Documentation de synthèse principale

Contexte

Je suis Emilien Ternois--Libraire, technicien système et réseau au sein de la société HEALTH NORTH, une entreprise créée en 1987, spécialisée dans les services médicaux, notamment les prélèvements, les analyses biologiques et l'hospitalisation à destination des particuliers.

HEALTH NORTH s'est développé à l'échelle européenne grâce à l'acquisition progressive de nombreux laboratoires et cliniques, et compte aujourd'hui environ 12 000 employés. À la suite d'une récente fusion avec un groupe d'hospitalisation privée présent dans plusieurs pays d'Europe (Suède, Norvège, Finlande, France et Royaume-Uni), l'entreprise est devenue un acteur majeur du secteur médical sur le continent. Cette évolution s'accompagne d'un besoin important de reconstruction du système d'information afin d'harmoniser les infrastructures existantes, d'améliorer la sécurité des données et de garantir une meilleure disponibilité des services.

L'organisation de HEALTH NORTH repose sur deux grandes composantes. En premier, un système d'information interne, utilisé par le personnel médical et administratif pour les opérations quotidiennes (accès aux postes, applications métiers, gestion des patients, etc.). La deuxième composante étant un système d'information externe, permettant aux patients et aux professionnels de santé d'accéder à certains services à distance, tels que la prise de rendez-vous ou la consultation de dossiers.

En France, l'entreprise s'appuie sur plusieurs structures distinctes telles que les laboratoires de prélèvement, les centres d'analyse et les cliniques. Ces différentes entités doivent échanger en continu des données médicales sensibles, ce qui nécessite une infrastructure informatique fiable, sécurisée et performante, notamment pour respecter les délais de traitement des analyses fixés à 24 heures pour les analyses standard et 72 heures pour les analyses complexes.

Problématique

La principale problématique du projet est de reconstruire une infrastructure réseau fiable, sécurisée et résiliente pour la clinique Health-North de Guadeloupe. Les enjeux sont très importants, car l'entreprise manipule et stocke une quantité non négligeable de données médicales sensibles, et il est important de garantir un accès continu au système d'information.

Objectifs

Dans ce contexte, la clinique de Guadeloupe est de ce fait concernée par cette reconstruction de l'architecture système et réseau. Sous la responsabilité du DSI, j'ai ainsi été missionné pour intervenir sur cette refonte de l'architecture système et réseau pour cette clinique. Pour cela, mon intervention est divisée en cinq missions suivantes :

- Mise en place de l'architecture réseau de base;

- Mise en place des services vitaux;
- Mise en place de la documentation;
- Mise en place des services annexes;
- Mise en place de la haute disponibilité des services principaux.

Présentation générale de l'architecture

Mon architecture comme nous pouvons le voir ci-dessous est composée de deux pare-feu pfSense physique, un switch 24 ports manageable suivi de trois hyperviseurs.

Les pare-feu assurent le routage inter-VLAN, le filtrage, le NAT, les accès VPN et la haute disponibilité réseau. Le switch permet le transport des VLAN et la segmentation des flux.

Les services sont hébergés sous forme de machine virtuelle dans un cluster Proxmox.

