KeycloakとFreeIPAを用いたユーザ情報の認証・認可の一元管理

東京都立産業技高等専門学校2年
ニノ方 理仁

序論：サーバの仮想化とユーザ管理コストの課題

複数VMによる仮想化の背景

- 情報インフラストラクチャの規模は増大傾向にある。
- 1つの物理サーバに**複数の仮想マシン (VM)** を構築すると、サーバの効率化や省エネルギー化、異なるOSの利用が可能となる利点がある。

課題

- 新規ユーザの作成・既存ユーザの変更など**管理コストの増大**
- 管理作業が複雑化することによる**ミスの増加**
- VMごとに権限を付与することで起こる**セキュリティ上の課題**

シングルサインオン：Single Sign-On（SSO）とは

代理サーバを設置してユーザの代わりに認証を行う代理認証方式である。複数サービスへのログインが1組のID・パスワードで可能となる。

目的

シングルサインオンシステムと**アイデンティティ管理システム**を用いたユーザ管理・認証システムを構築することで、**ユーザ管理コストを低減**できる。

ユーザ管理・認証を一元化したシステムを構築し、運用手続き実施に関する時間およびミスの低減を定量評価する。

方法：インフラストラクチャ構築と仕様

本研究では、KeycloakとFreeIPAを用いて、Identity Providerが統一された認証システムを作成した。

Keycloakとは

Javaベースのオープンソースソフトウェアである。シングルサインオン（SSO）やAPIアクセスの認証・認可制御、およびID管理やアクセス管理（IAM:Identity and Access Management）を可能にする。

FreeIPAとは

Linuxネットワーク環境用のオープンソースのアイデンティティおよび認証管理システムである。内部にLDAPサーバやSSSD等が含まれており、Linuxの認証を簡略化できる。

仕様

- インフラストラクチャは、Proxmox VE上に構築した。
- RockyLinux9上にFreeIPA、Ubuntu Server 22.04上にKeycloakを構築した。
- KeycloakにFreeIPAのLDAPサーバを設定し、Keycloakがユーザ情報をFreeIPAから参照できるようにした。
- Web上の管理システム(SP)は、OIDC・SAMLやOAuthなどでKeycloak(IdP)を介してユーザ情報を取得する。

Linux VMへのログイン処理フロー

1. ユーザがVMにログイン情報を送信する。
2. VM上のSSSDがFreeIPAのLDAPサーバへ問い合わせる。

SPへのログイン処理フロー

1. ユーザが管理システムにアクセスする。
2. Keycloakにリダイレクトする。
3. ユーザがKeycloakにログイン情報を送信する。
4. KeycloakがFreeIPAのLDAPサーバへ問い合わせる。

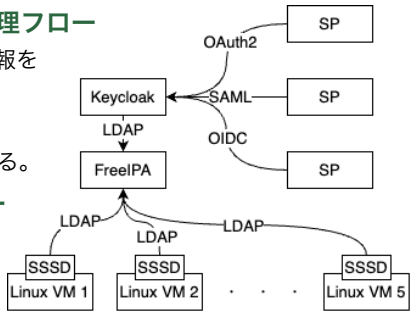

図1. インフラストラクチャの構造

Ansibleレポジトリ
http://git.reetok.net/reetok/freeipa_ansible

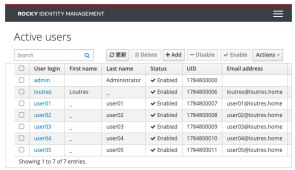

図2. FreeIPAのダッシュボード

評価：ユーザ管理コストの評価

対象

高専情報システム工学科2年の学生3名を対象とした。

- 評価は、提案システムとLinux VMを用いた既存システムを比較することで行った。
- ユーザ管理作業として、ユーザ新規登録5件およびアクセス権限の停止操作5件をそれぞれのシステムで行った。
- 既存システムとしては、Linux VMを5個用いたシステムを構築した。Ubuntu 22.04、認証システムとしてLinux PAMを用いた。

評価指標

- 作業完了までにかかった時間およびミスの回数を計測し、作業内容ごとに作業時間とミスの減少を評価した。

結果と考察

結果

提案システムを利用してユーザ情報管理操作を行い、既存システムと比較した結果は以下の通りである。

- 新規ユーザの登録にかかった時間は、既存システムが平均5分13秒、提案システムが3分4秒で作業時間は**62.5%減少**した。
- 新規ユーザの登録時のミスは既存システムの平均3.5回に対し、提案システムは平均1回に減少した。
- アクセス権限の停止作業は既存システムが平均28秒、提案システムが6.5秒で作業時間は**76.7%減少**した。
- アクセス権限停止作業時のミスは既存システムが平均0.5回だったのに対し、提案システムは0回に減少した。
- ミスの内容は作業内容を理解しているにも関わらず起こる行動ミス（スリップ）であった。具体的には、ユーザ情報の入力ミス、パスワードのタイプミスといった**ヒューマンエラー**であった。

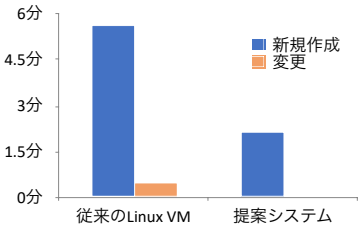

図3. 作業時間の比較

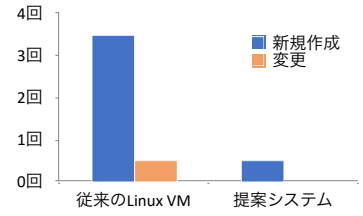

図4. ミス回数の比較

結論

結論

複数のVMを物理サーバ上に立てる仮想化が一般的になったことにより、ユーザの認可・認証を行うため管理者のコストは増大した。そのため、作業の煩雑化による管理コストの増大、ヒューマンエラーの増加が起こるリスクも増加した。本研究では、SSOを採用したシステムを構築し、ユーザ認証・認可を一元的に管理することで、**作業時間とミスの発生が低減することを定量的に評価**できた。同様に、ヒューマンエラーの低減はセキュリティ上のリスクを減らす効果につながると考える。

課題

本研究の提案システムによるユーザ情報の一元管理がサーバのセキュリティを強化することへの定量評価は今後の課題である。また、本研究の対象は情報システム工学コースの学生3人であったため、より広い知識・技術レベルのサーバ管理者を対象とした評価も今後の課題である。

参考文献

Christie, M., Bhandar, A., Nakandala, S., Marru, S., Abeysinghe, E., Pamidighantam, S., & Pierce, M. (2020). Using Keycloak for Gateway Authentication and Authorization
, *Future Generation Computer Systems*. 111. pp.780-785.