
UKRI
Science and Technology Facilities Council
Scientific Computing
Welcome

Scientific Computing

Overlay VPN Network

Donald Chung (donald.chung@stfc.ac.uk)

Agenda

1 Scenario & Problem Statement

HA-IAM

2 Benefit for IRIS Community

IRIS-IAM and other use cases

3 Solutions and Software Available

Review Available Software: Netbird, Defguard etc.

4 Discussion & Questions

Uses within the IRIS community

UKRI Science and Technology Facilities Council

Scientific Computing

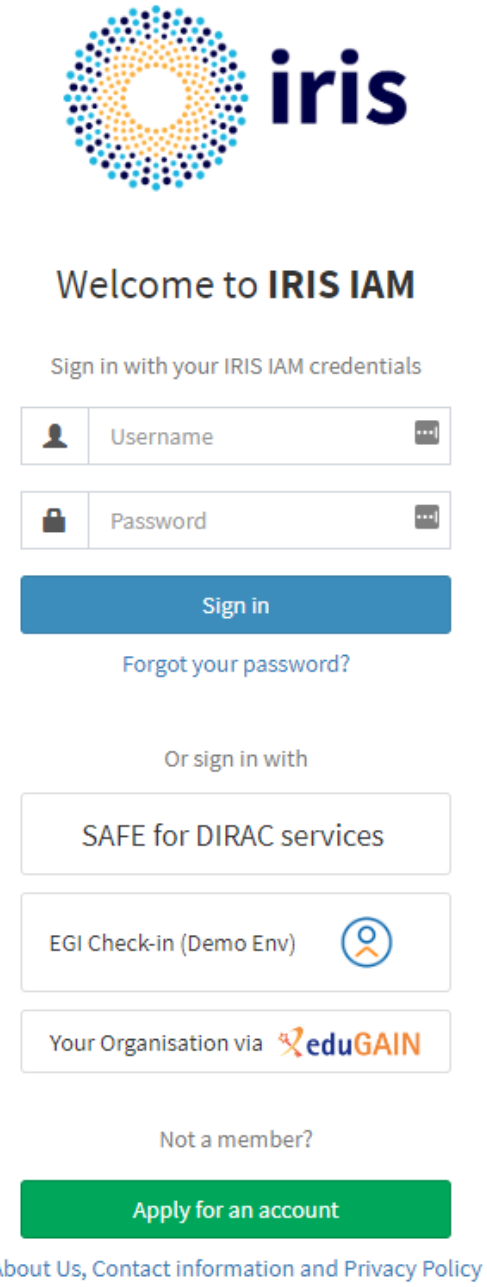
Scientific Computing

Scenario & Problem Statement

What is HA-IRIS-IAM?

- Single sign on service created for
  - IRIS system
  - Related organisation
- Federated identities from university credentials
  - No new AC needed
- Make it highly available
  - Distributing the service across multiple data centre
- Plan
  - Move to Rocky 9
  - Migrate to HA-DB and v1.8.3/v1.8.4
  - Migrate to HA Frontend

Source: IAM for IRIS IAM-Log in (stfc.ac.uk)