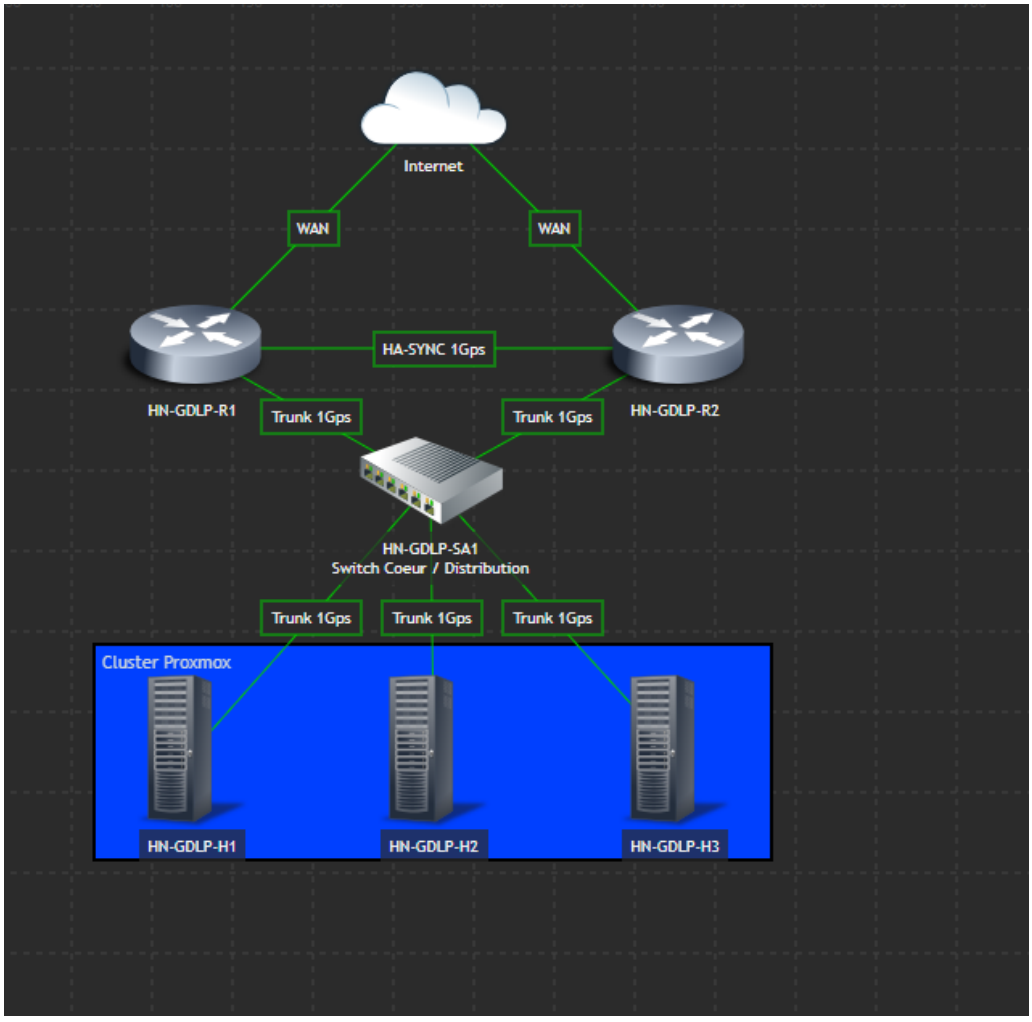
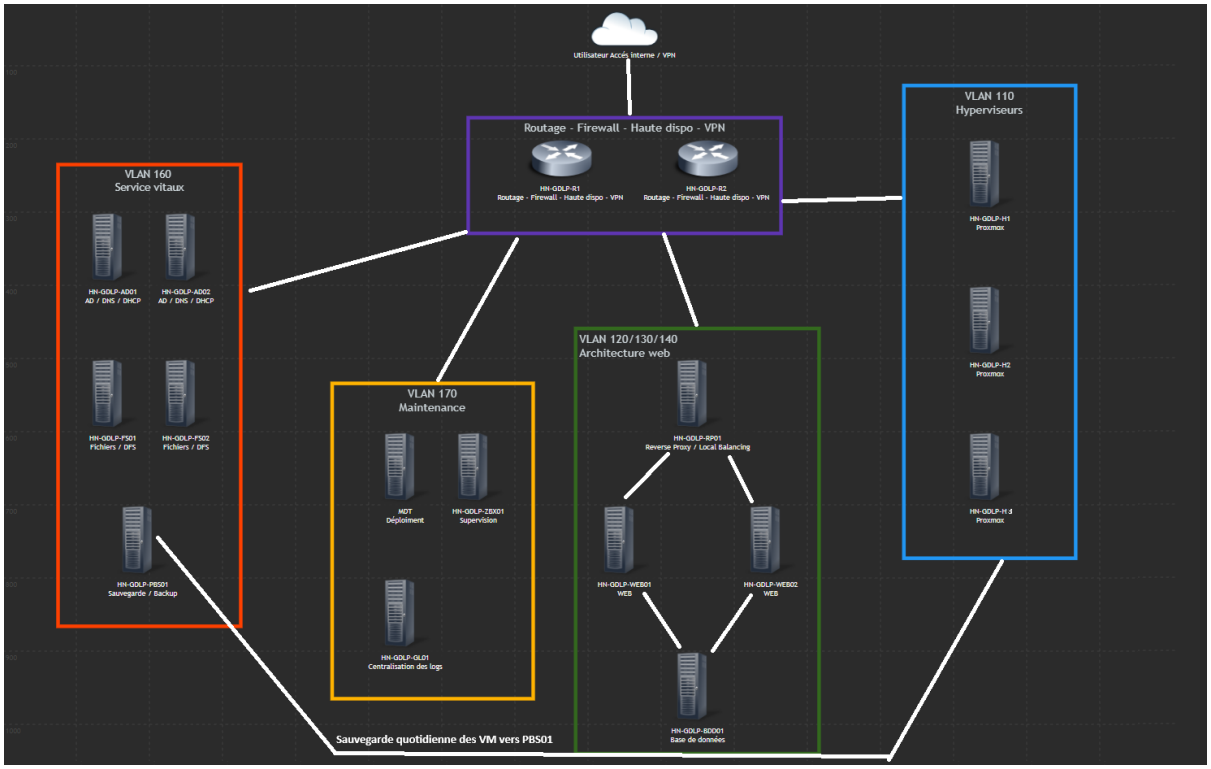


