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

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). Un VLAN est une technique de segmentation logique qui divise un réseau physique en plusieurs réseaux virtuels isolés, sans câblage séparé. 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

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. Il correspond au traitement des demandes courantes et des incidents simples, avant escalade vers un niveau supérieur si la complexité dépasse les habilitations du technicien. 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.

Les équipements mobiles (tablettes et smartphones professionnels) étaient gérés via une solution **MDM** (*Mobile Device Management* — gestion des appareils mobiles). Un MDM est un 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 à chaque appareil.

La gestion du parc impliquait également du **recyclage de composants** : lors du démontage de postes obsolètes, les barrettes de mémoire vive (RAM — *Random Access Memory*, mémoire volatile utilisée par le processeur pour stocker temporairement les données en cours de traitement) encore fonctionnelles étaient récupérées et réaffectées. Cette démarche répond à une logique de **maîtrise budgétaire** et de **réduction des déchets électroniques (DEEE)**.

Résultats

Traitement quotidien de plusieurs demandes des utilisateurs avec résolution en autonomie pour la majorité des incidents de niveau 1. Aucun incident escaladé à tort : la qualification du niveau d'incident était correcte dans tous les cas. 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 de façon simple, à ne pas utiliser de jargon, et à valider la compréhension de l'utilisateur avant de clôturer le ticket. Une autre difficulté était l'identification rapide des composants sur des machines sans étiquetage visible : j'ai pris l'habitude de consulter le numéro de série pour retrouver la fiche constructeur avant toute intervention.

2.2 Déploiement industrialisé de postes (PXE / mastérisation)

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 dans les délais impartis, 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 spécifiques) était assurée par le technicien habilité lorsqu'un compte administrateur était nécessaire.

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 non pas depuis son disque dur local, mais depuis le réseau. Au démarrage, le poste envoie une requête **DHCP** (*Dynamic Host Configuration Protocol* — protocole permettant l'attribution automatique d'une adresse IP et de paramètres réseau) en diffusion. Un serveur DHCP lui répond en indiquant l'adresse d'un serveur **TFTP** (*Trivial File Transfer Protocol* — protocole simplifié de transfert de fichiers utilisé pour transmettre un mini-système de démarrage). Le poste télécharge alors un **bootloader** (programme de démarrage minimal) qui se connecte au serveur de déploiement pour récupérer l'image système.

Étapes réalisées en production :

1. **Préparation matérielle** — Déballage et 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** — Le **BIOS** (*Basic Input/Output System*) ou **UEFI** (*Unified Extensible Firmware Interface*, son successeur moderne) est le micrologiciel qui s'exécute au démarrage avant le système d'exploitation. Il gère l'initialisation du matériel et l'ordre de

démarrage. Deux paramètres étaient à configurer : activation du démarrage réseau (PXE) en première priorité, et désactivation du **Secure Boot** — mécanisme UEFI qui vérifie la signature cryptographique de chaque élément du processus de démarrage pour empêcher l'exécution de code non autorisé, mais qui bloque le PXE lorsque l'image réseau n'est pas signée.

3. **Déploiement de l'image** — Chaque poste contacte le serveur de déploiement, reçoit l'image correspondant à son modèle matériel, et procède à l'écriture secteur par secteur sur son disque. Un nom de machine conforme à la nomenclature interne lui est attribué.
4. **Finalisation** — Intégration au **domaine Active Directory** (enregistrement de la machine auprès de l'annuaire, lui permettant d'appliquer les **GPO** — *Group Policy Objects*, politiques de groupe définissant les configurations et restrictions appliquées aux postes et utilisateurs du domaine), puis livraison avec les applications métiers.

Résultats

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

Difficultés et solutions

La principale difficulté technique rencontrée était l'**échec du démarrage PXE sur certains modèles**, dû à une activation du Secure Boot par défaut non détectée lors de la configuration initiale. Le diagnostic a consisté à observer le message d'erreur affiché au boot, identifier la cause dans les paramètres UEFI, et systématiser la vérification du Secure Boot dans la procédure de préparation pour tous les postes suivants. Une autre difficulté était la **gestion des conflits de noms de machines** lorsqu'un poste recevait un nom déjà attribué dans l'annuaire : le serveur de déploiement signalait l'erreur, et il fallait corriger la nomenclature avant de relancer.

2.3 Virtualisation, supervision et sécurité

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, de la création de la clé USB bootable jusqu'aux tests de connectivité des VM, en autonomie supervisée. Pour le projet de supervision, mon rôle était celui d'un technicien en phase d'apprentissage : participer à l'installation de la pile logicielle et aux premiers tests d'ajout d'hôtes supervisés.

Démarche — Virtualisation

La virtualisation est la technique qui consiste à faire fonctionner plusieurs **machines virtuelles (VM)** — systèmes d'exploitation complets, isolés les uns des autres — sur un même serveur physique, grâce à un logiciel appelé **hyperviseur**.

Il existe deux types d'hyperviseurs :

- **Type 1 (bare-metal)** : l'hyperviseur s'installe directement sur le matériel, sans système d'exploitation hôte. Il offre de meilleures performances et est utilisé en production.
- **Type 2 (hosted)** : l'hyperviseur s'installe sur un système d'exploitation existant. Moins performant, il est utilisé pour les postes de développement.

La solution installée est un hyperviseur de **type 1**, administrable via une interface web. Étapes réalisées :

- Création d'une **clé USB bootable** contenant l'image ISO de l'hyperviseur.
- Configuration du BIOS du serveur pour activer la **virtualisation matérielle** — ensemble d'instructions processeur (Intel VT-x ou AMD-V) qui permettent à l'hyperviseur de gérer les VM de façon plus efficace et sécurisée.
- Attribution d'une adresse IP conforme au plan d'adressage interne et configuration d'un **VLAN test dédié** pour l'accès à l'interface d'administration.
- Sécurisation : restriction des IP autorisées à se connecter, configuration du **pare-feu intégré** (filtrage des connexions entrantes et sortantes selon des règles définies), définition de 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 désigne l'ensemble des mécanismes permettant de surveiller en temps réel l'état des équipements et services d'un SI. Elle repose sur trois mécanismes principaux :

- Les **agents** : petits programmes installés sur chaque machine supervisée, qui collectent des métriques (utilisation CPU, RAM, espace disque, état des services) et les transmettent au serveur central.
- Le protocole **SNMP** (*Simple Network Management Protocol*) : protocole standard permettant d'interroger des équipements réseau (switchs, routeurs, pare-feu) qui ne peuvent pas accueillir d'agent logiciel.
- Les **checks actifs/passifs** : en mode actif, le serveur interroge les équipements à intervalles réguliers ; en mode passif, les équipements envoient spontanément leurs données.

La solution s'installe sur un serveur Linux et nécessite une pile logicielle complète : un **serveur web** (pour l'interface de consultation), un **interpréteur PHP** (langage de scripts côté serveur utilisé par l'interface), et un **SGBD** (*Système de Gestion de Bases de Données*) relationnel pour stocker l'historique des métriques. J'ai participé à l'installation de cette pile et aux premiers tests d'ajout d'hôtes supervisés via agents et SNMP.

Démarche — Sécurité (observations)

Durant le stage, j'ai pu observer deux situations concrètes de sécurité :

- Un **audit de sécurité Active Directory** conduit par un prestataire spécialisé en tests d'intrusion. L'audit portait sur les comptes à **privilèges excessifs** — comptes disposant de droits d'administration non justifiés, représentant un vecteur d'attaque majeur. Les recommandations visaient à appliquer le **principe du moindre privilège** : n'accorder à chaque compte que les droits strictement nécessaires à sa fonction.
- La **détection d'une tentative d'exploitation** d'une vulnérabilité connue affectant l'interpréteur de commandes Bash sur les systèmes Linux, permettant dans certaines conditions l'exécution de code arbitraire à distance. La détection a été faite par analyse des **logs du pare-feu** — fichiers journaux qui enregistrent toutes les connexions avec leur adresse IP source, le port ciblé, et le verdict d'autorisation ou de blocage. La réaction a été immédiate : identification de l'IP source, blocage au niveau du pare-feu, vérification de l'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 sur l'environnement de test : 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

Lors de l'installation de l'hyperviseur, j'ai rencontré un **problème de compatibilité réseau** : la carte réseau du serveur n'était pas reconnue par le système après installation, empêchant l'accès à l'interface web. Le diagnostic a consisté à identifier le modèle exact de la carte réseau via les logs du système, rechercher le pilote manquant, et l'intégrer manuellement. Pour la supervision, la principale difficulté était la **configuration du protocole SNMP** sur des équipements réseau aux interfaces d'administration hétérogènes : chaque constructeur dispose de son propre menu de configuration, ce qui a nécessité de consulter la documentation technique de chaque équipement.

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			✅		

Mission	C1 — Patrimoine	C2 — Incidents	C4 — Mode projet	C5 — Mise à disposition	C6 — Développement pro
(phase initiale)					
Observations sécurité / audit		✅			
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), et de la virtualisation (rationalisation des ressources serveurs).

C2 — Répondre aux incidents et aux demandes : mobilisée en support N1 avec une méthode de diagnostic structurée (qualification, résolution ou escalade documentée), 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 et documenté, le support assurant la continuité de service, et la mise en production de la plateforme de virtualisation.

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