Ressources Documentaires – Réalisation Professionnelle n°2

Examen / Épreuve	BTS Services Informatiques aux Organisations (SIO) - Option SISR - Épreuve E6
Intitulé du projet	Mise en place d'une infrastructure réseau redondante et hautement disponible
Candidat	MALAUSSENA Maxence
Établissement	Lycée Saint-Exupéry - Saint-Raphaël
Période de réalisation	05/09/2025 - 26/05/2026

1. Contexte et besoins

1.1 Présentation de l'organisation

Le Port de Cherbourg est une structure d'importance stratégique majeure gérant des flux constants de passagers, de fret maritime, de croisières ainsi que des opérations de maintenance navale. Le fonctionnement optimal de ces activités repose entièrement sur la disponibilité et la robustesse de son infrastructure informatique locale.

1.2 Problèmes identifiés

Suite à un audit de sécurité interne approfondi, plusieurs vulnérabilités critiques ont été mises en évidence dans l'architecture d'origine :

- Le switch central de l'infrastructure représentait un point de défaillance unique (SPOF). Une panne matérielle sur cet équipement coupait l'intégralité du trafic réseau local (LAN).
- Le serveur de gestion de parc et de helpdesk (GLPI) était centralisé sur une seule machine virtuelle, sans réplication ni mécanisme de bascule, risquant d'interrompre le suivi des incidents en cas de crash.
- La maintenance de ces services s'avérait complexe et chronophage en raison de cette absence de redondance, interdisant toute intervention en heures de production.

1.3 Objectifs fixés

Afin de moderniser et de sécuriser l'environnement technique, les objectifs suivants ont été définis :

- Garantir la tolérance aux pannes au niveau de la commutation centrale du réseau informatique.
- Assurer la haute disponibilité de l'application de gestion GLPI et de ses données.
- Renforcer la sécurité périmétrique globale en préparant l'intégration de firewalls redondants.

2. Solutions envisagées et solution retenue

2.1 Comparatif des solutions d'infrastructure

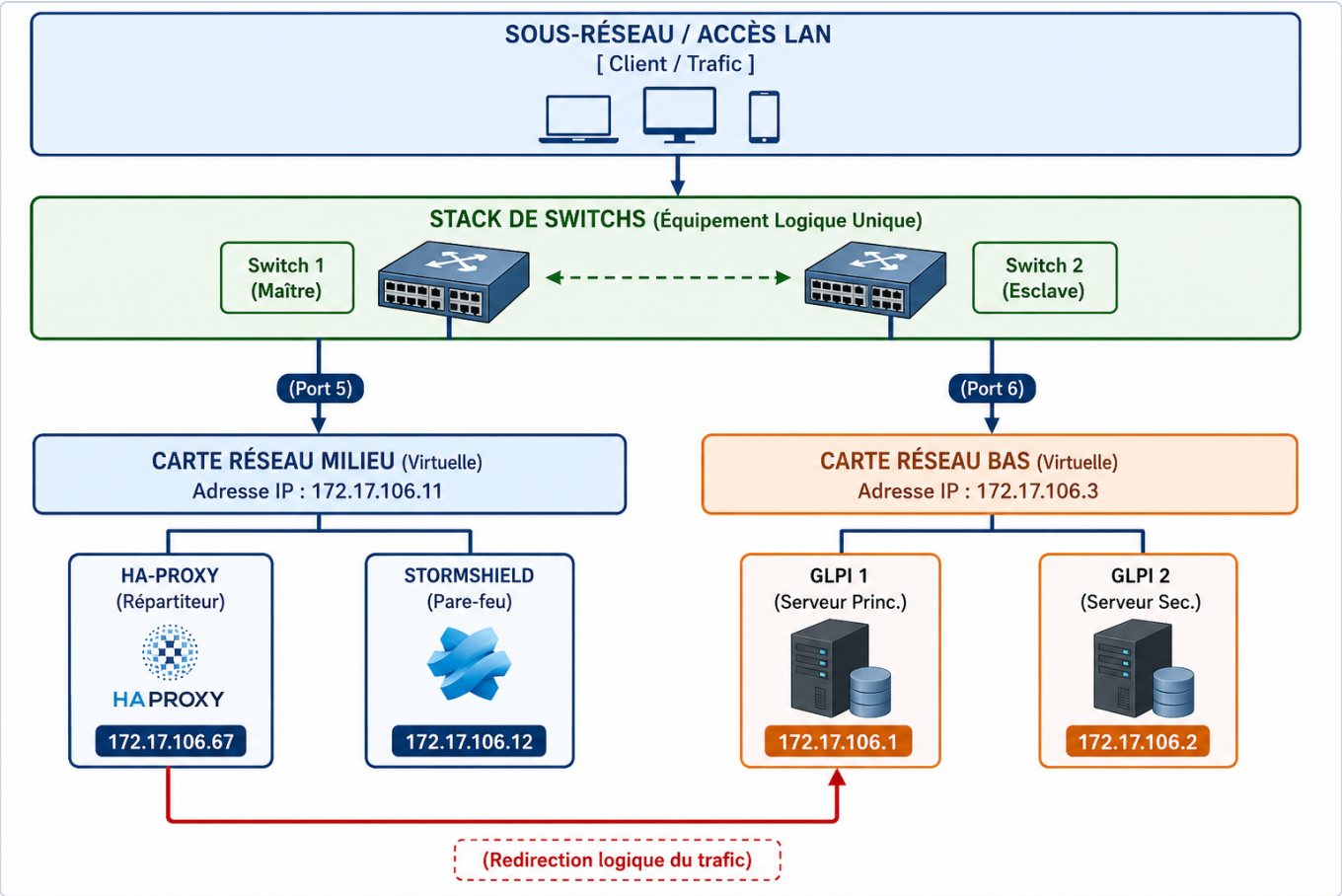
Solution envisagée	Avantages	Inconvénients
Stacking de switchs d'interconnexion	Équipement logique unique, basculement matériel instantané, agrégation de liens facilitée.	Nécessite des équipements de gamme identique et compatibles matériellement.
Cluster GLPI avec HAProxy	Répartition de charge transparente, tolérance à la panne d'un nœud applicatif, continuité de service.	Configuration plus complexe de la réplication de la base de données.
Pare-feu Stormshield HA	Sécurisation périmétrique redondante, synchronisation des états de session.	Complexité de mise en œuvre initiale des politiques de sécurité.

