Meeting invite:
https://zoom.us/j/93588012340?pwd=eINMTzJKM0xzbzh6T1NtQndyZTdzUT09

Upcoming:

-

Aug 27, 2025

Attendees:

- A
- B
- C

Jul 23, 2025

Attendees:

- Major topics/gaps
- CVE fixing/dependency update topic that Steve is driving (on Kata side)
- B
- C

Apr 23, 2025

Attendees:

- Incubation status
  - https://github.com/cncf/toc/issues/1504#issuecomment-2605176375
  - TOC board: https://github.com/orgs/cncf/projects/27/views/9
- Major release
  - Less pushback on not doing it 🙂
  - Specific gaps we need to address
  - Documentation, usability, use cases in the CI
    - **(1) Stable APIs**
    - **(2) Debugability**
    - **(3) Documentation (although it has improved)**
    - (4) Snapshotter issues
    - (5) E2E use cases which are working, a supporting CI

        - (6) kata agent policies
        - (7) Trustee productization
    - Setting a target data at this point would be a little too early
    - First lets close the major gaps and then we can consider a date
    - Could we have TOC members owning those gaps and driving them to completion
    -
- Next release
    - Init data
    -
- Future plans and strategy
    -
-
- C

Mar 26, 2025

Attendees:

- For tomorrow can we talk about the major release for CoCo?
    - If so we need people to come with an opinion…
    - What is a major release?
    - What should it include?
    - What is the bare minimum?
- Use case driven development via CI
    -
-
-

Feb 26, 2025

Attendees:

- **[Ariel/Pradipta] Requesting to be selective on new RUST versions being added to CoCo** - Using latest and greatest Rust is making life difficult for downstream users
    - We are asking for
        - Slow the RUST bumping process
        - Provide an update on it happening
    - We are supposed to have an issue to develop a process to cover these problems
        - https://github.com/confidential-containers/confidential-containers/issues/258
    - Can we change something on the upstream to simplify things?
        - It's about dependencies that force us to update the RUST version
    - Pradipta to provide details on what exactly is creating problems for downstream when the upstream RUST versions are bumped (and for what components)

    - What is the bump policy in general for RH/MS?
- [Tobin] Ideas for fun ways to celebrate 4 years
    - March 11th
    -
-

Jan 22, 2025

Attendees:

- [Ariel] Waiting for CNCF for feedback on the incubisstocuesation support
    - 1504Is our issue posted on their dashboard?
    - https://github.com/cncf///
- [Tobin] Future of the operator
    - Discussion on moving to helm charts
    - Kata has does it for installing stuff
    - Kata deploy vs operator? Questions which are asked (what the value the operator provides)?
    - Moving out of the operator?
    - This would simplify the release process and would not work with the RH operator approach
    - Maybe having another way to install things not via the operator?
    - So helm approach for the simple things
    - We'd still use operators for customers that need upgrades, proper deployment etc…
        - Dependencies for example
    - For every kata release you now get the helm charts (corresponding)
    - Operator SDK also added helm support
    - This is since for now we are only deploying manifests (not changing CRDs)
    - Today we have multiple operators you need to install for that
    - We don't need to connect the upstream flow to RH (operator wise)
    - Our goal should be how to make it simple for maintenance
    - For kata
        - Helm was added to simplify the mess we had before
    - What about enclave-CC?
        - It release on the operator flow and we don't have helm charts
        - We could add helm charts to Trustee and other components as well
    - What about the GPU operator and its connection?
        - It would be hard to connect a kata/CoCo operator with that operator
    - We still want to make sure we have a CoCo helm chart to separate from kata
    - The proposal
        - A single way to deploy CoCo via the helm charts (not using the CoCo operator)
    - Trustee operator

        - For Trustee we should consider keeping it since it's simpler then the CoCo operator
        - It's adds additional capabilities such as integration with external secret stores
    - Our proposal
        - **Dropping the CoCo operator and moving to CoCo helm charts**
        - Having a CoCo repository to store those helm charts (similar to the CoCo operator)
        - Timeline?
        - We also need additional people to know how to use the helm charts
        - We need to put this as a topic for the upstream meeting
        - Tobin will run this with the CoCo CI team to see what they think
    - For kata the helm charts are tested by the CI/CD
    -
- [Mikko] Release owner (not Tobin 🙂)
    - Rotating (not Tobin 🙂)
    - 6th release Tobin has done…
    - The people management aspect is a pain however doing the release isn't so hard
    - Can we find newbies from IBM-Z/RH/Nvidia/AMD/Intel
    - Could we define roles for the releases?
        - Release owner
        - Make the PRs for the operator (+2 people to approve), helps if same TZ
        - Release notes
    - We'd put someone to shadow this so they can take it on later on
    - Ariel to put forward a plan for mapping companies (2 companies per release) for 2025
- Hygon
    - Ding introduced a few new developers from Hygon (HW manufacturer)
    - More people on the project
    - Tomorrow the topic is from them
    - Introducing CSV which is their TEE and their plans for CoCo
    - We will see how active they contribute
    - They could also join this meeting
    - What about theri CI/CD?
- Connecting peer-pods release with the CoCo release
    - Could we try and align the timelines?
    - Maybe a similar process?
    - What happened last time that it didn't work?
    - Maybe only a nice to have topic?
    - Peer-pods priorities are a little different
    -
- [Ariel] Moving to use case driven development
    -
-

