Dépôt dossier : Fiches descriptives de projet 1 (1er dépôt)

E5 – Option « Solutions d'infrastructure, systèmes et réseaux »

Administration des systèmes et des réseaux

Énoncé

AUCUNE RÉPONSE SUR CE DOCUMENT

Notation :

Votre examen comporte :

✔ Cet **énoncé** qui vous présente le contexte et les missions à réaliser pour votre épreuve E5

✔ Une **copie à rendre** (Annexe de l'E5 au format Word) que vous devez télécharger, remplir informatiquement et déposer dans l'espace prévu à cet effet.

Renommez votre copie à rendre Word ou Excel comme suit :

E5-SISR-PROJET1_copiearendre_NOM_Prenom

Aucune version manuscrite de copie à rendre ne sera acceptée.

Toutes **vos réponses**, dont les calculs, doivent être **justifiées** pour être prises en compte.

Lorsque vous indiquez des chiffres, ils doivent être alignés avec un espace pour séparer les milliers : 1 000.

Durant la réalisation de votre sujet toutes les ressources et communication avec autrui sont autorisées et même conseillées, cependant lors des oraux d'entraînement, votre **téléphone portable doit être éteint** et tout échange avec un autre autrui est interdit durant l'épreuve. Vous êtes autorisé à naviguer uniquement sur les sites métiers. Sachez que votre connexion est tracée durant l'examen, nous sommes donc alertés en cas de fraude.

À vous de jouer !

Présentation de l'entreprise

La société HEALTH NORTH fait partie des leaders européens sur les prélèvements médicaux pour les particuliers.

Fondé en 1987 avec l'ouverture de trois laboratoires diagnostiques et d'imagerie au Danemark, le groupe s'est rapidement développé en appliquant une stratégie d'acquisition de laboratoires partenaires de qualité sur l'ensemble du continent européen.

Cette année, Health NORTH fusionne avec la grande entreprise d'hospitalisation privée, présente en Suède, en Norvège, en Finlande, en France et au Royaume-Uni. Grâce à cette fusion, la structure devient alors le leader incontesté des services diagnostiques et d'hospitalisation en Europe.

Health NORTH exploite son expertise en médecine de laboratoire, en imagerie et en pathologie pour fournir des réponses aux questions diagnostiques dans toutes les disciplines médicales. Notre catalogue de services couvre tous les aspects du diagnostic, notamment dans les domaines suivants :

- Chirurgie ambulatoire;
- Hospitalisation;
- Imagerie médicale;
- Médecine reproductive et génétique;
- Cytopathologie et biologie médicale;
- Tests spécialisés.

La biologie médicale est une composante importante du système de santé. Elle concourt au diagnostic, au dépistage, à l'évaluation des risques, au suivi des patients, etc.

Quelques chiffres :

- Nombre d'employés : 12 000 €
- Nombre de médecins : 5000
- Nombre de cliniques : 300
- Nombre d'imagerie : 1200
- Chiffre d'affaires : plus de 50 milliards (annuel)
- Nombre d'analyse : 8 millions/an

Suite à la fusion, North HEALTH se doit de travailler sur la refonte des systèmes d'information de ses cliniques et laboratoires français.

Actuellement, on distingue sur le territoire Français, plusieurs types :

- Les laboratoires de prélèvement
- Les centres d'analyse où les prélèvements sont analysés
- Les cliniques

Il y a un engagement afin de fournir un résultat d'analyse sous :

- 24h pour une analyse standard
- 72h pour une analyse complexe

Les grandes lignes du SI

L'organisation de North HEALTH est découpée en plusieurs scopes :

- **SI Interne :** permettant l'accès aux services des cliniques et laboratoires (connexion sur les postes, accès aux réseaux, partage de fichiers, applications métiers de suivi de patient, de facturation, de réservation de bloc opératoire, d'affectation de chirurgien, etc.), mais également les services de gestion du système d'information de l'entreprise.
- **SI Externe :** permettant aux patients de prendre la réservation de leurs examens, chambres et services connexes et permettant aux professionnelles de santé d'accéder au dossier patient.

