Theme: Shanghai library FOLIO project
Time: September 15, 2020 07:00pm (EST) / September 16, 2020 07:00am (GMT+8)

Attendees:
Vincent Bareau (Enterprise Architect, EBSCO)
Gang Zhou (Project manager, Shanghai library)
Sha Jiang (Technical Director, Jiatu)
Lucy Liu (Product Owner, Folio China)

Notes:

1. **Permanent token**

   Sha Jiang: Currently we provide the user with a permanent token when log in through Okapi. Will this be changed in the near future?

   Vince:

   - We have session tokens now that don't expire. We will introduce a model that has session tokens and refresh tokens. The session token expires quickly. Then the user can use the refresh token to get a new session token automatically and go back to the pages where they left.
   - This need has been captured in Jira. Not sure when the Core-platform can work on this.

Jira#	Type	Priority	Status	Dev team	Reporter	Assignee
FOLIO-2524 Security Audit raised issues	Umbrella	P2	Open	Core-platform	Jakub Skoczen	Jakub Skoczen
FOLIO-2556 SPIKE: investigate refresh tokens support in FOLIO	Task	P3	Blocked	Core-platform	Jakub Skoczen	Craig McNally
MODAT-64 Enforce access token expiration	Story	P2	Open	Core-platform	Craig McNally	Unassigned

   Sha Jiang: A temporary alternative solution is to take the timestamp from the payload and make the token expire. Mod-authtoken will check the timestamp. We can do it locally, just for the SHL project.

   Vince:

   - If you modify mod-authtoken, it will work off the branch. Then you won't benefit from the work around mod-authtoken.
   - For example, a work ongoing is to optimize performance. They want to cash the tokens so that they don't always have to go back and do the extra calls to mod-authtoken to validate tokens. But there are request IDs

that are embedded in the token that breaks the cash. So they made some changes to remove the request IDs. These changes are not finished now.

- Vince will reach out to Craig and ask him if he has any plans soon to implement it.
- If we introduce expiration of the tokens and the tokens are defaulting to however long, it's going to be a change of behavior for other implementers in production now. But if we can configure the expiration and set a long date, then it should be ok.

Lucy: Do we have a timeline for this? When must this be solved?
Sha Jiang: Ideally it should be solved by this year.

2. **User registration**

Sha Jiang: Are we going to allow public users to register?
Vince:

- We don’t have a plan for this because the current implementers don’t have such a scenario. Students have a mechanism to auto-register by connecting to a system. But the patrons never log in to folio directly.
- One way to get around it is to implement SAML logins/authentication. Then folio will defer to SAML, and it will create a user if the user is valid.
- Vince will check with Patty, PO to ask if there is a plan to implement this.
- So you have many libraries. You want the library staff to automatically create their own accounts. How do you control who is able to register themselves?

Sha Jiang: We want to have a page to allow staff to register themselves. Maybe it can only be accessed by local networks.
Vince: I don't know if we have support for local IP restrictions built into folio. You have to build that on the outside with a bouncer or nginx.
Sha Jiang: How to grant registered users the default permission?
Vince:

- This falls under mod-user. I will contact Patty to inquire about how to do it.
- So you want to define a default permission set and apply to any user. Each module defines its own permission. So it’s module by module. How do you coordinate the changes with the current modules? So you create a small frontend for user registration. The user can get to it by the restricted IP address. Then they enter details and submit a request to create a user. You have a predefined permission set that you managed within that application. Then it makes an additional call to register that user to the permissions. Then you can basically run that permission set as a file or as

some sort of the configuration list. And you can update it as new permissions come and go. Does this work for you?

Sha Jiang: Yes. We have a plan. If the community doesn't have a plan, we will use our alternative one.

3. **New performance test report**

   Sha Jiang: The conclusion is that k8s works as good as the original Okapi cluster. We decided to use k8s for container management in our production environment.

   Vince: That's good news.

4. **Trial run**

   Lucy: SHL is using the Q1 2020 release and decided to skip Q2 2020. It's not decided yet whether to skip Q3 2020 and Q1 2021. The trial run will start December 2020.

   Vince: How will you do the trial run?

   Gang Zhou: We will start with one branch. The library that starts the trial run will only use folio. If it works well, then more libraries will join in the trial. If it doesn't work, we will roll back to the current system.

   Sha Jiang: This trial is actually go-live.

   Vince: Then this raises the importance of the release SHL chooses to go live. There are a lot of defects in the Q1 2020 release. But the Q3 should be robust.

5. **Digital resources**

   Sha Jiang: How does folio manage digital resources, for example, videos? I mean storage management, not metadata.

   Vince: Folio doesn't actually have any plans for storing content itself. There are extensions being worked on for storage management, like remote storage, plan for archival systems and institutional repository. No plan for storage of videos right now.