- [Ariel] Engagement with Tekton and Kubeflow
    -
- C

Aug 28, 2024

Attendees:

- [Tobin] Removing inactive maintainers
    - You aint active for 6 month, we can remove you 🙂
    - We talked about it however we didn't do anything with that yet
    - What should be the next steps?
    - Tobin/Mikko will prepare a list (haven't contributed for 6 month) and then Ariel will follow up with the relevant people to point this out
    - Tobin will also open an issue to point this out
    - Ariel to add this to the Thursday CoCo meeting agenda
- [Mikko] CODEOWNERS update and process
    - Updating the code owner file with the actual people who are the maintainers
    - Tobin says we don't need it 🙂
    - Discussing the pros and cons of adding specific people (how do you maintain it over time…)
    - We agree that the files contain only the maintainers team and not specific people's names
    - Creating PRs to change the files
- Fossa GPL non-compliance findings in kata-containers in tools/packaging
    - We fixed it? Yep
    - People have access to it and fixed the problems
- TAG security presentation
    - Disappointing
    - 2 people attended (+ James and Pradipta) :-(
    - EMEA is definitely not the right call to present this on
    - Seems the presentation was OK, how can we now present this on the US meeting?
    - Working to get a date…
    - At least the slidedeck is ready…
    - Joint security assessment
    - Next step is for James to get us a meeting with the US TAG security team
    - We should start with our self security assessment (and then progress to the joint)
    - James to get someone from the TAG security to come and present their work
- Incubation updates
    -
- [Mikko] Roadmap update

    - The doc is not updated: https://github.com/confidential-containers/confidential-containers/blob/main/roadmap.md
    - Can we create a doc showing the matrix of use cases we support with the relevant HW?
    - What about feature support?
    - Ariel will work to get a matrix from the RH product
    - Dan will see if he can get something from Azure
-
-

Jul 24, 2024

- Release 0.9.0
    - On track for this week
- Release 0.10.0
    - Will start working on that plan once 0.9.0 is out
    - Equal to the CCV0 content
    - We know the main things we want to deliver
    - Ariel/Tobin to create and populate a github board for it
- Major release for CoCo
    - What would that contain?
    - How can we connect it to the use case driven development work?
    - We need to go back to the stability issues as well
    -
- Weekly meetings
    - Objections to moving the technical topic to 45 minutes instead of 30 minutes?
        - Nop 🙂
- CI board issues
    -
- Proposal to submit the CoCo incubation in October
    - CoCo CNCF incubation task force
    - Everyone agrees :-)

Jun 26, 2024

- Proposal to submit the CoCo incubation in October
    - CoCo CNCF incubation task force
    - Everyone agrees :-)
    - But, should we have a target stable release for this point of time?
    - We also need a stable upstream release for other CNCF projects who want to try out CoCo
        - Today we are not there…

    -
- Updates on the use case driven work
    - Confidential containers use cases driven development
- Always green CI
    - https://github.com/kata-containers/kata-containers/issues/9892
- Project status
    - https://github.com/orgs/confidential-containers/projects/6/views/21
    - https://github.com/orgs/kata-containers/projects/38/views/3
    - Key issues for 0.9.0
        - Init containers
        - SNP support
        - Stability
- Removing maintainers
    - Could we start using files to manage the maintainers?
    - Can we contact those who haven't reviewed and politely kick them out
    - We also need more reviews for the docs
    - Ariel will help with the reviews of the release notes
- Trustee and CCC
    - Next steps here?
    - What are the synergies here?
    - Trustee as one example
- Trustee and Keylime
    - Thoughts on win-wins here?
    - Nvidia and Intel also have their attestation services so how does it all play nicely together?
    - Multi round attestation as one example
    - Will Trusty be the entity who reaches out to all the other services?
    - Keylime is really focused on run-time attestation
    - So Trustee/Keylime could potentially work together
    - Maybe we could show something?
- Provenance discussion
    - provenance management in coco project
- B
- C
- D
- E

May 22, 2024

- Removing defunct reviewers/maintainers
    - We want to propose a criteria for adding and removing maintainers

    - Can we add files to manage the maintainers?
    - Can we propose a criteria of 6 months with no review as the point where we ask a maintainer to drop from a specific area?
- Provenance
    - A set of measurements
    - The golden value of an artifact we create to verify it's what we intended it to be
    - Handling measurements in CoCo
    -
- Trustee and CCC
    - Could we get an endorsement from the CCC as well for Trustee?
    -

Apr 24, 2024

Agenda

- [Fabiano] Containerd 2.0, ImageTransfer service, sandbox API, and what do those mean to us?
    - Can we take advantage of the ImageTransfer service?
        - From a quick look, not really, as it would still require the pause image to be pulled in the host
            - Can sandbox API help with that?
                - Most likely, yes, but Kata Containers sees the sandbox API as a runtime-rs only feature, and my gut feeling tells me we don't want to jump into that ship right now
        - What does it mean for the CRI-O integration?
    -

Mar 27, 2024

Attendees:

-

Agenda:

- Merge to main next steps
    - The board: https://github.com/orgs/kata-containers/projects/38/views/2
    - 8870 https://github.com/kata-containers/kata-containers/pull/8870
    - https://github.com/kata-containers/kata-containers/issues/9058 should be connected to 8870

