

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 sperimentazione
- 4 Conclusioni



Figura: Logo di Athesys Srl

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

- Identità digitale
- Sistemi di autenticazione



Figura: Logo di Monokee Srl

- Soluzioni di sicurezza informatica
- 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).

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



Figura: Logo di FreeIPA

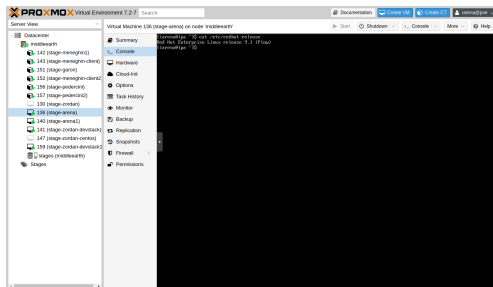
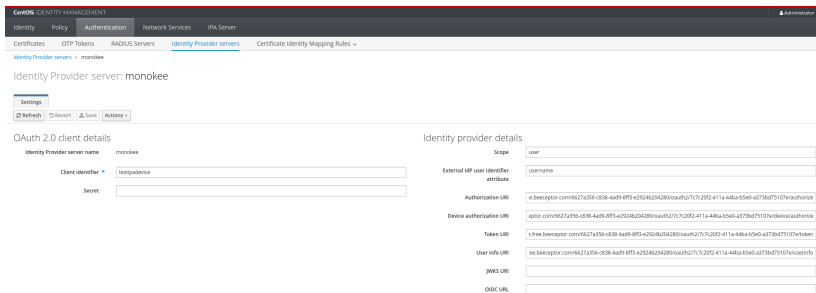


Figura: Schermata VM Proxmox

- Configurazione macchine CentOS, RHEL e Ubuntu
- Installazione FreeIPA

- Studio documentazione PAM
- Analisi dello sviluppo di moduli PAM
- Realizzazione PoC modulo PAM e app PAM-aware

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



The screenshot displays the 'Identity Provider server: monokee' configuration page in the FreeIPA web interface. The page is divided into two main sections: 'OAuth 2.0 client details' on the left and 'Identity provider details' on the right.

OAuth 2.0 client details:

- Identity Provider server name:** monokee
- Client identifier:** testipadvice
- Secret:** (empty field)

Identity provider details:

- Scope:** user
- External IDP user identifier attribute:** username
- Authorization URI:** e.beecaptor.com/6627a356-c838-4a69-8ff3-e2924b254280/oauth2/7c7c20f2-411a-44ba-b5e0-a373bd75107e/authorize
- Device authorization URI:** agnor.com/6627a356-c838-4a69-8ff3-e2924b254280/oauth2/7c7c20f2-411a-44ba-b5e0-a373bd75107e/device/authorize
- Token URI:** s.free.beecaptor.com/6627a356-c838-4a69-8ff3-e2924b254280/oauth2/7c7c20f2-411a-44ba-b5e0-a373bd75107e/token
- User info URI:** ee.beecaptor.com/6627a356-c838-4a69-8ff3-e2924b254280/oauth2/7c7c20f2-411a-44ba-b5e0-a373bd75107e/userinfo
- JWTs URI:** (empty field)
- OIDC URL:** (empty field)

Figura: Schermata FreeIPA IdP

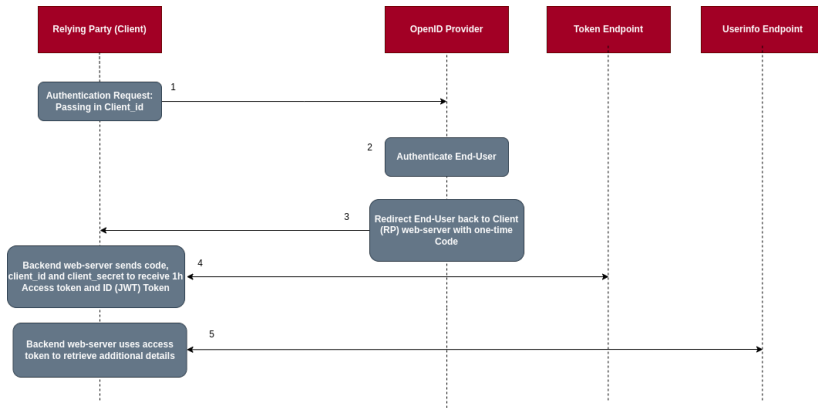


Figura: Flusso autenticazione OIDC

Configurazione OAuth2 e OIDC su Monokee



Management 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

ivanantonino.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/ee3a7ff

JWKS URI

https://test.monokee.com/6627a356-c838-4ad9-8ff3-e2924b204280/oauth2/ee3a7ff

Grant types supported

Token endpoint authentication methods supported

Revoke endpoint authentication methods supported

Introspect endpoint authentication methods supported

SCOPES

CANCEL SAVE

ADD

Figura: Schermata setup OIDC Monokee

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

Figura: Schermata setup utente FreeIPA

```
[larena@ipa ~]$ kinit -n -c ./fast.ccache
[larena@ipa ~]$ kinit -T ./fast.ccache monokee1
Authenticate at https://test.monokee.com/6627a356-c838-4ad9-8ff3-e2924b284280/oauth2/7c7c28f2-411a-44ba-b5e0-a373bd75107e/device?user_code=XYhv-HksZ and press ENTER.:
[larena@ipa ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: monokee1@ARENA.STAGE

Valid starting    Expires          Service principal
04/28/2023 14:33:54  04/29/2023 13:56:33  krbtgt/ARENA.STAGE@ARENA.STAGE
[larena@ipa ~]$
```

Figura: CLI PoC

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

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