

Projet personnel encadré 2

Document d'exploitation

BRUNO KYLIAN

BTS SIO 26

SOMMAIRE :

1. Introduction

- A. Contexte
- B. Objectif technique

2. Architecture

- A. Plan d'adressage IP
- B. Schéma
- C. Prérequis
- D. Serveur Windows
 - a) Active directory
 - b) DNS
 - c) PKI ADCS
 - d) Serveur Web IIS
 - e) Serveur de fichiers
 - f) Compte utilisateurs
- E. Serveur Linux

INTRODUCTION

A. Contexte

Une entreprise du nom de Altalis décide de faire appel à un administrateur des systèmes et réseau, afin de sécuriser son infrastructure via des certificats/PKI. Pour cela il est nécessaire de mettre en place un certificat pour protéger les services, les données des utilisateurs et enfin les droits d'accès.

B. Objectif technique

Mettre en place une PKI interne afin de sécuriser l'infrastructure de l'entreprise. L'objectif est de déployer des certificats pour protéger les services, sécuriser les données des utilisateurs et contrôler les accès, afin de renforcer la sécurité globale du système d'information.

Architecture

A. Plan d'adressage IP

Réseau : 192.168.10.0 /24

Domaine : Altalis.fr

Adresse IP du serveur AD : 192.168.10.1 /24

Adresse IP du serveur Linux : 192.168.10.100 /24

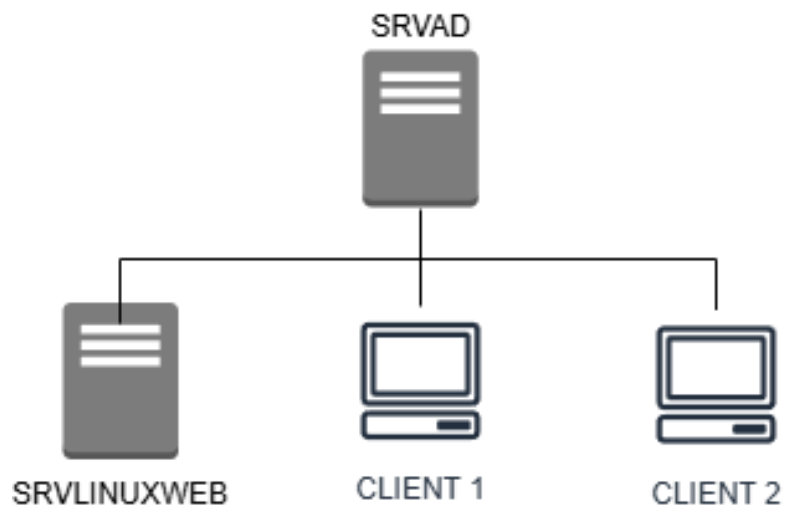
Adresse IP du Client1 : 192.168.10.10 /24

Adresse IP du Client2 : 192.168.10.15 /24

Gateway : 192.168.10.1

DNS : 192.168.10.1

B. Schéma



Ressources utilisées :

- Une VM Windows Server 2022
- Deux VM Windows 11
- Une VM linux Debian 12

C. Prérequis

Pour l'installation du domaine, il faut attribuer une IP fixe au serveur Active Directory et changer le mot de passe local. (Promeo60.)

Les deux clients sont joints au domaine altalis.fr

Il faut aussi installer les rôles essentiels afin de faire fonctionner les certificats :

- Le rôle AD DS (annuaire des comptes utilisateurs)
- Le rôle DNS (pour établir des connexions via un nom de domaine)
- Le rôle IIS (pour créer des sites web) et l'option Authentification par mappage de certificat client
- Le rôle AD CS (pour installer une autorité de certification)

D. Serveur Windows

a) Active directory

Le serveur est configuré comme contrôleur de domaine.

Le domaine est altalis.fr

b) DNS

Le serveur DNS permet de résoudre :

-> intranet.altalis.fr

-> www.altalis.fr

c) PKI (AD CS)

La PKI permet de créer les certificats serveur et la création de certificats utilisateurs.

d) Serveur Web IIS

Le serveur d'altalis est configuré en HTTPS.

Cela permet de sécuriser l'intranet de l'entreprise et d'utiliser un certificat signé par la CA.

L'accès à l'intranet est possible en utilisant ce lien :

<https://intranet.altalis.fr>

e) Serveur de fichier

Un partage est configuré :

P:\Partages\Commun

L'accès est donné aux utilisateurs du domaine grâce à une GPO.

f) Compte utilisateurs

Une OU a été créée pour répertorier les utilisateurs du domaine :

Nom/Prénom	Identifiants
Martin Lucas	lma
Bernard Emma	ebe
Dubois Hugo	hdu
Moreau Léa	lmo

Il se connecte à leur session avec leur trigramme et utilise un mot de passe générique qui est Promeo60.

Ainsi que 3 groupes :

-> RH

-> Achat

-> Compta

Le groupe RH comporte lmo.

Le groupe Compta comporte hdu.

Le groupe Achat comporte ebe et lma.

E. Serveur Linux

Le serveur est un serveur Web avec les services suivant installés :

-> Apache2

-> OpenSSL

Le serveur possède un site Web sécurisé en https grâce à un certificat délivré par la CA Windows.

Le site Web est disponible à l'adresse suivante :

<https://www.altalis.fr>