    - AMD CI not running for a week and we may have some issues that need to be checked
- Doing an earlier release to test the water
    - Resources to work on it
    - Who could we find to work on it?
    - What would be our MVP here before cutting a release?
    - Can we propose an MVP?
    - On the other hand, what happens if we continue this release for another 3 months?
    -
- Proposal (the Tobin/Fabiano proposal 🙂)
    - Release a non TEE merge-to-main release (not platforms for now)
    - Targeting it for 2 weeks
    - Then focusing on platform support and having another release in 4-6 release

Feb 28, 2024

Attendees:

- Tobin
- Larry Dewey
- Ariel Adams
- Vincent Batts
- Pradipta Banerjee
- Ryan Savino
- Dan Mihai
- Fabiano Fidêncio
- Samuel Ortiz

Agenda:

- The discussion on the data sets in rego or json
- What should go in the host data?
    - The policy
    - The init data
- Using immutable TEE field to verify the integrity of Agent Policy and/or initialization data
- The key problem with init data is the double encapsulating of the policy to be added to the json
- We want to have a meeting next week to focus on this topic (Ariel will schedule)
    - CoCo policy discussions
- We will prepare a document with the use cases we need the policy for, the different solutions we have, pros/cons etc…

Jan 24, 2024

Attendees:

- Ariel Adam
- James Magowan
- Dan Mihai
- Tobin
- Vincent Batts
- Fabiano Fidêncio
- Samuel Ortiz
- Zvonko Kaiser
- Pradipta Banerjee

Agenda:

- Shall we cut v0.8.1 due to the security issue raised by Peter?
-

Dec 13, 2023

Attendees:

- Fabiano Fidêncio
- Ariel Adam
- James Magowan
- Peter Zhu
- Samuel Ortiz
- Tobin Feldman-Fitzthum
- Vincent Batts
- Zvonko Kaiser

Agenda:

- A security vulnerability of CoCo
    - We plan to enable private issues in the CoCo github
- Using the CoCo project downstream
    - What are the consumption models consumers use?
    - How many versions do we support and how?
    - What are our assumptions on someone opening a bug on the project? What happens if they deploy things in a different way?
    -
- C

Nov 29, 2023

Attendees:

- Tobin Feldman-Fitzthum
- Larry Dewey
- Samuel Ortiz
- Zvonko Kaiser
- Pradipta Banerjee
- James Magowan
- Ariel Adam
- Fabiano Fidêncio
- Vincent Batts

Agenda:

- Do we need to move this meeting given the conflict with the weekly CoCo Ci meeting?
    - Tobin and Fabiano are needed on that meeting as well
- How to improve transparency.
- Do we want to "manage" the "merge to main"?
    - If so, conversations have happened about having all the companies who are part of the SC involved in the process. How do we want to ensure this will happen?
- Do people want to know the high level plan for ensuring that, at least the same amount of tests present for the CCv0 branch will now be present for the `main` branch?
    - This can be deferred to a later session, after Wainer organizes the working group
- About Thilo's presentation, what have we learned and what's the path we want to take from that?
    - Are there any steps that the projects could already be focusing on to ensure a smooth ask for Incubation?
        - If so, what's the focus we want to have? Who would be the owners for that?
- A CoCo conference???????
    - There are some (time sensitive) opportunities for this in 2024
- How should we think about downstream consumers of CoCo?

Action Items:

- Follow-up on how we conceptualize downstream consumption of the project?

Oct 25, 2023

Attendees:

- Thilo Fromm (Microsoft / Flatcar Container Linux)
- B

- C

Agenda:

- Security processes for CoCo
    - We already have security owners for different repositories
    - How can others join if needed?
- Vincent Batts will talk about the incubation process for Flatcar
    - https://github.com/cncf/toc/pull/991
- Thilo is going talk about the Flatcar incubation submissions
    - What was the hardest part?
        - It's straightforward
        - Discussion about licenses
            - That's more specific for Flatcar who are more about integration and testing
            - Less relevant for CoCO
            - The point however is that licensing can take a lot of time
        - The security review was also hard
            - They will shake the project and identify all the issues
            - Threat models etc…
            - There is also a lightweight process however for us the recommendation is to go with the full (long) process
        -
    - How long has your process been going on for?
        - Overall it's still ongoing (started in Q2)
        - They saw other sandbox projects completing this process in 2-3 month if they come prepared
        -
    - Who was your sponsor?
        - Duffey
        - Nikhita
        - People they knew from working on Flatcar support to a few relevant projects
    - Who and how many end users were you asked to show?
        - Yes, not a problem for flatcar
        - They have a lot of users using it for years now
        - They also have support connections to relevant companies who they pinged and connected to the sponsors
        - They were interviewed
        - They also had a bunch of statistics around the users including market spaces from public clouds
        - The sponsors went and talked with them
    - What about adopters who are also involved in the project?
        - For example public clouds
        -

        - What else did they ask you to prove?
            -
        -
- B
- C

September 27th, 2023

Attendees:

- Fabiano Fidêncio (Intel)
- Dan Middleton (he/him)[Intel / outgoing]
- Vincent Batts (MSFT)
- Pradipta Banerjee (Red Hat)
- Ananya Garg (MSFT)
- Zvonko Kaiser (NVIDIA)
- Ariel Adam (RH)
- James Magowan (IBM)

