

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

CORSO DI LAUREA IN INFORMATICA



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

Tesi di laurea

Relatore

Prof. Davide Bresolin

Laureando

Ivan Antonino Arena

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

— Oscar Wilde

Dedicato a ...

Abstract

Lo scopo della tesi è illustrare il lavoro eseguito con Athesys, system integrator specializzato nello sviluppo di soluzioni di Identity and Access Management (IAM), in termini di innovazione e ricerca applicate all'ambito dell'integrazione di servizi web con sistemi unix-based. Nello specifico, si discute la collaborazione con il team infrastructure ed il team dedicato alla ricerca in materia di identità digitale e la conseguente realizzazione di un componente Single Sign-On compatibile con Unix Pluggable Authentication Module (Unix PAM).

“Life is really simple, but we insist on making it complicated”

— Confucius

Ringraziamenti

Innanzitutto, vorrei esprimere la mia gratitudine al Prof. Davide Bresolin, relatore della mia tesi, per l'aiuto e il sostegno fornitomi durante la stesura del lavoro.

In secondo luogo, vorrei ringraziare di cuore l'azienda ospitante, Athesys Srl, in particolare, il mio tutor esterno Mattia Zago, Roberto Griggio e Leonardo Speranzon, per la disponibilità e l'impegno con cui mi hanno affiancato durante il periodo di stage.

Desidero, inoltre, ringraziare con affetto i miei genitori per avermi appoggiato in ogni mia scelta durante il mio periodo universitario e per avermi fornito il supporto ed i mezzi per portarlo a termine con serenità.

Infine, ci terrei a ringraziare tutte le amicizie più significative che ho stretto a Padova, che mi hanno regalato gioie e sorrisi durante questi tre emozionanti anni.

Padova, Maggio 2023

Ivan Antonino Arena

Indice

1	Introduzione	1
1.1	L'azienda	1
1.2	Il progetto	2
2	Processi e metodologie	3
2.1	Organizzazione del lavoro	3
2.2	Tecnologie utilizzate	3
2.2.1	FreeIPA	3
3	Studio tecnologico	5
3.1	Single Sign-On	5
4	Configurazione dei sistemi	7
4.1	Creazione ambienti virtuali	7
4.2	Configurazione FreeIPA	7
4.3	Configurazione Monokee	7
5	Ricerca e sperimentazione	9
5.1	Unix PAM	9
5.2	FreeIPA IdP	9
6	Implementazione e documentazione	11
6.1	Configurazione FreeIPA	11
6.2	Configurazione Monokee	11
6.3	Testing	11
6.4	Documentazione	11
7	Conclusioni	13
7.1	Consuntivo finale	13
7.2	Raggiungimento degli obiettivi	13
7.3	Conoscenze acquisite	13
7.4	Valutazione personale	13
	Acronimi e abbreviazioni	15
	Bibliografia	17

Elenco delle figure

1.1	Logo di Athesys Srl	1
1.2	Logo di Monokee	1

Elenco delle tabelle

Capitolo 1

Introduzione

In questo capitolo vengono descritti l'azienda ospitante ed il progetto dell'attività di stage curriculare.

1.1 L'azienda

Athesys Srl è un'azienda di consulenza informatica nata a Padova nel 2010 "dalla sinergia di affermati professionisti del settore IT", specializzata in ambito System Integration, Database Management, Sicurezza applicativa, Governance Cloud Platform, Hyperconvergenza e Sviluppo Software in modalità Agile.

Athesys comprende la start-up Monokee, fondata nel 2017 come soluzione cloud-based per la gestione dell'identità e dell'accesso (IDaaS), la quale offre, come funzionalità principale, un sistema di Single Sign-On basato su diversi tipi di autenticazione, sia passwordless che tramite soluzioni di Self-Sovereign Identity (SSI).



Figura 1.1: Logo di Athesys Srl



Figura 1.2: Logo di Monokee

1.2 Il progetto

L'idea per l'attività di stage nasce proprio dall'esigenza dell'azienda di aumentare la portata di Monokee estendendo il relativo Single Sign-On anche a livello macchina, per poter, successivamente, configurare dei terminali che possano gestire accesso e sessioni degli utenti Monokee già da sistema.

