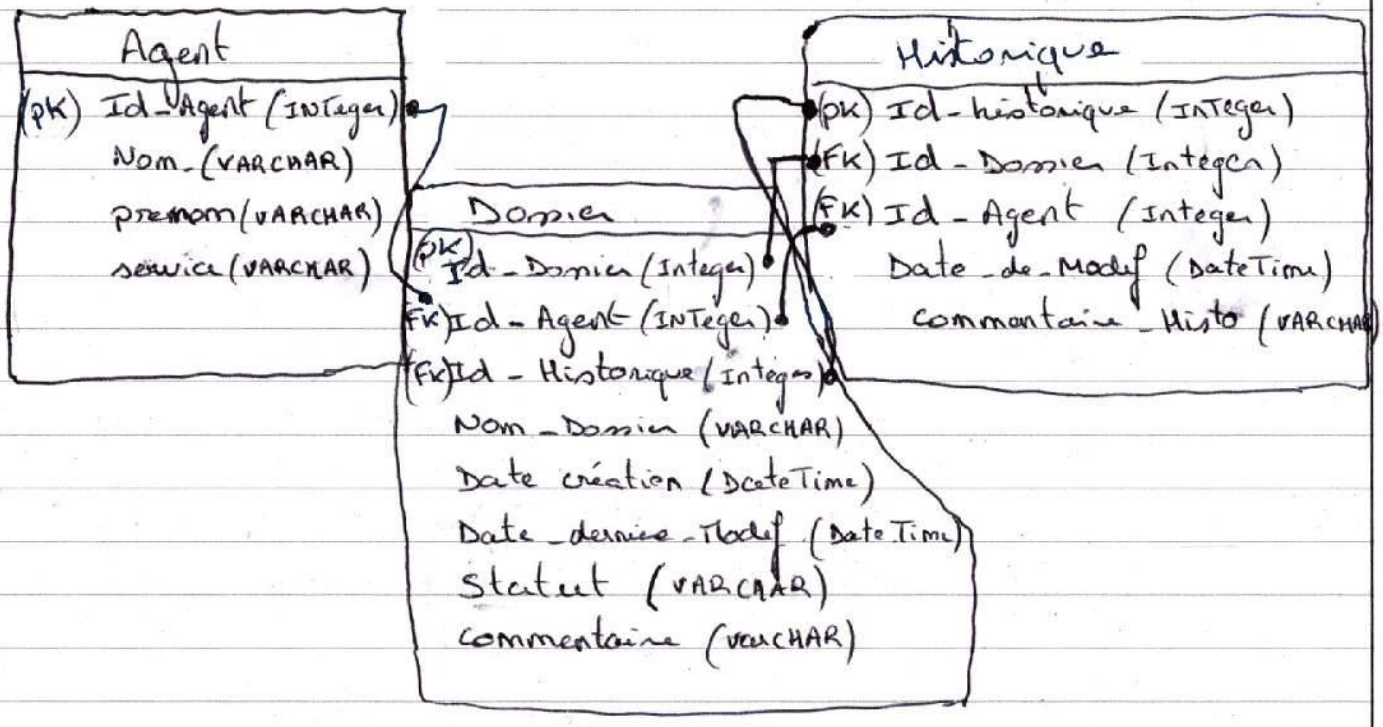
Intitulé de l'épreuve : Informatique

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Etape 1 :

Question 1 : Le MLD est le suivant :



Les liens entre les tables sont établis grace aux clés primaires et aux clés étrangères.

Les cardinalités sont :

Agent 1,n ——— 1,n Dossier

Dossier 1,n ——— 1,n Historique 1,n ——— 1,n Agent

2) La modélisation se fait sur les 3 tables principales : Agents, Dossier, Historique.

L'aspect collaboratif est pris en charge à travers la table Historique qui fait le lien entre Id_Historique de collaboration et les différents Id_Agent et Id_Dossier. La table Historique conserve chaque modification apportée par les agents.

Ainsi les agents peuvent intervenir en temps réel sur le dossier

Question 2 : Architecture cible

L'application traitant les dossiers sensibles sera positionnée dans une DMZ interne et sécurisé pour les accès aux agents internes.