Schéma logique de l'architecture



Ce schéma logique présente la répartition des services dans les différents VLAN. Nous pouvons distinctement remarquer la séparation entre les services vitaux et les services de maintenance, ainsi que l'isolation de l'architecture Web.

Récapitulatif du matériel utilisé

Nom de l'équipement	Type	Rôle
HN-GDLP-R1	Tour physique pfSense	Pare feu principal
HN-GDLP-R2	Tour physique pfSense	Pare feu secondaire
HN-GDLP-SA01	Switch manageable 24 port	Segmentation VLAN
HN-GDLP-H1	Hyperviseur Proxmox	Hébergement des VM
HN-GDLP-H2	Hyperviseur Proxmox	Hébergement des VM
HN-GDLP-H3	Hyperviseur Proxmox	Hébergement des VM
Box internet	Router opérateur	Accès WAN

Les pare-feu R1 et R2 sont installés sur deux tours physiques équipées de plusieurs cartes réseau pour séparer les flux WAN, LAN/VLAN et synchronisation HA. Les hyperviseurs Proxmox hébergent les machines virtuelles du projet.

Les machines virtuelles déployées

VM	IP	OS	Rôle	Hyperviseur

HN-GDLP-AD01	10.160.0.10	Windows Server 2022	AD / DNS principal	H1
HN-GDLP-AD02	10.160.0.11	Windows Server 2022	AD / DNS secondaire	H2
HN-GDLP-FS01	10.160.0.20	Windows Server 2022	Fichiers / DFS / FSRM	H1
HN-GDLP-FS02	10.160.0.21	Windows Server 2022	Fichiers / DFS / réplication	H2
HN-GDLP-PBS01	10.160.0.30	Proxmox Backup Server	Sauvegarde	H3
HN-GDLP-ZBX01	10.170.0.10	Linux	Supervision Zabbix	H1
HN-GDLP-GL01	10.170.0.11	Linux	Centralisation logs Graylog	H1
HN-GDLP-DPL01	10.170.0.20	Windows Server 2022	MDT / déploiement	H1
HN-GDLP-RP01	10.120.0.10	Linux	Reverse proxy	H1
HN-GDLP-WEB01	10.130.0.10	Linux	Serveur web GLPI	H1
HN-GDLP-WEB02	10.130.0.11	Linux	Serveur web GLPI	H2
HN-GDLP-BDD01	10.140.0.10	Linux	MariaDB / NFS	H1

