

MSPR

“Conception et protection d'une base de données”

Intervenant : Allan Kinic - allan.kinic@mail-formateur.net

Mise à jour : 02/10/2025

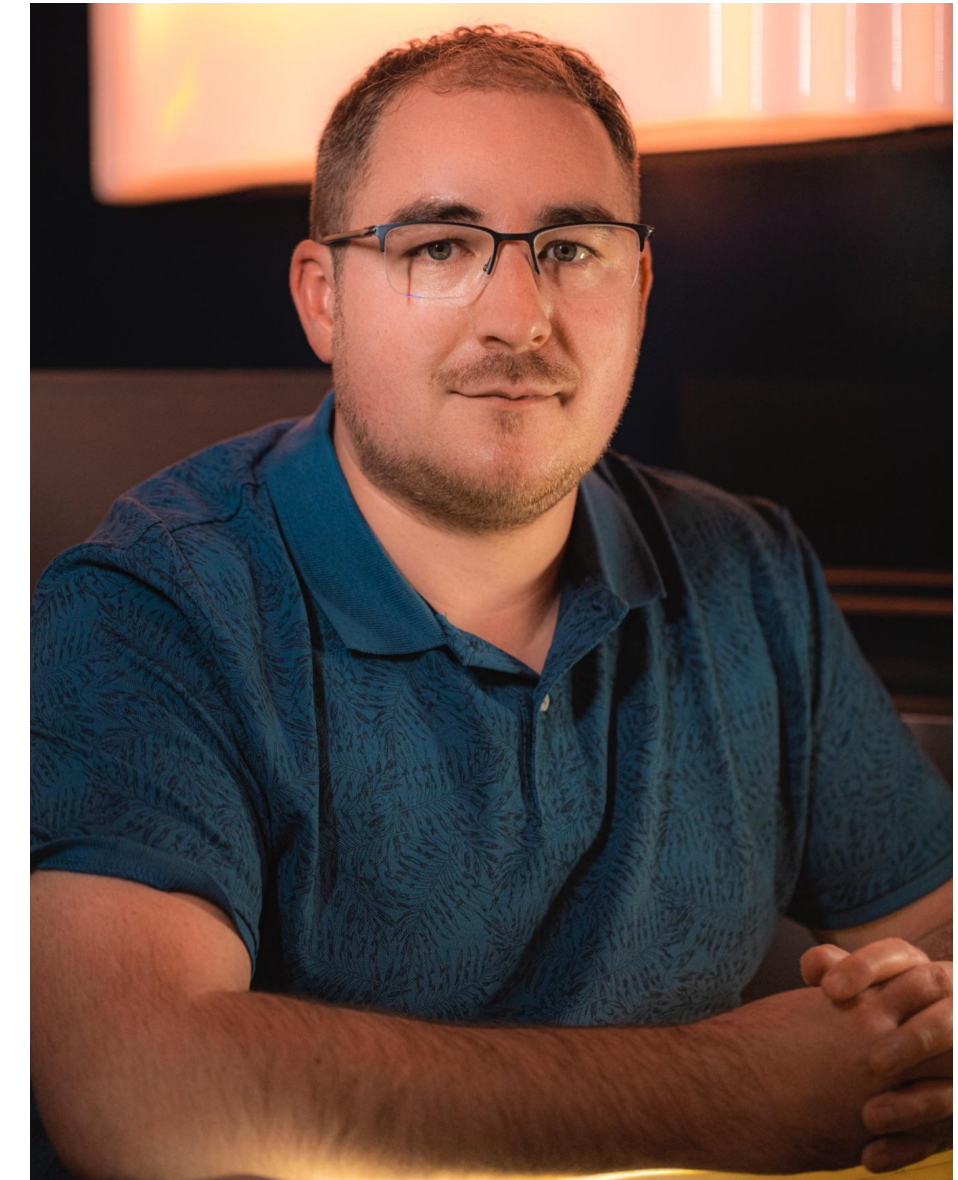


Membres de HEP
EDUCATION

Présentation

Formateur Référent

- Accompagne les étudiants tout au long de l'année
- Point de contact privilégié pour toutes vos questions et besoins
- Fait le lien avec les formateurs et l'équipe pédagogique en cas de difficulté
- Aide à comprendre les cours, les compétences et la pédagogie de la formation
- Soutient l'organisation, la motivation et la progression individuelle
- Oriente et conseille sur la poursuite d'études ou la carrière professionnelle
- Suit l'évolution de chacun via des échanges
- Favorise la réussite, l'autonomie et l'épanouissement de tous les étudiants



Allan KINIC :

allan.kinic@mail-formateur.net

Les modules

- Coaching : Conception et protection d'une base de donnée
- Comprendre la cybersécurité: Enjeux, acteurs etc
- Ateliers pratique (RootMe)
- Atelier Red Team

Les certifications

- Certification Comptia Sécurité +
- Certification Google Cloud Digital Leader
- Google Cybersecurity Engineer

MSPR “Conception et protection d'une base de données”

COMPÉTENCES ÉVALUÉES :

- Concevoir et sécuriser une base de données.
- Justifier le choix d'un SGBD
- Administrer les bases de données avec méthode selon la configuration requise pour leur mise en production
- Mesurer et analyser les performances pour optimiser le stockage en vue de faciliter les accès.
- Améliorer les performances des bases de données en optimisant l'emplacement des stockages.
- Mettre en place un plan périodique de restauration permettant de vérifier l'intégrité des données.
- Surveiller, analyser et auditer les bases en utilisant les outils et fichiers appropriés.
- Utiliser des outils spécifiques de sauvegarde

PHASE 1

Durée de préparation : 54 heures

Mise en œuvre : Travail d'équipe constituée de 3 apprenants

Calendrier :

18/11 - Matin

26/11 - Journée