L'obiettivo del progetto del tirocinio era, dunque, era la ricerca e l'eventuale sviluppo di una soluzione che consentisse di accedere a macchine UNIX Debian-like e RHEL-like tramite il proprio account Monokee in modo nativo, sfruttando l'infrastruttura di Single Sign-On fornita dalla start-up.

Il framework da utilizzare era FreeIPA, un gestore delle identità e degli accessi (Identity and Access Management, IAM) gratuito ed open-source che combina tecnologie quali Linux, LDAP, MIT Kerberos, NTP, DNS ed SSSD e consta di un'interfaccia web e di strumenti di amministrazione tramite command-line.

L'attività, dalla durata totale di circa trecento ore, si è sviluppata inizialmente in un fase di ricerca e sperimentazione con l'installazione del software FreeIPA su più macchine virtuali CentOS, RHEL e Ubuntu, messe a disposizione dall'azienda.

La seconda fase è stata dedicata alla ricerca di un metodo che consentisse di effettuare l'autenticazione con il proprio account Monokee su tali macchine; in tal senso, è stata approfondita la parte relativa a Unix PAM (Pluggable Authentication Modules) per studiare la possibilità dello sviluppo di un modulo aggiuntivo.

In seguito a tale ricerca, ho deciso di optare per il sistema di autenticazione tramite Identity Provider esterno messo a disposizione dall'applicativo di FreeIPA e di procedere, dunque, con la configurazione di un'applicazione Monokee OAuth2 e di un provider OpenID Connect (OIDC) che fornissero gli end-point e l'infrastruttura necessaria alla comunicazione con il server di FreeIPA e la successiva implementazione degli stessi su di esso.

Verificato il corretto funzionamento di questo sistema di autenticazione da [Command-Line Interface \(CLI\)](#), ho proseguito cercando di implementare questo sistema anche tramite SSH fino al raggiungimento delle ore previste.

Capitolo 2

Processi e metodologie

In questo capitolo vengono descritte le modalità con cui si è svolto lo stage e le tecnologie utilizzate.

2.1 Organizzazione del lavoro

Il lavoro è stato suddiviso in n periodi.

Nel primo ho fatto xyz

2.2 Tecnologie utilizzate

2.2.1 FreeIPA

FreeIPA è un sistema di Identity and Access Management ecc.

Capitolo 3

Studio tecnologico

In questo capitolo vengono illustrati nel dettaglio i concetti e le tecnologie utilizzate.

3.1 Single Sign-On

Single Sign-On significa ecc

Capitolo 4

Configurazione dei sistemi

In questo capitolo vengono descritti i procedimenti attuati per configurare i sistemi utilizzati.

4.1 Creazione ambienti virtuali

4.2 Configurazione FreeIPA

4.3 Configurazione Monokee

Capitolo 5

Ricerca e sperimentazione

In questo capitolo viene descritto il processo di ricerca e sperimentazione di una soluzione efficace per l'implementazione del SSO nativo

5.1 Unix PAM

5.2 FreeIPA IdP

Capitolo 6

Implementazione e documentazione

In questo capitolo viene illustrato il processo di implementazione della soluzione trovata e la stesura della documentazione relativa.

- 6.1 Configurazione FreeIPA
- 6.2 Configurazione Monokey
- 6.3 Testing
- 6.4 Documentazione

Capitolo 7

Conclusioni

7.1 Consuntivo finale

7.2 Raggiungimento degli obiettivi

7.3 Conoscenze acquisite

7.4 Valutazione personale

Acronimi e abbreviazioni

CLI [Command-Line Interface](#). 2, 15

Bibliografia

Riferimenti bibliografici

James P. Womack, Daniel T. Jones. *Lean Thinking, Second Editon*. Simon & Schuster, Inc., 2010.

Siti web consultati

Manifesto Agile. URL: <http://agilemanifesto.org/iso/it/>.