Présentation des missions :

En tant que technicien système réseau, Mr Vasquez (dsi) vous missionne sur la refonte de l'architecture système et réseau de la clinique de Guadeloupe. Votre responsable a pu découper le projet en différentes missions afin de planifier la mise en production. Voici les missions identifiées par Mr Vasquez :

- **Mission 1 :** mise en place de l'architecture réseau de base
- **Mission 2 :** mise en place des services vitaux
- **Mission 3 :** mise en place de la documentation
- **Mission 4 :** mise en place des services annexes
- **Mission 5 :** mise en place de la haute disponibilité des services principaux

Les 5 missions sont dépendantes les unes des autres, et nécessitent le bon fonctionnement des services précédents. Un brief plus précis est disponible dans chacune des missions.

Dans ce 1er sujet, vous allez réaliser les missions 1, 2 et 3.

Dossier 1 : Mise en place de l'architecture réseau de base

À l'aide des annexes et de vos connaissances, suivez les questions afin de permettre une mise en production dans les meilleures conditions possibles.

1. **Mission 1 :** Identifiez les dernières adresses IP de chaque réseau et remplissez la colonne passerelle par défaut.

2. **Mission 2 :** Reproduisez le schéma en exploitant au choix une architecture physique ou virtuelle (gns3, pkt peut être utilisé pour des tests, mais pas pour le rendu final). *(Attention, dans le cadre du BTS SIO, les outils de simulation tels que packet tracer ne sont pas autorisés. Il vous faudra réaliser une reconstitution réseau sur le matériel du centre d'examen)*

3. **Mission 3 :** Réalisez la configuration LAN afin de permettre la communication intervlan.

4. **Mission 4 :** Réalisez la configuration WAN afin de permettre les accès vers le réseau internet *(éventuellement simulé)*.

Amélioration possible* :

1) Matrice de flux et la mise en étanchéité.
2) Implémentation d'un service de proxy sur les réseaux utilisateurs.
3) Rendre votre réseau compatible ipv4/ipv6 (dualstack).
4) Réaliser une sauvegarde manuelle ou automatique des équipements.

** Les améliorations possibles ne sont pas obligatoires, elles ont pour rôle de permettre à des apprenants d'aller plus loin que le sujet attendu.*

Dossier 2 : Mise en place des services de base

1. **Mission 1 :** Implémentez une machine virtuelle dans les réseaux « Service Vitaux » et dans le réseau « Service Direction ». Puis vérifier que la communication entre les deux machines est possible.
2. **Mission 2 :** Implémentez le service d'annuaire et DNS et réalisez la configuration nécessaire (unités d'organisations, groupes, utilisateurs, enregistrement direct et inversé des serveurs …).
3. **Mission 3 :** Implémentez le service DHCP.
4. **Mission 4 :** Implémentez un utilisateur dans chaque service et réaliser les tests d'authentification, de lecteur réseau, de partage de fichier …
5. **Mission 5 :** Implémentez un script de création des utilisateurs.
6. **Mission 6 :** Implémentez deux machines permettant d'héberger l'application web.

Amélioration possible* :

1) Planifiez la création d'utilisateurs provenant d'une liste Excel tous les lundis matin.
2) Implémentez les services de prise en main à distance.
3) Sécurisez les services.
4) Automatisez le déploiement d'un service web.

** Les améliorations possibles ne sont pas obligatoires, elles ont pour rôle de permettre à des apprenants d'aller plus loin que le sujet attendu.*

Dossier 3 : mise en place de la documentation

1. **Mission 1 :** Implémentez un service de gestion d'incident ;
2. **Mission 2 :** Réalisez une documentation professionnelle pouvant regrouper l'intégralité de la documentation de l'architecture ;

Amélioration possible* :

1) Inventorier de façon automatique l'ensemble des postes dans GLPI.
2) Stocker la documentation sur une plateforme de documentation.
3) Réaliser un rétroplanning des tâches réalisées ainsi qu'un planning des tâches futures.

** Les améliorations possibles ne sont pas obligatoires, elles ont pour rôle de permettre à des apprenants d'aller plus loin que le sujet attendu.*

Annexe 1 :

Problématique

En vue du projet de refonte global du SI, un cabinet a été mandaté de réaliser un préaudit en vue de la certification ISO27001. Lors de la partie analyse des risques, de nombreux risques furent identifiés :

Sécurité :

- Vol de données de santé ;
- Blocage des automates des laboratoires permettant de générer les résultats d'analyse
- Ransomware des données de santé.
- Application peu sécurisée (api en accès libre, peu de nivellement des droits d'accès aux informations patient)
- Utilisateur non nominatif dans chaque laboratoire avec des mots de passe simples (3 caractères) sans aucune stratégie de mot de passe.

