Date
15 Feb 2019

Attendees
- Craig Boman
- Chris Creswell
- Greg Delisle
- Robert Douglas
- Mike Gorrell
- Ingolf Kuss
- Tod Olson
- Jason Root
- Wayne Schneider
- Zeno Tajoli
- Brandon Tharp
- Patty Wanninger

Goals
- Clarify security issues

Discussion items

<table>
<thead>
<tr>
<th>Time</th>
<th>Item</th>
<th>Who</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Welcome</td>
<td>Ingolf</td>
<td>who will be the note taker ? Tod Olson</td>
</tr>
</tbody>
</table>

| 25 |  | **Deployment issues**<br>Ingolf, Mike Gorrell, all | Review deployment issues discussed last week:  
- Dependency resolution, separation of the build and run stage. We want to build the backend outside of Okapi.  
- Impose these as guiding principles: [https://12factor.net/](https://12factor.net/)  
- We need a versioning of data base schemas in order to be able to upgrade modules.  
- Data integrity needs to be ensured from release to release.  
- Maintaining a principle of decoupling of the modules.  
- We need a disaster recovery perspective. A way to rollback changes. We need to be able to start up the system from a (cloud application) backup.  
Relate these issues to the findings of the OTS Project Health Report.  
Began with Mike Gorrell presenting this writeup.  
Discussion:  
Is TC taking this report as a roadmap? First action was to ask PC to ask Stakeholders for a security audit. Took all of the recommendations and reviewed and came to consensus on priorities/severities. One cluster of issues was around technical documentation, and TC is recommending a Technical Writer sometime in the fairly near future, as a time-bounded engagement.  
What about pulling from different npm repositories? Some recommendations come from the perspective of small companies wanting to stand up FOLIO, have custom modules, etc. From the project perspective, that may not be our highest priority right now, may be focused more on fleshing out core modules.  
SysOps problem is that currently have to pull all modules, all versions of the whole set of modules.  
Wayne Schneider There are two issues. The report is specifically talking about how you build a UI, and we sort of have a monolithic npm repository structure right now and OTS is suggesting we become more flexible. The issue that has come up in the SysOps is that we have a very naïve way of distributing modules, here's everything and good luck.  
Mike Gorrell The OTS report does go into some of that. TC priorities are reflected in the order in the TC writeup.  
A lot of work has been done between TAMU and the Core on deployment with Kubernetes.  
Patty Wanninger a question about the Tech Writer, there is still a lot of documentation that has not been created, it's still hard to even discover what terms mean. Can that not be scoped too narrow. Mike Gorrell The Tech Writer is not in the OTS report, but came out of the TC as a way to address some issues. In the PC yesterday, Paula Sullenger mentioned that the need for a Tech Writer for things like user manuals has come up in other channels. So it seems the community may come together around this.  
Wayne Schneider, Jason Root This comes at a really good time, thank you for the TC and to EBSCO for sponsoring this.  
For comments, please make comments on the OTS Project Health Report wiki page, on the #tech-council channel, on the Tech Council, or by email.  
Upcoming Meeting Agenda Items  
30 |  | **How to secure FOLIO on the network?**<br>all |  
- Strategies to protect Okapi services  
- How to grant and constrain access  
- Issues about how the X-Okapi-Token is handled and passed for certain Okapi communications to backend modules  
- Is the system secure so that only sys admins can do complete data dumps from the system?  
Jason Root At TAMU, we've gone beyond the documentation in [Securing Okapi installation](https://github.com/folio-org/okapi) on the Okapi GitHub page. Our secure-okapi Dockerfile in the folio-install kube-rancher branch uses a script that is based on the Okapi documents. Our scanning tool Security Center (Nessus) has not turned up major problems when scanning the Kubernetes cluster nodes where Folio resides. Still looking at solutions to provide database access from within Kubernetes/Rancher cluster to system librarians who need to look at the data structure. Other infrastructure mechanisms provide layers of security: reverse-proxy, SSL certs, packet encapsulation, changing default database admin user and password, etc...  
Wayne Schneider The browsers need to access Okapi, and we expose the one endpoint by using nginx, how are others securing this? Chris Creswell has set up Apache as a reverse proxy to Okapi. TAMU using the default nginx in Docker to make the Okapi endpoint available, have certificate on that.  
Similarly, how are people securing the backups?  
Seeing slowdown loading data through API, has also been a concern in Data Migration. Need to surface this to the devs.  
Rancher has some modules to stand up Prometheus and ??? to monitor pods.  
How might we test for scaling? Maybe come to a common set of tests that we can run. (Does this imply a common set of data?)  
Existing JMeter performance tests: [https://github.com/folio-org/folio-perf-test](https://github.com/folio-org/folio-perf-test) A couple devs at EBSCO are leading this, Eric Valuk and Hong Wei Ji, and may be willing to talk about this on Slack.  

**Action items**