, merged)
  - HBASE-27562 Publish SBOM artifacts (Maven, CycloneDX, published)
  - MAVEN/MPOM-346: publish SBOM on release (Maven, CycloneDX, published)
  - ORC-1342: Publish SBOM artifacts (Maven, CycloneDX, published)
  - PARQUET-2224: Publish SBOM artifacts (Maven, CycloneDX, published)
  - SPARK-41893: Publish SBOM artifacts (Maven, CycloneDX, published)
  - SOLR-16796: Publish an SBOM for Solr artifacts (Gradle, CycloneDX, not published)
  - SYNCOPE-1746: Provide Software Bill Of Materials (SBOM) (Maven, CycloneDX, published)
  - ZOOKEEPER-4857: Publish SBOM artifacts (Maven, CycloneDX, published)