Les machines virtuelles sont réparties sur les hyperviseurs de manière à assurer un minimum de services en cas de panne de l'un d'entre eux.

Choix techniques

pfSense a été choisi pour assurer le routage inter-VLAN, le filtrage réseau, le NAT, les accès VPN et la haute disponibilité réseau. Il permet également de mettre en place des règles pare-feu.

Proxmox a été choisi pour héberger l'ensemble des machines virtuelles du projet. Cette solution permet de centraliser l'administration, de répartir les VM sur plusieurs hôtes et de faciliter les sauvegardes avec Proxmox Backup Server.

Proxmox backup Serveur (PBS)

PBS est utilisé pour assurer la sauvegarde des machines virtuelles hébergées dans Proxmox. Il permet de planifier les sauvegardes, de vérifier leur intégrité et de réaliser des restaurations très simplement et rapidement.

Windows Server 2022 est utilisé pour les services Active Directory, DNS, DHCP, fichiers, DFS, FSRM, GPO et MDT. C'était le choix le plus logiques au vu des attendus de création d'utilisateurs, de règle de sécurité, de serveur DHCP.

Debian et Ubuntu ont été utilisés pour les services web, reverse proxy, base de données, supervision et centralisation des logs. Ce choix était pertinent du fait de leur robustesse, leur légèreté et leur grand choix de solution techniques.

Le découpage réseau

Num	Id vlan	Nom	Réseau	Passerelle par défaut	Description
1	69	Poubelle	10.69.0.0/24		Toutes les interfaces non utilisées des commutateurs sont dans ce vlan
2	99	Natif	10.99.0.0/24		Prévu pour les trames non tagué
3	100	Management des actifs	10.100.0.0/24		Les commutateurs et équipements de routage ont une IP dans ce réseau. Ce réseau permettra l'accès en SSH sur les actifs.
4	110	Hyperviseur	10.110.0.0/24		Hyperviseur (esx, hyperv, proxmox, kvm, ...)
5	120	Reverse Proxy	10.120.0.0/24		Serveur de load balancing
6	130	Web	10.130.0.0/24		Serveurs web
7	140	BDD	10.140.0.0/24		Serveurs de base de données.
8	150	VOIP	10.150.0.0/24		Service de téléphonie IP
9	160	Service vitaux	10.160.0.0/24		Active Directory, DHCP, DNS, Partage de fichier, GPO, serveur de backup.
10	170	Service de maintenance	10.170.0.0/24		Serveur de Supervision, serveur de log (sai), serveur ITSM (gestion d'incident), déploiement
11	180	Bastion	10.180.0.0/24		Service de centralisation des managements équipements
12	300	Service informatique	10.3.0.0/24		Utilisateurs
13	301	Service infirmier	10.3.10.0/24		Utilisateurs
14	302	Service Chirurgie	10.3.20.0/24		Utilisateurs
15	303	Service Laboratoire	10.3.30.0/24		Utilisateurs
16	304	Service Direction	10.3.40.0/24		Utilisateurs
17	400	Wifi Service	10.4.0.0/23		Utilisateurs
18	401	Wifi Patient	10.4.10.0/23		Utilisateurs

Le découpage réseau et assez strict et repose sur une demande très précise à respecter de la direction de HEALTH NORTH.

