

Introduction

Notes - Bazel supply chain weekly sync

- We hold a weekly meeting to discuss Bazel supply chain related issues.
 - Thursday 2:30 pm CET / 8:30 AM EST
 - Meet link: <https://meet.google.com/qop-eyei-cfh>
- Old meeting notes for the monthly rules_license meeting:
[DEPRECATED] rules_license monthly sync
- Code: <https://github.com/bazel-contrib/supply-chain/>
- Projects:
 - `license` rule: Antonio Di Stefano yannic@engflow.com Tony Aiuto
 - Design SBOM toolchains/rules/etc Antonio Di Stefano Tony Aiuto
 - Design a release pipeline Yannic Bonenberger
 - Figure out if Aspect's GHA tooling can work with multiple modules per repo fwe@google.com
- Need to invite people
 - Salesforce?

Topics for a future meeting

- [aiuto] Re-visiting earlier concern about having every attribute write data only instead of passing it up. Since we never pass up info in a provider, it becomes impossible to do any sort of bazel query to see the stuff life. You must analyze the target, then create a tool to read the files, and print the relevant data from that
- [aiuto] Why is purl privileged? It is just another attribute?
- [aiuto] working on <https://github.com/bazel-contrib/supply-chain/pull/41>

Jul 30, 2026

Jul 30, 2026

Only 3 showed up. So we cancelled after 5 minutes.

Jul 23, 2026

Jul 23, 2026

Attendees: mark.zeren@broadcom.com lavoie.richard@gmail.com
simon.m.stewart@gmail.com yannic@engflow.com antonio@engflow.com
kaloyan.raev@broadcom.com tony.aiuto@datadoghq.com

Agenda:

-

Notes:

- Both Bazelcon proposals accepted. BoF and main talk. Aspect intends to host a hackathon on Friday, but have not communicated that well.
- aiuto: short brainstorm on idea of a provider about the packaging
 - You use a rule to build a deb/rpm/pkg file, information like the architecture, and version should go into the SBOM. Should pkg_* rules pass up a provider that allows a supply chain rule to generate the SBOM directly from that as a dependency?
 - Excellent rubber duck session. => just add an attribute which is a name:value pair where the name is an SPDX label.
- We absolutely need a workspace BOM PoC.
- Missing rule sets
 - rules_img - might need it
- We need some better examples.
- Mark: Internal package manager. Need to provide finer grained things. Some files might have extra metadata provided. The package manager may create multiple repositories with different metadata in each. Eg. a toolchain target (with compiler and debugger, with different licenses). Can we do that without new features?
 - for targets, we can use default_package_metadata,
 - for source files, we can wrap the file in a filegroup()
 - or standard injection mechanism we are planning.
 - hypothetical case of package under two license and you pick a different one based on jurisdiction.
 - => we don't think we have to build anything right now.

-

Jul 2, 2026

Jul 2, 2026

Attendees: lavoie.richard@gmail.com mark.zeren@broadcom.com
simon.m.stewart@gmail.com yannic@engflow.com Tony Aiuto

Notes:

- Merged registry data for purl PR
- Where do we put CPE?
 - Discussion about keeping important ones in metadata or a new module.
 - outcome: create folder attributes
- What else do we add
 - What about the situation of a fork of another package. You want to credit the upstream. This is SPDX "DERIVED-FROM".
https://www.google.com/search?q=SPDX+attribute+to+represent+a+fork+of+another+project&rlz=1C5GCCM_en&oq=SPDX+attribute+to+represent+a+fork+of+another+project&gs_lcrp=EgZjaHJvbWUyBggAEFUYOdIBCTEzNDM5ajBqN6gCCLACAQ&sourceid=chrome&ie=UTF-8
 - The current thinking is that we have an attribute that is a link to another metadata bundle.
- Toolchains
 - Aspects can not descend to toolchains yet
 - Richard has a bazel fork that starts to make this possible
- What's next?
 - Examples to back up BazelCon presentation
 - Metadata 1.0
 - SBOM 1.0
-

Jun 25, 2026

Jun 25, 2026

Attendees: yannic@engflow.com simon.m.stewart@gmail.com
kaloyan.raev@broadcom.com antonio@engflow.com Tony Aiuto
mark.zeren@broadcom.com

Notes:

- Trying a release
 - Rate limiting from maven makes the doc generation flaky
- PR cleanup
 - MetadataInfo needs review
 - Delete #47
- Discusison of <https://github.com/bazel-contrib/supply-chain/issues/172>
-

Jun 18, 2026

Jun 18, 2026

Attendees: simon.m.stewart@gmail.com mark.zeren@broadcom.com
yannic@engflow.com Tony Aiuto kaloyan.raev@broadcom.com

Notes:

- Bazelcon proposal almost ready
- patch to disable purl normalization is merged
- Let's do a release.
-

Jun 11, 2026

Jun 11, 2026

Attendees: Tony Aiuto simon.m.stewart@gmail.com mark.zeren@broadcom.com
antonio@engflow.com yannic@engflow.com

Notes:

- <https://github.com/bazel-contrib/supply-chain/pull/190> fixes the BCR release workflow
- But.... the loop with purl means BCR testing fails until purl is in BCR. purl depends on packages_metadata, so we need a complex bootstrap.
- Conclusion:
 - We are overthinking this.
 - Move purl back to package_metadata and change the purl API so people can pass in their own validators. So we can pull those from any repo, rather than just purl.bzl
 - <https://github.com/bazel-contrib/supply-chain/pull/192> is the revert
-

Jun 4, 2026

Jun 4, 2026

Attendees: kaloyan.raev@broadcom.com lavoie.richard@gmail.com Tony Aiuto
mark.zeren@broadcom.com

Notes:

- We talked about Bazelcon talks in general.
- Do you use an internal fork of bazelisk?
 - VMWare uses one to gather and download things from the internal package manager before bazel starts
 - they build bazel from source
 - The general problem is that we always want to insert our local package manager in front of anything bazel downloads.
- BazelCon 2026 CFPs discussion

----- below BazelCon 2026 CFP proposals -----

Presenters: Antonio Di Stefano

Yannic Bonenberger

Format: Technical talk (30 min)

No bytes left untracked - Bazel Supply Chain Security

Bazel is known for fast, correct builds, but "correct" must include "secure". The Supply-Chain SIG is on a mission to help the Bazel community secure their builds and account for every byte in their artifacts. Marking the 1.0 release of `package_metadata` and core tooling, this talk provides a technical guide to production-ready supply chain tracking.

Our goal is to provide extensibility points for organizations to inject data and policy checks without patching dependencies or relying on coarser, ecosystem-specific manifests (e.g., `pom.xml`, `go.mod`, `package.json`). We will demonstrate how to leverage the `package_metadata` framework to enforce these custom compliance rules and generate provenance, natively integrated with industry-standard SBOM formats (SPDX and CycloneDX).

We will also discuss our upcoming roadmap for tackling deeper ecosystem challenges, such as tracking rules, module extensions, or macro definitions and their dependencies, while mapping

out the path toward strict build-level enforcement. This session delivers the concrete implementation patterns needed to ship trustworthy artifacts to your users.

Supply-chain BoF CFP

With the 1.0 release of `package_metadata` and core tooling, the Bazel ecosystem has a solid foundation for supply chain security. But a framework is only as good as the community using it. This Birds of a Feather (BoF) session is an open, unscripted forum for ruleset maintainers, security engineers, and compliance teams to share real-world experiences and shape what comes next.

We want to hear from you. What are your biggest pain points when generating SBOMs (SPDX/CycloneDX) or chasing SLSA compliance? Where do existing ecosystem-specific manifests fall short in your production Bazel builds?

This is your space to directly influence the Supply-Chain SIG's roadmap. We will openly discuss upcoming challenges, like tracking rules, module extensions, and macro definitions, and debate the path toward strict build-level enforcement. Bring your corporate compliance checklists, your technical edge cases, or just your questions. Let's collaborate to figure out exactly what the community needs next to account for every byte.