Agenda:

- Welcome new members
    -
- The path to incubation and the role of the steering committee
    - CNCF TOC Project Board for reference
        - Notice how long it can take…
    - How will we drive our incubation strategy?
        - Should the steering committee drive incubation efforts or should we create an open working group?
        - What is the right time to request an incubation?
    - Flatcar from MS is an example of almost becoming incubation: https://github.com/cncf/toc/pull/991
        -
- What should the steering committee do?
    - Connection to the CNCF
    - Can we change the name?
    -
- Moving to use case driven development (connected to incubation)
    - Putting use cases the CoCo community can focus on
- For reference
    - CNCF Governance Guidance

Wed July 26, 2023 (12-13 UTC)

Attendees (please add your name)

- Larry Dewey
- Samuel Ortiz
- Pradipta Banerjee
- Peter
- Tobin
- James
- Ariel

Agenda:

- Merge to Main outstanding items -> Merge to main
  Wainer, Steve, Fabiano to help with discussion?

  Goal : How do we progress through this list faster?
  - Answer the questions?
  - Remove the blockers
  - Define what this looks like?

  - What happens if we finish the merge to main and then we need to fit into the kata cadence instead of the 6 week cadence CoCo currently has?
  - Kata actually has 4 week alpha releases which CoCo could piggyback on
  - Can we define a minimum set of features that are required to switch to main?
    - Refining the list and pushing some parts to the future
    -
  - Some of the issues on the list are still in design state and no final solution on the HOW (image pull for example)
    - **Thus blockers for this work**
  - When do the releases move from CCv0 to main?
  - Can we go with an approach of dropping features, starting from main and having a bunch of regressions we need to handle?
  - We need to understand who are the right people to work on the tasks in the list
  - Do we have a plan for things when Kata doesn't want a given feature?

- CNCF Incubation (Samuel)

Jun 28, 2023

Attendees (please add your name)

- Dan Middleton, he/him, intel
- Pradipta Banerjee, he/him, Red Hat

Agenda:

- Add a link to the doc and recording for Thursday's CoCo meeting
- [pradipta] Copyright guidance for the project. Ref: https://github.com/cncf/foundation/blob/main/copyright-notices.md#ownership-of-copyrights-in-cncf-project-contributions
    - In the github projects we are using we have different copyrights
    - It's not an issue for CNCF
    - We do need to have guidelines internally when things are changing
    - Could put the recommendation in here: https://github.com/confidential-containers/confidential-containers/blob/main/CONTRIBUTING.md
    - **We'd like to provide guidelines however not enforce them**
    - https://docs.google.com/document/d/1E3GLCzNgrcigUlgWAZYlgqNTdVwiMwCRTJ0QnJhLZGA/edit
    - *The recommended copyright statement is "(C) Copyright Confidential Containers Contributors".*
    -
- B
- C
-

May 24, 2023

Attendees (please add your name)

-

Agenda:

-

May 3, 2023

Attendees (please add your name)

- **Larry Dewey**
- **Dan Middleton**
- **Ariel**
- **Pradipta**
- **James**

- **Tobin**
- **Fabiano (after first ~15 min)**

Agenda:

- Summary: everyone got to chat freely about the release process and frustrations as well as communication methods. The process changes listed below were recognized and it is intended that they be brought to the community and adopted. Everyone left on a positive note. [Dan's editorial]

- Action Items:
    - Better communication between individuals and within the community
    - Adjust dates to guarantee that releases do not fall around the times of conferences.
    - We need to have a release owner/owners.
    - There is great value in letting the release date be delayed when appropriate.
    - Be aware of, and contribute to:
        - https://github.com/confidential-containers/community/pull/86
- (Fabiano) Collaboration with AMD has been challenging
    - *During the v0.5.0 release process some heated discussion happened as Fabiano took over the tasks that Larry said he'd work on the day before, but didn't.*
        - The discussion about the date is recorded as part of the CoCo meeting on Apr 13th, 2023
        - Fabiano took over the tasks in order to proceed with the release planned for Apr 14th
        - Fabiano's been accused of "not giving the opportunity" for Larry to work on something he said he'd do in the day before
        - This is the message that originated the whole situation:
            - https://cloud-native.slack.com/archives/C039JSH0807/p1681448539903759
        - With further discussion here:
            - https://cloud-native.slack.com/archives/C039JSH0807/p1681472299161629
        - Fabiano's expectation was one of the two:
            - A message saying it'd be handled on the next day
            - Not receive an "kinda angry" message for taking the tasks over
            - This could have been avoided with any of those two actions mentioned above.
    - *This is not the first time something goes out of control, as in the past Fabiano has been accused to be "purposefully blocking AMD"*
        - This happened in a PR that was not fixing an issue, was wrong, and was already superseded by another PR that was addressing the real issue
        - Discussion got heated on Slack

