LSP integration and PDAC Meeting 2018-11-29

Date

29 Nov 2018

Attendees

- Gregory Dubois-Felsmann
- Michelle Butler
- Fritz Mueller
- Kian-Tat Lim
- Fabio Hernandez
- Loi Ly
- Igor Gaponenko
- Brian Van Klaveren
- Simon Krughoff

Goals

- Advance the integration of the LSP components and their collective functionality

Discussion items

Time	Item	Who	Notes

	Plan for implementing Phase 1 authorization	Gregory Dubois-Felsmann	• See DMTN-094 (LSP Authentication Design) by Brian Van Klaveren
			• Extensive discussion of the rights-checking API proposed by Unknown User (xiuqin) at the LSP Workshop and further discussed at a recent LSP Integration & PDAC (LSPIP) meeting:
			  • Rights such as "may use the Notebook Aspect", "may use the Portal Aspect", etc. will be modeled as membership of corresponding LDAP groups.
			  • This check must be made by each Aspect at the time the user first encounters it, e.g., in a fresh browser session. The check could be performed by Aspect-specific code knowing the appropriate LDAP group name and looking in the group list in the user's OAuth2 identity token for this group. However, this requires Aspect code to know the site-specific LDAP group name.
			  • It is expected to be helpful to the portability / relocatability of the implementation of the LSP components for the "magic string" that the Aspect needs to know, in order to perform the correct check, to be site-independent, representing just the site-independent abstract concept of, e.g., "may use the Portal Aspect".
			  • The recent LSPIP meeting reached a consensus that this would be done through a RESTful network API, in preference to the provision of language-specific APIs, which would have been needed in at least Java, JavaScript, and Python.
			  • Gregory Dubois-Felsmann proposed, to move things forward, adopting a portion of the syntax of the proposed IVOA Group Membership Service (see the recent Working Draft, specifically Section 4.1) for this API:
			  • Concretely: `GET /search/{group}`
			  • For our purposes, we will consider the "group name" to be a "virtual group" with a site-independent name (see below) which the rights-checking service knows how to map to an actual LDAP group name. We are not at this time anticipating using the proposed rights-checking API service to check for membership in LDAP groups representing collaborations or otherwise as a general LDAP-querying service.
			  • The API indicates the holding (non-holding) of the tested right (i.e., membership (non-membership) of the associated LDAP group) with HTTP status codes 200 (OK) or 403 (Forbidden), respectively. This makes for a very simple test in the Aspect-specific code that invokes it.
			  • The API must accept an OAuth2 identity token in its header, and the user in question is determined by inspection of the token; we do not at this time propose using the optional user= or principal= parameters of the IVOA GMS.
			  • Most likely the membership of the desired right-representing LDAP group will be determined by a simple inspection of the group list in the identity token, but this is an implementation detail.
			  • We do not at this time propose implementing the GMS's `GET /search` method (with no group name supplied) for obtaining a list of groups. However, it's not difficult to see ways in which this might be useful, and it's a possibility for future work.
			  • We will not, at this time, make a public claim that our rights-checking service "is" an IVOA GMS, in view of the limited scope above, but we may discuss this work in the appropriate IVOA mailing list and/or present it at the next InterOp.
			  • The endpoint for this service will be under the common hostname for all the components of an instance of the LSP, and each LSP instance will have its own instance of this service, located under the "/api" branch of the pathname space.
			  • Therefore, for instance, the "lspdev" (lsst-lspdev.ncsa.illinois.edu) and "PDAC" (lsst-pdac.ncsa.illinois.edu) instances will have separate rights-checking services.
			  • For the sake of concreteness, the proposed endpoint is `https://{instance-DNS-name}/api/lsp-rights/search/{virtual-group}`
			  • Virtual group names "portal-x" and "nb-x" for "may use the Portal" (respectively, "Notebook") are proposed, with the strings derived from the previously agreed pathname prefix for the Aspect and from the notion that "use" is an execute-like right (as opposed to, say, "read" or "write").
			  ☐ Brian Van Klaveren will include these names and other rights-checking virtual group names of relevance to the LSP design in an update to DMTN-094. **12 Dec 2018**
			  • It is expected that the Aspect implementation groups will, as an additional investment in future flexibility, embed these names (e.g., "portal_x" in the Portal implementation) in configuration files and not in the source code itself.
			  • Fritz Mueller bravely accepted the (small, we believe) upscope of implementing this service and indicated that the development of a prototype version could be undertaken in December.
			  ☐ Fritz Mueller will create epic/story ticket(s) as appropriate to represent the rights-checking service work in the S19 cycle. **06 Dec 2018**
			  • It is intended that the instance-specific, site-specific mapping of the instance-independent rights-representing virtual groups to actual LDAP groups will be set out in a config file for this service.
			  • Note that the implementation of Phase 1 authorization in the Portal is blocked on this work.
			  • It is intended that the rights-checking service be used by the Notebook Aspect as well. As there is an existing implementation of authorization-checking in the Jellybean code, which would have to be migrated to this design, and as there was no developer representation from that group at this LSPIP meeting:
			  ☐ Adam Thornton and others, as appropriate, should look at the rights-checking service design and comment ASAP, and, if possible, report at the **13 Dec 2018** LSP Integration & PDAC meeting.
			
