Theme: Shanghai library FOLIO project

Time: October 12, 2021 07:00pm (EST) / October 13, 2021 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. **Does FOLIO have specifications for security and access control for Kafka and ElasticSearch? (Gang Zhou)**

Vince:

- Yes and no. We have a prescribed mechanism to ensure that FOLIO security is maintained when using ElasticSearch and Kafka.
- The way we treat ElasticSearch, from the security perspective, is pretty much the same way that we treat PostgreSQL. They are external to FOLIO, meaning they need to be set up and configured outside of FOLIO. And then FOLIO makes use of them. So policies around user accounts, credentials, how to set up configurations, etc., are all set up at the tool level, in ES and PostgreSQL. From the FOLIO perspective, the way that this is connected is that these are all environmental variables and credentials for ES. And they are injected to the system you want. There is a Jira created for this https://issues.folio.org/browse/MSEARCH-64. If you don't provide credentials, FOLIO will attempt to use ES in an automated fashion.
- This wiki page (https://wiki.folio.org/display/~mage.air/Kafka+Security) describes how FOLIO deals with Kafka security. We implement separation of the Kafka system from Okapi and the modules. The modules prescribed with Kafka are required to implement certificates. Those certificates are in the keystore and can be protected with passwords. We use Kafka's native access control list (or ACLs) to restrict the access as needed. The modules obviously provide an independent tenant context. And we have that tenant context continuing into Kafka as well.
- Again, the setup of ES and Kafka is done outside of FOLIO. You have to separately configure ES to the security level that you wish. There are no plans to configure this from FOLIO.

Lucy's notes: answers received on Slack after the meeting:

- From **Mikhail Fokanov**:
  "As stated in https://wiki.folio.org/display/DD/Search data for each tenant is stored in separate index.
  There is only one user for Elasticsearch and we mod-search use BASIC auth to make calls. The creds are provided in environment variables. HTTPS is used.

The similar is true for Kafka, e.g. there is a separate Kafka topic for each tenant. For Kafka please see:
https://wiki.folio.org/display/FOLIJET/Enabling+SSL+and+ACL+for+Kafka
https://wiki.folio.org/display/DD/Temporary+Kafka+security+solution"

- From **Craig McNally**:
  "There was a proposal earlier this year. I don't know off-hand where it stands. Here's the link: https://wiki.folio.org/display/~mage.air/Kafka+Security"
  "Looks like there are several JIRAs which are already closed. and two that are still open.
  https://issues.folio.org/browse/FOLIO-3173
  https://issues.folio.org/browse/FOLIO-3174
  IIRC there are also parts of this that fall upon the hosting provider/SysOps."

2. **At present, we deploy two OKAPIs in virtual machines, but when the mod in a Docker is not working, OKAPI cannot sense and continue to distribute call requests to this mod. (Gang Zhou)**
   Vince: The simple answer is that OKAPI can not and does not sense the health of modules. Typically you will manage the state of modules outside of OKAPI for health checks. For example, you can use orchestration mechanisms like Kubernetes or ECS with AWS, which can be used to detect that. It can monitor that and if it detects something has been made unavailable to operate, you can spin up the instance of the module and proceed to register with OKAPI and let OKAPI know about it. If a module stops working, OKAPI doesn't know and will keep sending messages. And if you want to stop OKAPI from sending messages, you have to deactivate that module from OKAPI.
   Gang Zhou: We have health checks in the premises, i.e., the monitor system, and can detect failures of all the modules in FOLIO. But we can't control OKAPI to route requests. If a module goes down, we hope OKAPI will route the request to another module. Any future plans for this function?
   Vince: I don't think so. The only option you have now is to detect the failed module and deregister it from OKAPI. Then OKAPI will stop sending traffic. If you have three modules, OKAPI will send requests to M1, M2, M3, M1, M2...If M3 is not working and is deactivated, OKAPI will immediately send requests to M1, M2, M1, M2...If you add M4, OKAPI will send requests to M1, M2, M4, M1… So if you deactivate or add a module, it will be handled externally. Typically, it will use the orchestration of your system, for example, Rancher, ECS, K8S.
   Gang Zhou: Should we use K8S to realize this functionality?
   Vince: Yes, whichever choice of orchestration you have. It's something the hosting providers need to do for themselves.

3. **How to detect failed modules in the case of dual nodes and/or non-containerized OKAPI clusters? Can we use KeepAlive for the health check? (Sha Jiang)**

Vince: Sure. But when you detect a bad health, OPAKI can't do anything about it.
Sha Jiang: Now we deploy two OKAPIs into the wire machines. One OKAPI cluster has two nodes. And we have FOLIO modules in these two wire machines. We don't have a container for this deployment.
Vince: If you don't containerize, you can use other tools, not necessarily a Docker deployment. Simply register the modules with OKAPI. The benefit of deploying modules and OKAPI separately is that it will be easy to deactivate bad modules.

4. **How to discover modules that are still alive but run at low efficiency? (Sha Jiang)**
   Vince: There is no universal health check design for FOLIO. It's something you need to figure out on the hosting basis. You may need to run scripts that basically attempt a particular API. The API reads something and you can access whether it's too slow, then kill it and put a new one. There's no built-in mechanism for FOLIO to do this at this time.

5. **FOLIO Day Warm Up October 22, 2021 (Vince)**
   Link to the Benevolence wiki page https://wiki.folio.org/display/FOLIJET/2021-9
   Forward the latest OLF newsletter to Vince. (done)

6. **Will SHL or other libraries in China be interested in the LDP app? (Lucy)**
   Gang Zhou: Not now. Maybe we will think about it when it's more mature.