E5 - BTS Services Informatiques aux Organisations (SIO)
parcours SISR

C17 – DÉPLOIEMENT D'UN SERVICE

Présenté par:

MECHRAFI-LACROIX Steven

Année académique : 2024/2026

Objectifs du document

Ce document a pour objectif de présenter le **déploiement d'un service**. Le déploiement consiste à mettre en place et rendre disponible un service pour les utilisateurs, après validation des tests. Ce document couvre le déploiement de plusieurs types de services : système, réseau et sécurité.

Il aborde les volets suivants :

1. **Configuration d'un load balancer HAProxy** (continuité des services).
2. **Contribution aux projets monétique (TPE)** de micro-dons.
3. **Déployer un service système** : Windows Server (AD, DNS, DHCP).
4. **Déployer un service sécurité (pare-feu)** : pfSense / OPNsense.
5. **Déployer un service système** : GLPI.
6. **Déployer un service réseau** : supervision avec Zabbix.
7. **Déployer un service sécurité (SIEM)** : Wazuh.

Configuration d'un load balancer HAProxy (continuité des services)

HAProxy est une solution de répartition de charge assurant la **continuité des services**. Placé en frontal de plusieurs serveurs, il distribue les requêtes et retire automatiquement un serveur défaillant grâce aux contrôles de santé (*health checks*).

Le déploiement comprend l'installation de HAProxy, la configuration du fichier `haproxy.cfg` (sections *global*, *defaults*, *frontend*, *backend*), le choix de l'algorithme de répartition (*roundrobin*, *leastconn*…) et la mise en place des contrôles de santé.

Configuration détaillée : voir C4.

Contribution aux projets monétique (TPE) de micro-dons

La mise en place d'un service de **micro-dons** via la **monétique** permet au client, lors d'un paiement, d'ajouter un don au profit d'une association via le **terminal de paiement (TPE)**. Le déploiement implique la configuration des TPE, l'information des clients et le suivi des montants collectés en vue de leur reversement.

Voir également la contribution monétique présentée en C10 et C13.

Déployer un service système : Windows Server (AD, DNS, DHCP)

Le déploiement d'un **serveur Windows Server** (2019, 2022 ou 2025) constitue le socle d'un système d'information centralisé. Trois rôles essentiels y sont déployés :

- **Active Directory (AD DS)** : annuaire centralisé gérant les utilisateurs, ordinateurs et droits d'accès (domaine).
- **DNS** : résolution des noms en adresses IP, indispensable au fonctionnement du domaine.
- **DHCP** : attribution automatique des adresses IP aux postes du réseau.

Étapes principales

1. Installer Windows Server et configurer l'adressage réseau (IP fixe).
2. Ajouter le rôle **AD DS** et promouvoir le serveur en **contrôleur de domaine**.
3. Installer et configurer le rôle **DNS** (souvent automatique avec AD).
4. Installer le rôle **DHCP**, créer une **étendue** (plage d'adresses) et l'activer.
5. Vérifier le bon fonctionnement (jonction d'un poste au domaine, attribution d'adresse).

Déployer un service sécurité (pare-feu) : pfSense / OPNsense

pfSense et **OPNsense** sont des solutions open source de **pare-feu** et de routage. Elles protègent le réseau en filtrant le trafic et en segmentant les accès.

Étapes principales

1. Installer pfSense / OPNsense (sur machine physique ou virtuelle).
2. Configurer les **interfaces** (WAN, LAN).
3. Définir les **règles de filtrage** (autorisations et interdictions de trafic).
4. Mettre en place les services complémentaires si besoin (VPN, DHCP, portail captif).
5. Vérifier la protection et la connectivité.

Déployer un service système : GLPI

GLPI est une solution de gestion de parc et de services informatiques (tickets, inventaire). Son déploiement met à disposition un outil central pour la gestion du SI.

Étapes principales

1. Préparer un serveur (Linux) avec les prérequis : serveur web, PHP et base de données (MariaDB/MySQL).
2. Créer la **base de données** dédiée à GLPI.
3. Installer GLPI et lancer l'**assistant d'installation** (connexion à la base).
4. Configurer les comptes, les profils et les entités.
5. Mettre en place l'**inventaire automatique** (agent GLPI) pour remonter le parc.

Déployer un service réseau : outil de surveillance Zabbix

Zabbix est un outil open source de **supervision réseau**. Il surveille en temps réel l'état des équipements et des services et déclenche des **alertes** en cas d'anomalie.

Étapes principales

1. Installer le serveur Zabbix et son interface web (avec base de données).
2. Installer les **agents Zabbix** sur les hôtes à surveiller.
3. Déclarer les **hôtes** et associer des **modèles** de supervision (CPU, mémoire, disponibilité…).
4. Configurer les **déclencheurs** (seuils d'alerte) et les **notifications**.
5. Visualiser l'état du parc via les tableaux de bord.

Déployer un service sécurité (SIEM) : Wazuh

Wazuh est une solution open source de type **SIEM** (*Security Information and Event Management*). Elle collecte et analyse les journaux de sécurité, détecte les menaces et facilite la réponse aux incidents.

Étapes principales

1. Déployer le **serveur Wazuh** (Wazuh manager et indexeur) et son tableau de bord.
2. Installer les **agents Wazuh** sur les machines à surveiller.

3. Configurer la **collecte des journaux** et les règles de détection.
4. Suivre les **alertes de sécurité** et les événements depuis le tableau de bord.
5. Mettre en place les réponses adaptées (analyse, remédiation).

Synthèse

Le déploiement d'un service suit toujours une démarche structurée : préparation, installation, configuration, vérification puis suivi. Ce document a présenté le déploiement de services variés — **continuité** (HAProxy), **monétique** (micro-dons), **système** (Windows Server avec AD/DNS/DHCP, GLPI), **sécurité** (pfSense/OPNsense, Wazuh SIEM) et **réseau** (Zabbix). La maîtrise de ces déploiements permet de mettre en place une infrastructure complète, disponible et sécurisée.