Contribution ID: **29** Type: **Presentation long (25 mins)**

Federated access for SSH with OpenID Connect

Wednesday, 20 October 2021 16:30 (25 minutes)

Federated Identity Management, as modelled in the AARC blueprint architecture, has established itself as a de-facto standard for authentication and authorisation in research infrastructures.

Yet, federated access to shell-based services comes with a number of challenges, since it typically requires local identities that need prior provisioning, as well as deprovisioning when no longer needed. Additionally, federated identities need to be securely mapped to local identities during authentication. Moreover, federated authorisation models based on Virtual Organisation (VO) membership, roles, and assurance levels need to be mapped as well to local privileges.

Here we present our solution to these challenges, with a focus on OpenID Connect and SSH. This solution is applicable to other services as well, and is similarly being implemented for a webDAV service.

In contrast to existing solutions for SSH that either require modified client and server software (GSI-based), or an additional step for obtaining additional credentials for the service (portal-based), the presented approach overcomes these limitations. Instead, we developed a set of client and server-side tools that complement but do not modify existing SSH software.

The client tool (mccli), is implemented as a command line wrapper around the Unix-based SSH client. It enables on-the-fly account provisioning and transparent local account management: the users can directly log into the service with their federated credentials, without any prior application for an account. The server-side software consists of a lightweight web server (motley_cue) and a PAM module (pam-ssh-oidc). The key features of motley_cue are the mapping of federated to local identities with respecting site-local policies, as well as support for federated authorisation (VOs). The service administrators have full control over who is allowed to access their service, with the ability to only support certain VOs, filter users based on levels of assurance, and even specify authorised users individually. Via a generic and extensible interface, motley_cue is able to forward provisioning events into the local user management system (support exists for Unix accounts, Pooled Unix accounts, LDAP, and KIT user management). Admins can extend this to plug in their custom systems or username policies. Due to its modular design, motley_cue does not need to run on the same host as the service. SSH authentication uses PAM to prompt for an OpenID Connect Access Token and validate it via the REST API exposed by motley_cue.

All software is free to use and is available on GitHub under MIT license, with support for the major Linux distributions. The software was tested with several major AAIs, such as EGI-Checkin, Helmholtz AAI, or DEEP IAM. Work is underway to enhance the service, including to add Windows support on the client side, deprovisioning, and extend support for other local user management systems.

speaker info:
https://www.linkedin.com/in/diana-gudu-aba07b10/?originalSubdomain=de

Most suitable track

Delivering services and solutions

By submitting my abstract, I agree that my personal data is being stored in accordance to conference Privacy Policy

I agree

Primary authors: GUDU, Diana (KIT); HARDT, Marcus (KIT-G); KALISZAN, Damian (PSNC); WOLNIEWICZ, Paweł (PSNC)

Presenter: GUDU, Diana (KIT)

Session Classification: Innovating Services Together: Presentations