Science and Technology Facilities Council
Scientific Computing

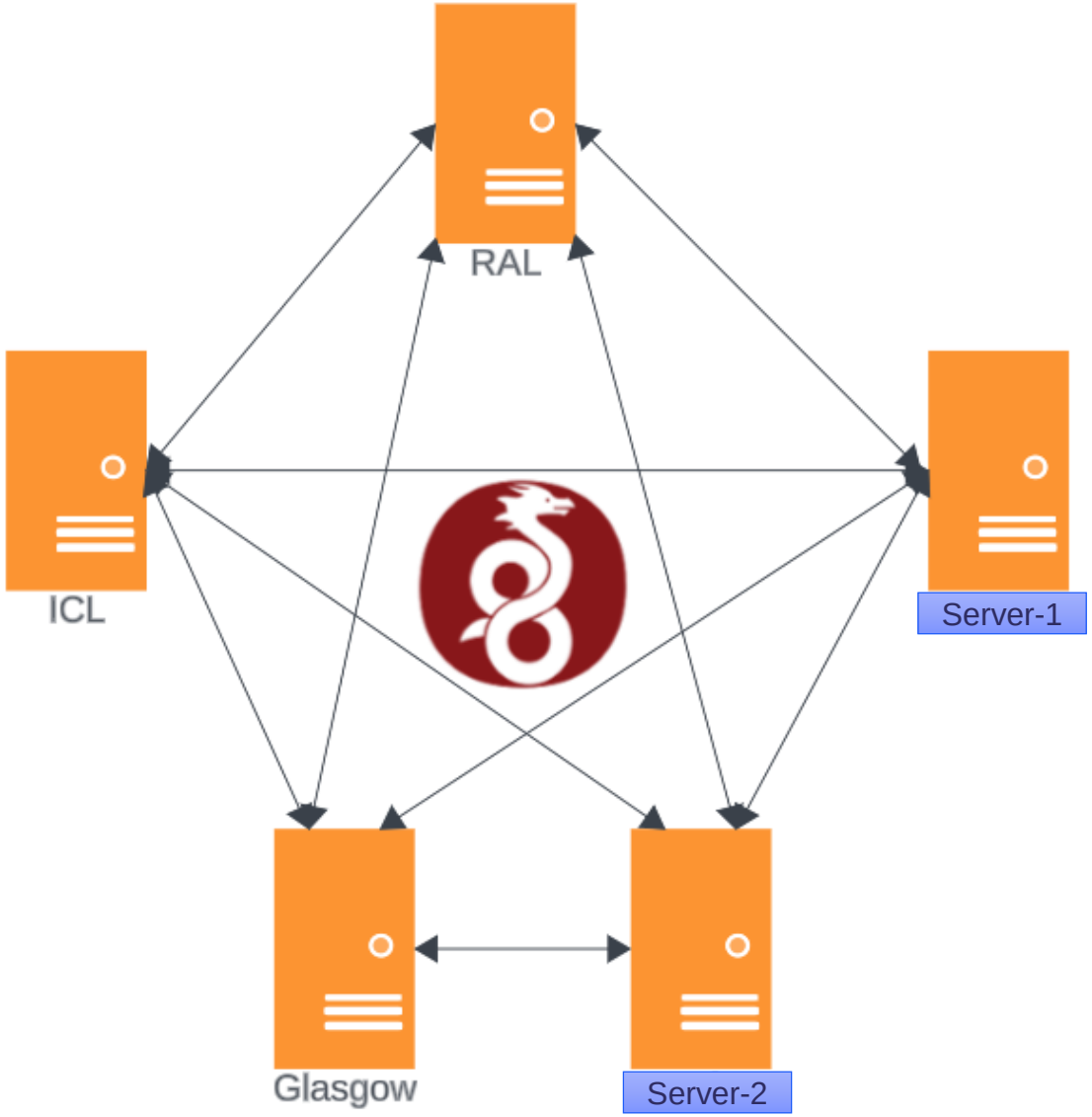
Scenario – HA-IRIS-IAM

- Need to construct site-to-site VPN server for multiple sites
- Not on the same network – VPN
  - State storage
    - Redis HTTP session
    - SQL for other data
  - Need secure channel to communicate
    - Site-to-site mesh VPN