                - https://cloud-native.slack.com/archives/C039JSH0807/p1669840688935609
        - *Fabiano is looking for a long-term solution on how to better collaborate with AMD folks, mainly related to:*
            - Commitment on the tasks
            - Reliability of the AMD CI
                - Including acting on, debugging, and giving status reports when the CI is broken
            - Always having public conversations instead of private ones
            - Understanding that no-one is here to block other company's progress, but rather grow the project together
        - *This has been affecting also other members of the community, mainly the ones working directly with Kata Containers*
        - *Fabiano would like to be present in the TSC meeting where / when this is discussed*
- (Larry) Permissions, Release Timing, and Communication Issues with 0.5.0 (Larry)
    - *Would it be beneficial to extend or adjust the release cadence and code freeze durations?*
        - Is the current release process sustainable?
        - Would it make more sense to move to an 8-week schedule?
        - Regardless, we need to begin the release process earlier in the code freeze phase to mitigate problems before the last-minute.
    - *Having a greater distribution of responsibilities and permissions to mitigate the responsibilities falling specifically on to one – or a couple – individuals.*
        - Perhaps having individuals in several time-zones?
            - PRC
            - USA
            - EUR
    - *The release checklist would benefit from some updating and cleanup; specifically regarding expectations and processes of the defined steps.*
    - *What is the TCS's view on resolving conflicts related to the project?*
        - Though resolution is important, public forums are not appropriate venues for resolving personal conflicts.
            - Fabiano: This is not personal, at least from my point of view. I do believe this is a community issue.
            - There are multiple sides to any conflict, so it is important that everyone is treated with the same respect. Fabiano provided the comment above, but this discussion point was not related to this…
- Github Issues (Larry)
    - Permissions issues across multiple products.
- Fabiano: All the topics raised above lead to having a proper retrospective after each release, maybe outside of the CoCo weekly meeting, where folks involved in the release can evaluate what went wrong, what went right, the whys, and the possible ways to improve it.

    - Although super important, doing this in the CoCo weekly meeting may take too much time of other technical topics
    - Thanks Steve, for the suggestion.
- James: I think the real answer here is “Let the release fail”. I don’t mean that in a bad way, more to avoid any one person feeling the pressure and need to keep things moving at times when it can seem the support from wider community just isn’t there.
    - *My experience suggests that a longer code freeze or changing release cadence will not solve the challenges/issues. I feel longer code freezes would still put pressure on those building a release by desire to merge code, and longer release cadence makes for bigger releases and same problems (accept less frequently though)*
    - *I believe we should be aiming for a very small code freeze but my view does depend upon trust in our CI/CD pipeline and tests and we know we have more to do there. And indeed some continue to work and improve that area*
    - *I do agree that more people involved in the release and especially geographically spread can help, I created a wiki page to push Wainer’s Issue forwards more -> https://github.com/confidential-containers/community/issues/81*
    - *I also created an issue https://github.com/confidential-containers/community/issues/84 not to reinvent the wheel but just to capture in writing some simple things mentioned in discussions .*
    - *In terms of updating the release checklist in issue 84 I called out the task of updating the release checklist to be a key part of a release. The release owner can ensure it happens but as with all delegation that could be as simple as creating the issue with info on what needs updated? But of course anyone can propose changes to the checklist via issue or code PRs.*
    - *I believe the release currently falls on too few people and the pressure can be felt at times. On a positive note, we continue to improve the process with every release and slowly have more people involved but what can we do to have more people able/willing and with time to help?*
    - *Can we get release owners signing up?*
    - *Can we get enough volunteers around them with time and confidence to help at release time?*
    - *Can we keep reminding ourselves and the entire community that the release process shouldn’t feel pressurized?*
    - *Releasing a day or a week or even longer late may be a better choice to break the cycle of feeling pressure and helping the community appreciate the areas that need more focus/attention to make the cycle run smoothly?*

Mar 22, 2023

Attendees (please add your name)

- James, Aiel, Larry, Samuel, Dan, Tobin

Agenda:

- Increase the release velocity
    - Issues with the CI stability
    - The topic of CI networking issues
    - Azure are bringing 25K$ of cloud resources for our CI
    - Running CI locally
- 0.5.0 progress and main features
    - Board: https://github.com/orgs/confidential-containers/projects/6/views/2
    - Generic KBS
    - Resource URI
    - Encryption format for the images
    - Peer-pods
    - Enclave-CC + CI
- PR for the 0.5.0 release and kubecon EU
    - Generic KBS https://github.com/confidential-containers/community/issues/68
        - Can we
    -
- 0.6.0 release
    -
- Next conferences related to CoCo
- Incubating project in 2023?
    -
- D
- E

Mar 1, 2023

Attendees (please add your name)

- James, Ariel, Pradipta, Peter, Larry, Dan

Meeting Agenda / Minutes

- (Larry) Fractured communication:
    - CNCF Slack
    - Kata Containers Slack
    - Multiple Github Issues,PRs,Repositories,Project Boards, etc
    - No unified communication.
        - Very easy to git disconnected, miss conversations, and lose priority.
    - So what can we do to simplify/improve things?
        - Possibly implement special Slack notifications.
        - Potentially suggest capturing Slack conversations inside of issues, or vice-versa?
    - Can we split the CoCo project into well defined areas?