Plan d'adressage résumé

VLAN	Nom du Réseau	Plage Réseau	Passerelle / VIP	Éléments principaux
100	Management	10.100.0.0/24	10.100.0.254	pfSense, switchs
110	Hyperviseur	10.110.0.0/24	10.110.0.254	Proxmox H1 / H2 / H3
120	Reverse Proxy	10.120.0.0/24	10.120.0.254	RP01
130	Web	10.130.0.0/24	10.130.0.254	WEB01, WEB02
140	BDD	10.140.0.0/24	10.140.0.254	BDD01
160	Services vitaux	10.160.0.0/24	10.160.0.254	AD01, AD02, FS01, FS02, PBS01
170	Maintenance	10.170.0.0/24	10.170.0.254	Zabbix, Graylog, MDT
300	Informatique	10.3.0.0/24	10.3.0.254	Postes informatiques

301	Infirmier	10.3.10.0/24	10.3.10.254	Postes infirmier
302	Chirurgie	10.3.20.0/24	10.3.20.254	Postes chirurgie
303	Laboratoire	10.3.30.0/24	10.3.30.254	Postes laboratoire
304	Direction	10.3.40.0/24	10.3.40.254	Postes direction
400	WiFi Service	10.4.0.0/23	10.4.1.254	WiFi interne
401	WiFi Patient	10.4.10.0/23	10.4.11.254	WiFi isolé

Les passerelles sont portées par des adresses VIP CARP, gérées par les deux pare-feu pfSense, ce qui permet de conserver la même passerelle et facilite la haute disponibilité réseau.

Les services mis en place pour la bonne réalisation du projet

Plusieurs services ont été mis en place afin de répondre aux besoins du projet :

- Active Directory pour l'authentification et la gestion des utilisateurs
- DNS pour la résolution de noms internes
- DHCP pour la distribution dynamique des adresses IP
- DFS et FSRM pour les partages de fichiers et le contrôle du stockage
- GLPI pour la gestion d'incident
- Proxmox Backup Server pour les sauvegardes
- Zabbix pour la supervision
- Graylog pour la centralisation des logs
- MDT pour le déploiement des postes
- OpenVPN pour l'accès à distance sécurisé
- Une architecture web séparée avec reverse proxy, serveurs web et base de données

Résilience et sauvegarde

La résilience de l'infrastructure repose sur plusieurs éléments :

- Les deux pare-feu pfSense sont configurés en haute disponibilité avec CARP, pfsync et XMLRP.
- Pour les services vitaux, elle est assurée par deux contrôleurs de domaine qui assurent la redondance de l'Active Directory, du DNS et du DHCP. Le stockage des fichiers et assuré par FS01 et FS02 avec DFS et la réplication.
- Pour le WEB, GLPI et fourni par un reverse proxy reposant sur deux serveurs web.

- Les sauvegardes des machines virtuelles les plus importantes sont assurées par Proxmox Backup Server afin de pouvoir restaurer les services très rapidement en cas de panne.

État D'avancement

Architecture réseau / VLAN	Réalisé
pfSense / HA / VPN	Réalisé
Services vitaux	Réalisé
Script utilisateurs	Réalisé
Partages / DFS / FSRM	Réalisé
GLPI / architecture web	Réalisé
Proxmox / PBS	Réalisé
Zabbix	Réalisé
Graylog	Réalisé
MDT	Réalisé
Documentation technique	Réalisé

Conclusion

Le projet concernant l'entreprise HEALTH NORTH a abouti à la conception et au déploiement d'une toute nouvelle infrastructure complète et structurée organisée autour des services essentiels. Cela a permis de couvrir l'ensemble des besoins identifiés de l'entreprise, notamment en ce qui concerne la segmentation du réseau, les services critiques, la gestion des incidents, la supervision, la gestion des sauvegardes, la centralisation des logs, le déploiement des postes ou encore la mise en place d'un VPN.

Cette architecture constitue une fondation importante permettant le renforcement de la sécurité globale, de faciliter l'administration du système d'information et d'améliorer sa disponibilité.