Science and Technology Facilities Council
Scientific Computing

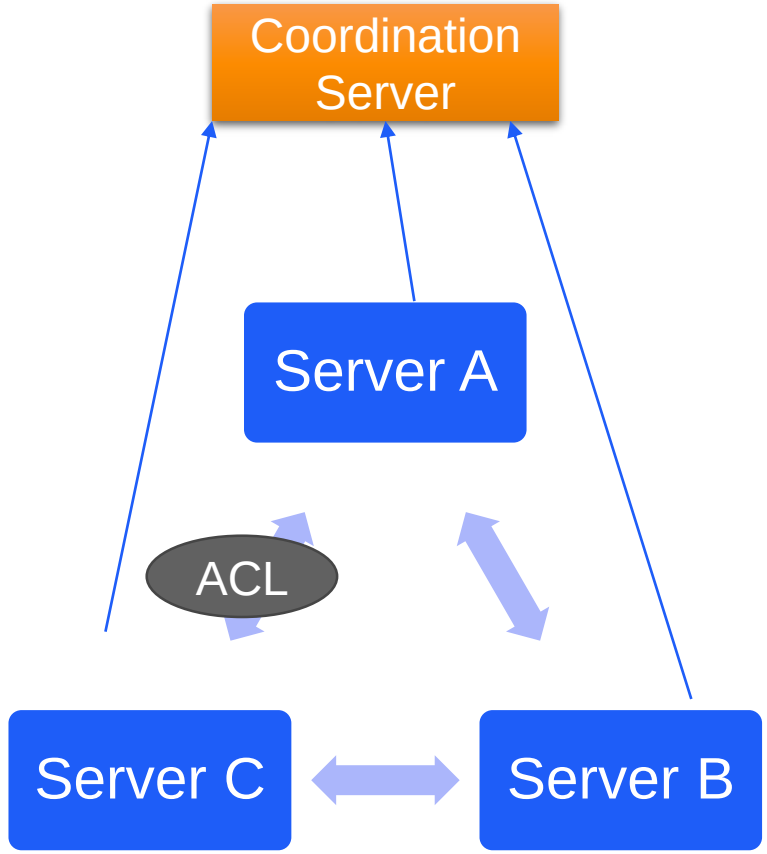
Problem – HA-IRIS-IAM

- Pre-share key like public private key implementation
  - Communication is encrypted between server
- Lacks feature that one would expect from similar software e.g. OpenVPN
  - User authentication
  - User management
  - ACL
    - Managed locally via iptables/ufw
- Wireguard is designed as a foundation to be built upon
- Zero-trust coordination server helps improve security, management and user experience



Solution – Coordination server

- Coordination Server
  - User Authentication
  - Server On boarding
    - Fetch Pub-Key
    - Generate Configuration
      - ACL rules
    - Connect via mesh topology
  - Monitoring
    - Correct server is connected
  - Defining software based network



Scientific Computing

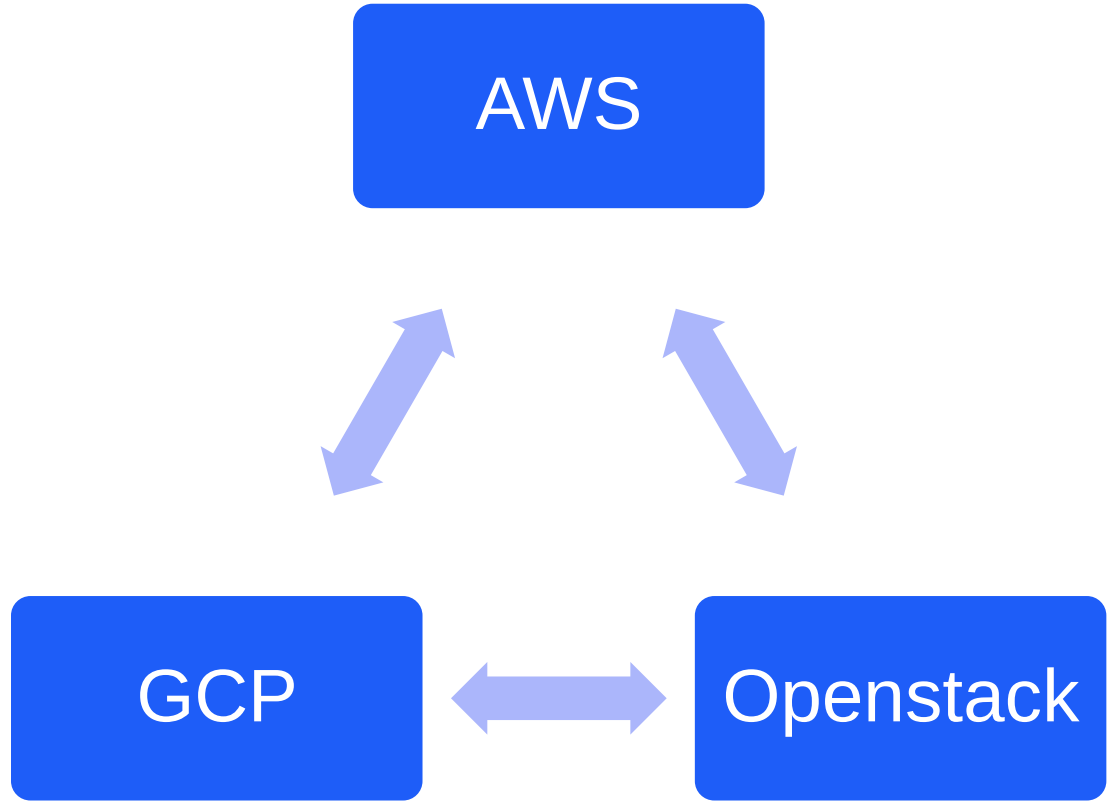
Can IRIS/IRIS-IAM benefit from this?

