Freitas Allan
BTS SIO SISR 26

PPE2

Sécurisation de données, de services et d'utilisateur à l'aide de certificat et d'une PKI

PPE 2 en lien avec TECHNOVA

Suite à la modernisation de l'infrastructure vers la virtualisation, TechNova Solutions doit désormais renforcer la sécurité de ses échanges internes. L'objectif est de s'affranchir des mots de passe simples pour certains services critiques et de garantir l'identité des serveurs auprès des utilisateurs;

Besoins identifiés :

- Authentification forte : Déployer des certificats numériques pour les utilisateurs.
- Confidentialité : Chiffrer les flux web internes (HTTPS) et les accès distants.
- Centralisation : Gérer le cycle de vie des certificats (émission, renouvellement, révocation) via une autorité interne.

2. Solution Technique : L'Infrastructure à Clés Publiques (PKI)

Le choix s'est porté sur l'installation d'une Autorité de Certification (AC) intégrée à l'environnement Windows Server déjà existant.

- Rôle AD CS (Active Directory Certificate Services) : Configuration du serveur Windows en tant qu'Autorité de Certification racine pour le domaine.
- Protocoles : Utilisation de TLS/SSL pour la sécurisation des services web Linux et Windows.
- Déploiement : Utilisation des stratégies de groupe (GPO) pour distribuer automatiquement le certificat racine aux postes clients.

3. Architecture et Configuration

L'infrastructure s'appuie sur les serveurs précédemment mis en place, avec l'ajout de services de sécurité.

Tableau d'adressage et rôles :

Équipement	Adresse IP	Rôle de sécurité
SRV-AD-PKI	192.168.200.140	Autorité de Certification (AC) & AD
SRV-WEB-SEC	192.168.200.111	Serveur Debian avec HTTPS (Apache/Nginx)
Poste Client	192.168.200.110	Client authentifié par certificat

Domain = PPE.LOCAL / https://intranet.pki.lan

Réalisations effectuées :

1. Installation de l'AC : Configuration des services de certificats Active Directory sur le serveur Windows.
2. Génération de CSR : Création d'une demande de signature de certificat pour le serveur Web Linux.
3. Signature et Installation : Émission du certificat par l'AC et installation sur le serveur Debian pour activer le port 443 (HTTPS).
4. Test de révocation : Mise en place d'une liste de révocation (CRL) pour invalider les certificats des anciens collaborateurs.

- Authentification forte : Déployer des certificats numériques pour les utilisateurs afin de s'affranchir des mots de passe simples.
- Confidentialité : Chiffrer les flux web internes (HTTPS) et les accès distants.
- Centralisation : Gérer le cycle de vie des certificats (émission, renouvellement, révocation) via une Autorité de Certification (AC) interne.
- certificats des anciens collaborateurs.