IRIS IAM
Federated Identity Management for IRIS

Thomas Dack
Will Furnell
Agenda

1 Introduction to IRIS and the IRIS IAM
2 Progress and Challenges
3 Command Line Integration
4 Next Steps
But what is IRIS?

• eInfrastructure for **Research and Innovation for STFC**
• Collaboration between **Science Activities** and **Provider Entities**
  • Driven by the physics communities supported by UKRI STFC
• A coordinating body for the provision of STFC eInfrastructure
• IRIS does not run infrastructure **directly**
  • Commissions deployment of resources available to all science activities
• IRIS 4x4 is a capital project coordinated by IRIS
  • £4 million per year for 4 years
  • No money for operations
  • Can issue grants for equipment and grants to make things
    • Such as the IRIS IAM
• Identity management is required for IRIS resources to function as a coherent infrastructure
IRIS Partner Examples

- IRIS Provider Entity examples:
  - STFC Scientific Computing Department
  - The Hartree Centre
  - The Ada Lovelace Centre (SLC)
  - DiRAC [HPC]
  - GridPP [HTC]
  - The DLS Computing Department
  - CCFE computing

- IRIS Science Activity examples:
  - ALMA
  - ATLAS
  - CCFE
  - CLF
  - CMS
  - CTA
  - DLS
  - DUNE
  - eMERLIN
  - EUCLID
  - GAIA
  - ISIS
  - LHCb
  - LIGO
  - LSST
  - Lux-Zepelin
  - SKA
IRIS Background

- Need some common elements to support these communities working together:
  - Policy and Trust Framework
  - Identity Management
  - Resource Accounting
  - Monitoring

Identity management is required for IRIS resources to function as a coherent infrastructure.
The IRIS IAM

• INDIGO IAM selected for use due to existing capabilities and support
  • Originally developed as part of the INDIGO Datacloud Horizon2020 project
  • For more info, see Andrea Ceccanti’s talk on Monday: https://indico.egi.eu/event/5000/contributions/14488/

• Aims of the IRIS IAM:
  • Provide users with a consistent authentication experience across IRIS services
  • Provide science communities with central authorization through group management capability

• Observer in AEGIS, active participant in FIM4R
Current Status of the IAM

• Production standard service based on AARC blueprint
  • Primary authentication a number of IRIS services, including Accounting Portal, MISP Security Portal and OpenStack Clouds
  • Primary means of authorization for IRIS Users within the SCD Cloud

• Small team supporting the service development and operations
  • Currently looking to expand effort in order to better serve community

• Close liaison with IRIS Policy and Trust Framework
  • Ensure that the IAM follows collaboration polices and policies reflect what is possible
  • For more information see yesterday’s talk here

• Testing IdP-of-last-resort usage with select science communities
IRIS IAM: AARC Blueprint based

- Federated Identities via eduGAIN
- SIRTFI compliant with REFEDS status asserted
- GÉANT COC compliant

IRIS IAM: AARC Blueprint Architecture based on the AARC Blueprint Architecture

- Federated Identities via eduGAIN
- SIRTFI compliant with REFEDS status asserted
- GÉANT COC compliant
Challenges

• How to provide access to services which operate only over command line
  • Will will discuss next
• Assurance for users who do not have an eduGAIN IdP
  • Using the IRIS IAM as an IdP-of-last-resort
  • How best to ensure registration approvals follow security policies
• Community and Client Buy In
  • The service is in production and serves some IRIS communities
  • Slow uptake from others – the service is fully in operation, but challenge in getting adoption from people with existing solutions
• Full delegated group management is not currently implemented
  • This is due to be improved in IAM 2.0
SSH Access
Via IRIS IAM

Will Furnell
SSH access via IAM

- PAM Module
  - [https://github.com/stfc/pam_oauth2_device](https://github.com/stfc/pam_oauth2_device)
  - Fork of [https://github.com/ICS-MU/pam_oauth2_device](https://github.com/ICS-MU/pam_oauth2_device)
- No client side software needed
- Integrates well with IRIS IAM & Openstack
- No special/custom SSH server required
- Not just SSH!
SSH access via IAM

- Demo video
SSH access via IAM

- Other options considered, but...
- Moonshot
  - Needs client software, which is no longer supported on Windows
  - All institutions need to deploy a RADIUS server with Moonshot support
- Vault
  - Needs client software (which does work on Windows)
  - More management involved (just IAM UI is better for us)
Next Steps

- Integration of more IRIS services and communities
  - Including particular focus on Command Line services
    - This includes services such as RUCIO, Dynafed, and DiRAC [HPC]
- Adoption of FITSM
  - Service is operating fine, but adoption of FITSM would help with sustainability
- Adoption and Migration of INDIGO IAM 2.0 when available
  - Improved multi-tenancy support
INDIGO IAM Users Workshop

https://indico.cern.ch/event/970568

January 27th - 28th 2021 with provisional times of 14:00 - 17:00 (UTC) each day (depending on number of talks, and scheduling)

The aim of this workshop is to facilitate user led discussion around best practice, administration and deployment experience between the different communities who utilise the INDIGO IAM Authentication and Authorization service.
Questions?
Thank you