

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

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, des interventions terrain en autonomie, 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 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

Contexte

Les administrateurs système accédaient aux serveurs critiques via le protocole **RDP** (*Remote Desktop Protocol*) — protocole Microsoft permettant la prise en main graphique à distance d'un poste ou serveur Windows) 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 priviléges.

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 (*Secure Shell* — protocole de connexion à distance sécurisé par chiffrement, utilisé pour l'administration des serveurs Linux) en flux web chiffrés.

L'architecture technique repose sur trois composants distincts :

- Un **moteur proxy** compilé depuis les sources : programme compilé directement à partir du code source au lieu d'être installé depuis un paquet précompilé, ce qui permet d'activer précisément les fonctionnalités souhaitées (support RDP, SSH, enregistrement vidéo) et de contrôler les dépendances.
- Un **serveur d'applications Java** qui héberge l'interface web accessible via navigateur.
- Un **SGBD relationnel** (*Système de Gestion de Bases de Données*) 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 de production : déploiement à partir d'un modèle de serveur Linux 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 chiffrer les échanges HTTPS.
3. **Authentification multifacteur (MFA)** : déploiement d'une extension **TOTP** (*Time-based One-Time Password*) — mécanisme d'authentification à deux facteurs dans lequel l'utilisateur saisit, en plus de son mot de passe, un 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** (*Universally Unique Identifier* — identifiant unique de 128 bits garantissant l'unicité de chaque enregistrement). Une politique de rétention de 90 jours est appliquée via des tâches planifiées automatiques, 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 (le **KDC** — *Key Distribution Center*). Il est utilisé dans les environnements Active Directory comme alternative à NTLM (*NT LAN Manager* — protocole d'authentification Windows plus ancien, basé sur un mécanisme de défi-réponse, interdit pour les membres du groupe Protected Users en raison de ses faiblesses cryptographiques connues). GSSAPI (*Generic Security Services Application Program Interface*) 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 montrait que la connexion aboutissait uniquement lorsque le compte était retiré du groupe, ce qui confirmait le bon fonctionnement général de la passerelle mais révélait un problème d'authentification spécifique. L'investigation a permis d'identifier la cause racine : la version de la bibliothèque client RDP open source fournie par les dépôts officiels de la distribution Linux utilisée ne supporte pas le protocole GSSAPI/Kerberos. Cette limitation n'est pas liée à la configuration mais à la chaîne logicielle elle-même. La solution a nécessité de **recompiler la bibliothèque depuis les sources** en activant explicitement les flags de support Kerberos, ce qui a impliqué la résolution de nombreuses dépendances de compilation. 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

Contexte

Le service disposait d'une solution de supervision centralisée déjà installée, mais incomplète : un grand nombre d'équipements n'étaient pas encore supervisés, la sécurité du protocole de supervision était insuffisante, et il n'existe 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 un protocole de supervision sécurisé, la maintenance continue lors des migrations réseau, et la construction de dashboard.

Démarche

La supervision repose sur le protocole **SNMP** (*Simple Network Management Protocol*) pour interroger les équipements réseau. Ce protocole existe en plusieurs versions aux niveaux de sécurité très différents :

- **SNMPv1 et v2c** : les données transitent en clair sur le réseau, la seule protection est une chaîne communautaire (*community string*) envoyée sans chiffrement — équivalent d'un mot de passe visible en texte clair.
- **SNMPv3** : version sécurisée intégrant l'**authentification** (vérification de l'identité de l'émetteur via un algorithme de hachage) et le **chiffrement** des données en transit. La migration progressive vers SNMPv3 sur les équipements compatibles a été réalisée pour éliminer le risque d'interception des données de supervision.

La configuration de chaque hôte dans la solution de supervision implique : définition de l'adresse IP cible, sélection du mode de collecte (agent logiciel installé sur les serveurs, ou SNMP pour les équipements réseau), association à un **template** (modèle prédéfini regroupant un ensemble de métriques et de seuils d'alerte adaptés à un type d'équipement), et classement par unité territoriale pour faciliter la lecture.

La **carte interactive** a été construite via l'**API** (*Application Programming Interface* — interface programmatique permettant d'interroger ou de piloter une application via des requêtes structurées, sans passer par l'interface graphique) de la solution de supervision. Cette 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 pour un fonctionnement normal, rouge en cas d'incident critique (chute d'un pare-feu, d'un commutateur ou d'un lien réseau).

La maintenance continue du parc supervisé a représenté une charge non négligeable : lors de chaque migration réseau liée au nouveau système d'information des secours, les adresses IP des équipements concernés étaient modifiées, nécessitant une mise à jour immédiate dans la solution de supervision 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 est livrée avec un tableau de bord global permettant 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 et d'une arborescence de menus différente pour activer et configurer SNMPv3. La démarche a consisté à consulter la documentation technique de chaque modèle d'équipement avant intervention. Une seconde difficulté était le **positionnement géographique incorrect de certains sites** sur la carte : l'API retournait des coordonnées imprécises pour quelques localités, nécessitant une correction manuelle des coordonnées dans la configuration.