27/11 - Aprem

02/12 - Matin

10/12 - Journée

11/12 - Matin

PHASE 2

Objectif : mettre en avant et démontrer que les compétences visées par ce bloc sont bien acquises

Moyen : L'équipe utilise un support de présentation

Durée totale par groupe : 50 mn se décomposant comme suit :

20 mn de soutenance orale par l'équipe.

30 mn d'entretien collectif avec le jury (questionnement complémentaire).

Jury d'évaluation : 2 personnes (binôme d'évaluateurs) par jury

Calendrier :

15/12 - Aprem

Le sujet

I - CONTEXTE

NFL IT – National Football League Information Technology est une société de services numériques (SSII) créée au début des années 2020 par deux associés français. Elle fournit des prestations d’infogérance, d’audit, de conseil et d’intégration orientées infrastructures informatiques pour des organisations multisites à forts enjeux de disponibilité.

Historiquement, NFL IT s’est spécialisée dans l’accompagnement des équipes de football américain (gestion d’équipes, statistiques, applicatifs métiers), domaine que les fondateurs connaissent bien pour y avoir exercé comme développeurs chez l’éditeur de référence du secteur.

Depuis 2020, NFL IT est titulaire d’un contrat d’exclusivité de plusieurs millions de dollars avec la National Football League (NFL), qui regroupe 32 franchises. L’entreprise compte plus de 100 collaborateurs (environ 30 techniciens/ingénieurs itinérants, 30 personnels support, et ~40 fonctions supports). Le siège est situé à Kansas City (Missouri) ; les clients sont répartis sur tout le territoire américain.

Pour ses besoins d’hébergement, NFL IT s’appuie également sur un datacenter en France (Roubaix) pour certaines applications clients et internes. Dans la continuité de cette stratégie, l’entreprise initie le programme “Seahawks monitoring”, destiné à réduire les interventions sur site, industrialiser la supervision et améliorer la maintenabilité du parc chez les franchises, avec une perspective d’extension vers la ligue européenne (ELF).