May 28, 2026

May 28, 2026

Attendees: mark.zeren@broadcom.com simon.m.stewart@gmail.com Tony Aiuto
kaloyan.raev@broadcom.com yannic@engflow.com

mark.zeren@broadcom.com

From Broadcom discussion: Want to know the direct dependencies in the workspace BOM. That is, you want to know what is directly in MODULE.bazel vs. what is transitive. Same thing for product SBOMs. This is mostly for internal facing security work rather than customer facing.

They did a PoC by looking at lock files during the build rather than the aspect. bazel run step after the build.

- related info from Rules Authors meeting this week. Google is OK with PRs that add repository events into BES.

A key problem is that bzlmod defers to external package manager that will create things. How do we get visibility into that?

`bazel run @maven//:direct_deps` to get all the first-order deps of a java dep (gathered by aggregating all the `install` (and other) tags

Tony Aiuto Multi release needs updates to `publish_to_bcr`. There are people who are willing to work with me on that.

<https://github.com/bazel-contrib/supply-chain/pull/188>

- A discussion of names.
- Module name: `purl.bzl`
- Top level folder: `purl`

yannic@engflow.com and antonio@engflow.com meeting next week to start on a BazelCon talk.

May 21, 2026

May 21, 2026

Attendees: simon.m.stewart@gmail.com lavoie.richard@gmail.com
kaloyan.raev@broadcom.com yannic@engflow.com antonio@engflow.com Tony Aiuto

https://mpregional.org/documents/2015/1/Whos_on_First.pdf

Status updates:

- Richard: Generic purl parser with extensions
- Antonio: Working on turn output to a pure graph structure
- Working on a doc to annotate edges with the relationship type
- Yannic: working on trying to make a less memory hungry graph
- Tony: Publish workflow failed at attestation checking in the BCR PR. That checks for explicit use of the publish workflow at `bazel-contrib/publish-to-bcr`, but we have a private version. The way attestation checking is set up requires a specific publish script, so we have to upstream this.

Extensible purl parser

<https://github.com/bazel-contrib/supply-chain/issues/185>

Do we add a module extension to add to the purl parser?

- Richard's use was to parse the purl, add some additional data and re-normalize.
- Every user has to bring in the extension
- Injecting things can modify the way purl parsing works, and that breaks sbom generation.
 - Does that matter? If a user does it to themselves, the tools don't work
 - We need to not accept PRs to the contrib section that would do that
- How do we keep up with new purl declarations
 - Churn in metadata release versions is not good.
- Do we need the parser in `package_metadata`?
 - Not really, we can just use the constructor to provide the string.
 - Parsing and normalization can happen in sbom generation.
 - Except for Richard's case.
- The proposal that seemed to get the least resistance was to move purl parsing into a separate module.
-

May 7, 2026

May 7, 2026

Attendees: Tony Aiuto kaloyan.raev@broadcom.com mark.zeren@broadcom.com
lavoie.richard@gmail.com

Notes:

- Tony Aiuto has a PR out to allow submodule release.
<https://github.com/bazel-contrib/supply-chain/pull/170>
- Discussed purl parser/validator <https://github.com/bazel-contrib/supply-chain/pull/171>
 - We will need an extension point
 - It probably should be a submodule.
 - Or a toolchain?

Apr 30, 2026 | Bazel supply chain
weekly sync

Apr 30, 2026 | 📅 Bazel supply chain weekly sync

Attendees: shs@block.xyz emrah.yasar@broadcom.com Lipsa Rout
tony.aiuto@datadoghq.com kiril.raykov@broadcom.com Luis Pino billie.alsup@gmail.com
salazar@engflow.com Yannic Bonenberger Mark Zeren aiuto@bazel.build
elitsa.shishkova@broadcom.com kaloyan.raev@broadcom.com sugak@meta.com
simon.m.stewart@gmail.com ANKUSH KUMAR Florian Weikert sluongng@gmail.com
Alex Eagle gspencer@nvidia.com steve.barrau@gmail.com lavoie.richard@gmail.com
tony@aiuto.dev ~~fabian@meumertzhe.im~~ ~~Antonio Di Stefano~~ ~~Yaar Schnitman~~
~~fwe@bazel.build~~

Notes

- 0.0.10 release
 - Release process bug has been fixed, but the publish-to-bcr app sent an error via email
 - PR: <https://github.com/bazelbuild/bazel-central-registry/pull/8634>
-

Action items



Apr 23, 2026

Apr 23, 2026

Attendees: simon.m.stewart@gmail.com yannic@engflow.com fwe@google.com
lavoie.richard@gmail.com kaloyan.raev@broadcom.com Tony Aiuto antonio@engflow.com

Notes

- Call for BazelCon papers is out. <https://sessionize.com/bazelcon-2026/> deadline is in June
 - For now, default is to keep same format as last year. BoF and a status talk
- [Florian] Who will attend the Hackathon in MUC on May 12th?
 - Tony won't be able to travel
 - No one from Broadcom can go either
 - Most likely only Yannic, Antonio, Florian and maybe Helen?
 - Florian will post in the Slack channel to see if there are other participants
- Tony still looking at why we can't release
- We should start on an [Agents.md](#) file or two
 - Tony will try
- Richard
 - Topics from slack.
<https://bazelbuild.slack.com/archives/C04AZC3E729/p1776183985345459>
 - <https://bazelbuild.slack.com/archives/C04AZC3E729/p1776606604314269>
- Workspace BOM
 - Current line of work requires a `bazel fetch all` (or equivalent). Is that going to cause problems for anyone.

Apr 9, 2026 | Bazel supply chain weekly sync

Apr 9, 2026 | 📅 Bazel supply chain weekly sync

Attendees: Antonio Di Stefano shs@block.xyz emrah.yasar@broadcom.com Lipsa Rout
tony.aiuto@datadoghq.com kiril.raykov@broadcom.com Luis Pino billie.alsup@gmail.com
salazar@engflow.com Yannic Bonenberger Mark Zeren aiuto@bazel.build
elitsa.shishkova@broadcom.com kaloyan.raev@broadcom.com sugak@meta.com
simon.m.stewart@gmail.com ANKUSH KUMAR Florian Weikert sluongng@gmail.com
alex@aspect.build gspencer@nvidia.com steve.barrau@gmail.com tony@aiuto.dev
~~fabian@meumertzhe.im~~ ~~Yaar Schnitman~~ ~~fwe@bazel.build~~

Notes

- Hackathon
 - [fwe] Secured a room for the May 12th hackathon (Google ARN60 office where the Bazel team is located - <https://maps.app.goo.gl/DSZgEhmfKvxq9YL89>)
 - [fwe] I'll send a survey regarding attendance and food options (there will be lunch + snacks, maybe breakfast)
 - Who will attend?
- Release seem broken
 - Tony will try a release day
- Workspace BOM
 - There is an existing flag that can dump all the repo info post build
 - This works for most people
 - build packages
 - post process workspace info dump into SBOM
- There is a thread slack about adding dependency edges
 - The current implementation is probably doing the single level up from the SBOM entries to find the root causes of dependencies.
 - Not sure if that matches the request in
 -

Action items

- ☐ Send a survey for the hackathon May 12, 2026
- ☐

Mar 26, 2026

Mar 26, 2026 | 📅 Bazel supply chain weekly sync

Attendees: shs@block.xyz emrah.yasar@broadcom.com Lipsa Rout
tony.aiuto@datadoghq.com kiril.raykov@broadcom.com Luis Pino billie.alsup@gmail.com
salazar@engflow.com Yannic Bonenberger Mark Zeren aiuto@bazel.build
elitsa.shishkova@broadcom.com kaloyan.raev@broadcom.com sugak@meta.com
simon.m.stewart@gmail.com ANKUSH KUMAR Florian Weikert sluongng@gmail.com
Alex Eagle gspencer@nvidia.com steve.barrau@gmail.com tony@aiuto.dev
~~fabian@meumertzhe.im~~ ~~Antonio Di Stefano~~ ~~Yaar Schnitman~~ ~~fwe@bazel.build~~