        - CI/CD
        - CCV0 to kata main\
        - Attestation
        - SEV
        - Image download
        -
    -
- Containerd next steps
    - We are still using the fork of containerd. How will we be getting CCv0 back? We need to take some action to help push this forward.
    - Transfer API missing some logic which CoCo needs.
    - Also a Kata Container issue. We should move to 1.7 Beta.
    - Alibaba has committed to adding engineering resources to this effort.
    - With changes proposed from Microsoft, we may not need the forked APIs?
- CCV0 merge into kata main next steps
    - Does this change anything about our versioning
    - Good opportunity to change the branch name, but not mandatory.
    - Containerd
    - CI/CD? In order
    - Additional architectural / library support to line up with Kata requirement?
        - Nydus (Software)
        - ARM
        - RISC-V
    - Sync with Fabiano & Steve (issue or conversation?)
- Use case driven development
    - https://docs.google.com/document/d/1LnGNeyUyPM61Iv4kBKFbfgmBr3RmxHYZ7Ev88obN0_E/edit#heading=h.ytpf8y33y0mn
        - Azure
        - IBM cloud
        - Ali cloud
    - Find an equal balance between innovative and use-case-based development.
    - Retrospectively investigate the outcome of those use-cases.

Feb 2, 2023

Meeting recording:
https://zoom.us/rec/share/IuVp7yu9T8boNFbbo6jCMjirWh4nvRH2fWvPC9EUJBtmjyuVTzfU0-PThUiISAyJ.hfPMDEwK-07ttrYv
Attendees (please add your name)

- James Magowan - IBM
- Samuel Ortiz - Rivo
- Larry Dewey - AMD

- Pradipta Banerjee - Red Hat

Meeting Agenda / Minutes

- Discussion with Azure on the CoCo project
    - Amar and Pradipta have been talking about CoCo for some time
    - MS are leading the space of CC with big investments
    - A number of proposals from MS on multiple aspects
    - They want to bring their learning into the project based on their lessons learned
    - Are trying to understand if there are specific parts of the CoCo project that need more attention (code or definitions)
        - Protecting container images
        - Storing them, pulling them
        - How do you actually use CoCo?
        - Where are the main performance issues that we need to address?
        - It seems we are close to the original architecture we planned so the question is how do we now move to a production level
        - SEV support has a few gaps as well
        - CI needs help
            - Schedule a meeting with Wainer, he's your guy
            - Could we use Azure environments for the CoCo CI?
        - Attestation flow and the model with CoCo
            - Is the current attestation model we are focusing on work?
            - Azure for example don't force customers to use AS on the boot flow but rather let them use it later on in the flow
            - A lot of customers want to start small with a CC solution
        -
    - Would like to offer Azure as a platform to run part of the pipelines for CoCo such as CI
    - It seems there are a number of MS teams in the CoCo, who is who :-)
        - Amar part of the product in CC, 3 years there
        - Azure host (linux service) - kata, kernel etc…
        - ACC - CC dev team
        - AKS upstream members - a company MS bought
    - **Any specific use cases Azure are targeting and can share?**
        - Can we drive our development from use cases customers need and not from features (top down and not bottom up)
        - We need to focus on the infrastructure persona and not asking dev to changing their processes
        - There are some greenfields customers however the infra persona seems to be the one we should focus more on
        - Customers want a consistent experience plus the same level of protection
        - Talking about including the metadata in the attestation data
        -

    - Request for Amar (MS), Gerry (Albaba) and James (IBM) to send Ariel a number of use cases so we can share with the community and help focus the development on use cases and not features
- How will we merge into kata main
    - Via the CoCO major release after we merge into kata main
    - The blocker in the containerd fork which is supposed to converge in containerd 1.7
    - Ali are helping with a number of changes there as well
    -
- Review the agenda from the last meeting, and review the governance document.
    -

Jan 25, 2023

Attendees (please add your name)

- James Magowan - IBM
- Larry Dewey - AMD
- Samuel Ortiz - Rivos

Meeting agenda / Minutes

- Unclear if the meeting was canceled or not due to calendar/technology problems.
- Held a discussion regarding the committee (ideas captures in the PR https://github.com/confidential-containers/community/pull/56)
    - Should there be a cadence for which the committee dissolves and re-establishes itself?
        - What should that look like?
    - Are there specific roles which members of the committee should be fulfilling which are being missed?
    - Would it be beneficial to select members of the committee to act as liaison between different organizations, such as the CNCF, to keep up-to-date on upcoming events and also to evangelize the project to the parent organization wherever possible?
    - Would it be beneficial to have members of the committee encouraging, and even asking, members of the community to present specific topics/ideas/work at various CNCF events to strengthen the project's presence and visibility in the organization?
    - Should the committee dedicate specific meetings, say every n-th meeting, to discussing the roadmap and direction of the project?
    - All members of the committee should review, comment, and approve the governance document, and take part in the on-going discussions.
- Discussed the current state of the firecracker project and CC, and the difficulties in getting required changes into the project unless those changes are AWS specific

business needs. Samuel pointed out that Cloud Hypervisor is an excellent project alternative.

