Contribution ID: **64**   Type: **Demonstration**

motley-cue: SSH access with OIDC tokens

Wednesday, 21 September 2022 11:30 (25 minutes)

OpenID Connect (OIDC), an authentication protocol that allows users to be authenticated by an external trusted identity provider, is becoming the de-facto standard for modern Authentication and Authorisation Infrastructures (AAI). Although typically used for web-based applications, there is an increasing need for integrating shell-based services, such as Secure Shell (SSH), with federated AAIs.

SSH requires local identities that need prior provisioning, and additional credentials such as SSH keys. Using OIDC for SSH can simplify user management for service administrators, and eliminate the need for SSH key management for users.

Our solution for SSH access via OIDC enables on-the-fly account provisioning and provides a flexible authorisation concept, without modifying existing SSH software or requiring additional service credentials. We developed a set of client and server-side tools that seamlessly integrate with existing SSH software and local identity management policies.

The client-side tools allow users to directly log into a server with their federated credentials via valid OIDC tokens, without any prior application for an account.

This contribution aims to present the server-side component, its architecture, and latest developments. The server-side consists of a custom PAM module and a daemon for mapping OIDC identities to local identities (motley-cue). motley-cue uses federated authorisation models for configuring user access, based on Virtual Organisation membership and assurance levels. Moreover, it provides an extensible interface able to forward provisioning events into any local user management system — support exists for Unix accounts, LDAP, and KIT user management, but admins can extend this to plug in their custom systems. Most recent developments include LDAP integration and support for approval-based provisioning of local accounts.

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 or Helmholtz AAI.

Any relevant links

https://github.com/EOSC-synergy/ssh-oidc
https://motley-cue.readthedocs.io

Topic

Security, Trust & Identity

Primary authors: GUDU, Diana (KIT); HARDT, Marcus (KIT-G); ZACHMANN, Gabriel (Karlsruhe Institute of Technology)

Presenters: GUDU, Diana (KIT); HARDT, Marcus (KIT-G); ZACHMANN, Gabriel (Karlsruhe Institute of Technology)

Session Classification: Demonstrations

Track Classification: Security, Trust & Identity