Enjeu business : aujourd’hui, l’absence d’outils unifiés de maintenance et de visibilité entraîne des déplacements coûteux et des délais de résolution élevés. NFL IT porte donc une feuille de route visant à standardiser la collecte d’informations techniques, centraliser la supervision, et outiller le support pour intervenir à distance lorsque c’est possible.

II – CAHIER DES CHARGES

NFL IT a racheté la société NordTransit Logistics (NTL), une PME de logistique implantée dans les Hauts-de-France. NordTransit Logistics (NTL) opère un siège à Lille et trois entrepôts à Lens (WH1), Valenciennes (WH2) et Arras (WH3). Un cross-dock saisonnier, c'est-à-dire une zone de transit rapide des marchandises sans stockage, est activé lors des périodes de forte activité (montées de charge e-commerce, soldes) avec des moyens informatiques volontairement limités.

Chaque entrepôt dispose d'un lien opérateur managé d'environ 200 mégabits par seconde, tandis que le siège bénéficie d'un accès plus capacitaire. La croissance des volumes et des échanges entre sites accroît la dépendance aux services centraux et met en évidence des limites de résilience réseau, de supervision orientée « service » et de gouvernance sur les usages Microsoft 365.



L'activité quotidienne se déroule sur deux amplitudes qui se chevauchent : arrivages et réception dès 5 h 30, puis préparation et expédition jusqu'à une fermeture administrative autour de 18 h 30, avec des ouvertures possibles le samedi matin pour absorber les pics. Les créneaux techniques réellement sûrs pour intervenir sont donc courts et principalement nocturnes. En journée, tout incident doit être résolu sans immobiliser les quais ni interrompre l'impression d'étiquettes, la lecture par terminaux radiofréquence (lecteurs mobiles en Wi-Fi) et les échanges électroniques avec les transporteurs (échanges de données informatisés).

II – CAHIER DES CHARGES

NTL emploie environ 240 personnes en vitesse de croisière et peut monter autour de 300 avec l'intérim en haute saison. Environ 180 salariés travaillent dans les entrepôts, organisés en équipes « matin » et « après-midi » et renforcés lors des pointes. Chaque site est piloté par un responsable d'entrepôt, appuyé par deux chefs de quai (un par amplitude) et par des encadrants de proximité dédiés à la préparation, à la réception et au contrôle qualité.

La planification transport, le service client et l'ordonnancement regroupent une quinzaine à une vingtaine de personnes présentes sur une large plage horaire, de l'ordre de 6 h à 19 h, les chauffeurs étant majoritairement fournis par des transporteurs partenaires. Les fonctions support rassemblent environ 18 à 20 personnes hors informatique, couvrant les ressources humaines (administratif et lien avec l'éditeur de paie), la finance et la comptabilité (achats, facturation), le commerce et l'administration des ventes pour les grands comptes, ainsi que la qualité, la sécurité et l'environnement. L'équipe informatique reste volontairement compacte mais réaliste pour ce profil de PME : un responsable en charge des priorités et du budget, un administrateur systèmes et réseau itinérant, un technicien support et un alternant focalisé sur l'inventaire et des automatisations simples. Pour sécuriser l'exploitation au quotidien, un réseau de référents « super-utilisateurs » du système d'entrepôt est identifié sur chaque site et pour chaque amplitude, même si leur reconnaissance formelle et leur temps dégagé restent à préciser.

