Contribution ID: **2** Type: **Oral Presentation**

A Token based solutions from KIT for SSH with OIDC

Thursday, March 23, 2023 1:30 PM (30 minutes)

OIDC (OpenID Connect) is widely used for transforming our digital infrastructures (e-Infrastructures, HPC, Storage, Cloud, ...) into the token based world.

OIDC is an authentication protocol that allows users to be authenticated with an external, trusted identity provider. Although typically meant for web- based applications, there is an increasing need for integrating shell- based services.

This contribution delivers an overview of several tools, each of which provides a solution to a specific aspect of using tokens on the commandline in production services:

- oidc-agent is the tool for obtaining oidc-access tokens on the commandline. It focuses on security and manages to provide ease of use at the same time. The agent operates on a users workstation or laptop and is well integrated with graphical user interfaces of several operating systems, such as Linux, MacOS, and Windows. Advanced features include agent-forwarding which allows users to securely obtain access tokens from remote machines to which they are logged in.
- mytoken is both, a server software and a new token type. Mytokens allow obtaining access tokens for long time spans, of up to multiple years. It introduces the concept of “capabilities” and “restrictions” to limit the power of long living tokens. It is designed to solve difficult use-cases such as computing jobs that are queued for hours before they run for days. Running (and storing the output of) such a job is straightforward, reasonably secure, and fully automisable using mytoken.
- pam-ssh-oidc is a pam module that allows accepting access tokens in the Unix pluggable authentication system. This allows using access tokens for example in ssh sessions or other unix applications such as su. Our pam module allows verification of the access token via OIDC or via 3rd party REST interfaces.
- motley-cue is a REST based service that works together with pam-ssh-oidc to validate access tokens. Along the validation of access tokens, motley-cue may - depending on the enabled features - perform additional useful steps in the “SSH via OIDC” use-case. These include
- Authorisation (based on VO membership)
- Authorisation (based on identity assurance)
- Dynamic user creation
- One-time-password generation (in case the access token is too long for the SSH-client used)
- Account provisioning via plugin based system (interfaces with local Unix accounts, LDAP accounts, and external REST interfaces)
- Account blocking (by authorised administrators in case of a security incident)
- mccli is a client side tool that enables clients to use OIDC access-tokens that normally do not support them. Currently, ssh, sftp and scp are supported protocols.
- oidc-plugin for putty makes use of the new putty plugin interface to use access tokens for authentication, whenever an ssh-server supports it. The plugin interfaces with oidc-agent for windows to obtain tokens.

The combination of the tools presented allows creative new ways of using the new token-based AAIs with old and new tools. Given enough time, this contribution will include live-demos for all of the presented tools.

Primary authors: Dr GUDU, Diana (KIT); Dr HARDT, Marcus (KIT); Mr ZACHMANN, Gabriel (KIT)

Presenter: Dr HARDT, Marcus (KIT)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations