

Integrazione di Single Sign-On in Unix Pluggable Authentication Module (Unix PAM)

Dipartimento di Matematica "Tullio Levi-Civita"
Università degli Studi di Padova
Laurea in Informatica

Ivan Antonino Arena
20 luglio 2023



UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- 1 Introduzione
- 2 Tecnologie utilizzate
- 3 Ricerca e sviluppo
- 4 Conclusioni



Ricerca e sviluppo in ambito di sicurezza informatica con Athesys Srl:

- Identità digitale
- Sistemi di autenticazione



- Identity as a Service
- Single Sign-On
- Self-Sovereign Identity

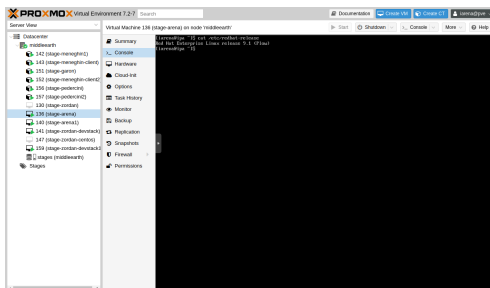
Obiettivo

Ricerca e sviluppare una soluzione che consenta di effettuare l'accesso a Monokey utilizzando il relativo SSO da riga di comando di dispositivi Linux (CentOS e RHEL).

- 1 Studio tecnologico
- 2 Ricerca soluzione (PAM/FreelPA)
- 3 Sviluppo PoC

- FreeIPA
- LXC/Proxmox
- Secure Shell (SSH)





- Configurazione macchine CentOS, RHEL e Ubuntu
- Installazione FreeIPA

- Studio documentazione PAM
- Realizzazione PoC modulo PAM e app PAM-aware

- Configurazione OAuth2 e OIDC su Monokee
- Configurazione FreeIPA IdP
- PoC CLI Monokee SSO



Configurazione OAuth2 e OIDC su Monokee



Manage federation connections

Administration > OAuth Providers

OAUTH PROVIDERS OPENID PROVIDERS

Default Provider OpenID

GITEA Monokee Provider

CyberArk OpenID

Test Sara

OIDC-IPA

AWARE

Hitachi Rails

Monokee Demo ivanantonio.arena@studenti.unipd.it

Add a new OpenID Provider

CORE ADVANCED SIGNATURE ENCRYPTION

Core

☐ Display metadata ☐ Allow self-registration of a client

Provider name

ISSUER
<https://test.monokee.com/6627a356-c838-4ad9-8ff3-e2924b204280/oauth2/ee3a7ff1>

JOINTS url
<https://test.monokee.com/6627a356-c838-4ad9-8ff3-e2924b204280/oauth2/ee3a7ff1>

Grant types supported

Token endpoint authentication methods supported

Revoke endpoint authentication methods supported

Introspect endpoint authentication methods supported

Scopes

CANCEL SAVE

ADD

User authentication types ⓘ

- ☐ Password
- ☐ RADIUS
- ☐ Two factor authentication (password + OTP)
- ☐ PKINIT
- ☐ Hardened Password (by SPAKE or FAST)
- ☒ External Identity Provider

RADIUS proxy configuration

RADIUS proxy username

External IdP configuration

External IdP user identifier

Caso d'uso: un utente registrato vuole operare su una macchina virtuale fornita da Monokee

- 1 L'utente accede alla macchina virtuale;
- 2 L'utente inserisce i comandi per l'autenticazione;
- 3 L'utente segue il link fornito e si autentica con il metodo che preferisce;
- 4 L'utente ritorna al terminale e preme "Invio";
- 5 L'utente è correttamente autenticato e può operare sulla macchina.

```
[iarena@ipa]$ kinit -n -c ./fast.ccache  
[iarena@ipa]$ kinit -T ./fast.ccache monokee1  
Authenticate at  
https://test.monokee.com/6627a356/device?user\_code=XYhv-Hks  
and press ENTER.:  
[iarena@ipa]$ klist
```

Stato attuale

- SSO Monokee (implementato con FreeIPA)
- Documentazione (in formato Markdown)

Sviluppi futuri

Accesso da remoto (SSH) ai dispositivi Linux con FreeIPA e Monokee SSO implementato.

Obiettivi raggiunti

Implementato l'SSO Monokey da terminale Linux.

Conoscenze acquisite:

- Migliorata conoscenza degli ambienti Linux
- Concetti di SSO e SSI
- Protocolli moderni di autenticazione e autorizzazione

Grazie per l'attenzione.