II – CAHIER DES CHARGES

Au siège, une vingtaine de machines virtuelles hébergent les services internes, sous Linux et sous Windows. L'annuaire d'entreprise Microsoft Active Directory et le service de noms de domaine (DNS) sont centralisés à Lille. Malgré l'adoption de Microsoft OneDrive et SharePoint, un serveur de fichiers local conserve des partages critiques (historiques, macros, modèles), ce qui entretient un double modèle de travail et complexifie la traçabilité des habilitations. L'application cœur de métier, le système de gestion d'entrepôt (Warehouse Management System), fonctionne sur une machine virtuelle Linux avec une base de données MySQL ; son indisponibilité provoque l'arrêt immédiat des opérations de réception et d'expédition sur les quatre sites entre 5 h 30 et 18 h 30. Les sauvegardes s'appuient sur un serveur de stockage en réseau (NAS) et des scripts, sans campagne de restauration planifiée ni objectifs clairs sur le temps de reprise et la perte de données acceptables. Restaurer en urgence une machine virtuelle est maîtrisé, mais l'absence de tests réguliers, de copies immuables et d'externalisation systématique expose l'entreprise à un risque opérationnel élevé pour un service aussi critique. La supervision demeure surtout technique (présence d'hôtes, capacité disque) et couvre insuffisamment l'expérience service, par exemple la santé du système d'entrepôt, les délais d'impression d'étiquettes, l'état de l'annuaire, du DNS, de la réplication MySQL ou des flux EDI vers les transporteurs.

II – CAHIER DES CHARGES

Sur le périmètre réseau et services connexes, le pare-feu et l'accès distant sécurisé (VPN) ont été déployés par un intégrateur sans contrat de maintenance formalisé ; une prestation annuelle assure les mises à jour, le reste se traite à la demande. La téléphonie sur IP et l'impression sont externalisées mais intégrées au réseau local et opérées au quotidien par l'informatique interne. Le site web institutionnel est géré par une agence. L'application de gestion des ressources humaines (paie et temps) est fournie en mode service en ligne (SaaS), l'équipe interne assurant l'intégration des accès et des échanges. Les liens des entrepôts, dimensionnés au minimum viable, suffisent pour le système d'entrepôt, la bureautique et les scans, mais ils deviennent tendus avec les usages collaboratifs en temps réel (Teams), les synchronisations Microsoft 365 et les pics d'échanges transporteurs.

La modernisation vers le cloud est engagée côté collaboration avec Microsoft 365 ; l'annuaire cloud Microsoft Entra ID est en place. L'authentification multifacteur n'est activée pour l'instant que pour l'équipe informatique, ce qui n'est plus en ligne avec l'exposition réelle liée aux accès distants, à la messagerie et au partage de liens externes. Les droits sur OneDrive et SharePoint reposent largement sur l'héritage par défaut, d'où une granularité faible et un risque de surexposition de documents. Aucune machine virtuelle n'a encore été testée dans Microsoft Azure et il n'existe pas de landing zone cloud. Plusieurs services applicatifs en ligne se sont ajoutés au fil de l'eau ; quand l'intégration à Entra ID est simple elle est utilisée, sinon des comptes spécifiques sont créés, ce qui disperse les identités et rend la révocation d'accès hétérogène.

II – CAHIER DES CHARGES

Le support aux utilisateurs repose sur un outil de ticketing, mais la plupart des sollicitations arrivent encore par téléphone, avec une saisie des tickets a posteriori. Les indicateurs de support sont donc incomplets et certaines demandes mal cadrées, ce qui fausse la priorisation et génère des retours atelier inutiles.

L'informatique couvre principalement le jour ouvré, avec une astreinte informelle pour certaines opérations sensibles. La documentation existe mais reste dispersée dans des dossiers partagés. L'adoption de Teams et de Microsoft 365 progresse à des rythmes différents selon les sites, freinée par l'hétérogénéité des pratiques et par l'absence de responsabilité fonctionnelle claire sur les espaces collaboratifs.

En synthèse, NTL fonctionne avec des fenêtres de maintenance très courtes, une forte dépendance aux services centraux et une équipe informatique réduite. Les enjeux majeurs tiennent à la continuité du système d'entrepôt et de ses flux, à la résilience réseau des sites et à l'unification des identités et usages Microsoft 365. Le reste relève de la mise en qualité : sauvegardes réellement restaurables, supervision orientée service, accès distants sécurisés et gouvernance claire des espaces.