IRIS-IAM

- IRIS-IAM
  - With OAuth support
    - Security platform that provides secure private networks for IRIS users
  - In addition to indigoiam capabilities
    - UI to manage user, networks, security keys
  - Enhance the functions of IRIS-IAM

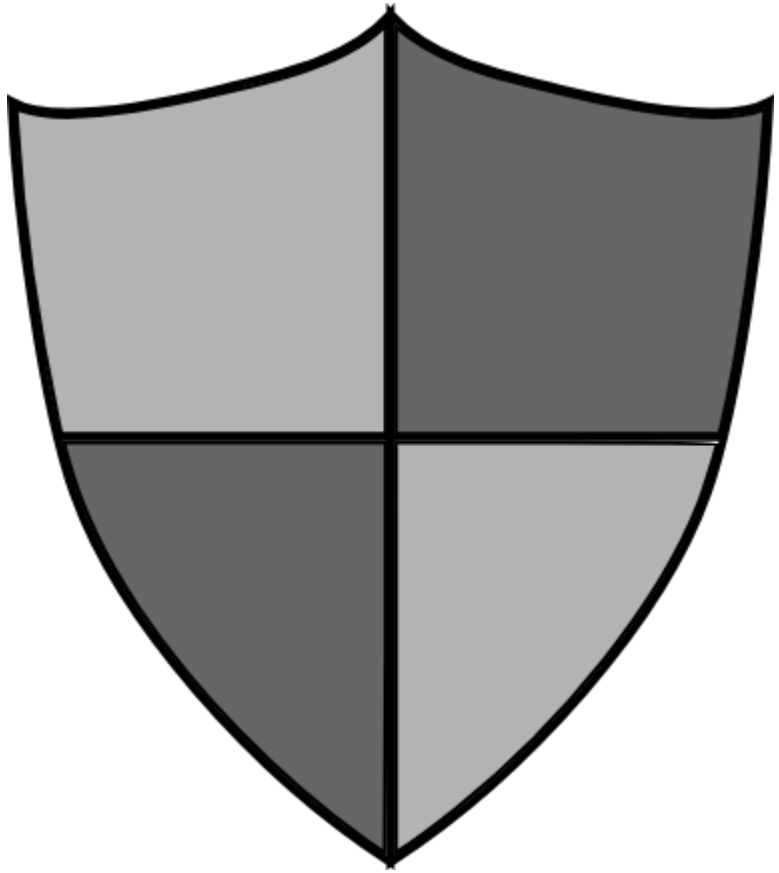
Multi-cloud/data center deployment

- Improve availability/failover with multi location approach
- Leverage resources from partners
- Gives improved management and visibility to the networking



Securely deploy open source software

- Some security features are offered as paid tier
- Exposing the software to internet might pose unnecessary risk
- Need to share service to external partners
- Managed access controlled by IRIS-IAM and VPN
- Encrypted communication offsite



Source: https://openclipart.org/detail/339018/shield

Additional layer of user authentication

- Robust user management might not be built-in for some open-source software
- Using IRIS-IAM with VPN may allow access for certain user to certain application

