Accessing SSH resources using IRIS IAM

Will Furnell

STFC

will.furnell@stfc.ac.uk

Science and Technology Facilities Council

Context

- SSH keys
- x509 Certificates
- Managed by LDAP/custom solutions
- AD/LDAP authentication

SSH access via IAM

- PAM Module
  - https://github.com/ICS-MU/pam_oauth2_device - developed by the Institute of Computer Science at Masaryk University
  - Forked by STFC for changes
- No client side software needed
- Integrates well with IRIS IAM & Openstack
- No special/custom SSH server required
- Not just SSH!

Science and Technology Facilities Council

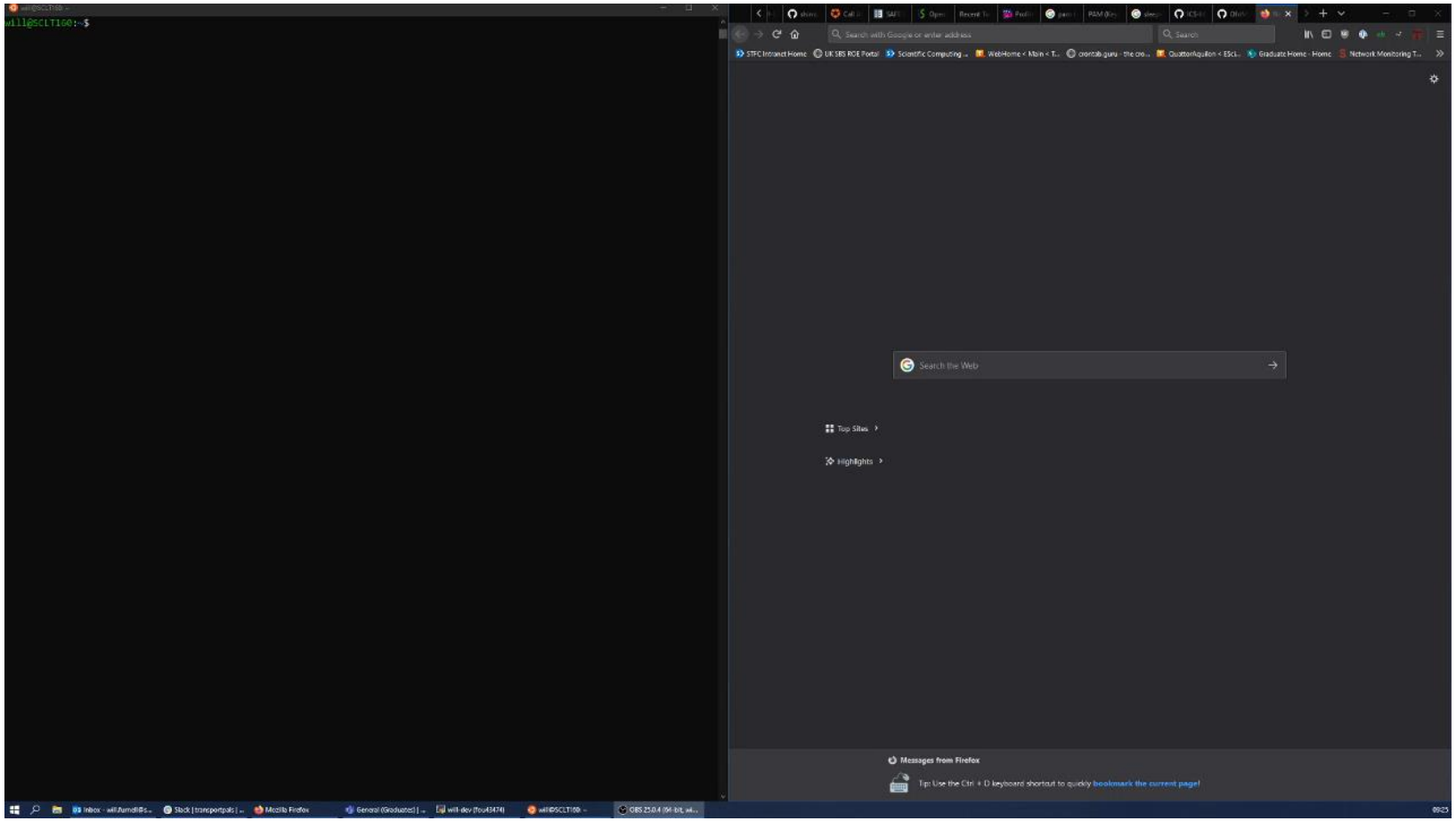
SSH access via IAM

- Discussions ongoing to merge our (STFC) changes back into the upstream repository
- Deployment on one or two IRIS & STFC HPC systems to be tested soon
  - (more development work required)

Group based auth

- Get list of user's groups from the userinfo endpoint
- Check whether one of these matches the specified group in the configuration
- Check the users IAM username matches the username they are trying to log in as
  - (with optional suffix to prevent clashes)
  - IAM username -> IAM username attribute in future?

Demo video



Science and Technology Facilities Council

Alternative software

- 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
  - We've now decommissioned our instances
- Vault
  - Needs client side software/scripts (which does work on Windows)
  - More (user) management involved (just IAM UI is better for us)
  - Otherwise an interesting option!

Alternative software

- Other OAuth2 Device Flow PAM modules exist!
  - https://github.com/search?q=pam+oauth2
  - All have varying states of stability, support and development history

Thank you

will.furnell@stfc.ac.uk

Science and Technology Facilities Council