			• We asked Loi Ly about any other remaining blockers for implementation in the Portal of the Phase 1 authentication and authorization plan.
			  • He reminded us that the question is still open of the provision of an "OAuth2 proxy" to handle some of the details of the complex series of redirections and other transactions involved in using CILogon to obtain, ultimately, the needed tokens. (The alternative being making each Aspect responsible for implementing this logic.)
			  ☑ Kian-Tat Lim and Brian Van Klaveren promised to provide a concrete specification by the next LSPIP meeting on 13 Dec 2018 of what the design is in respect of an OAuth2 proxy,
			  and
			  ☑ Brian Van Klaveren retains the action of providing at least a prototype implementation of an OAuth2 proxy in the near future. (On 13 Dec 2018 we will revisit the design and schedule for that.)
			  ~~**DM-16694**~~ - Determine whether and how to use OAuth2 proxy DONE

	Kubernetes fabric consolidation	Fritz Mueller , Michelle Butler	• The integration of the existing PDAC hardware into the Kubernetes Commons will proceed next week (the week of 03 Dec 2018).
			  • The Qserv czar and worker hardware will be tagged with "taints" and "labels" to ensure that it is excluded from eligibility for use in the Notebook Aspect and other non-Qserv applications, and can be identified successfully as part of instantiating an integrated Qserv instance on that hardware.
			  • The same will be needed to ensure that the distinctively large-memory Firefly server hosts are set aside for that purpose. After some discussion the tentative proposal is to recycle the old Firefly load-balancing server host (superseded by the Kubernetes ingress mechanisms) as a third Firefly/Tomcat host; it has the same specs as the others.
			  • Matthew Thomas Long and Loi Ly will get in touch with each other to ensure that the necessary taints and labels are applied to the Firefly server hardware integrated into the Commons, and that naming conventions consistent with those used for the Qserv hardware are chosen. 06 Dec 2018
			  • The intent is to operate **two complete instances of the LSP** in the Commons (`lsst-lspdev` and `lsst-pdac`), though only the latter will have a large-scale Qserv instance behind it, for now. Each will have its own JupyterHub/Lab instance and Firefly servers, and the two instances may have different sets of authorized users.
			• A few issues associated with the overall management of the Kubernetes cluster and the integration of LSP components into it were discussed, in respect of which we realized that there are still grey areas in responsibilities of this nature. They are becoming more important to resolve as we proceed further with integration.
			  ☑ Kian-Tat Lim , Michelle Butler , and Fritz Mueller were encouraged to discuss this, perhaps at a coord meeting, and report back at the next LSP Integration and PDAC meeting on these cross-cutting responsibilities. 13 Dec 2018

	DAX group status update	Fritz Mueller	• Christine Banek has demonstrated the basic ability to communicate from the CADC-derived TAP server, via Presto, to a Qserv instance. Much remains to be done, e.g., integration of ADQL spatial query language with Qserv's spatial query functionality, but this is a very promising development. • Kenny Lo is beginning to work on the implementation of a SODA service as a successor to the cutout service part of the previous `imgserv` functionality.
	WebDAV service plans	Brian Van Klaveren	• Brian Van Klaveren is still responsible for setting up a prototype WebDAV service and may be able to work on this during December. ~~DM-16695~~ - Select a WebDAV package for the User File Workspace DONE

Action items

☐