Source: https://pxhere.com/en/photo/1444789

Sending data securely to/from devices

- Sharing data
  - Real-time data
  - Unprocessed data
  - No application frontend

Source: https://www.flickr.com/photos/nasaearthobservatory/6290956707

IRIS-IAM

- IRIS-IAM
  - With OAuth support
    - Security platform that provides secure private networks for IRIS users
  - In addition to indigoiam capabilities
    - UI to manage user, networks, security keys
- Wider IRIS use case
  - Multi-cloud/data centre deployment
    - Improve availability/failover with multi location approach
  - Securely deploy open source software
    - Some security features might be behind “enterprise tier”
  - Additional layer of user authentication
    - Can be tagged on access to certain user within IRIS-IAM
  - Sending data securely to/from edge devices

Scientific Computing

Solutions and Software Avaliable

What is needed from the software?

- Wireguard based
  - Faster, easier to setup mesh topology
- Good uptime
  - Server/node are in mesh so availability requirement is lower
- Good recovery
  - Use proper DB as backend
- Open-source
  - Ideally project should be free for foreseeable future
- Support multiple network via software definition
  - Better isolation
- Support OpenID/SAML login
  - Use IRIS-IAM to login
- User-friendly CLI client
  - Easier to setup

Defguard

- WireGuard MFA/2FA & integrated OpenID Connect SSO
- Pros
  - Fully open-source – no paid version
  - Support multiple network
  - Desktop client
  - Proper database – Postgres
  - More powerful free version compare to others
- Cons
  - Newer project – missing key features
    - CLI client
    - OpenID provider but no Oauth/SAML login

Repo: https://github.com/DefGuard

Netbird

- Configuration-free peer-to-peer private network and a centralized access control system
- Pros
  - Popular with good review
  - Better performance compare to other service
  - CLI and desktop client
  - Built in OAuth as it doesn’t
  - Group management
- Cons
  - Free version use SQLite
    - Not as production ready
  - No separate network by definition
    - Controlled via group ACL
  - User management is a paid feature

Repo: https://github.com/netbirdio/netbird

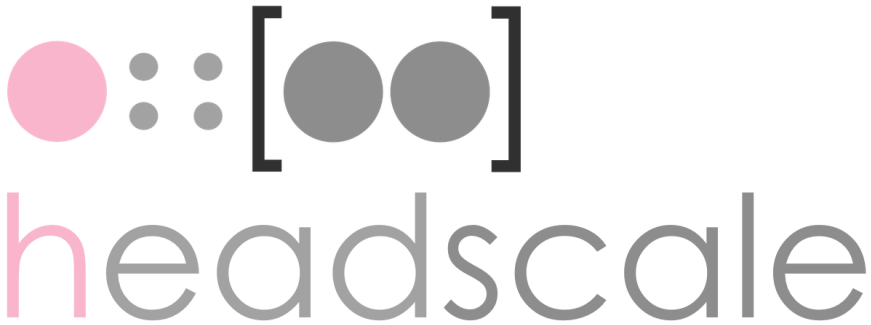
Netmaker

- Overlay network maker
- Pros
  - Support multiple network
  - Use PostgreSQL as DB
  - Support OAuth
  - Have CLI and desktop client
- Cons
  - Volatile
    - Introduce breaking changes between version
  - Performance issues
  - Useful features behind “upgraded” version

Repo: https://github.com/gravitl/netmaker

Other solutions

- Headscale
  - Open source of tail scale
    - Only support 1 network with no ACL
    - Slower fixed with pending update



Repo: https://github.com/juanfont/headscale

- Firezone
  - Make self hosting difficult at 1.0

Repo: https://github.com/firezone/firezone

Discussions

Discussions

- Is it useful/ going to be useful for IRIS
- Is IRIS willing to fund this?
  - Investigation/ Prototyping
  - Attach to IRIS-IAM?
- Any other existing/potential use case?
- Any further requirements for your potential use case
  - E.g. must have a desktop client etc.

Scientific Computing

Questions?

Science and Technology Facilities Council

Scientific Computing

Thank you

scd.stfc.ac.uk

@SciComp_STFC