Concurrence :

- Le marché est hyper concurrentiel, il y a de nombreux acteurs sur le marché, la moindre indisponibilité est visible sur une échelle nationale et soumise à une déclaration à l'ARS.
- L'application web et mobile de l'entreprise n'est pas simple d'utilisation.
- Les services proposés dans les cliniques et laboratoires sont en dessous des services de la concurrence notamment sur le fort enjeu du wifi.
- L'aide pour le dépistage du COVID est un accélérateur pour le projet informatique.

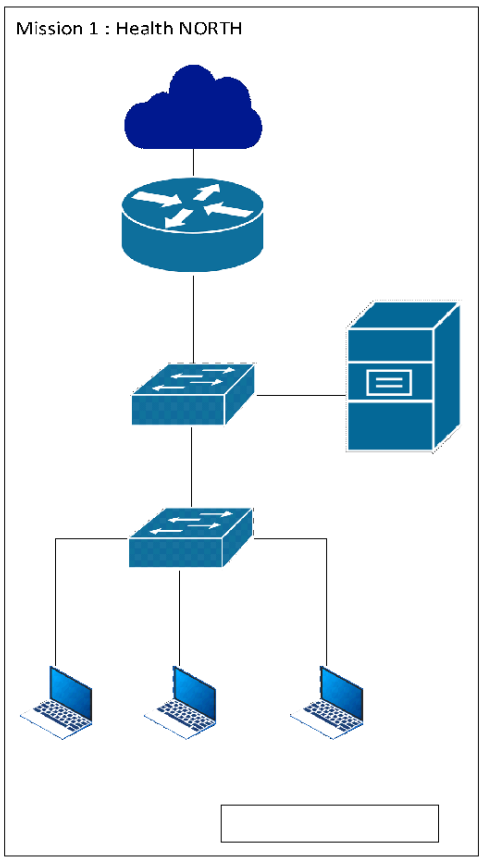
Exploitation :

- La solution devient trop complexe à administrer, les incidents s'enchaînent.
- Les serveurs commencent à saturer tant sur la partie performance que pour le stockage des données.
- Les applications sont de plus en plus difficiles à maintenir dû à des développements from scratch et sans framework.
- L'IT entre chaque laboratoire est hétérogène, cela provoque des coûts supplémentaires afin d'infogérer les différents services.

Annexe 1 : Dossier 1

Architecture réseau cible

Mr Vasquez souhaite prévoir la mise en place de la configuration réseau permettant de donner l'accès au réseau internet de l'organisation à l'ensemble de la clinique. Voici le schéma proposé par votre responsable :



Le schéma a été réalisé à l'aide de l'outil https://draw.io et les images proviennent de la bibliothèque https://vecta.io

Voici les préconisations proposées par Mr Vasquez :
HN-GDLP-R1 doit pouvoir assurer :

- Le routage intervlan ;
- Le nat ;
- La mise en place d'un serveur mandataire ;
- L'accès à distance du service et du réseau ;

HN-GDLP-SD1 et HN-GDLP-SA1 doivent pouvoir assurer :

- La segmentation des flux.
- L'accès à distance de l'équipement.

La direction générale du groupe a prévu un découpage réseau strict :

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

Annexe 2 : Dossier 2

Mr Vasquez vous félicite pour l'implémentation réseau et vous demande désormais de commencer la configuration des services vitaux de l'entreprise :

- Un service d'annuaire
- Un service de résolution de nom ;
- Un service de distribution de configuration réseau ;
- Un service de partage de fichier ;
- Un service d'hébergement web ;

Voici les précisions pour chacun des services :

- **Le service d'annuaire**

L'annuaire de l'entreprise doit permettre de recevoir les collaborateurs

	Service	Prenom	Nom	Tel
1	Laboratoire	Zenaida	Tucker	03 09 02 60 20
2	Direction	Camille	Cameron	06 17 07 66 84
3	Informatique	Chaney	Molina	06 78 60 70 46
4	Laboratoire	Hamish	Singleton	04 80 52 33 14
5	Chirurgie	Camden	Norman	06 61 92 74 53
6	Direction	Deanna	Ratliff	06 04 21 68 06
7	Chirurgie	Zorita	Morgan	02 08 61 80 83
8	Chirurgie	Yardley	Gill	04 37 90 07 82
9	Informatique	Elijah	Joyce	04 26 50 66 80
10	Informatique	Shannon	Sharp	02 26 04 85 33