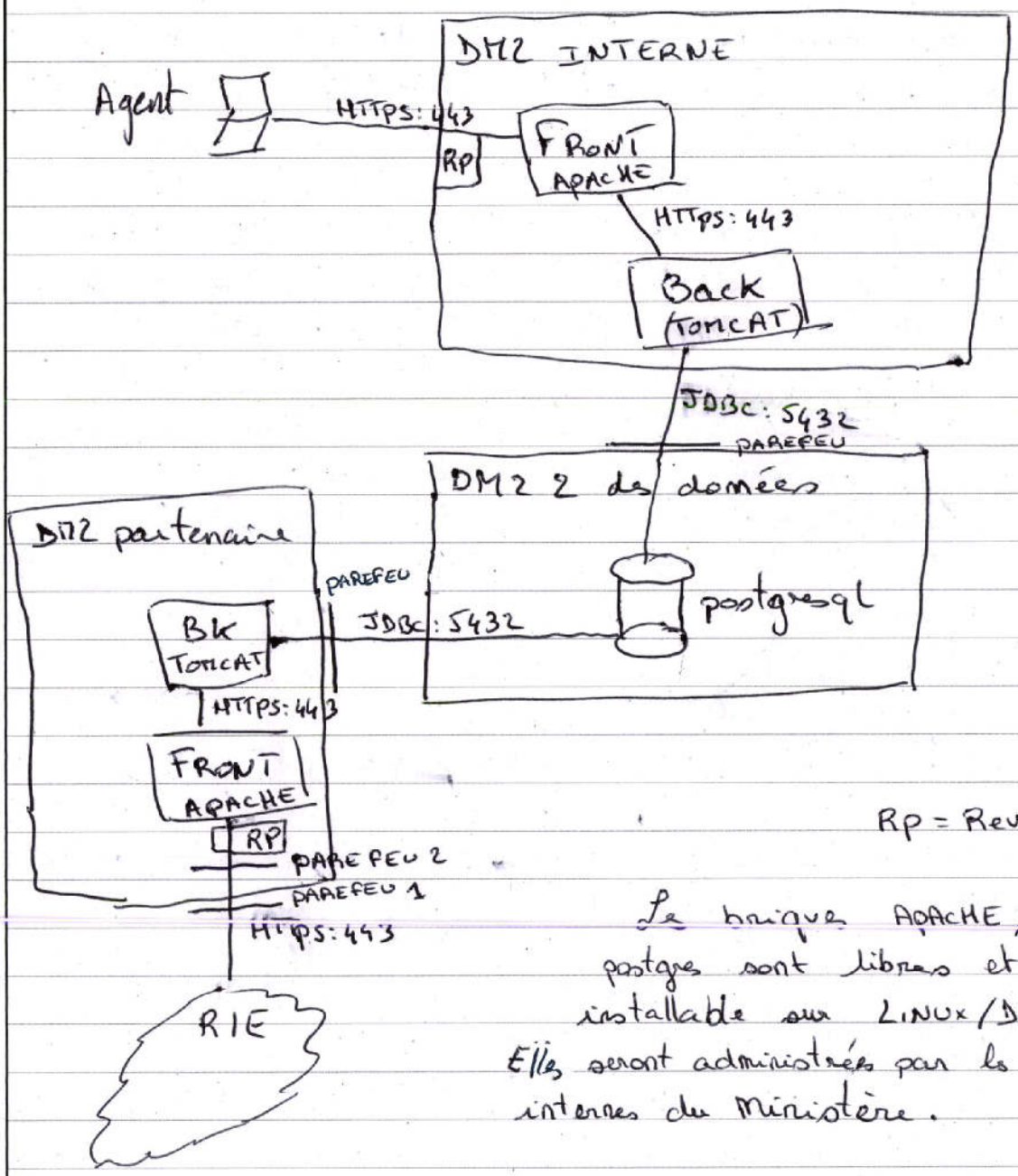
L'application pour les partenaires sera déployer dans une DMZ partenaire afin de l'isoler

La Base de données (BDD) sera positionner dans une DMZ pour les données (dédiée aux données).

L'application sera réalisée avec un framework de développement comme SpringBoot compatible avec le CCT des ministères dont le code est en Java ("cadre de cohérence technique")
La BDD sera une Base Postgresql isolé dans sa DMZ 2
Les serveurs sont des serveurs LINUX de type DEBIAN.

N° 2.111

schema simplifié :



Rp = Reverse proxy

Les briques APACHE, TOMCAT et postgre sont libres et facilement installable sur LINUX/DEBIAN. Elles seront administrées par les equipes internes du Ministère.