Notes

- Hackathon in Munich on May 12, one day after the Build Meetup
 - Florian is looking into getting Google to host it, and will keep everyone updated.
- Yannic: Tried to create a release some weeks ago, but the pipeline failed for some weird reason
 - <https://github.com/bazel-contrib/supply-chain/actions/runs/23058544378>

Action items

- ☒ ~~Florian Weikert~~ Cancel next week's meeting (Easter holidays)
- ☒ ~~Florian Weikert~~ Cancel the APAC meeting (no one has attended in six months)
- ☐ Organize location for the May 12 hackathon
- ☐ Jayson Salazar Look into release pipeline failure:
<https://github.com/bazel-contrib/supply-chain/actions/runs/23058544378>

Mar 5, 2026

Attendees: Mark Zeren yannic@engflow.com tony.aiuto@datadoghq.com Kaloyan Raev
Jayson Salazar

Notes:

- Draft of workspace BOM idea went out
 - Fabian pointed out some problems. Back to research phase
 - Current thinking is that it may have to be post process
- EngFlow London meetup got cancelled, so we don't have a venue for that.
- Multi release: <https://github.com/bazel-contrib/supply-chain/pull/142>
 - The publish to BCR workflow does modules, but only at the same version number, so it doesn't help
 - Tony is trying to figure out a low cost (in development time) replacement.

Feb 26, 2026

Feb 26, 2026

Attendees: tony.aiuto@datadoghq.com Mark Zeren simon.m.stewart@gmail.com
~~Florian Weikert~~ gspencer@nvidia.com Yannic Bonenberger @jayson.salazar
kaloyan.raev@broadcom.com

Agenda:

- <https://github.com/bazelbuild/remote-apis/issues/368>
- Should we release things?

Notes

- Mark Zeren and tony.aiuto@datadoghq.com chatted about package compare tools but then we switched to the real meeting.
- Discussed  Design Document: Incremental Repository Resolution Tracking in Bazel
 - the proposal is sort of out of date before it was published
 - risk that compliance issues get in the way of performance
- Later post identifies three areas of discussion
 - https://bazelbuild.slack.com/archives/C04AZC3E729/p1772040120541089?thread_ts=1771519057.442229&cid=C04AZC3E729
- Should the workspace lock info be available to rules
 - at repo loading time?
 - at analysis time?
 -

Feb 5, 2026

Feb 5, 2026

Attendees: shs@block.xyz tony.aiuto@datadoghq.com Mark Zeren
simon.m.stewart@gmail.com ~~Florian Weikert~~ gspencer@nvidia.com Yannic Bonenberger
@jayson.salazar kaloyan.raev@broadcom.com

Notes

- rules_jvm_external shipped last night
- purl functions merged last night
- upstream tests cases found an encoding problem.
- Kaloyan reports internal broadcom success with workspace bom.
 - still requires a patched bazel
 - almost ready to show it and open it for discussion in slack
- Tony out the next two weeks.
-

Jan 29, 2026 | Bazel supply chain
weekly sync

Jan 29, 2026 | 📅 Bazel supply chain weekly sync

Attendees: fabian@meumertzhe.im Antonio Di Stefano shs@block.xyz
tony.aiuto@datadoghq.com Mark Zeren simon.m.stewart@gmail.com Florian Weikert
gspencer@nvidia.com ~~Yannic Bonenberger~~ ~~fwe@bazel.build~~

Notes

- https://github.com/bazel-contrib/rules_python/pull/3531
 - adding metadata to python wheels
 - pinged yannic@engflow.com
- Mark working on workspace BOM but still not ready.
- gspencer@nvidia.com gave an intro.
 - dev automation team at nvidia
 - security groups want SBOMs
 - also cares about build profiles
- Meetup?
 - Maybe London Feb?
 - Munich June
- This to work on
 - landing js patch
 - test cases for aspect traversal

Action items



Jan 22, 2026

Jan 22, 2026

Attendees: yannic@engflow.com Mark Zeren

Notes

- Mark built a demo for Alex Eagle to present at Endor Labs meetup Jan 15, 2026
 - <https://github.com/bazel-contrib-supply-chain-extras/selenium/pull/3>
- Tony, Antonio and Kaloyan are out this week. Yannic will miss next week for AMS meetup.
- antonio@engflow.com can you take a look at the cyclone dx PR: <https://github.com/bazel-contrib/supply-chain/pull/143> ?
- Yannic is still working on the PURL builder. Type specific normalization will need to be follow-on PRs.
- Kaloyan Raev and Emrah Yasar continue to work on workspace BOM patches. We identified a design issue this week where we currently require a clean build. We'll do further investigation to resolve that.

Jan 15, 2026

Jan 15, 2026

Attendees: simon.m.stewart@gmail.com yannic@engflow.com
mark.zeren@broadcom.com Tony Aiuto alex@aspect.dev kaloyan.raev@broadcom.com

Notes:

- Kaloyan working on workspace BOM. Near the point where it works. It is a patch against Bazel upstream. Working with 8.4.2.
- Request for an example project that works with the ssc rules
 - Forks of rules in [git@github.com:bazel-contrib-supply-chain-extras/rules_js.git](https://github.com/bazel-contrib-supply-chain-extras/rules_js.git)
 - <https://github.com/bazel-contrib-supply-chain-extras/selenium/tree/topic/mzeren/example-license-info>
- Have we upstreamed all the work in the repos in supply-chain-extras?
 - jvm_external: yes.
 - rules_python: Tony will try
 - rules_js:
 - rules_rust: Alex will try.
- For multi-module publishing
 - look at rules python
 - need to extend the publish to BCR module to accept a list of modules to publish
 - Send PRs to Derek
 -
- <https://github.com/bazel-starters>
 - Alex will add SBOM examples there.
- Yannic working on the extended purl encoder.
 - almost there
 - led to side discussion about purls in the BCR to identify upstream repos that the BCR wraps.
- Build Foundation
 - Sub foundation from Linux Foundation
 - Funds various efforts
 - One of the examples is BCR outage last week. It could run a mirror of that.
- Next meetup time
 - Tony might be in Paris March 16-20
 - Engflow summit in Munich this year. Maybe piggyback on that.

Jan 8, 2026

Jan 8, 2026

Attendees: Tony Aiuto yannic@engflow.com simon.m.stewart@gmail.com
kaloyan.raev@broadcom.com

Notes:

-

Dec 18, 2025

Dec 18, 2025

Attendees: Tony Aiuto mark.zeren@broadcom.com simon.m.stewart@gmail.com
yannic@engflow.com

- <https://github.com/bazel-contrib/supply-chain/pull/140> to do separate releases
 - did quick review
- will turn off renovate, added issues to come back to a better configuration
- Do we do a release for docs and examples?
 - No, so just push to the doc site
- Separate all the releases.

Purl builder

- looking for Fabian's PR to add

We should start a project to upgrade modules in the BCR

- Example: A an old C project with a BCR entry that just adds a BUILD file
- Yannic: Add two metadatas with two PURL.
 - One for the upstream
 - One for the module.
- Tony: This is perfect jobs for vibe coding
 - Pull the upstream repo
 - Find the license files
 - See what we can find
- Tony: would like to have a copyright attribute in place first.

