Introduction

Dans ce module, nous allons explorer l'architecture et les fonctionnalités de CAS tout en couvrant les aspects pratiques liés à son installation et à sa configuration. Vous apprendrez à mettre en œuvre un système d'authentification unique (Single Sign-On) avec CAS, accompagné de la configuration d'un reverse proxy sécurisé et de la double authentification.

Présentation du module

Le CAS (Central Authentication Service) est un protocole open source d'authentification unique (SSO) pour le web. Il permet :

- Aux utilisateurs d'accéder à plusieurs applications avec une seule connexion.
- Aux applications web d'authentifier les utilisateurs sans gérer directement leurs mots de passe.

Composants principaux de CAS :

- Un serveur basé sur Java (Spring Webflow/Spring Boot).
- Des bibliothèques clientes (disponibles en PHP, JavaScript, Python, etc.).

Objectifs

Objectif principal

1. Mettre en place un serveur CAS Enterprise Single Sign-On en intégrant un annuaire LDAP et une double authentification.

Objectifs secondaires

1. Déployer une infrastructure via Docker pour simplifier les tests et la production.
2. Intégrer un reverse proxy pour gérer HTTPS et la redirection des requêtes.
3. Assurer la documentation et la sécurisation complète de l'infrastructure.

Méthodologie

- Analyse critique : Identifier les besoins techniques.
- Planification : Établir un cahier des charges clair.
- Itération : Tester chaque étape avant de passer à la suivante.

Infrastructure requise

Technologies et outils

- Docker : Conteneurisation des services (CAS, LDAP, reverse proxy, etc.).
- Reverse Proxy (NGINX) : Pour la gestion des requêtes HTTPS.
- LDAP (OpenLDAP) : Stockage des informations des utilisateurs.
- Double authentification (Duo Security) : Pour renforcer la sécurité.

Architecture

Serveur CAS :

- Protocole utilisé : HTTPS avec certificats X.509.
- Système de tickets (similaire à Kerberos).

Reverse Proxy :

- Redirection des requêtes du WAN vers les services internes.
- Exemple :
  - https://wordpress.cpnv-cas1.ch → Serveur WordPress.
  - https://moodle.cpnv-cas1.ch → Serveur Moodle.

Serveur LDAP :

- Domaine de base : dc=cpnv-cas1,dc=ch.
- Exemple d'utilisateur :
  - user01 → mot de passe : Mot2Pa$$301.

Contraintes

- Exclusivité Docker : Tous les services doivent être conteneurisés.
- Sécurité : Seule la machine reverse proxy est exposée au WAN.
- Sauvegarde et restauration : Les configurations doivent être sauvegardées.

Étapes de réalisation

- Installation et configuration CAS
- Mise en place du reverse proxy
- Configuration LDAP
- Activer la double authentification

Livrables

1. Dockerfiles et fichier docker-compose.yml :
    a. Contiennent toutes les configurations nécessaires.
2. Documentation PDF :
    a. Instructions détaillées pour reproduire l'infrastructure.
3. Infrastructure fonctionnelle :
    a. Serveur CAS intégré avec LDAP et reverse proxy.
    b. Double authentification opérationnelle.
4. Preuve de concept :
    a. Démonstration de l'authentification sur WordPress et Moodle via CAS.

Évaluation

- Déploiement Docker : 10 points.
    - Utilisation correcte des Dockerfiles pour chaque service.
    - Fichier docker-compose.yml fonctionnel et bien structuré.
    - Tests réussis pour vérifier que tous les conteneurs démarrent correctement.
- Intégration CAS + LDAP : 10 points.
    - Configuration fonctionnelle de l'intégration LDAP dans CAS.
    - Tests réussis de connexion avec plusieurs utilisateurs LDAP.
    - Gestion correcte des filtres LDAP pour limiter l'accès à certains groupes ou utilisateurs.
- Configuration HTTPS avec reverse proxy : 10 points.
    - Mise en place correcte du reverse proxy NGINX.
    - Certificats HTTPS fonctionnels (Let’s Encrypt ou auto-signés).
    - Redirection des requêtes HTTP vers HTTPS.
- Double authentification : 10 points.
    - Configuration de Duo Security ou équivalent dans CAS.
    - Vérification que tous les utilisateurs configurés doivent utiliser la double authentification.
    - Documentation des étapes pour activer ou désactiver la MFA pour un utilisateur.
- Documentation : 5 points.
    - Clarté et précision des instructions fournies.
    - Utilisation d’un format cohérent et structuré (titres, sous-titres, tableaux, etc.).
    - Présence de captures d’écran pour illustrer les étapes clés.
- Sauvegarde et restauration : 5 points.
    - Script de sauvegarde automatisé pour les données critiques (LDAP, configurations, certificats, etc.).
    - Tests réussis de la restauration complète de l’infrastructure.

Ce module met l'accent sur l'apprentissage par la pratique et l'acquisition des compétences clés nécessaires pour déployer des solutions SSO sécurisées. N'hésitez pas à adapter ces étapes aux besoins spécifiques de votre environnement !