Les utilisateurs devront être créés à l'aide d'un script powershell, ce dernier devra être en mesure de calculer leur login (ex. : pnom), de calculer leur adresse email prenom.nom@health-north.fr. Il est également attendu de les affecter dans les bonnes unités d'organisation (ex. : OU=Laboratoire, OU=Utilisateurs, DC=Guadeloupe, DC=health-north ,DC=FR)

Les utilisateurs auront des profils itinérants, leurs partages de fichier seront implémentés de façon automatique par des lecteurs réseaux, les utilisateurs ne pourront pas lancer l'invite de commande Windows et recevront une politique de gestion de mot de passe basé sur préconisation de l'ANSSI. Selon les services, ils recevront également un fond-écran et une liste d'applications selon la matrice ci-dessous :

Service	VLC	7zip	Acrobat Reader	Firefox	Putty	Winscp
Laboratoire	x		x			
Chirurgie	x					
Informatique	x	x	x	x	x	x
Direction	x		x			

- **Le service de distribution de configuration réseau**

L'ensemble des services comportant des utilisateurs doivent pouvoir recevoir des adresses IP de façon dynamique. Les baux des réseaux wifi sont limités à 2 heures alors que les réseaux classiques délivrent des baux de 8h.

Le service DHCP distribue :

- Des adresses IP dans les réseaux comportant des utilisateurs *(les 50 premières adresses IP sont réservées pour une attribution statique)*.
- Une passerelle par défaut.
- Un service de temps.
- Un service de déploiement.
- Plusieurs services de résolution de nom.

- **Le service de résolution de nom**

Le service de résolution de nom est en mesure de résoudre les noms de domaines et nom des équipements pour le réseau LAN exclusivement.

- **Le service de partage de fichier**

Le service de partage de fichier doit pouvoir permettre d'héberger plusieurs répertoires et une politique d'accès :

- Seuls les utilisateurs habilités peuvent voir et consulter les répertoires
- Il est interdit de déposer des fichiers types vidéo (avi, mkv, …).
- Chaque utilisateur à un profil itinérant et un partage personnel, et chaque service possède un partage commun (ex. : SERVICE_COMMUN) ouvert avec les autres membres des autres services.

Voici la politique d'accès aux répertoires :

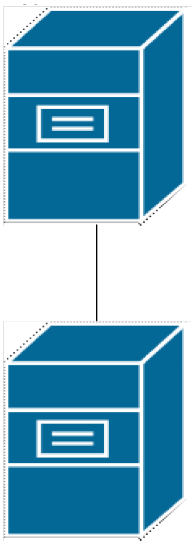
Dossier / Service	CE	Laboratoire	Chirurgie	Informatique	Direction
Laboratoire	r	rw			
Chirurgie	r		rw		
Informatique	r			rw	
Direction	rw	r	r	r	rw

- **Le service d'hébergement d'application web**

La partie service web doit permettre l'hébergement de l'application web de l'entreprise *(cette dernière pourra être simulée par la mise en place d'un service telle que GLPI ou un wordpress, ou un code quelconque avec du code serveur et une base de données)*.

L'organisation souhaite sécuriser l'accès à ce service et souhaite une isolation forte entre les services.

Afin de respecter les bonnes pratiques, il est conseillé de respecter un serveur = un service, il est donc préconisé d'installer le service web et le service de base de données sur deux machines distincte (voir schéma ci-dessous)



Annexe 3 : Dossier 3

Après la mise en place de vos différents services, votre responsable vous demande la réalisation d'une documentation de votre architecture, cette dernière devra comporter les éléments suivants :

- Un schéma réseau (logique et physique) avec un outil professionnel ;
- Un plan d'adressage réseau ;
- Un plan de sauvegarde ;
- La liste de vos préconisations d'implémentation de service (argumentés) pour le nouveau système d'information ;
- La documentation des services et équipements implémentés ;