Next meetup:

- still hunting
-

Dec 11, 2025

Dec 11, 2025

Attendees: tony.aiuto@datadoghq.com yannic@engflow.com Mark Zeren
kaloyan.raev@broadcom.com

Updates from last week:

- aiuto: CI is fixed - just by waiting long enough for Bazel to fix the rolling release.
-

New topics:

- Fabian's proposed bazel change
 - Splice in metadata for modules without REPO.bzl
 - This would make behavior very different between the bazel versions
 - It doesn't really help for modules that wrap something non-bazel with a BUILD file. We want metadata pointing to the upstream project, not the bazel module.
- Kaloyan described what he is doing
 - Hooks to get good workspace info out
 - We should get the two together to compare.
- [aiuto] purl cleanliness
 - PR reviews
 - <https://github.com/bazel-contrib/supply-chain/pull/38>
 - <https://github.com/bazel-contrib/supply-chain/pull/133>
 - purls for generic http download
 - <https://github.com/bazel-contrib/supply-chain/issues/124>
 - Proposal:
 - Agree that
pkg:generic/attr@2.5.1?download_url=<https://download.savannah.gnu.org/releases/attr/attr-2.5.1.tar.xz> Is the right syntax.
 - provide a function in purl.bzl to create this
- Override rule
 - Let's go.
- <https://github.com/bazel-contrib/supply-chain/pull/134>
 - investigate if we really need this.
- Do another hackathon
 - Around Build Meetup is best.
 - London is good timing, but need dates
-

Dec 4, 2025

Dec 4, 2025

Tony Aiuto simon.m.stewart@gmail.com mark.zeren@broadcom.com fwe@google.com
yannic@engflow.com kaloyan.raev@broadcom.com

Notes:

- Need to review the outstanding PRs.
 - <https://github.com/bazel-contrib/supply-chain/pull/129>
 - <https://github.com/bazel-contrib/supply-chain/pull/38>
- Complaints from people that it doesn't work.
- Dealing with multi-release:
 - Do not merge: <https://github.com/bazel-contrib/supply-chain/pull/122>
 - How do we store.
 - Proposal: Name the releases <name>-<version>, so that we have metadata-0.0.7, supply_chain_tools-0.1.0, ..
 - Github UI makes it ugly
 - We can work around that with a clever readme
 - ~~The BCR UI needs some fixing because~~
 - Tony will take a look
- Discussion about override
 - Do we do this as a toolchain in the aspect
 - or as a list of overrides to sbom rule
 - toolchain allows us to override an sbom rule from a dependency. Like envoy with the sbom rule they have.
 -
- Urgent bit:
 - releasing new tools
- BCR update
 - https://registry.bazel.build/modules/supply_chain_tools
- Cancel 12/25 and 1/1

Nov 20, 2025

Nov 20, 2025

mark.zeren@broadcom.com kaloyan.raev@broadcom.com fwe@bazel.build

Topics

- fwe@bazel.build still working on BoF notes.
- We need to release 0.0.7 because .6 is missing a fix in supply-chain-go, reported in Slack. Need to coordinate on Slack.
- Kaloyan Raev has made progress on workspace BOM internally. Current best solution requires a patch to Bazel, which will require socializing.

No quorum, as expected. Next week is a US holiday so expecting to meet again Dec. 4

Nov 13, 2025

Nov 13, 2025

Tony Aiuto mark.zeren@broadcom.com kaloyan.raev@broadcom.com

multi release?

- The registration for tools is unstable.
- Go library is paired with metadata
- When do we create a new release?
 - We do a release at any change
 - but the BCR entries are the same.
- Should we look at git large blob store
- Ankush and Mark looking into it.
- proposal:
 - The "release" page based on metadata
 - Other tools build artifacts and push to that release. There may be many versions of each module in the download page.
 - When metadata changes, we need everything else anyway, so we push everything.

Meeting time change

- Kaloyan has a repeating conflict, but maybe resolved

Workspace BOM

- Kaloyan working on a flag for bazel that brings back the equivalent of the old resolved file.
- Also tried, exposing data through a native method.
- If it emits a file, you need to be able to depend on it, but don't make it volatile.

Copyright

- Should we handle it as an attribute? Build a tool to scan the likely sources for author info (LICENSE, AUTHORS, ...) and produce the list?
- Or should this be offline and checked in.

Nov 2, 2025 - working session

Nov 3, 2025

Notes

-  Bazelcon 2025 - supply chain
- I inverted the tabs in this document. Newest on top.
- Need README / doc for <https://github.com/bazel-contrib/supply-chain/tree/main/lib/supplychain-go>
- Can BCR have a pointer into a subdirectory of a repo?
 - Tony will investigate
 -
- Add Tony to maintainers for https://registry.bazel.build/modules/package_metadata
- <https://github.com/bazel-contrib/supply-chain/>
 - Documentation -> <https://github.com/bazel-contrib/supply-chain/blob/main/docs/tools> is a 404
- We should have toolchain contributions to composition on our roadmap
-

Sildes notes

- Tony added some slide backgrounds from 2023 or 2024 into the placeholder deck.
 - We gave this link to the LF person:  Supply Chain Rules
 - Joint intro
 - don't want to keep you from lunch
 - Not just just, also Antonio, Yannic, Kaloyan, Simon, Florian ...
-

Oct 30, 2025

Oct 30, 2025 Attendees: Mark Zeren yannic@engflow.com tony.aiuto@datadoghq.com
simon.m.stewart@gmail.com fwe@bazel.build antonio@engflow.com Kaloyan Raev

Demo Org: <https://github.com/bazel-contrib-supply-chain-extras>

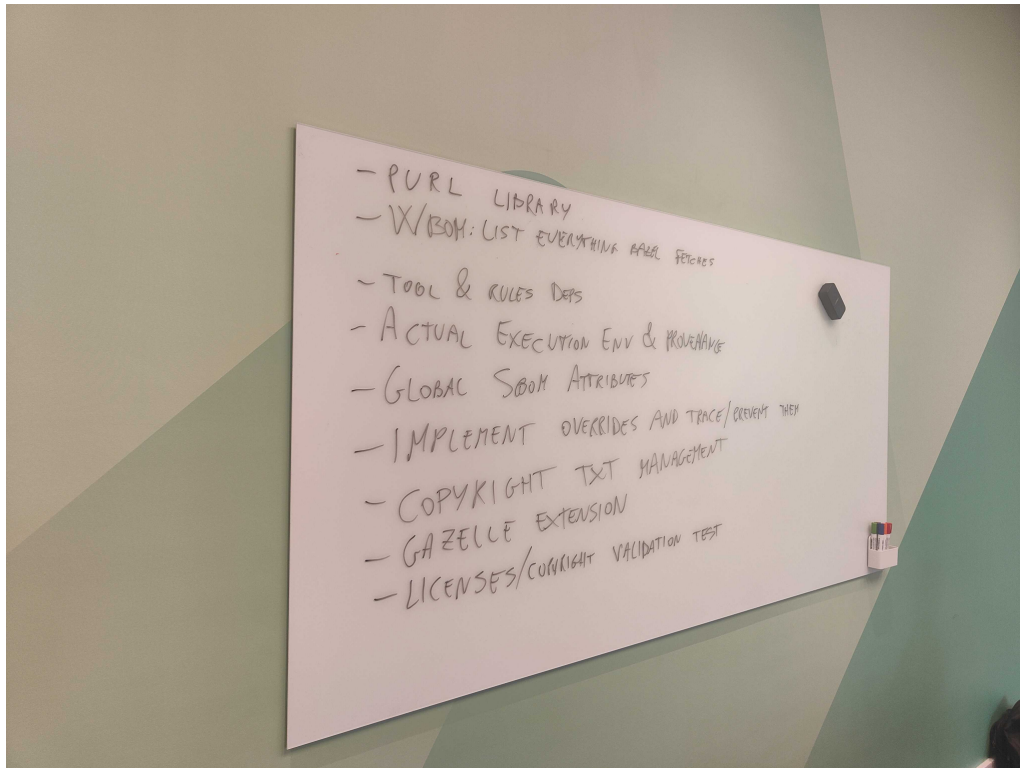
Oct 27, 2025 - working session

Oct 27, 2025 working session

Attendees: Mark Zeren antonio@engflow.com tony.aiuto@datadoghq.com
yannic@engflow.com Kaloyan Raev

AI:

- rules_python - antonio@engflow.com : it's missing an integration tests and then PR
- rules_js - Mark Zeren : upstream changes
- another ruleset Antonio forgot about
- antonio@engflow.com writing roadmap issues from the infamous whiteboard



- launch supply-chain survey
- BOF agenda - Supply-Chain BOF - BazelCon 2025 Slides:
 - ▣ Supply Chain Rules
- pretty slides and material for the talk
- launch override mechanism
- test SPDX more extensively and fix any pending bugs
- yannic@engflow.com override mechanism
- Legacy license support tony.aiuto@datadoghq.com antonio@engflow.com
- <https://github.com/bazel-contrib/supply-chain/pull/82>
-

Oct 23, 2025

Oct 23, 2025

Attendees: yannic@engflow.com Mark Zeren antonio@engflow.com
tony.aiuto@datadoghq.com fwe@bazel.build

Aiuto joining late (around 8:45)

Topics

- aiuto@ rewrote the gathering tool to be much closer to the old way
 - examples/sample_reports/licenses_used.bzl is a good example of how to walk it
 - the outer loop is to expand a depset of all the targets where we have explicitly set attributes via package_metadaa.
 - the inner loop is to expand the depset of attributes for that target.
 - pr #93 has it
- Moving examples to top level.
 - Let's just do a "rip the bandaid off" PR and move that.
- Talk
 - Outline looks good
 - Let's do a primitive local override. I can work that into a license report
 - Basically just a lookup table of package to Copyright
 - Why that way? Because copyright stuff is not often in BUILD files and every company has their own process for how they guess it from LICENSE files.
 - We can do this in the writer action.
 - We do need a diagram of how these late overrides work.
 - Override in mid flight (like the toolchain approach for static vs shared) will
- The mock rules_license that emits Attributes is ready. It is still a little hard to use
 - You can bring it in to the repo pretty easily from a tag that we publish.
- Internally Kaloyan Raev has been experimenting with
`--experimental_repository_resolved_file` this requires a `--nobuild` and then a normal build.

```
http_archive(  
  name = "package_metadata",  
  sha256 = "5bd0cc7594ea528fd28f98d82457f157827d48cc20e07bcfdbb56072f35c8f67",  
  strip_prefix = "supply-chain-0.0.6/metadata",  
  urls = ["https://github.com/bazel-contrib/supply-chain/archive/refs/tags/v0.0.6.tar.gz"],  
)
```

the rules_license overlay will never be available in the BCR, for obvious name confusion reasons.

```
http_archive(  
  name = "rules_license",
```

```
# sha256 = TBD,  
strip_prefix = "supply-chain-dd_test/rules_license",  
urls = ["https://github.com/aiuto/supply-chain/archive/refs/tags/dd_test.tar.gz"],  
)
```

.
And this works for any rules_license instances we get explicitly (vendored code) but if rules_license comes in from bzlmod via bzl_dep() bzlmod uses that reference. Sigh. That's just broken. I think the easiest solution is to provide a fake BCR entry for the fake rules_license. People will have to vendor that be in and splice it via a command line flag from .bazelrc. I'll try that today, but we don't have to block the first PR on that instance.

Oct 20, 2025 - working session

Oct 20, 2025 working session

Attendees: yannic@engflow.com antonio@engflow.com tony.aiuto@datadoghq.com

Mark Zeren

Notes:

-

Slides:

- (Mark brainstorming for  Bazelcon 2025 - supply chain)
- Title
- Intro
 - Compliance requirements
 - Reduce toil
 - Call to action
- History
 - rules_license
 - Independent impls and talks: VMware, Google, Apple, Engflow, .
- New generation
 - bazel-contrib/supply-chain
 - Packages
 - https://registry.bazel.build/modules/package_metadata
 - Aspect?
 - package_metadata_extensions
 - Overrides
 - Aspect?
 - TBD: sbom example
- Selenium demo
 -
- Local overrides
 - Needs diagram
- Future work
 - Workspace BOMs
- Other concerns
 - Come to BoF
 - BCR attestations
 - ... ?
- Conclusion and Call to Action
 -

Oct 16, 2025

Oct 16, 2025

Attendees: Tony Aiuto mark.zeren@broadcom.com antonio@engflow.com
yannic@engflow.com kaloyan.raev@broadcom.com

Notes:

- Tony's idea to make rules_license a module may not work. Going to modify rules_license instead.
- Yannic on override toolchain. Not much progress (lack of time), but has a workable idea.
- We are all overworked in our day jobs.
 - Set up working group meeting for Monday

AI:

- Antonio Di Stefano share last year's survey results 
https://docs.google.com/forms/d/1NQhgtNnrocU7jSic80A4wR8G6smDPQSVA2dgPPP-G0w/edit#response=ACYDBNizHwo3Bclle-ks9_6a7QgJ60CvYWCDZFF5QtkCpkCvh1fjXA4-doE1QkiJLmhlHJY
- Tony Aiuto Add CI check for examples

Oct 9, 2025

Oct 9, 2025 Mark Zeren simon.m.stewart@gmail.com fwe@bazel.build Jayson Salazar

Topics

- Survey:
 - Jayson Salazar will ping antonio@engflow.com regarding Bazelcon survey
- Renovate
 - We should, within <https://github.com/bazel-contrib/supply-chain/tree/main>, not be renovating our module quickly. This makes migration more expensive for consumers
 - Instead we should be renovating a *test* that document / proves we can work with the latest version.
 - <https://blog.engflow.com/2025/07/08/migrating-to-bazel-modules-aka-bzlmod---maintaining-compatibility-part-1/>
 - Created: <https://github.com/bazel-contrib/supply-chain/issues/81>
- rules_oci
 - Would be a good next thing in selenium
 - simon.m.stewart@gmail.com suggested requiring each image to define a platform. Simon can help introducing to folks at Apple.
- BazelCon
 - Mark Zeren will start on presentation in next few days (even though he's been saying that for a while)
- Workspace bom in bzlmod
 - simon.m.stewart@gmail.com : One strategy is to crack all the lock files.
 - Set of possible lock files is manageably small.
 -

Oct 2, 2025

Oct 2, 2025

Tony Aiuto yannic@engflow.com alex@aspect.dev Jason Salazar

Rambling discussions about

- Deprecation of rules_foreign_cc
 - aiuto@ will do unconference session at bazelcon to compare notes with Andre Briscoe and David Z.
- Lack of governance of the BCR for anything that is not a Bazel rule
 - The source.json points to the upstream repo (e.g. zlib), but we want to point to the project that maintains the BUILD file for the upstream C++
 - This is another Bazelcon discussion topic
- Pushing our WIP code upstream
 - To happen mostly during the Bazelcon hackathon day
-

Sep 25, 2025

Sep 25, 2025

- Upgrading legacy rules_licenses.
 - Should we just provide alternate implementation that makes the attributes?
 - You would have to vendor it in and use local_repository_override.
 - Or maybe single_version_override with a custom registry that fakes our own.
- We are all sort of stunned today...
- gatherer returns a function?
- Alex Eagle published aspect starter projects
 - <https://blog.aspect.build/announcing-bazel-starters>
 -
 - We should get stuff working with his
 -

Sep 18, 2025

Sep 18, 2025

Attendees: Mark Zeren Kaloyan Raev yannic@engflow.com salazar@engflow.com
antonio@engflow.com

- Mark is still on the upstreaming part of the Amsterdam work and starting on the BazelCon talk presentation
- Yannic is looking at toolchain options for different Bazel versions
- Antonio is still on the upstreaming from last week
- BazelCon
 - Jayson asked if he could undertake some work/items - one option is anonymising last year's poll data so we can create a new poll for this year's BazelCon
 - Asking the community about current use cases and what their needs are at the moment
- Heavy schedule for most of us, so wrapping up a bit early

Sep 11, 2025

Sep 11, 2025

Attendees: Mark Zeren yannic@engflow.com tony.aiuto@datadoghq.com fwe@bazel.build
antonio@engflow.com

- AI review bot
 - <https://github.com/bazel-contrib/supply-chain/pull/72/files>
 - fwe@bazel.build will ask pcloudy@google.com how / where this is configured
 - Mark Zeren would like the prompt to encourage being more concise (review comments word count N x overall review)
- BazelCon
 - Mark Zeren will go to Aspect hackathon Wed. Tony Aiuto not sure.
- yannic@engflow.com looking at how we do overrides
 - Thinks he has a solution for overriding parts of the metadata
 - It might involve a Bazel change. That can open the possibility of a cyclic dependency on toolchains, so it is controversial.