III – LES BESOINS EXPRIMÉS

La direction de NFL IT confie à votre équipe la conception et l'industrialisation de la nouvelle base WMS sur laquelle s'appuiera l'application de gestion d'entrepôt. Vous êtes responsables du choix technologique, de l'architecture de haute disponibilité, de la sécurité, des performances et de l'exploitabilité.

1/ Modèle de données et intégrité

Le schéma doit couvrir et relier les entités suivantes avec règles d'intégrité explicites et contraintes implémentées :

- Clients : séparation des données par client.
- Sites / entrepôts : chaque stock / transaction est rattachée à un site.
- Articles / SKU : catalogue unique avec dimensions/poids indispensables aux calculs d'expédition.
- Localisations : où et comment est stocké l'article.
- Stock actuel
- Mouvements : entrées / sorties horodatées.

2/ Exigences de performance et de continuité

Vous êtes encouragés à optimiser au mieux votre base de données en imaginant les usages (requêtes) les plus fréquents. Vous devrez prendre en compte un RTO à 1h et un RPO de 15 min.

III – LES BESOINS EXPRIMÉS

3/ Choix SGBD et architecture HA / PRA

Justifier le SGBD retenu et concevoir une architecture HA adaptée au contexte de l'entreprise. Décrire le PRA en cas de perte de la base de données et les éléments permettant sa mise en place (sauvegardes, tests de restauration).

4/ Sécurité des accès

Définir la politique d'accès à la base de données en respectant le principe de moindre privilège.

5/ Supervision et exploitation

Proposer un tableau de bord contenant 5 indicateurs critiques pour la supervision de la base de données. Ils peuvent être orientés hardware et software. Pour chaque indicateur, donner les seuils d'alerte et prévoir une procédure d'analyse en cas d'alerte.

Les livrables

IV – LES LIVRABLES

À l'issue de la mission, NFL IT attend une série de livrables clairement identifiés, qui permettront à la fois de vérifier la qualité du travail accompli et d'utiliser l'architecture livrée.

1. Le dossier

Le dossier devra contenir les éléments suivants :

- Document d'architecture technique : MCD et MLD, justification du SGDB, schémas d'architectures, hébergement et hardware, index et optimisations, politiques d'accès, politiques de sauvegardes, etc.
- Plan de reprise d'activité
- Guide de supervision avec indicateurs, seuils et procédures de remédiation.
- Démarche suivie pour l'optimisation de la base de données (usages, tests, scénarios, résultats obtenus, etc.).

2. Support de soutenance

En complément des livrables, l'équipe projet devra préparer un support de présentation destiné à la soutenance finale devant le client (public technique). Il est important de souligner que l'évaluation de cette MSPR repose sur la combinaison des trois éléments suivants :

- la qualité du travail réalisé au cours du projet,
- la pertinence et l'exhaustivité des livrables remis et la capacité de l'équipe à présenter, justifier et valoriser ce travail lors de la soutenance orale.

IV – LES LIVRABLES

Les équipes devront donc s'assurer que la soutenance reflète bien l'ensemble des compétences attendues, en démontrant à la fois la maîtrise technique et la capacité à communiquer efficacement auprès d'un client professionnel.

Les ressources

V – RESSOURCES FOURNIES

Dans le cadre de votre mission, l'équipe IT de NFL met à disposition les documents d'infrastructure existants de l'entreprise NordTransit Logistics (NTL).

Il est à noter que ces documents sont le reflet d'une infrastructure qui a connu peu de modifications structurelles ces dernières années, les budgets de l'entreprise ayant été majoritairement concentrés sur la croissance opérationnelle et d'autres postes de dépenses que l'IT.

De ce fait :

- L'exhaustivité et la date de dernière mise à jour de ces documents ne sont pas garanties.
- Ils décrivent l'état existant de l'infrastructure (matériels, réseaux, services) mais peuvent manquer de précision sur certains détails de configuration, notamment ceux confiés historiquement à des prestataires externes.