Jan 9, 2023

Attendees (please add your name)

- Dan Middleton (he/him) Intel
- James Magowan (he/him) IBM
- Tobin Feldman-Fitzthum (he/him) IBM
- Ariel Adams (he/him) Redhat
- Pradipta Banerjee (he/him) Redhat

Meeting agenda / Minutes

- Meeting recording: https://zoom.us/rec/share/YLgaOoL4Li7zI0O3ZVmbPP4NP6JvKds3AVtJXkgOH20z31U5xIMunwR7BZC8wAfW.E_P_NKkhXQ89Rvk-
- Attendance:
    - Alibaba, AMD, Rivos absent. No voting today but initiated the discussions below to make progress
- What should be our strategy for integrating CCV0 into kata main?
    - Will be covered in the community
- What should be our community's goals for 2023?
    - Becoming an incubation project - consumption by 2+ customers
    - Merge CCV0 to kata main
    - More people joining the community
    - A major release in 2023
        - Documenting the security model for our control plane and identifying the possible security issues we have
        - Containerd and CRIO changes formally delivered
        - Peer-pods being part of the release as a mature solution
        - Define quality criteria for major release
    - We will work to create a google doc with use cases from IBM cloud and Azure to help steer the discussion on goals for 2023
    - Obviously others can then add use cases to the document (however not starting with a blank page 🙂)
- We know that Azure will want to join the TSC, how should we manage this (or others interested)?
    - They want to talk with the TSC and not necessarily join the TSC
    - Proposing to Azure a meeting on the 18th of January 8AM PST
- What is the election/nominee cadence for the TSC?
    - https://github.com/confidential-containers/community/pull/56
- TSC meeting with Azure CoCo stakeholders *(key folks based out of PST TZ)*

Oct 26, 2022

Attendees (please add your name)

-

Meeting agenda / Minutes

- **Hardware for CoCo CI from CNCF**

Oct 5, 2022

<No agenda posted by 10/4. No meeting.>

Sep 21, 2022

Attendees (please add your name)

- Larry Dewey
- Dan Middleton (he/him) Intel
- James Magowan
- Ariel Adam
- Samuel Ortiz
- Pradipta Banerjee
- Tobin (the one and only ;-))
- Peter

Meeting agenda / Minutes

- First Release feedback (we can do that post release):
    - Github Board
    - Anonymous Form
        - For those less familiar with creating issues
        - Move those over after.
- Discuss the need for unified standardization across the organization.
    - Ex. Number of reviewers automatically set before a PR may be merged
    - Ex. What level of CI/CD/Code Coverage do we expect new features to implement before they are accepted?
        - Regression needs to pass (CoCo E2E integration tests), we can't break something we released before (unless it's intentional)
- Organizational need for additional members with review rights (at minimum) to help mitigate blockage.
    - Have reviewers perform reviews more than the number of individuals with rights.

- Make a final decision for our versioning system before first release.
    - Semver - 0.1.0 - As release cadence.
- MVP for Release Notes
    - Drafts designed to be a starting point which encourages interaction and contributions from the community.
    - Github Release Note location update?
    - The documentation repository would make sense to have two reviewers.
    - Separate release notes from user guide?
- Feature Freeze / Code Freeze Discussion
    - Define terminology
- Signature verification image-rs
    - Overall PR for tracking efforts: https://github.com/confidential-containers/community/issues/57
    - Not going to make it in? Pending PR for removing legacy dependencies.
    - One remaining PR: https://github.com/kata-containers/kata-containers/pull/5202

Jul 27, 2022

Attendees (please add your name)

- A
- B
- C

Meeting agenda / Minutes

- New TSC interest <Tobin>
- Enforcing development standards <Dan>
    - https://github.com/confidential-containers/community/blob/main/CONTRIBUTING.md
    - https://github.com/confidential-containers/community/blob/main/PR-Review-Guide.md
- Scope creep <Dan>
- Other?

Jun 29, 2022

Attendees (please add your name)

- A
- B
- C

Meeting agenda

- Meeting Rec:
- CC first release plan
    - https://github.com/orgs/confidential-containers/projects/6/views/1
- B
- C

Jun 15, 2022

Attendees (please add your name)

- Dan Middleton (he/him; intel)
- Samuel Ortiz (Rivos)
- Jiang Liu (Alibaba)
- Pradipta Banerjee (Red Hat)

Meeting agenda

- Meeting Recording:
    - https://zoom.us/rec/share/SvP2im0dQx0H3Pq0F3RgKMBEnCDczYJ8esFe7-RQT7rj1enR3ogMK8EsRVpVuJWX.rzLhaV8BJIlxG-PR
- COCO first release
    - Propose tag: cc-first-release
    -
- Status on the CNCF onboarding tasks
    - CNCF onboarding tasks
- Overview on kubecon COCO discussion and talks (James/Samuel)
    - A good chunk of people listening
    - Discussions with Azure
    - TAG security discussions
- Interaction with the TAG security team and next steps
- SIG security meeting - how can we engage with them?
    -
- TAG security team white paper:
    - https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf
    - https://github.com/cncf/tag-security/tree/main/security-whitepaper
- How do we fit into the supply chain mentioned in this white paper?
    -
- CC community develop roadmap and status track
- Governance topics (Tobin)

-

May 30, 2022

Attendees (please add your name)

-

Meeting agenda

- Status on the CNCF onboarding tasks
- Overview on kubecon COCO discussion and talks (James/Samuel)
- Interaction with the TAG security team and next steps
- TAG security team white paper:
    - https://github.com/cncf/tag-security/blob/main/security-whitepaper/v2/CNCF_cloud-native-security-whitepaper-May2022-v2.pdf
    - https://github.com/cncf/tag-security/tree/main/security-whitepaper
- How do we fit into the supply chain mentioned in this white paper?
    -
- CC community develop roadmap and status track