Als

- Tony Aiuto will work on "Auto-grab old license and synthesize PackageAttributeInfo"
- Tony Aiuto will try the rules_js patch internally

Sep 4, 2025

Attendees: Mark Zeren yannic@engflow.com tony.aiuto@datadoghq.com
simon.m.stewart@gmail.com fwe@bazel.build Kaloyan Raev antonio@engflow.com
Jayson Salazar

Notes Recap of last week

- The best we can do is gather all the attribute files and give reference implementation of a gatherer and SBOM printer. Organizations will blend their overrides into their printer instance.
- Noticed that the purl spec is annoyingly complex. We need to build a better encoder for that.
- Collect purls, best effort for everything else. Need to model duplicate purl but different metadata label.
- Simon described a common thing seen where in the same purl and maven coordinates exist in a large code base. Other attributes will distinguish them.
- Do we collect data files only or allow things in memory. Tony concedes and will not die on the hill of analysis time computation. We can deal with that capability (if needed) in 2026Q1.
- Need to also capture build graph.
- Mark talked about Jason Cappos' work with attestations
 - Capture all files & network access during the build.
 - Compare with our output to make sure there are not rogue files.
 - Should we mention this in the Bazelcon talk
- Whiteboard AI
 - purl library
 - Workspace BOM list everything Bazel fetches
 - Tool & Rule defs
 - Actual execution env and provenance
 - Global SBM attributes
 - Implement overrides and trace/prevent them.
 - Copyright text management
 - Gazelle extension
 - Licenses / Copyright validation test

New topics

- Copyrights. How are we extracting them at our own companies?

Action items:

- How to re-integrate our work
- We have forked several repos
 - <https://github.com/orgs/bazel-contrib-supply-chain-extras/repositories>
 - Selenium - because it is an example
 - rules_python

- rules_js
 - rules_jvm_external
 - rules_ruby
 - rules_esbuild
- Collection
 - <https://github.com/bazel-contrib/supply-chain/pull/64>
 - Add dep graph edges
 - Pull up patch for dict of label attributes
 - see <https://github.com/bazel-contrib/supply-chain/compare/main...topic/mzere n/fixup-gather#diff-16f5daadee004663f55627bb22f655f4d736ace9bdb134be44648addbdb34362R64>
 -
 - Auto-grab old license and synthesis PackageAttributeInfo
-

Aug 21, 2025

Aug 21, 2025 Bazel supply chain weekly sync

antonio@engflow.com tony.aiuto@datadoghq.com Mark Zeren Kaloyan Raev
simon.m.stewart@gmail.com

Agenda:

- Last minute plans for hackathon
 - Meet at 2pm at OSS con site.
 -
 - What our our success outcomes?
 - i. That we have a plan for BazelCon.
 - Outline of Bazelcon presentation
 - Then plan for what we can do in 2 months that make the preso better.
 - ii. Basic SBOM generator. selenium is proposed target
 - iii. Mark: have plan for how Broadcom (as one example) can upstream their work to the tools repo.
 - iv. rules_java integration maybe?
- [aiuto]: Release cadence
 - We can't do release on every tools change. That causes needless renovate bot churn.
 - So, we need policy on how people will use it.
 - i. bcr will only contain metadata pointer and we encourage git commit pin for tools?
 - ii. bcr only has metadata pointer and vendor in tools periodically
 - iii. roll your own.
 - Who will own writing this guidance? AI: Tony Aiuto
- If someone can review PR for gathering tool, that would be great.
-

Aug 14, 2025

Aug 14, 2025

Notes

- Discussion about the complaint about the way we do the release.
- We will have to fix that someday, when we start doing differential releases. But not today.
- Yannic has a PR out to set package_metadata into platforms
 - <https://github.com/bazelbuild/platforms/pull/122>
 - We agree it should work.
 - fwe: should be the approver
 - mz: should try at broadcom
- Meetup end of Aug.
 - Mark/Kaloyan are there all week
 - Tony arrives Wednesday morning
 - Datadog office. [Herengracht 601, 1017 CE Amsterdam, Netherlands](https://www.google.com/maps/place/Herengracht+601,+1017+CZ+Amsterdam,+Netherlands/@52.3655782,4.8964532,17z/data=!3m1!4b1!4m6!3m5!1s0x47c6099590c67f55:0xfc66d4cab37bcf7e!8m2!3d52.3655782!4d4.8986419!16s%2Fg%2F11c21sj1xk)
 - <https://www.google.com/maps/place/Herengracht+601,+1017+CZ+Amsterdam,+Netherlands/@52.3655782,4.8964532,17z/data=!3m1!4b1!4m6!3m5!1s0x47c6099590c67f55:0xfc66d4cab37bcf7e!8m2!3d52.3655782!4d4.8986419!16s%2Fg%2F11c21sj1xk>
 -

Aug 7, 2025

Aug 7, 2025

Attendees: Tony Aiuto mark.zeren@broadcom.com Kaloyan Raev

- Long discussion of passing up attribute vs. only JSON
- Use cases
 - Fail hard quick if you mix tagged data
 - go.mod support - Need to add that to roadmap
 - import package metadata.
- We need a use case document
 - [Bazel Supply Chain Use Cases](#)
 - *Kaloyan I didn't have your email in my bazel.build account, so you can open it and ask for write access.*
- Should purl be privileged or just another attribute
 - A: Because it must be unique.
 -

31 Jul 2025 | Bazel supply chain weekly
sync

31 Jul 2025 | 📅 Bazel supply chain weekly sync

Attendees: mark.zeren@broadcom.com aiuto@bazel.build

Notes

- tony.aiuto@datadoghq.com has reserved a room at DataDog AMS Thurs. Aug. 28 - Fri. Aug 29. Adjacent to <https://events.linuxfoundation.org/open-source-summit-europe/>
 - yannic@engflow.com is OOTO this week. antonio@engflow.com can't answer about AMS this week.
 -

24 Jul 2025 | Bazel supply chain weekly
sync

24 Jul 2025 | 📅 Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com
kaloyan.raev@broadcom.com lipsa.rout@broadcom.com fwe@bazel.build
simon.m.stewart@gmail.com kiril.raykov@broadcom.com Florian Weikert
sluongng@gmail.com Yannic Bonenberger mark.zeren@broadcom.com
aiuto@bazel.build Antonio Di Stefano billie.alsup@gmail.com fabian@meumertzhe.im
alex@aspect.build Jayson Salazar tony.aiuto@datadoghq.com shs@block.xyz
tony@aiuto.dev ~~davidkurkov@lyft.com~~ ~~yaar@google.com~~ ~~Luis Pino~~

Notes

- tony.aiuto@datadoghq.com started creating tools to collect package metadata
 - <https://github.com/bazel-contrib/supply-chain/pull/41>
- Yannic Bonenberger created 0.0.5
 - Ran into issues where BCR publish created draft PR

Action items



17 Jul 2025 | Bazel supply chain weekly
sync

17 Jul 2025 | 📅 Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com
kaloyan.raev@broadcom.com lipsa.rout@broadcom.com davidkurkov@lyft.com
fwe@bazel.build simon.m.stewart@gmail.com kiril.raykov@broadcom.com
Florian Weikert sluongng@gmail.com Yannic Bonenberger mark.zeren@broadcom.com
aiuto@bazel.build billie.alsup@gmail.com fabian@meumertzhe.im alex@aspect.build
Jayson Salazar tony.aiuto@datadoghq.com shs@block.xyz tony@aiuto.dev
~~yaar@google.com~~ ~~Antonio Di Stefano~~ ~~Luis Pino~~