V – RESSOURCES FOURNIES

Annexe A — Plan d’adressage et statut des sites NordTransit Logistics (NTL)

| Site / Rôle | Réseau IP local (LAN) | Masque | Passerelle (pare-feu/routeur) | Statut | Remarques succinctes |
|-----------------------------|-----------------------|--------|-------------------------------|---------------------------------|----------------------------------|
| Siège social (Lille) | 192.168.10.0 | /24 | 192.168.10.254 | Opérationnel | Services centraux (AD/DNS, VMs) |
| Entrepôt WH1 (Lens) | 192.168.20.0 | /24 | 192.168.20.254 | Opérationnel | Pas de lien de secours documenté |
| Entrepôt WH2 (Valenciennes) | 192.168.30.0 | /24 | 192.168.30.254 | Opérationnel | QoS/VLAN non documentés |
| Entrepôt WH3 (Arras) | 192.168.40.0 | /24 | 192.168.40.254 | Opérationnel | Impression/étiquettes critique |
| Cross-dock (CDK) | 192.168.50.0 | /24 | 192.168.50.254 | Opérationnel (saisonnier) | Moyens IT réduits |
| Landing Zone Azure | À définir | — | À définir | Réservé / planification à faire | Hub/Spoke non défini |

V – RESSOURCES FOURNIES

Annexe B — Équipements principaux NordTransit Logistics (NTL)

| Type d'équipement | Désignation / Modèle | Nb. | Localisation | Spécifications / Rôle principal |
|----------------------------|--------------------------------|-----|--------------------|---|
| Hyperviseur | Dell PowerEdge R630 | 1 | Lille (Siège) | 2× Xeon E5-2630 v3, 128 Go RAM, VMware ESXi 6.5 |
| Stockage (VMs) | NAS (6 To utiles en RAID5) | 1 | Lille (Siège) | Disques SAS 10K tr/min, dépôt sauvegardes |
| Pare-feu périmètre | Fortinet FortiGate 80D | 1 | Lille (Siège) | Sécurité périmètre, terminaison VPN site-à-site |
| Routeurs/pare-feu distants | DrayTek Vigor 2860 | 3 | WH1, WH2, WH3 | VPN site-à-site vers le siège |
| Switchs d'accès | 24 ports (marque non précisée) | 4 | WH1, WH2, WH3, CDK | Distribution LAN locale |
| Postes de travail | PC fixes + terminaux légers | ≈65 | Tous sites | Windows 11 (siège), Windows 7/10 légers aux quais |
| Postes téléphoniques | Cisco IP Phone | ≈70 | Tous sites | Téléphonie IP (PoE) connectée au LAN |
| Passerelle SIP | Logiciel/équipement opérateur | 1 | Lille (Siège) | Terminaison du trunk SIP externalisé |

V – RESSOURCES FOURNIES

Annexe C — Machines virtuelles et rôles NordTransit Logistics (NTL)

| Nom de la VM | Système | Rôle principal | Adresse IP | Enjeu / Criticité |
|--------------|---------------------------------------|--|---------------|--|
| IPBX-VM | Linux (CentOS) | Serveur logiciel de téléphonie (IPBX) | 192.168.10.40 | Point de défaillance unique pour les appels |
| WMS-DB | Linux (Ubuntu 20.04) | Base MySQL du système d'entrepôt (WMS) | 192.168.10.21 | Base critique pour réception/expédition |
| WMS-APP | Linux (Ubuntu 20.04) | Application WMS | 192.168.10.22 | Serveur d'application critique |
| DC01 | Windows Server (édition non précisée) | Contrôleur de domaine principal (AD/DNS) | 192.168.10.10 | Redondé par DC02 |
| DC02 | Windows Server (édition non précisée) | Contrôleur de domaine secondaire | 192.168.10.11 | Haute disponibilité AD/DNS |
| SUPER-01 | Windows Server (édition non précisée) | Supervision technique (Zabbix) | 192.168.10.50 | Supervision surtout technique, partielle côté services |

Merci !

Intervenant : Allan Kinic - allan.kinic@mail-formateur.net

Membres de **HEP**
EDUCATION