May 18, 2022

Attendees (please add your name)

- Ariel Adam, B, C

Meeting agenda

- The maintainers trademark forum signing
    -
- CNCF onboarding tasks
    - Tobin will reach out to Amye to ask her to check off the remaining onboarding tasks and provide us with zoom session we can record (for weekly COCO meeting and TSC meeting)
- Aligning the participants press release once CNCF goes out with it's press release
    - Confidential containers CNCF sandboxed project introduction
- Blogs and blog series for COCO
    -
- COCO project releases

    - What should be our next steps on pushing the community to a formal release?
    - What do we think are the gaps?
    - Timing and contents of first CC release
- Release discussions
    - Can we put out a 0.1 release just to get things rolling?
    - Even to get to that we would need to have a few releases before that
    - Can we take CCV1 as the 0.1? Do we need to add/remove anything from it?
    - To clarify, this is not a 1st formal release but rather something that is **stable enough**, **simple to deplo**y and **usable**
    - Can we separate releases that the community uses for development vs official ones even if it's a 0.1?
    - Proposal for COCO use case for creating scenarios
    - We could propose to release the operator with the payload and take specific labels of payloads which support a small subset of features which we expose to the user
    - Next step is to define what our 0.1 release would contain and how does it gradually grow
- C

May 3, 2022

Attendees (please add your name)

- A, B, C

Meeting agenda

- List of maintainers sent to Amye :-)
    - Remaining CNCF onboarding tasks: https://github.com/orgs/confidential-containers/projects/2
- Review COCO releases proposal - to be presented to all COCO on 12th of May
    - Do we want to start with a prerelease?
    -
- Aligning the participants press release once CNCF goes out with it's press release
    - Confidential containers CNCF sandboxed project introduction
- Licenses
- (Carry Over Last Meeting)
    - Discuss policy and merge cadence of project after forking
        - At what point should we push projects back to upstream for upstream maintenance.
        - Is there an expectation of having full ownership of projects vs. relying on up-stream for support of previously forked projects

- Kata-containers
- Containerd
- Generic KBS

Apr 20, 2022

Attendees

- A, B, C

Meeting agenda

- Introductions
- Decide on the meeting cadence and time slot
  - Can we stick with this timeslot or do we need another one?
  - Proposal: every 2 weeks assuming we have an agenda in place
  - **Agreed to go with every 2 weeks**
- **[Key topic for today]** How can we sign the CNCF logo and trademark request so we can move on with the CNCF press release?
  - The current situation is that most of the people on the TSC can't sign or it will take them a long time to get legal approval to do this
  - The proposed solution is to provide the CNCF a smaller list of maintainers who all can sign (RH, some from IBM, maybe Alibaba etc…) and then gradually add more people to the maintainers list as people get approval from their companies (and we share it with the CNCF)
  - What do people think?
  - We agree the following:
    - Ariel/Pradipta will sign it
    - Tobin to consider
    - Jian/Jia to consider
    - **We are submitting the list of maintainers on the 27th of April (next Wednesday)**
    - Being on this list implies you will sign it
      - LInke to the document to sign
- Ratifying the Governance document
  - What are our responsibilities?
  - How should TSC members be selected in the future?
- Creating repositories for Generic KBS
  - Is this even a topic for the TSC to decide on?
  - Could we focus our discussion on blocking issues or areas of conflict?
- Discuss policy and merge cadence of project after forking
  - At what point should we push projects back to upstream for upstream maintenance.

    - Is there an expectation of having full ownership of projects vs. relying on up-stream for support of previously forked projects
        - Kata-containers
        - Containerd
        - Generic KBS
- Releases for the COCO project
    - Can we propose a release plan for COCO now that we are part of the CNCF?
        - **What should be the duration of each release?**
            - The proposal is a release every 6 month (2 releases per year for now)
            - Each release is composed of 6 drops each 4 weeks with a clear goal of delivery
            - Every 4 weeks we have demo of the content which was delivered and we can adjust things on the release as needed
            - Every 4 weeks we cut a drop (time based drop)
            - We can then provide a clear visibility to the drops, releases and what is coming there way
            - The drops will be managed on a github kanban board and the release content will be documented on our github site (under roadmap) + making sure it is up to date (content and dates)
            - 2 releases per year the overhead we have of supporting the releases is not too high to start with
        - **What are the short stoppers we have for the 1st release?**
            - Containerd/CRIO fork although short term we can base on work on the forks including the kata fork
                - Using a beta release for containerd/kata would also work in this case
                - **This is the most risky part**
            - CI/CD to run this
            - HW support matrix
            - Simple deployment strategy (operators, automations etc…)
            - Debugging/logging tools for accessing an encrypted guest and disabling the encryption all together
        - **Important dates we need to consider?**
            - Intel TDX HW in CI/CD
            - ARM HW in Ci/CD
            -
        - **What content do we want to have in each release?**
            - **Release 1**
                - Sw emulation for testing the solution locally (laptop)
                - Basic memory encryption support (such as SEV/SEV-ES)
                - Remote attestation based solution for VMs based confidential computing (TDX/SEV-SNP)

        - Remote attestation based solution for process based confidential computing (SGX)
        -
    - **Release 2**
        - TBD
        - …
        - ….
        - ….
    - **Release 3**
        -
    -
- C
- D
- E