Notes

- tony.aiuto@datadoghq.com Found mailing list
 - Now in the readme
- Yannic Bonenberger did a release. 0.0.4
- Discussion of the purl building PR
 - Bazel 8 changed how json.decode works w.r.t the latin-1 trick. Now it reads as UTF-8, changing to UCS-16
 - The tests are failing on Bazel 7. Do we drop them or try to fix?
 - Purl spec:
 - encode string as UTF-8, then % encode
 - Consider adding to starlark
 - String as bytes -> sequence of the latin-1 trick bytes
 - byte list to string w/ no interpretation
 - Jul 18, 2025 Followup - aiuto did alternate version without json.encode()
- Hackathon time
 - Tony looks likely to get space in Amsterdam Aug 29.
 - Continue discussion in Slack

Action items



14 Jul 2025 | Bazel supply chain weekly
sync

14 Aug 2025 | 📅 Bazel supply chain weekly sync

Attendees: Mark Zeren yannic@engflow.com tony.aiuto@datadoghq.com
simon.m.stewart@gmail.com fwe@bazel.build Kaloyan Raev

Topics:

- We discussed tagging vs. branching and will continue with existing workflow.
 - <https://github.com/bazel-contrib/supply-chain/issues/50>
- <https://github.com/bazelbuild/platforms/pull/122/files>
 - Asking fwe@bazel.build for help with approval from Bazel team
 - Mark Zeren / Kaloyan Raev will look at consuming internally.
 -

Jul 10, 2025

Jul 10, 2025

Agenda:

- Quick exchange of PR status
- Proposal for talk submitted
- Yannic is about to do a new release
- Constructing PURL for `package\_metadata` is hard
 - Yannic Bonenberger to focus on improving this next
 - Likely blocker for wider adoption
- Tony will start on an aspect.
 - Discussion about likelihood of every company needing it to fork or not.
 -
- Hackathon events possibilities
 - Slack thread
<https://bazelbuild.slack.com/archives/C04AZC3E729/p1752153983218899>
 - Amsterdam OSSSummit
 - Aug 25-27 <https://events.linuxfoundation.org/open-source-summit-europe/>
 - Aug 28 <https://events.linuxfoundation.org/container-plumbing-days/>
 - Aug 28 <https://events.linuxfoundation.org/openssf-community-day-europe/>

Action items

- ☒ ~~Check why the mailing list seems invisible~~
- ☒ ~~When that is resolved add to [README.md](#)~~
- ☐

July 3, 2025 | Bazel supply chain
weekly sync

Jul 3, 2025 | 📅 Bazel supply chain weekly sync

antonio@engflow.com mark.zeren@broadcom.com yannic@engflow.com fwe@google.com

Tony Aiuto

Agenda:

- [aiuto] Let's discuss coupling of releases. The metadata and tools need to be distinct, so metadata can rev very slowly, while the rest of the stuff can move at faster pace.
 - Maybe we can't do that with github directly, because they don't support multi-releases
 - Can we do sub-projects
 - Can we at least decouple BCR, so that MODULE.bazel for the core data does not rev unnecessarily.
 - Solutions
 - 1: update BCR tooling to allow separate metadata + tools
 - 2: make tags of the form 'metadata-x.y'
 - 3:
- yannic@engflow.com
 - Gazelle extension is published
 - Some packages in BCR depend on package_metadata
 - alex@aspect.dev added package metadata to
 - https://registry.bazel.build/modules/package_metadata
 - Yannic Bonenberger added to @gazelle_cc, PR against @platforms is open
- BazelCon
 - 📅 BazelCon 2025 - supply-chain proposal
 - Mark Zeren will submit
- Other conferences?
 - DPE summit San Francisco Sept 23-24.
 - Tony will be in Paris in October. 6-10, can probably get space in Datadog Paris office for hackathon
 - Japan?
- Rules_java
 - Primary contact: hvd@google.com (<https://github.com/hvadehra>)
 - Secondary contact: ilist@google.com (<https://github.com/comius>)

Action items;

- ☑ aiuto: https://github.com/bazelbuild/rules_license/issues/153
- ☑ Reminder for tony.aiuto@datadoghq.com to do it

Jun 26, 2025 | Bazel supply chain
weekly sync

Jun 26, 2025 | 📅 Bazel supply chain weekly sync

simon.m.stewart@gmail.com yannic@engflow.com Kaloyan Raev fwe@bazel.build
tony.aiuto@datadoghq.com antonio@engflow.com

Notes:

- Discussion about <https://github.com/bazel-contrib/supply-chain/issues/4>
 - Most modules in the BCR are expected to use these tools, so having a very small number of dependencies is good
 - Open to accepting PRs in supply_chain
- BazelCon proposal

Action items;

- ☐ aiuto: https://github.com/bazelbuild/rules_license/issues/153
 - ☐ Reminder for tony.aiuto@datadoghq.com to do it
- ☐ 📑 BazelCon 2025 - supply-chain proposal

Jun 19, 2025 | Bazel supply chain
weekly sync

Jun 19, 2025 || 📅 Bazel supply chain weekly sync

Mark Zeren antonio@engflow.com @salazar@engflow.com

- Created https://docs.google.com/document/d/1cotKFI9ttUzFZH1n6_kLrD6weS8wSO90-trjvRwAMdY/edit?tab=t.0#heading=h.gi4hefymxq44 to track mark.zeren@broadcom.com 's proposal for bazelcon 2025
 - Will add BoF. Prep for submission next week.
- Antonio Di Stefano review Yannic Bonenberger 's PRs
- Richard is just looking at improving SBOM for his company's monorepo. Predominantly Go, but a bit of everything else too.
- Relevant docs for the ruleset: <https://github.com/bazel-contrib/supply-chain/tree/main/docs/metadata>

Jun 12, 2025 | Bazel supply chain
weekly sync

Jun 5, 2025 | 📅 Bazel supply chain weekly sync

yannic@engflow.com Kaloyan Raev Mark Zeren tony.aiuto@datadoghq.com

- BazelCon CFP is open. We should propose something for bazel-contrib/supply-chain
 - Mark Zeren is planning to go.
 - Mark Zeren will draft proposal.
- tony.aiuto@datadoghq.com has not made progress on deprecation.
- Kaloyan Raev internally has been experimenting with “workspace manifests” that work with bzlmod, with rules_jvm_external for now.
- yannic@engflow.com is still waiting for PR reviews.
- We will move the meeting to 8:30 AM Eastern.

Talk Notes

- Introl to bazel-contrib/supply-chain
- Demo project, ideally published in BCR
- Deprecation and maintenance of rules_license
- Future directions.
- A lightning talk is do-able today. 30 minute slot.

Jun 5, 2025 | Bazel supply chain weekly sync

Jun 5, 2025 | 📅 Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com
kaloyan.raev@broadcom.com Lipsa Rout davidkurkov@lyft.com
simon.m.stewart@gmail.com kiril.raykov@broadcom.com Florian Weikert
sluongng@gmail.com Yannic Bonenberger Mark Zeren aiuto@bazel.build
billie.alsup@gmail.com fabian@meumertzhe.im alex@aspect.build Luis Pino
salazar@engflow.com tony.aiuto@datadoghq.com tony@aiuto.dev ~~fwe@bazel.build~~
~~Yaar Schnitman~~ ~~Antonio Di Stefano~~

Notes

- BCR had 84 dependents on rules_license. Can we query to “burn down” to 0 for most recent versions.
 - we should focus on package managers first. crate, go
- Yannic looking at how to inject/replace metadata to override what might be in the upstream repository.
- Can we auto-inject bzlmod package into metadata
 - It is in the lock file. We can read it.
- Futures:
 - Why did this dependency get include? Tools to answer that?
 - In this final binary, why did module X load. Have to consider if this is a linked dep vs. a tool.

