2022-03-10 Meeting notes

Date

10 Mar 2022

Attendees

- Craig McNally
- Julian Ladisch
- Brandon Tharp
- Chris Rutledge
- Axel Dörrer
- Jakub Skoczen
- John Coburn
- Ryan Berger

Discussion items

Time	Item	Who	Notes
5 min	Chris Rutledge replacing Brandon Tharp?	Team	Latest update, next steps, etc. Did the TC approve? - YES Next Steps: - Update the wiki - Add Chris to the slack channel - Get him a meeting invite - Grant him access to the SECURITY JIRA project - email distro list. - Remove Brandon from these various places too! Craig McNally to continue onboarding Chris Rutledge
5 min	Update on ☑ **FOLIO-3317** - Spike - investigate possible file upload vulnerability `OPEN`	Axel	Continue to monitor - not a ton has changed here since we last checked.
5-10 min	🔖 **RMB-902** - Reject tenant with invalid characters and possibly sanitize `OPEN` 🔖 **OKAPI-1081** - Reject invalid tenant ids `BLOCKED`	Team	Notes from previous week: - Prioritized as P2 - hopefully we can get this fixed in Morning Glory - Next steps: - Review the set of restrictions - are we missing anything? - Julian Ladisch to discuss details with members of the Core-platform team. - Reach out to the implementers once we have an agreed-upon set of restrictions. The purpose is two-fold: - A) See how prevalent this problem is. And - B) let them know that they shouldn't be creating new tenants based on the restrictions outlined in OKAPI-1081. - Maybe we should have OKAPI reject new tenants based on these restrictions, but allow pre-existing tenants that are already in place. - Brainstorm what migrations would look like - what is the scope? Stripes-config, edge API --- Discussions are ongoing, currently blocked on a decision being made. - Document the options on the wiki to facilitate these discussions and the decision making process. - Julian Ladisch to take this on. - By this group? By the TC? - How do we constrain the module names? If so, where/how? - Various restrictions: Postgres, Hosting infrastructure (Kubernetes/ECS/etc.) - What about the tenantId restrictions? - Also part of the above discussion/decision.
5-10 min	☑ **STCLI-190** - Update dependencies (CVE-2021-3807) `CLOSED`	Team	There's a PR that hasn't' moved in a while... What's the status? How do we move this forward? - Ryan Berger / John Coburn to help push this along. Was there another PR against stripes-testing? - already merged (ui-test:94)
*	Review the Kanban board.	Team	

Action items

- [x] Craig McNally to get Chris Rutledge setup with the various things mentioned above.
- [x] Julian Ladisch to document the options for restricting tenantId and module names on the wiki (Context:
  🔖 **RMB-902** - Reject tenant with invalid characters and possibly sanitize `OPEN` / 🔖 ~~**OKAPI-1081**~~ - Reject invalid tenant ids `BLOCKED`)