Fuentes - Résumé détaillé de stage 2

> **Établissement :** BTS SIO option SISR – 2ème année | **Entreprise d'accueil :** Service d'Incendie et de Secours du Bas-Rhin | **Période :** Janvier – Février 2026

Table des matières

Introduction

Ce second stage s'est déroulé dans le même établissement que le premier, au sein du même service informatique. Cette continuité m'a permis d'aborder des missions d'un niveau de complexité nettement supérieur, en bénéficiant d'une connaissance préalable de l'infrastructure, des outils et des contraintes métier. Là où le premier stage m'avait placé en position d'observation et d'exécution encadrée, ce second stage m'a confié des **responsabilités réelles** : deux projets d'infrastructure conduits en autonomie, des interventions terrain, la gestion d'incidents en conditions réelles, et la rédaction de documentation d'exploitation destinée à la production.

Le contexte reste identique : un système d'information critique réparti sur plus de 230 sites, où toute interruption non maîtrisée peut avoir des conséquences directes sur les opérations de secours.

1. L'infrastructure technique

L'infrastructure du service repose sur une architecture à plusieurs niveaux. La production s'appuie sur un **cluster de virtualisation de type 1** — hyperviseur installé directement sur le matériel physique, sans système d'exploitation hôte, offrant les meilleures performances et une isolation stricte entre machines virtuelles. Un second environnement de virtualisation open

source est utilisé pour les tests, permettant de valider des configurations avant déploiement en production.

Le réseau est segmenté en **VLAN** et les sites distants sont interconnectés via des **liens MPLS** (*Multiprotocol Label Switching* — technologie de transport réseau gérée par un opérateur tiers, qui achemine les flux entre sites selon des étiquettes prédéfinies plutôt que par routage IP classique, garantissant des performances et une qualité de service contrôlées). La gestion des identités repose sur un annuaire **Active Directory** avec une politique de sécurité renforcée, notamment via le groupe **Protected Users** — groupe de sécurité Active Directory qui applique automatiquement des restrictions d'authentification très strictes à ses membres : interdiction du protocole NTLM, interdiction de la délégation Kerberos non contrainte, et durée de vie des tickets réduite.

Un projet de migration vers un nouveau système d'information des services de secours (NEXSIS) était en cours tout au long du stage, impliquant des reconfigurations réseau régulières sur les sites du département.

2. Projets principaux

2.1 Bastion d'administration sécurisé (Apache Guacamole)

Objectifs

Fournir un accès distant sécurisé, centralisé et auditable pour l'administration des serveurs critiques, en conformité avec la politique d'authentification Active Directory (groupe Protected Users, Kerberos) et en garantissant la traçabilité complète des actions d'administration.

Environnement technique

- Système hôte : Ubuntu Server 22.04 LTS (VM déployée sur cluster vSphere)
- Solution : Apache Guacamole 1.6.0
- Serveur d'applications : Apache Tomcat 9
- Base de données : MariaDB
- Protocoles d'accès distant : RDP (*Remote Desktop Protocol*), SSH (*Secure Shell*)
- Authentification multifacteur : extension TOTP (Google Authenticator / Microsoft Authenticator)
- Authentification SSO : Kerberos / GSSAPI (intégration Active Directory)
- Enregistrement des sessions : FFmpeg (compilation depuis les sources)
- Gestion des mots de passe : Passbolt

Contexte

Les administrateurs système accédaient aux serveurs critiques via RDP directement depuis leurs postes de travail, sans point de contrôle centralisé. Cette approche posait trois problèmes majeurs : absence de traçabilité des actions d'administration, impossibilité d'appliquer une authentification forte systématique, et incompatibilité avec la politique Active Directory imposant Kerberos pour les comptes à hauts privilèges.

Problématique

Comment fournir un accès distant sécurisé, centralisé, auditable et conforme à la politique d'authentification Active Directory pour l'administration des serveurs critiques ?

Mon rôle

J'ai conduit ce projet en autonomie quasi-totale, de la conception à la livraison : déploiement de la machine virtuelle, installation et configuration complète de la solution, résolution d'un blocage technique complexe avec appui d'un expert, rédaction de la documentation d'exploitation et passage de relais à l'administrateur système référent.

Démarche

La solution mise en place est une **passerelle d'administration sans client** (*clientless*) — architecture dans laquelle l'utilisateur se connecte aux serveurs cibles via un simple navigateur web, sans installer de logiciel dédié sur son poste. La passerelle agit comme intermédiaire : elle traduit les protocoles RDP et SSH en flux web chiffrés.

L'architecture technique repose sur trois composants distincts :

- Un **moteur proxy** compilé depuis les sources pour activer précisément les fonctionnalités souhaitées (RDP, SSH, enregistrement vidéo) et contrôler les dépendances.
- Un **serveur d'applications Java** (Tomcat) hébergeant l'interface web accessible via navigateur.
- Un **SGBD relationnel** (MariaDB) pour stocker les comptes, les connexions configurées et l'historique des sessions, indispensable à la traçabilité.

Le déploiement a suivi les étapes suivantes :

1. **Création de la machine virtuelle** sur le cluster vSphere : déploiement à partir d'un modèle Ubuntu préconfiguré conforme aux politiques internes, configuration réseau sur le VLAN de préproduction, ouverture des flux pare-feu nécessaires.
2. **Sécurisation de la plateforme** : séparation stricte des rôles entre le moteur proxy (exécuté sous un utilisateur dédié sans shell interactif) et le serveur web ; permissions restreintes sur les répertoires de configuration et d'audit ; mise en place d'un certificat auto-signé pour le chiffrement HTTPS.
3. **Authentification multifacteur (MFA)** : déploiement d'une extension **TOTP** (*Time-based One-Time Password* — code à usage unique généré toutes les 30 secondes par une application mobile synchronisée sur l'heure). Cette approche réduit drastiquement le risque lié au vol de mots de passe.
4. **Enregistrement des sessions** : toutes les sessions d'administration sont enregistrées automatiquement sous forme vidéo, chaque fichier étant identifié par un UUID unique. Une politique de rétention de 90 jours est appliquée via des tâches planifiées automatiques (cron), évitant la saturation du stockage.
5. **Intégration Kerberos** : Kerberos est un protocole d'authentification réseau basé sur des tickets chiffrés émis par un serveur d'authentification centralisé (KDC). Il est utilisé dans les environnements Active Directory comme alternative à NTLM (interdit pour les membres du groupe Protected Users). GSSAPI est la couche d'abstraction qui permet au moteur RDP d'utiliser Kerberos de façon transparente.

Résultats

La passerelle est opérationnelle en préproduction et livrée avec une documentation d'exploitation complète permettant à l'administrateur de finaliser l'intégration de l'ensemble des serveurs cibles. L'authentification multifacteur est fonctionnelle, les sessions sont enregistrées et consultables depuis l'interface web, et les connexions Kerberos pour les comptes Protected Users sont pleinement opérationnelles.

Difficultés et solutions

Le principal blocage technique a été l'**échec systématique des connexions RDP pour les comptes membres du groupe Protected Users**. L'analyse des logs du moteur proxy confirmait le bon fonctionnement général de la passerelle mais révélait un problème d'authentification spécifique à ce groupe. L'investigation a permis d'identifier la cause racine : la version de la bibliothèque client RDP fournie par les dépôts officiels de la distribution Linux ne supporte pas GSSAPI/Kerberos. La solution a nécessité de **recompiler la bibliothèque depuis les sources** en activant explicitement les flags de support Kerberos. Cette démarche a été conduite avec l'appui d'un expert en cybersécurité externe sollicité par l'administrateur système référent.

2.2 Supervision du SI à grande échelle (Zabbix — industrialisation)

Objectifs

Superviser l'intégralité des équipements réseau et serveurs du département (environ 700 hôtes), fiabiliser la remontée des alertes en migrant vers un protocole sécurisé, et offrir aux équipes une visualisation opérationnelle en temps réel via une carte interactive.

Environnement technique

- Solution de supervision : Zabbix (instance existante sur serveur Linux)
- Protocoles : SNMP v2c → migration SNMPv3 (authentification + chiffrement)
- Équipements supervisés : switchs, routeurs, pare-feux, serveurs (~700 hôtes)
- Carte interactive : construite via l'API Zabbix
- Outils complémentaires : PuTTY (accès CLI équipements réseau)

Contexte

Le service disposait d'une solution de supervision centralisée déjà installée lors de mon premier stage, mais incomplète : un grand nombre d'équipements n'étaient pas encore supervisés, la sécurité du protocole de supervision était insuffisante (SNMPv2c, données en clair), et il n'existait pas de vue cartographique permettant de visualiser l'état du SI par site géographique.

Problématique

Comment superviser l'intégralité des 700 équipements réseau et serveurs répartis sur le département, fiabiliser la remontée des alertes, et offrir aux équipes une visualisation opérationnelle en temps réel ?

Mon rôle

J'ai travaillé sur ce projet en collaboration avec deux alternants (réseaux et applicatif). Ma contribution personnelle portait sur l'ajout et la configuration des hôtes supervisés, la migration

vers SNMP, la maintenance continue lors des migrations réseau liées à NEXSIS, et la construction des dashboards.

Démarche

La supervision repose sur le protocole **SNMP** pour interroger les équipements réseau. Ce protocole existe en plusieurs versions :

- **SNMPv1 et v2c** : données transitant en clair sur le réseau, la seule protection étant une chaîne communautaire (*community string*) envoyée sans chiffrement.
- **SNMPv3** : version sécurisée intégrant l'authentification (hachage) et le chiffrement des données en transit. La migration progressive vers SNMPv3 a été réalisée pour éliminer le risque d'interception sur les équipements le supportant.

La configuration de chaque hôte dans Zabbix implique : définition de l'adresse IP cible, sélection du mode de collecte (agent ou SNMP), association à un **template** (modèle prédéfini regroupant métriques et seuils d'alerte adaptés à un type d'équipement), et classement par unité territoriale.

La **carte interactive** a été construite via l'**API Zabbix** — interface programmatique permettant de piloter la solution sans passer par l'interface graphique. L'API a permis de récupérer dynamiquement l'état de chaque site et de l'afficher sur un fond cartographique du département avec une signalisation par niveau de criticité (vert / rouge).

La maintenance continue du parc supervisé représentait une charge non négligeable : lors de chaque migration réseau liée à NEXSIS, les adresses IP des équipements étaient modifiées, nécessitant une mise à jour immédiate dans Zabbix pour maintenir la fiabilité des alertes.

Résultats

700 hôtes supervisés, classés par unité territoriale, avec des alertes opérationnelles et une carte interactive visualisant l'état en temps réel. La migration SNMPv3 a été réalisée sur l'ensemble des équipements compatibles. La solution a été présentée lors d'une réunion finale devant la DSI. Un tableau de bord global permet une lecture synthétique de l'état du SI.

Difficultés et solutions

La principale difficulté était l'**hétérogénéité des interfaces de configuration SNMP** : chaque constructeur d'équipement réseau dispose de sa propre interface d'administration. La démarche a consisté à consulter la documentation technique de chaque modèle avant intervention.

3. Missions opérationnelles transverses

3.1 Migration réseau — Interventions sur site (NEXSIS)

Objectifs

Reconfigurer le réseau de chaque caserne pour intégrer les nouveaux équipements NEXSIS (nouvelles adresses IP, réaffectation des VLAN, recâblage) sans interruption prolongée des services opérationnels, et maintenir la cohérence du parc supervisé dans Zabbix.

Environnement technique

- Équipements réseau : switchs

- Protocoles : VLAN 802.1Q, DHCP, SNMP
- Outils de test : ping, trace réseau, synchronisation Vigik, impression réseau
- Supervision : mise à jour des hôtes dans Zabbix après chaque intervention

Contexte et problématique

Le déploiement du nouveau système d'information NEXSIS impliquait une reconfiguration complète du réseau dans chaque caserne. Ces interventions devaient être réalisées sans interruption prolongée des services opérationnels, dans des environnements où toute coupure impacte directement la disponibilité opérationnelle.

Mon rôle

J'ai réalisé plusieurs interventions dans des casernes du département : identification et tracé des ports réseau actifs sur le panneau de brassage, réorganisation du câblage, modification des adresses IP et affectation des VLAN sur les équipements, tests fonctionnels de l'ensemble des services (accès NEXSIS, synchronisation du contrôle d'accès Vigik, impression réseau), puis mise à jour des hôtes correspondants dans Zabbix.

Résultats

Plusieurs interventions terrain réalisées, services opérationnels rétablis à l'issue de chaque intervention. La mise à jour systématique dans Zabbix a maintenu la fiabilité de la supervision tout au long de la migration.

Difficultés et solutions

La difficulté principale était la **gestion du risque d'interruption de service** : toute erreur de configuration pouvait priver une caserne d'accès aux applications opérationnelles. La méthode a consisté à préparer chaque intervention en amont (plan d'adressage, liste des équipements), à réaliser les modifications par étapes en testant chaque service avant de passer au suivant, et à documenter chaque changement pour permettre un retour arrière rapide.

3.2 Gestion du parc réseau — Inventaire et réinitialisation

Objectifs

Inventorier et réinitialiser des commutateurs réseau obsolètes avant leur cession au service logistique, en garantissant qu'aucune configuration sensible ne quitte l'organisation.

Environnement technique

- Équipements traités : switchs
- Accès CLI : PuTTY via câble console
- Commandes de réinitialisation : `erase startup-config`, `show running-config`, manipulation physique des boutons Clear/Reset sur certains modèles

Contexte

Dans le cadre du déménagement des bureaux, des commutateurs réseau anciens devaient être remis à zéro avant d'être transmis au service logistique pour revente. Cette étape est obligatoire pour garantir qu'aucune configuration sensible (VLAN, mots de passe, plans d'adressage) ne quitte l'organisation.

Mon rôle

J'ai réalisé en autonomie l'inventaire (relevé des numéros de série, identification des modèles, estimation de la valeur de revente, association des notices constructeur) et la **réinitialisation complète via interface CLI**. La procédure consistait à effacer la configuration de démarrage et à vérifier l'effacement via la commande d'affichage de la configuration active.

Résultats

Une vingtaine d'équipements inventoriés et réinitialisés, transmis au service logistique avec confirmation d'effacement. Cette démarche s'inscrit dans la politique de sécurité des données : aucun équipement ne quitte l'organisation sans effacement certifié.

Difficultés et solutions

Certains modèles nécessitaient une manipulation physique des boutons Clear et Reset au démarrage, combinée aux commandes CLI. La consultation des notices constructeur (retrouvées à partir des numéros de série) a permis d'adapter la procédure à chaque modèle.

3.3 Gestion MDM — Flotte mobile

Objectifs

Assurer la continuité opérationnelle des tablettes terrain en diagnostiquant les appareils défaillants, en gérant les obsolescences et en reconfigurant les appareils fonctionnels suite à une mise à jour de licence.

Environnement technique

- Solution MDM : Knox Manager (Samsung)
- Mode de fonctionnement : kiosk (verrouillage sur une application unique)
- Procédure de réinscription : désinscription via portail d'administration, réinitialisation complète, réinscription par scan de QR code

Contexte

Les tablettes terrain utilisées par les équipes opérationnelles sont gérées via une solution MDM en mode **kiosk** — mode qui verrouille l'appareil sur une application unique, empêchant l'utilisateur d'accéder au système d'exploitation ou à d'autres applications.

Mon rôle

J'ai pris en charge le diagnostic des tablettes défaillantes (déclaration en obsolescence pour les appareils hors service) et la reconfiguration des tablettes fonctionnelles lors d'une mise à jour de licence. La procédure de reconfiguration nécessitait : sortie du mode kiosk, désinscription depuis le portail MDM, réinitialisation complète de l'appareil, puis réinscription via scan d'un QR code généré par le portail permettant la récupération automatique du profil kiosk et l'activation de la nouvelle licence.

Résultats

Flotte reconfigurée avec la nouvelle licence, appareils défaillants déclarés en obsolescence. Continuité du service terrain assurée sans interruption prolongée.

Difficultés et solutions

La principale difficulté était la gestion de tablette dont la mise à jour de licence ne se faisait pas automatiquement suite à un changement récent de licence, empêchant l'accès au mode formation d'une application. La procédure de réinscription complète a résolu le problème.

3.4 Gestion d'incidents — Pannes de liens MPLS

Objectifs

Rétablir rapidement la connectivité des casernes privées d'accès au SI central suite à des pannes simultanées de liens MPLS, en priorisant les sites selon leur niveau d'activité opérationnelle.

Environnement technique

- Liens réseau impactés : MPLS opérateur (sites distants)
- Solution de secours : routeurs de secours préconfigurés (connectivité 4G / liaison internet alternative)
- Outil de gestion d'incidents : IWS (ticketing)
- Supervision : Zabbix (détection des coupures)

Contexte et problématique

Plusieurs liens MPLS reliant des casernes au SI central sont tombés en panne simultanément, privant ces sites d'accès aux applications critiques. La problématique était de gérer la continuité de service pour plusieurs sites simultanément avec une seule équipe disponible.

Mon rôle et démarche

Face à plusieurs sites impactés simultanément, j'ai participé à la gestion en parallèle des incidents : priorisation des sites selon leur niveau d'activité opérationnelle, déplacements physiques pour déployer des **routeurs de secours** (équipements préconfigurés pour établir une connectivité de substitution via 4G en attendant le rétablissement du lien principal), ouverture de tickets d'incident auprès du prestataire opérateur et suivi des délais de rétablissement.

Résultats

Connectivité de secours rétablie sur les sites prioritaires. Tickets d'incident ouverts avec les informations techniques structurées (identifiant du lien, heure de détection, comportement observé), ayant accéléré le traitement par le prestataire.

Difficultés et solutions

La difficulté principale était la **gestion simultanée de plusieurs sites** avec une seule équipe. La priorisation basée sur l'activité opérationnelle de chaque caserne a permis d'optimiser les déplacements. La coordination avec le prestataire MPLS a été facilitée par des tickets structurés avec des informations techniques précises.

3.5 Découverte de la téléphonie sur IP (XiVO)

Objectifs

Découvrir le fonctionnement de la téléphonie sur IP via la mise en place d'un environnement de test complet (IPBX, comptes utilisateurs, tests de communication), et rédiger une

documentation technique de mise en œuvre.

Environnement technique

- Hyperviseur de test : Proxmox VE
- Solution IPBX : XiVO (open source)
- Protocole : SIP (*Session Initiation Protocol*)
- Clients testés : téléphones physiques et softphones (logiciels sur poste de travail)

Contexte et démarche

En cinquième semaine, j'ai exploré un domaine non couvert par ma formation en collaboration avec un alternant réseaux. La **VoIP** (*Voice over Internet Protocol*) désigne l'ensemble des technologies permettant de transporter des communications vocales via un réseau IP. Un **IPBX** est le serveur qui gère le routage des appels dans un réseau téléphonique d'entreprise basé sur IP (comptes utilisateurs, règles de routage, files d'attente, interfaces vers le réseau public). Un **softphone** est un logiciel installé sur un poste de travail qui émule le comportement d'un téléphone physique via SIP.

J'ai déployé une instance XiVO sur Proxmox, configuré des comptes utilisateurs, testé les communications entre téléphones physiques et softphones, et rédigé une documentation technique de mise en œuvre.

Résultats

Environnement de test fonctionnel, communications validées entre téléphones physiques et softphones, documentation rédigée.

4. Participation à un audit de cybersécurité

Lors de la première semaine, j'ai assisté à une journée complète d'audit conduite par un prestataire spécialisé en **gestion de l'exposition aux menaces** (*Exposure Management* — XM Cyber). Contrairement à une analyse de vulnérabilités classique qui liste les failles sans évaluer leur exploitabilité réelle, cette approche simule le comportement d'un attaquant pour cartographier les **chemins d'attaque** réalistes dans le SI : séquences d'actions qu'un attaquant pourrait enchaîner depuis un premier point de compromission pour progresser vers des cibles à haute valeur (contrôleur de domaine, données critiques).

Cette journée m'a permis de situer les projets que je menais (bastion d'accès distant, supervision) dans une stratégie de sécurité globale, et de comprendre concrètement pourquoi des mécanismes comme le groupe Protected Users, le MFA ou la traçabilité des sessions d'administration ne sont pas de simples bonnes pratiques mais des réponses directes à des vecteurs d'attaque identifiés.

5. Compétences mobilisées — Référentiel E5

Mission	C1 — Patrimoine	C2 — Incidents	C4 — Mode projet	C5 — Mise à disposition	C6 — Développement pro
Bastion d'accès distant	✅		✅	✅	

Mission	C1 — Patrimoine	C2 — Incidents	C4 — Mode projet	C5 — Mise à disposition	C6 — Développement pro
(Guacamole)					
Supervision 700 hôtes (Zabbix)	✅		✅	✅	
Migration réseau NEXSIS	✅	✅		✅	
Inventaire / réinitialisation réseau	✅				
Gestion MDM	✅	✅			
Incidents MPLS		✅			
XiVO / Téléphonie sur IP				✅	✅
Audit cybersécurité					✅

C1 — Gérer le patrimoine informatique : mobilisée via la supervision de 700 hôtes (recensement complet, cycle de vie, convention de nommage), la gestion MDM (obsolescence, réinscription), l'inventaire et l'effacement certifié des équipements réseau, et la maintenance continue du parc lors des migrations NEXSIS.

C2 — Répondre aux incidents et aux demandes : mobilisée lors des pannes de liens MPLS (gestion multi-sites, priorisation, coordination prestataire avec tickets structurés), des incidents MDM (diagnostic, reconfiguration), et des interventions terrain lors de la migration réseau.

C4 — Travailler en mode projet : mobilisée sur les deux projets principaux — analyse de besoin, phases test/préproduction/production, gestion d'un blocage technique complexe avec escalade vers un expert externe, documentation et passage de relais formalisé. Présentation finale du projet Zabbix devant la DSI.

C5 — Mettre à disposition des services : mobilisée via la livraison de la passerelle d'administration en préproduction avec documentation d'exploitation, le déploiement de la supervision complète avec tableau de bord et carte interactive, les interventions terrain garantissant la continuité de service NEXSIS, et la mise en place de l'environnement VoIP de test.

C6 — Organiser son développement professionnel : mobilisée via la participation à l'audit de cybersécurité (compréhension des enjeux réels), la découverte de la téléphonie sur IP, la rédaction systématique de documentation, et la montée en compétences autonome sur des sujets non couverts en formation (Kerberos, compilation depuis les sources, API Zabbix).

6. Bilan

Ce second stage a représenté un saut qualitatif significatif par rapport au premier. Les deux projets principaux m'ont placé face à des problématiques d'infrastructure réelles, avec des

contraintes de sécurité et de continuité de service non négociables.

L'aspect le plus formateur a été la gestion du blocage Kerberos : face à un problème qui dépassait le cadre de la configuration logicielle, j'ai dû structurer une démarche d'investigation méthodique — formuler des hypothèses, les tester de façon isolée, remonter la chaîne logicielle jusqu'à la cause racine, et proposer une solution qui n'était pas dans le périmètre initial prévu. Cette expérience a consolidé ma capacité à ne pas me limiter aux symptômes apparents d'un incident.

La participation à l'audit de cybersécurité a également été déterminante : elle a donné du sens aux choix techniques que je réalisais au quotidien et m'a confirmé mon intérêt pour les métiers de la sécurité des infrastructures.

Rapport rédigé par Alessandro FUENTES — BTS SIO SISR 2ème année — 2026