2.2 Solution retenue

La solution finale met en œuvre une double couche de redondance : un **stack de switchs d'interconnexion physique** pour sécuriser le niveau de commutation matériel, combiné à un **cluster GLPI hautement disponible** virtualisé, dont le trafic est aiguillé en amont par un répartiteur de charge HAProxy.

3. Architecture réseau et plan d'adressage

3.1 Schéma de l'infrastructure déployée



3.2 Plan d'adressage IP

L'architecture réseau repose sur un adressage statique strict garantissant la stabilité des communications entre les briques applicatives et de sécurité :

Segment / Équipement	Interface / Carte réseau	Adresse IP	Masque	Rôle / Raccordement physique
Stack de Switchs	Équipement logique unique	-	-	Interconnexion centrale redondante (Switch 1 Maître / Switch 2 Esclave)
Zone Sécurité / Milieu	Carte réseau Milieu (Virtuelle)	172.17.106.11	/24	Passerelle intermédiaire connectée au **Port 5** du Switch 1
HAProxy	Répartiteur de charge	172.17.106.67	/24	Aiguillage et redirection logique du trafic client vers les serveurs GLPI
Stormshield	Pare-feu périmétrique	172.17.106.12	/24	Filtrage et sécurisation des flux réseau
Zone Applicative / Bas	Carte réseau Bas (Virtuelle)	172.17.106.3	/24	Segment des serveurs de production connecté au **Port 6** du Switch 1
GLPI 1	Serveur Principal	172.17.106.1	/24	Nœud applicatif primaire GLPI avec base MariaDB répliquée
GLPI 2	Serveur Secondaire	172.17.106.2	/24	Nœud applicatif de secours (reprise immédiate en cas de panne de GLPI 1)

> **Note technique importante :** Le stack de switchs déployé est un **stack de switchs d'interconnexion**. Les deux commutateurs physiques (Switch 1 Maître et Switch 2 Esclave) fonctionnent de concert pour former un seul équipement logique. Les connexions critiques de nos cartes réseaux virtuelles (Milieu sur le Port 5 et Bas sur le Port 6) se raccordent physiquement de manière stratégique pour pallier toute défaillance matérielle.

4. Mise en œuvre technique

Le déploiement a été articulé autour de quatre phases clés :

1. **Mise en place du Stack :** Liaison physique des commutateurs via les ports de stacking dédiés, élection du commutateur maître et validation de la console d'administration unique.
2. **Configuration des cartes réseaux virtuelles :** Déploiement des segments réseaux "Milieu" (172.17.106.11) et "Bas" (172.17.106.3) pour segmenter de manière étanche les flux de sécurité et les flux applicatifs.
3. **Déploiement du cluster GLPI :** Installation des deux serveurs Linux (GLPI 1 et GLPI 2), configuration de la synchronisation en temps réel des bases de données MariaDB.
4. **Configuration du Load Balancer :** Paramétrage de HAProxy (172.17.106.67) pour analyser l'état de santé (health check) des serveurs web GLPI et rediriger logiquement le trafic vers le nœud actif.

5. Validation et Tests de recette

Scénario de Test	Action réalisée	Résultat attendu	Résultat obtenu
Coupure du Switch 1 (Maître)	Déconnexion électrique du premier commutateur.	Le Switch 2 (Esclave) prend le relais immédiatement, aucun paquet perdu.	**OK** (Continuité LAN validée)
Panne du serveur GLPI 1	Arrêt forcé du service système sur GLPI 1.	HAProxy détecte la panne et redirige instantanément le trafic vers 172.17.106.2.	**OK** (Bascule transparente)
Cohérence des données	Création d'un ticket d'incident pendant la bascule.	Le ticket est enregistré et lisible sur les deux nœuds après rétablissement.	**OK** (Réplication fonctionnelle)

6. Bilan et perspectives

La concrétisation de cette infrastructure redondante élimine avec succès les principaux points individuels de défaillance (SPOF) qui menaçaient les opérations du Port de Cherbourg. Grâce au mécanisme de stack de switchs d'interconnexion et à la haute disponibilité applicative apportée par HAProxy et le binôme GLPI, la continuité d'activité est pleinement assurée. La prochaine étape planifiée consiste à basculer le pare-feu Stormshield (172.17.106.12) dans un cluster actif/passif hautement disponible afin de parfaire la tolérance aux pannes sur le périmètre de sécurité.