3. Missions opérationnelles transverses

3.1 Migration réseau — Interventions sur site

Contexte et problématique

Le déploiement du nouveau système d'information des secours impliquait une reconfiguration complète du réseau dans chaque caserne : nouvelles adresses IP, réaffectation des VLAN, recâblage des équipements. Ces interventions devaient être réalisées sans interruption prolongée des services opérationnels.

Mon rôle

J'ai réalisé plusieurs interventions en autonomie dans des casernes du département, en suivant une méthodologie définie : 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 au nouveau système d'information, synchronisation du contrôle d'accès, impression réseau), puis mise à jour des hôtes correspondants dans la solution de supervision.

Un **panneau de brassage** (*patch panel*) est un équipement passif installé en baie de brassage qui centralise les arrivées des câbles réseau et permet de les relier aux ports actifs des commutateurs via des cordons courts, facilitant la gestion et les modifications sans toucher au câblage structural.

Difficultés et solutions

La difficulté principale était la **gestion de l'interruption de service** : toute erreur de configuration ou de câblage 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 si nécessaire.

3.2 Gestion du parc réseau — Inventaire et réinitialisation

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) et la **réinitialisation complète via interface CLI** (*Command Line Interface* — interface en ligne de commande permettant d'administrer un équipement réseau en saisissant des commandes textuelles, accessible via un câble console et un émulateur de terminal). La procédure consistait à effacer la configuration de démarrage (`erase startup-config`) et à vérifier l'effacement via la commande d'affichage de la configuration active. Sur certains modèles, la réinitialisation nécessitait une manipulation physique des boutons hardware au démarrage.

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.

3.3 Gestion MDM — Flotte mobile

Contexte

Les tablettes terrain utilisées par les équipes opérationnelles sont gérées via une solution **MDM** (*Mobile Device Management*) en mode **kiosk** — mode de fonctionnement qui verrouille l'appareil sur une application unique ou un ensemble restreint d'applications, 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 dans le fichier de destruction 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 d'administration 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.

3.4 Gestion d'incidents — Pannes de liens MPLS

Contexte

Plusieurs liens MPLS reliant des casernes au SI central sont tombés en panne simultanément, privant ces sites d'accès aux applications critiques.

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 configurés à l'avance pour établir une connectivité de substitution via une liaison alternative (réseau cellulaire 4G ou liaison internet bas débit) en attendant le rétablissement du lien principal, ouverture de tickets d'incident auprès du prestataire opérateur et suivi des délais de rétablissement.

Difficultés et solutions

La difficulté principale était la **gestion simultanée de plusieurs sites** tombés en panne au même moment, alors qu'une seule équipe était disponible pour intervenir. La priorisation a été basée sur l'activité opérationnelle de chaque caserne. Une seconde difficulté était la

coordination avec le prestataire MPLS pour obtenir un diagnostic rapide : l'ouverture de tickets structurés avec les informations techniques précises (identifiant du lien, heure de détection, comportement observé) a accéléré le traitement.

3.5 Découverte de la téléphonie sur IP

Contexte

En cinquième semaine, j'ai eu l'opportunité d'explorer un domaine non couvert par ma formation : la téléphonie sur IP (VoIP). En collaboration avec un alternant réseaux, j'ai mis en place un environnement de test sur l'hyperviseur open source.

Démarche

La **VoIP** (*Voice over Internet Protocol*) désigne l'ensemble des technologies permettant de transporter des communications vocales via un réseau IP, au lieu d'une infrastructure téléphonique dédiée. Un **IPBX** (*Internet Protocol Private Branch Exchange*) est le serveur qui gère le routage des appels dans un réseau téléphonique d'entreprise basé sur IP : il gère les comptes utilisateurs, les règles de routage, les files d'attente et les interfaces vers le réseau téléphonique public. Le protocole standard utilisé est **SIP** (*Session Initiation Protocol*), qui gère l'établissement, la modification et la fin des sessions de communication. Un **softphone** est un logiciel installé sur un poste de travail qui émule le comportement d'un téléphone physique en utilisant SIP, permettant de passer et recevoir des appels via le poste informatique.

J'ai déployé une instance de solution IPBX open source sur l'environnement de test, configuré des comptes utilisateurs, et testé les communications entre téléphones physiques et softphones. Une documentation technique de mise en œuvre a été 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*). Contrairement à une analyse de vulnérabilités classique — qui liste les failles présentes 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
Supervision 700 hôtes	✓		✓	✓	
Migration réseau NEXSIS	✓	✓		✓	
Inventaire / réinitialisation réseau	✓				
Gestion MDM	✓	✓			
Incidents MPLS		✓			
Audit cybersécurité / VoIP					✓

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

C2 — Répondre aux incidents et aux demandes : mobilisée lors des pannes de liens MPLS (gestion multi-sites, priorisation, coordination prestataire), 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, documentation et passage de relais formalisé.

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, et les interventions terrain garantissant la continuité de service.

C6 — Organiser son développement professionnel : mobilisée via la participation à l'audit de cybersécurité (compréhension des enjeux réels de sécurité), 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).

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