2023-07-10 Architecture WG Meeting Notes

Date

10 Jul 2023

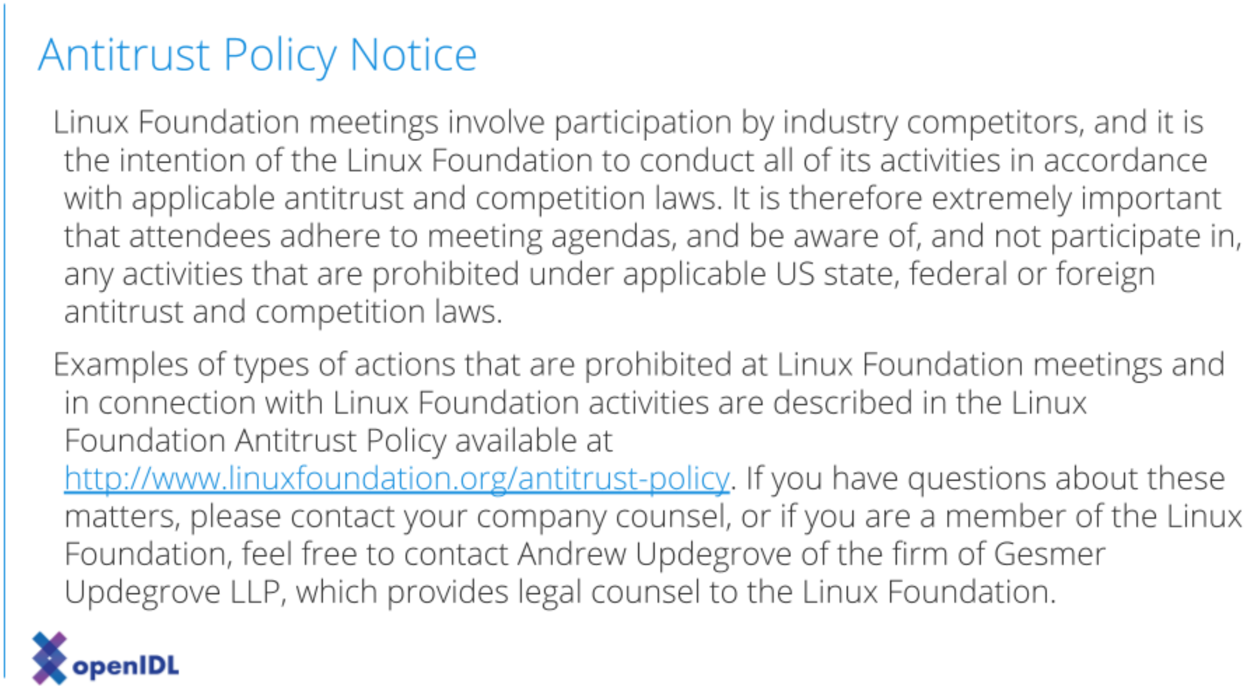
ZOOM Meeting Information:

Monday, July 10, 2023, at 11:30am PT/2:30pm ET.

Join Zoom Meeting

https://zoom.us/j/7904999331

Meeting ID: 790 499 9331



Antitrust Policy Notice

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

openIDL

Attendees:

- Ken Sayers (AAIS)
- Josh Hershman (openIDL)
- Jeff Braswell (openIDL)
- Peter Antley (AAIS)
- Ash Naik (AAIS)
- David Reale (Travelers)
- Faheem Z (Hanover)
- Joseph Nibert (AAIS)
- Tsvetan Georgiev (Senofi)
- Yanko Zhelyazkov (Senofi)

Agenda:

- Update on openIDL Testnet/Workshops (SeanB)
  - openIDL NodeBuilder Workshop 2023
- IWG update (YankoZ)
- Update on RRDMWG and internal Stat Reporting with openIDL (Peter Antley)
- AWG Goals:
  - document architecture to identify ingress and egress ports and content
  - identify technologies that cause issues (cognito, ses, postgreSQL)
  - discuss ci/cd technologies and containerization strategies

    - configuration options (SaaS, Multi-Tenant, Split, Whole Enchilada)
- AOB:

Notes:

- RRDMWG
    - Demoing table with multiple filters on OLGA at net AWG
    - Cognito doesn't pass spec with Hartford, would like to find auth service everyone likes
- AWG Goals
    - Consider setting goals, open questions, using Architecture Decisions to guide it
    - Couple tech components are challenging for diff carriers (Hanover + AWS, Hartford + Cognito)
    - Goal of this team - define arch of the 1.0, does or doesn't take into account these concerns
    - Carriers concerned about whats going in and out of their clouds
        - whats inside, what has to go out, what ports, what do we need to know about ingress and egress points
        - high level doc/diagram to represent it
        - need a doc that clearly answers question
    - One of the more challenging areas to deploy, "Whole Enchilada", installing whole node into carrier cloud - lot of CI/CD and IOC involved
        - while maybe same tools, maybe using open source vers and carriers use enterprise vers, config is an issue
        - seems like there is concern on IAC and CICD tech
        - supporting inside a carrier
        - Configuration options/ deployment options
        - whole enchilada vs split
        - adapter that listens for request for EP and then returns results
        - System as a service approach, everything hosted
        - multi-tenant approach
    - Step back and redefine some things our arch is founded on
    - get diagrams AND OPTion analysis
    - best place to start, goal of arch doc telling what ingress/egress are, ID tech causing issues, CI/CD, config options
    - goals this team could establish and work towards, sense of moving forward and it is time to establish to guide us in our work
    - too much reporting out and not enough moving forward
- What do we think about setting goals, are these good goals?
    - Point about access is the right thing - multi level/multi layer
    - Cognito vs Olga - a lot of cognito is for AWS space to get access - would OLGA be managed interface for data
    - OLGA as alt to cognito?
    - Validation in OLGA is validating data coming in
    - Cognito logs into OLGA
    - Cognito also for logging into AWS? No that's IAM (services in console), Cognito for app access, services underneath
    - Cognito gets you user access to certain roles, give you access to specific resources
    - On OLGA, going into this, season of building, idea - pretty much cloud agnostic app from user perspective, have button and modal to upload file, no direxct access to AAIS
    - GUI to send files, anything that requires access - app auth
    - intent of looking at OLGA as app to provide access, seems like carrier orgs would have other reasons for access to their AWS spaces
    - Way we will set up Cognito, no auth to do random things for AWS
    - Carriers use other tools than Cognito, not done that they wont allow Cognito at Hartford, but they dont want to, point there - ID tech causing issues, if 20 of them, then that tells you one thing, 4-5 is something else
    - Extra effort to make them abstract, openAPI (like OAuth)
    - OAuth recognized enterprise standards (instead of 20 diff things across carriers)
    - Broader Objective - und diff types of access to services and roles in the scope of what we are doing
        - AWS access: Kub, Fabric, etc.
        - often with access to DB apps, diff people have logins and inside the db there are logins, one of the issues to explore - where creds are verified and where others are group creds
    - Take the 4 configs on the bottom (SaaS, Multi-Tenant, Split, Whole Enchilada) what is in vs out for the carriers cloud?
        - because there is a lot of security, sec teams need to be able to und what is coming in and out
    - Picturing 4 diagrams with some lines that go in and out of the carrier cloud, documenting whats going across
- Travelers documented pain points
    - retro of some kind on nodebuilder
    - list of places where things are difficult
    - place to get the first level of identifying technologies that cause issues
- if things like AWS or Cognito cause trouble, this needs to be a pure SaaS offering
    - simple or it doesn't work
    - feels like a more general statement
    - get it defined and why it is like that
    - "install in your cloud" - not that easy
    - thinks we still have a lot of challenges there, try to bring into a cohesive statement
    - "this is why SaaS makes so much sense"
    - new wrinkle - not old tech, will have bifurcations of Azure vs AWS, OKTA vs ?, so many it will have to be, no stack amenable to more than a few people at any given time
    - gotta be packaged, how to articulate it
    - all have issues
    - even if biz folks on board, still having an internal challenge going to arch org to get an exception
    - so much easier to say "here is a SaaS platform"
- Goal of ent control of their own data, objective
- want a variety of diff ways of connecting to a network like system so there is choice (not all or nothing)
- aggregate makes sense, but any given carrier that optionality isn't a value, only want to do it one way (their way)
- in theory - over indexing how valuable
- get to point where all see where risks and probs are
- first and last bullet - optional footprints, level of ID where ins and outs are
- meat on these bones, have opinions but need to substantiate them

- if you are going to be a SaaS offering, who offers it?
- if standard was established, not single SaaS, implementation diff from deciding how it would happen
    - model has been to have a senofi, chainyard, be avail
    - AAIS and LF dont run infra, build, setup and maintain nodes on behalf of carriers
    - depends which parts of value prop want to maintain
    - standardize SaaS or set of standards?
    - how much of original value prop you want to maintain
- Pictured the split - a hybrid - everything you dont want in your cloud is SaaS, rest in carrier node (adapter)
- "why do i trust another entity any more than AAIS, what did I just solve?"
- AAIS needs to find another model, feeling comfortable with raw data, where trust moves
- very few times run their own cloud environments for corp data outside of workloads
- most of the time, when time to productionalize, will be in carrier-owned pub cloud or pure saas offering
- referring to carrier-owned cloud where IP are helping to maintain, providers with skillsets to make it easier
- even though a carrier might use IP, having them work within their cloud infra need to go thru tech governance, security and setup
- if you dont you are letting them live in their environment
- doesnt save much to outsource the work b/c still needs to support in their cloud
- diff ways to access diff services
- our specific issue for T, looking at it from an Arch perspective, have concerns
- dont think in the long run they wil be the only ones, more we get ahead and think through, easier to talk to other carriers
- gonna run into similar issues with other Carriers
- make it cleaner, dont go with a laundry list, "how to I set this up?" they want a clean answer, SaaS is cleaner
- need a yardstick, how are we doing convincing a carrier -

Time	Item	Who	Notes

Documentation:

Notes: (Notes taken live in Requirements document)

Recording: