Fuentes - Résumé détaillé de stage 1

> **Établissement :** BTS SIO option SISR – 1ère année | **Entreprise d'accueil :** Service d'Incendie et de Secours du Bas-Rhin | **Période :** Juin – Juillet 2025

Table des matières

Introduction

Ce stage de première année s'est déroulé au sein du service informatique d'un établissement public de secours départemental, réparti sur plus de 230 sites. La particularité de ce contexte est que le système d'information (SI) y est **opérationnel et critique** : une indisponibilité, même partielle, peut directement impacter la capacité d'intervention des secours. Cette contrainte a conditionné l'ensemble de mes observations et missions.

J'ai été intégré au sein du service chargé des moyens informatiques et de communication, où j'ai pu intervenir sur des missions allant du support utilisateur au déploiement massif de postes, en passant par la virtualisation et les premières étapes d'un projet de supervision.

1. L'organisme d'accueil et son infrastructure

L'établissement est un **service public de secours** dont le SI doit satisfaire à une exigence de **haute disponibilité**, notion qui désigne la capacité d'un système à rester opérationnel en continu, sans interruption planifiée ou accidentelle prolongée. Cette exigence est mesurée par un taux de disponibilité cible, souvent exprimé en pourcentage annuel (ex. 99,9 % correspond à moins de 9h d'interruption par an).

Le service informatique est organisé en domaines spécialisés :

Domaine	Missions principales
Systèmes	Administration des serveurs, annuaire, virtualisation
Réseaux	Gestion des flux, segmentation, interconnexion des sites
Sécurité	Protection du SI, audits, gestion des incidents
Parc informatique	Postes de travail, périphériques, équipements mobiles
Support	Assistance aux utilisateurs, gestion des demandes

L'infrastructure repose sur une **architecture distribuée** : les ressources informatiques sont réparties géographiquement sur l'ensemble du département, tout en étant administrées de façon centralisée via un **annuaire Active Directory (AD DS)**, service d'annuaire qui permet de gérer de manière centralisée les comptes utilisateurs, les droits d'accès, et les politiques de configuration appliquées aux postes du domaine.

Le réseau est **segmenté en VLAN** (Virtual Local Area Network), technique de segmentation logique qui divise un réseau physique en plusieurs réseaux virtuels isolés. Cette segmentation améliore la sécurité (en limitant la propagation des flux entre zones) et les performances (en réduisant les domaines de diffusion réseau).

2. Missions réalisées

2.1 Support utilisateur et gestion du parc

Objectifs

Assurer la continuité du service informatique auprès des utilisateurs répartis sur plus de 230 sites, traiter les demandes de niveau 1 en autonomie, et maintenir une traçabilité rigoureuse des équipements du parc.

Environnement technique

- Solution MDM : Knox Manager (Samsung)
- Gestion de parc et tickets : GLPI
- Systèmes : Windows 10/11, Android
- Communication interne : Rainbow, messagerie Outlook
- Équipements gérés : postes fixes, portables, tablettes, smartphones professionnels, imprimantes

Contexte

Le service informatique assure le support d'un parc distribué sur plus de 230 sites, pour des utilisateurs aux profils très variés : agents administratifs, sapeurs-pompiers professionnels et volontaires, encadrement. La gestion de ce parc et le traitement des demandes quotidiennes représentent une charge continue pour l'équipe.

Problématique

Comment assurer la continuité de service auprès d'utilisateurs dispersés géographiquement, avec des incidents de nature très diverse, tout en maintenant une traçabilité rigoureuse des équipements ?

Mon rôle

J'ai assuré le support de niveau 1 en autonomie : accueil physique et téléphonique des utilisateurs, diagnostic des incidents, résolution ou escalade vers un technicien habilité. J'ai également participé à la gestion physique du parc : préparation de postes, récupération de composants sur machines obsolètes, et configuration d'équipements mobiles sous la supervision d'un technicien.

Démarche

Le support de niveau 1 constitue le premier niveau de la chaîne d'assistance informatique. Ma méthode de diagnostic suivait une progression logique : écoute de l'utilisateur, reproduction du problème, vérification du matériel avant le logiciel, puis documentation de la solution ou transmission du ticket dans GLPI.

Les équipements mobiles (tablettes et smartphones professionnels) étaient gérés via une solution **MDM** (*Mobile Device Management*) — logiciel centralisé permettant de déployer des applications, d'appliquer des politiques de sécurité (verrouillage, chiffrement, effacement à distance), et de contrôler la conformité des équipements sans accès physique.

La gestion du parc impliquait également du **recyclage de composants** : lors du démontage de postes obsolètes, les barrettes de RAM encore fonctionnelles étaient récupérées et réaffectées, dans une logique de maîtrise budgétaire et de réduction des déchets électroniques (DEEE).

Résultats

Traitement quotidien de plusieurs demandes en autonomie pour la majorité des incidents de niveau 1. Les équipements traités étaient systématiquement tracés par numéro de série, assurant une mise à jour du parc sans rupture de traçabilité.

Difficultés et solutions

La principale difficulté était la **communication avec des utilisateurs non techniciens**, notamment les sapeurs-pompiers peu familiers des outils informatiques. J'ai appris à reformuler les questions de diagnostic sans jargon, et à valider la compréhension de l'utilisateur avant de clôturer le ticket.

2.2 Déploiement industrialisé de postes (PXE / mastérisation)

Objectifs

Déployer un système d'exploitation et des logiciels standards sur plus de 300 machines en un temps réduit, en garantissant l'homogénéité des configurations et l'intégration au domaine Active Directory.

Environnement technique

- Serveur de déploiement réseau : FOG Project
- Protocoles : PXE, DHCP, TFTP
- Postes cibles : Lenovo ThinkCentre (remplacement de postes incompatibles Windows 11)
- Système d'exploitation déployé : Windows 11
- Réseau dédié : VLAN de déploiement isolé du réseau de production
- Annuaire : Active Directory Domain Services (AD DS)
- Gestion et déploiement d'applications : WAPT

Contexte

Le service procédait au renouvellement d'un parc de plus de 300 postes fixes répartis sur l'ensemble du département. Une installation manuelle poste par poste aurait représenté une charge de travail impossible à absorber, avec un risque élevé d'hétérogénéité des configurations.

Problématique

Comment déployer un système d'exploitation et des logiciels standards sur plus de 300 machines en un temps réduit, tout en garantissant l'homogénéité des configurations et l'intégration au domaine ?

Mon rôle

J'ai réalisé de façon autonome les étapes de préparation matérielle et de configuration du BIOS pour chaque poste, puis j'ai piloté les déploiements par lots sous la supervision d'un technicien. La finalisation (intégration au domaine, installation des logiciels métiers) était assurée par le technicien habilité.

Démarche

La solution repose sur deux mécanismes complémentaires : la **mastérisation** et le **démarrage réseau PXE**.

La **mastérisation** consiste à créer une **image disque** — copie secteur par secteur du contenu d'un disque dur dans un état de référence, incluant le système d'exploitation, les logiciels et les paramètres de base — pour la déployer ensuite à l'identique sur un grand nombre de machines.

Le **PXE (*Preboot Execution Environment*)** permet à une machine de démarrer depuis le réseau. Au démarrage, le poste envoie une requête DHCP en diffusion. Un serveur DHCP lui répond en indiquant l'adresse d'un serveur **TFTP** qui fournit un bootloader minimal, lequel se connecte au serveur FOG pour récupérer l'image système.

Étapes réalisées en production :

1. **Préparation matérielle** — Mise en réseau des postes par lots de ~10 machines sur un VLAN dédié au déploiement, isolé du réseau de production.
2. **Configuration du BIOS/UEFI** — Activation du démarrage réseau (PXE) en première priorité et désactivation du **Secure Boot** (mécanisme UEFI qui bloque le PXE lorsque l'image réseau n'est pas signée).
3. **Déploiement de l'image** — Chaque poste contacte le serveur FOG, reçoit l'image correspondant à son modèle matériel et procède à l'écriture sur son disque. Un nom de machine conforme à la nomenclature interne lui est attribué.
4. **Finalisation** — Intégration au domaine Active Directory et livraison avec les applications métiers via WAPT.

Résultats

Plusieurs dizaines de postes déployés par jour avec une configuration homogène garantie par l'image commune. Le processus a permis de réduire drastiquement le temps d'installation par rapport à une procédure manuelle, en éliminant tout risque de variation de configuration entre les postes.

Difficultés et solutions

La principale difficulté était l'**échec du démarrage PXE sur certains modèles**, dû à un Secure Boot activé par défaut non détecté lors de la configuration initiale. Sa vérification a été systématisée dans la procédure de préparation pour tous les postes suivants.

2.3 Virtualisation, supervision et sécurité

Objectifs

Mettre en place un environnement de virtualisation de test isolé pour valider des configurations avant production, et poser les bases d'une solution de supervision centralisée capable de couvrir l'ensemble des sites du département.

Environnement technique

- Hyperviseur de test déployé : Proxmox VE (type 1, open source)
- Hyperviseur de production (observé) : VMware vSphere / ESXi
- Solution de supervision : Zabbix
- Pile logicielle Zabbix : Debian 12, Apache, MariaDB, PHP
- Protocoles de supervision : agents Zabbix, SNMP v2c
- Outil d'audit Active Directory : Purple Knight
- Réseau : VLAN dédié supervision

Contexte

L'infrastructure de production reposait sur des serveurs physiques et une solution de virtualisation propriétaire. Le service souhaitait disposer d'un environnement de test isolé pour valider des configurations avant mise en production, ainsi que d'une supervision centralisée de l'ensemble des équipements répartis sur le département.

Problématique

Comment mettre en place un environnement de virtualisation de test sans impacter la production, et poser les bases d'une supervision capable de couvrir plus de 230 sites ?

Mon rôle

Pour la virtualisation, j'ai réalisé l'installation complète de la plateforme en autonomie supervisée, de la création de la clé USB bootable jusqu'aux tests de connectivité des VM. Pour le projet de supervision, j'ai participé à l'installation de la pile logicielle et aux premiers tests d'ajout d'hôtes supervisés.

Démarche — Virtualisation

La virtualisation consiste à faire fonctionner plusieurs **machines virtuelles (VM)** sur un même serveur physique grâce à un **hyperviseur**. Un hyperviseur de **type 1** (*bare-metal*) s'installe directement sur le matériel, sans système d'exploitation hôte — c'est le modèle utilisé en production.

Étapes réalisées :

- Création d'une clé USB bootable avec l'ISO de Proxmox VE.
- Configuration du BIOS pour activer la **virtualisation matérielle** (Intel VT-x) et lancer l'installation.
- Attribution d'une adresse IP conforme au plan d'adressage interne et configuration d'un VLAN test dédié.

- Sécurisation : restriction des IP autorisées, configuration du pare-feu intégré, mots de passe robustes.
- Création de VM de test sous Linux et Windows Server pour valider le fonctionnement de la plateforme.

Démarche — Supervision

La supervision informatique permet de surveiller en temps réel l'état des équipements. Elle repose sur deux mécanismes : les **agents** (programmes installés sur les machines supervisées qui remontent des métriques) et le protocole **SNMP** (*Simple Network Management Protocol*) pour les équipements réseau qui ne peuvent pas accueillir d'agent. La solution Zabbix s'installe sur un serveur Linux avec une pile Apache/PHP/MariaDB. J'ai participé à l'installation de cette pile et aux premiers tests d'ajout d'hôtes via agents et SNMP.

Démarche — Sécurité (observations)

J'ai observé deux situations concrètes de gestion de la sécurité :

- Un **audit Active Directory** conduit par un prestataire (Purple Knight) : identification des comptes à privilèges excessifs et mise en place des recommandations pour appliquer le principe du moindre privilège.
- La **détection d'une tentative d'exploitation Shellshock** via analyse des logs du pare-feu : identification de l'IP source, blocage immédiat, vérification d'absence de compromission.

Résultats

La plateforme de virtualisation a été livrée fonctionnelle et sécurisée, avec des VM de test opérationnelles. Le projet de supervision a atteint ses objectifs de phase initiale : pile installée, premiers hôtes supervisés, alertes fonctionnelles. Ces deux environnements ont constitué la base des travaux approfondis menés lors du stage de deuxième année.

Difficultés et solutions

Pour la supervision, la configuration SNMP sur des équipements hétérogènes a nécessité de consulter la documentation technique de chaque constructeur.

2.4 Gestion Active Directory

Objectifs

Manipuler les objets d'un annuaire Active Directory en environnement de production — unités organisationnelles, comptes utilisateurs, groupes et politiques de groupe — en respectant le principe du moindre privilège et en consolidant les bases théoriques via un exercice pratique en autonomie.

Environnement technique

- Annuaire de production : Active Directory Domain Services (AD DS) — Windows Server
- Consoles d'administration : ADUC (*Active Directory Users and Computers*), GPMC (*Group Policy Management Console*)
- Outil de gestion de parc lié à l'AD : GLPI (synchronisation via connecteur LDAP)
- Environnement de test personnel : VMware + contrôleur de domaine virtuel

Contexte

L'annuaire Active Directory du SIS 67 est le référentiel central de l'identité numérique : tout compte utilisateur, tout poste intégré au domaine et tout droit d'accès y sont définis. Les administrateurs m'ont accordé des droits de consultation et, ponctuellement, de modification pour des tâches de support nécessitant la création ou la gestion de comptes. En parallèle, durant les temps de faible activité, un technicien m'a confié un exercice pratique sur VMware — sans lien direct avec l'infrastructure du SIS 67 — pour consolider mes bases avant toute manipulation en production.

Mon rôle

En production : consultation de l'annuaire pour le support (vérification des droits et des appartenances aux groupes), création et modification de comptes lors d'onboardings ponctuels, gestion des droits NTFS associés. Sur l'environnement de test : configuration d'un AD DS complet en autonomie et liaison avec GLPI.

Démarche

Un **annuaire Active Directory (AD DS)** organise les objets (utilisateurs, groupes, ordinateurs) en **Unités Organisationnelles (OU)** — conteneurs permettant d'appliquer des politiques différenciées selon les services ou les sites. Les **GPO** (*Group Policy Objects*) sont des ensembles de règles de configuration (restrictions logicielles, paramètres de sécurité, mappage de lecteurs réseau) poussées automatiquement aux machines et utilisateurs selon leur appartenance à une OU, selon une hiérarchie site > domaine > OU.

En production, j'ai participé à des opérations courantes : gestion des appartenances de groupes pour l'octroi de droits applicatifs, déplacement d'objets entre OU lors de changements organisationnels, réinitialisation de mots de passe et déverrouillage de comptes. Sur l'environnement de test, la liaison GLPI/LDAP a permis de synchroniser l'annuaire virtuel avec l'outil de gestion de parc — illustrant l'utilisation de l'AD comme source d'identité pour des applications tierces. Cet exercice, réalisé en autonomie sur VMware, n'avait pas de lien direct avec le SI du SIS 67 mais m'a permis de manipuler l'outil sans risque avant d'intervenir en production.

Résultats

Maîtrise opérationnelle des opérations courantes sur l'annuaire en environnement de production. Sur l'environnement de test : contrôleur de domaine fonctionnel, OU et comptes créés, synchronisation GLPI/LDAP opérationnelle.

Difficultés et solutions

La principale difficulté en production était de mesurer l'impact d'une modification sur les GPO associées avant d'agir : modifier l'appartenance d'un objet AD sans comprendre l'héritage des politiques peut affecter des dizaines de postes. La méthode adoptée a été de toujours vérifier la hiérarchie des politiques avant toute modification et de consulter un technicien senior en cas de doute.

3. Compétences mobilisées — Référentiel E5

Mission	C1 — Patrimoine	C2 — Incidents	C4 — Mode projet	C5 — Mise à disposition	C6 — Développement pro
Support utilisateur N1		✅		✅	
Gestion du parc / MDM	✅			✅	
Déploiement PXE / mastérisation	✅			✅	
Virtualisation	✅			✅	
Projet supervision (phase initiale)			✅		
Observations sécurité / audit		✅			
Gestion Active Directory	✅			✅	
Documentation, auto-formation					✅

C1 — Gérer le patrimoine informatique : mobilisée lors de la gestion du parc (traçabilité par numéro de série, recyclage de composants), du déploiement PXE (standardisation à grande échelle, homogénéité garantie par l'image), de la virtualisation (rationalisation des ressources serveurs), et de la gestion Active Directory (recensement des comptes, niveaux d'habilitation, conformité des droits).

C2 — Répondre aux incidents et aux demandes : mobilisée en support N1 avec une méthode de diagnostic structurée, et lors des observations de gestion d'incidents de sécurité (analyse de logs, identification de la source, blocage et vérification post-incident).

C4 — Travailler en mode projet : mobilisée dans le cadre du projet de supervision, avec une phase de cadrage (identification des besoins, choix de l'architecture réseau dédiée), une phase d'installation et des jalons de test mesurables.

C5 — Mettre à disposition des services : mobilisée via le déploiement de postes livrés aux utilisateurs finaux dans un état conforme, le support assurant la continuité de service, la mise en production de la plateforme de virtualisation, et la création de comptes Active Directory opérationnels pour les utilisateurs.

C6 — Organiser son développement professionnel : mobilisée via la prise de notes techniques systématique, la consultation de documentation constructeur en autonomie, et l'observation active des pratiques professionnelles de l'équipe.

4. Bilan

Ce stage a constitué ma première immersion en environnement de production sous contrainte critique. L'aspect le plus formateur a été de comprendre que chaque décision technique — une

segmentation réseau, un niveau de droits, un mécanisme de déploiement — répond à une contrainte réelle et mesurable : disponibilité, sécurité, maintenabilité, coût.

Les difficultés rencontrées (compatibilité matérielle, gestion des erreurs de déploiement, communication avec des utilisateurs non techniciens) m'ont appris à adopter une démarche de diagnostic méthodique plutôt que de chercher une solution immédiate. Les axes de progression identifiés — supervision avancée, automatisation, cybersécurité — ont guidé mon investissement lors du stage de deuxième année.

Rapport rédigé par Alessandro FUENTES — BTS SIO SISR 1ère année — 2025