Action items

- ☐ aiuto: https://github.com/bazelbuild/rules_license/issues/153
- ☐

May 29, 2025 | Bazel supply chain
weekly sync

May 29, 2025 |

Attendees: Yannic Bonenberger Mark Zeren

Notes

- rules_license CI is broken https://github.com/bazelbuild/rules_license
 - (09:07:42) **ERROR:** /workdir/tests/BUILD:82:1: name 'java_binary' is not defined (did you mean 'cc_binary'?)
 - <https://buildkite.com/bazel/rules-license/builds/173#019710ff-0fd6-47b4-b6c2-439731d08a5d>
 - Probably, we should promise to keep rules_license CI working.
 - Probably we should reject “nice to have” code cleanup.
- BCR had 84 dependents on rules_license. Can we query to “burn down” to 0 for most recent versions
- Broadcom is looking at how to implement “workspace manifests” in bzlmod. We need to know, for example, the download URLs for all http_archives in the current configuration. We might start with log parsing, but ideally we want to do this during a build. Ultimately this might require some new bzlmod API?

May 22, 2025 | Bazel supply chain
weekly sync

May 22, 2025 | 📅 Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com Lipsa Rout
davidkurkov@lyft.com simon.m.stewart@gmail.com kiril.raykov@broadcom.com
Florian Weikert sluongng@gmail.com Yannic Bonenberger Mark Zeren
aiuto@bazel.build billie.alsup@gmail.com fabian@meumertzhe.im alex@aspect.build
Luis Pino salazar@engflow.com tony@aiuto.dev ~~kaloyan.raev@broadcom.com~~ @
~~fwe@bazel.build~~ ~~Yaar Schnitman~~ ~~Antonio Di Stefano~~

Notes

- fwe@bazel.build Mark Zeren simon.m.stewart@gmail.com attending
- fwe@bazel.build reached out to the Envoy team, but is still waiting for a reply.
- fwe@bazel.build will not join May 29 due to public holiday.

Action items

- ☐ Mark Zeren still working on deprecation notices. Then fwe@bazel.build will archive rules_licence once we have Mark's deprecation notices.

May 15, 2025 | Bazel supply chain
weekly sync

May 15, 2025 | 📅 Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com
kaloyan.raev@broadcom.com Lipsa Rout davidkurkov@lyft.com
simon.m.stewart@gmail.com kiril.raykov@broadcom.com Florian Weikert
sluongng@gmail.com Yannic Bonenberger Mark Zeren aiuto@bazel.build
billie.alsup@gmail.com fabian@meumertzhe.im alex@aspect.build Luis Pino
salazar@engflow.com tony@aiuto.dev ~~fwe@bazel.build~~ ~~Yaar Schnitman~~
~~Antonio Di Stefano~~

Notes

- What to do with rules_license?
 - It's not really useable (deprecated), but supply chain is not ready yet
 - Make it a shim around the new stuff?
 - No: document it as deprecated, lead people to supply_chain project instead
 - People have questioned its current state
 - <https://bazelbuild.slack.com/archives/C04AZC3E729/p1745454546424869>
 - https://github.com/bazelbuild/rules_license/issues/153

Action items

- ☐ fwe: Talk to the Envoy team - juicy target for adding SBOMs, since multiple people package and ship it. Are they already creating SBOMs?
 - ☐ *Update May 20th*: Sent an email to an internal group
- ☐ Talk to Starlark team wrt symbolic macros / NO_DEP: [PR](#), [NODEP_LABEL](#)
 - ☐ *Update May 20th*: Reached out to the Starlark team, no reply yet.
- ☐ [Mark] Update Bazel docs to point to supply_chain instead
 - ☐ https://github.com/bazelbuild/rules_license/issues/153
- ☐ [Mark] Update rules_license README to show deprecation
 - ☐ Close https://github.com/bazelbuild/rules_license/issues/153
 - ☐ Archive the GitHub repo?

May 1

May 1, 2025

aiuto@ asks: Bueller?

Apr 10, 2025 | Bazel supply chain
weekly sync

Apr 10, 2025 | 📅 Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com
kaloyan.raev@broadcom.com Lipsa Rout davidkurkov@lyft.com fwe@bazel.build
simon.m.stewart@gmail.com kiril.raykov@broadcom.com Florian Weikert
sluongng@gmail.com Yannic Bonenberger aiuto@bazel.build Tony Aiuto
Antonio Di Stefano billie.alsup@gmail.com fabian@meumertzhe.im alex@aspect.build
~~Yaar Schnitman~~ ~~Mark Zeren~~

Notes

- No answer from Tony wrt impact of PR on Google
- Rules_license
 - Still highly experimental
 - package_metadata mostly stable
 - Split in providers vs toolchains BCR modules will likely remain
 - Alex: want to add to as many projects as possible, starting with rules_go
- Alex: need docs for rules maintainers
 - Likely only affects rulesets that rely on external package managers (for now)

Action items

- ☐ Florian: Follow up with Tony wrt impact of file creation on Google builds
- ☐ [Florian](#) + Kaloyan: sign up as a maintainer on the module
- ☐ Alex: try out integration with rules_js package manager
- ☐ Antonio: wrap up license rules PR

Mar 27, 2025 | Bazel supply chain
weekly sync

Mar 27, 2025 | 📅 [Tentative] Bazel supply chain weekly sync

Attendees: emrah.yasar@broadcom.com elitsa.shishkova@broadcom.com
kaloyan.raev@broadcom.com Lipsa Rout davidkurkov@lyft.com fwe@bazel.build
simon.m.stewart@gmail.com kiril.raykov@broadcom.com Florian Weikert
sluongng@gmail.com Yannic Bonenberger Mark Zeren aiuto@bazel.build Tony Aiuto
Antonio Di Stefano billie.alsup@gmail.com fabian@meumertzhe.im alex@aspect.build
~~Yaar Schnitman~~

Notes

- Updates since last meeting:
 - [PR](#) was merged, first release was published to BCR
- Call to add more BCR maintainers (just send a PR against bazel-central-registry, or ping Yannic via Slack)
- Future of rules_license
 - Idea: let rules_license depend on new package metadata. However, rules_license exports providers, which can be problematic.
- Yannic: need to figure out what to do wrt attributes, blocked on Tony atm.

Action items

- ☐ Florian Weikert follow up with Tony wrt impact of many file creation on Google presubmits
- ☐ Yannic Bonenberger to add more maintainers
 - ☐ kaloyan.raev@broadcom.com to send info on Slack
 - ☒ ~~fwe@google.com~~ to send info on slack

March 13, 2025

Mar 13, 2025

Attendees: Tony Aiuto fwe@google.com kaloyan.raev@broadcom.com
yannic@engflow.com

Notes:

- discussing the merits of writing a .json file from every metadata rule or not
- Tony's concern is extra resources on super large builds.
 - He should try at internally to see if it now OOMS on large (~1M target) builds
-

Mar 6, 2025

Mar 6, 2025

Attendees:

-

Feb 20, 2025 | Bazel supply chain
weekly sync

Feb 20, 2025 | 📅 Bazel supply chain weekly sync

Attendees: Tony Aiuto Tony Aiuto alex@aspect.dev antonio@engflow.com
billie.alsup@gmail.com daniel.machlab@broadcom.com davidkurkov@lyft.com
elitsa.shishkova@broadcom.com emrah.yasar@broadcom.com fabian@meumertzhe.im
Florian Weikert fwe@google.com kaloyan.raev@broadcom.com
kiril.raykov@broadcom.com Mark Zeren simon.m.stewart@gmail.com
sluongng@gmail.com yaar@google.com yannic@engflow.com ~~lipsa.rout@broadcom.com~~

Notes

-

Action items

