Contribution ID: **20** Type: **Oral Presentation**

IRIS Identity and Access Manager: UK Experiences with token based AAI

Thursday, 25 March 2021 11:10 (20 minutes)

Driven by the physics communities supported by UKRI-STFC (UK Research and Innovation Science and Technology Facilities Council) the eInfrastructure for Research and Innovation for STFC, or IRIS, is a collaboration of UKRI STFC, science activities and provider entities in the UK. Over the last few years the UK's IRIS collaboration and IRIS 4x4 project (£16m as £4m p.a. for four years) has worked to deploy hardware and federating tools across the range of physics supported by STFC.

The IRIS IAM (Identity and Access Manager) is IRIS' answer to federated access, providing a coherent framework for accessing a range of different computing resources. An identity proxy based on the AARC blueprint architecture and utilising the INDIGO IAM software (originally developed as part of INDIGO Data cloud), the IRIS IAM service provides federated access to IRIS resources and aims to remove friction for scientific communities and promises to facilitate a new generation of workflows across diverse resources. As well as acting as providing federated access to users affiliated with eduGAIN institutions, the IRIS IAM is also able to act as an IdP-of-last-resort for members of the IRIS community who do not have a home institution IdP. This is achieved through provisioning of locally managed IAM accounts, with new accounts vetted by a trusted community representative. The IRIS IAM has also been an important technical driver for ongoing parallel development of the IRIS Trust Framework security policy set.

The IRIS IAM also provides community attributes in the form of group memberships, which can then be used for authorization purposes. Delegation of management of these groups is possible, and this responsibility will usually be assigned to the administrators of the services behind the IAM or to trusted representatives of the science activities whose researchers need access. These group managers can then approve or deny membership request, which correspond to confirming access to controlled resources and services.

Development of the IRIS IAM service has been in parallel to other community Authentication and Authorization activities, such as FIM4R and the WLCG authorization project, in order to ensure that the IRIS solution aligns with and supports the work undertaken elsewhere. Three years since the project began, The IRIS IAM is now an established production service, providing access to a number of IRIS services, including OpenStack clouds, accounting dashboards and security portals and with work underway to connect both Rucio and Dynafed services, among others. Recent work has focused on enhancing the service's operational performance and features, including work investigating how best to utilise the OpenID Connect workflow over command line/ssh sessions. However, work is still underway to enhance the service's offering, including the range and scope of clients the IAM provides access too. This talk shall report on work to support web-based and command-line based services, progress thus far, notable challenges, and next steps and plans for the IRIS IAM service.

Summary

Over the last few years the UK's IRIS collaboration and IRIS 4x4 project (£16m as £4m p.a. for four years) has worked to deploy hardware and federating tools across the range of physics supported by STFC. Providing a coherent framework for accessing HTC, HPC and Open Stack cloud resources, the IRIS IAM (Identity and Access Management) service provides federated access to resources, removing friction for scientific communities and facilitates a new generation of workflows across diverse resources.

Primary author: Mr DACK, Tom (STFC UKRI)

Co-author: Mr COLLIER, Ian (STFC-RAL)

Presenter: Mr DACK, Tom (STFC UKRI)

Session Classification: Network, Security, Infrastructure & Operations Session

Track Classification: Network, Security, Infrastructure & Operations