Question 3° : Backlog

1)

- En tant que responsable du dossier, je veux créer le dossier afin qu'il soit accessible aux agents traitant.
- En tant qu'agent traitant, je veux accéder au dossier afin de contribuer à celui-ci par mes commentaires.
- En tant que partenaire je veux accéder au dossier en lecture afin de suivre son evolution.

N° 3.1111

2)

- Coté metier il faut définir une personne qui sera la MOA sur le projet ou le chef de product.

- Il faut associer le délégué à la protection des données afin d'avoir ses conseils sur le traitement des données.

- Il faudra également associer le responsable ou fonctionnaire de sécurité des systèmes d'information

Question 4 :

1) Il faut un comité projet pour suivre l'avancement des projet dans le temps. Et un comité technique chargé de la mise en oeuvre du projet.

2) Les trois etapes clés du workflow sur le projet sont :

1) => La définition des besoin representer par la MOA

2) => La conception et l'intégration des fonctionnalités assurées par les equipes MOE qui assurera les tests en lien avec la MOA qui validera le livrable finale.

3) La phase de déploiement - qu'il faut valider qui permettra d'ouverture du service en production après Homologation

N° 4.1.M

Intitulé de l'épreuve : Informatique

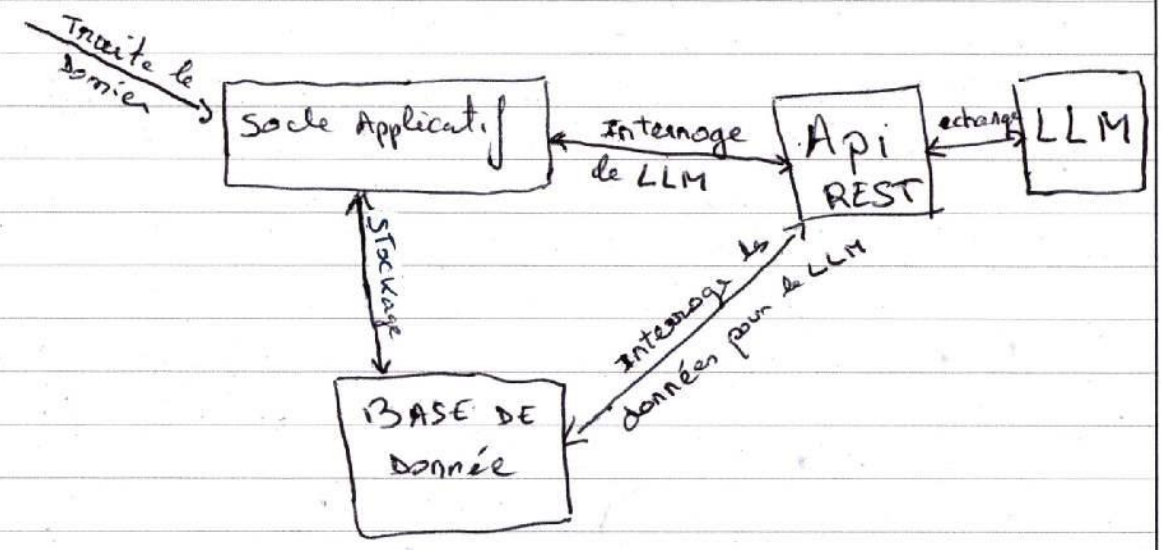
Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

Etape 2 :

Question 1 : schema de flux

1) Agent



2) Authentification des agents via le SSO interne en lien avec l'IDP (AROBAS)

- filtrage des requetes via l'Api REST et sécurisation via le protocole d'autorisation Oauth avec jeton JWT

- Journalisation de tous les evenements dans l'application a travers un fichier de log et une centralisation des log (type Syslog)

N° 5.1.M

Question 2 : Sécurité

1) Risque lié à la mauvaise interprétation des données par le LLM ou d'une compromission extérieur du LLM pour orienter les décisions des agents traitant.

- Risque d'accès aux données de la BDD si le LLM est compromis.

2) Il serait envisageable de placer un système de note sur les reponses fourni par le LLM afin de verifier le poids de sa reponse. Couplé à une verification d'un Hash ou d'une empreinte lier aux données en Base. Cela indique une note / poid visible par l'agent dans l'application.

Question 3 :

L'ajout du LLM impacte le backlog car cela ajoutera cette fonctionalité à mettre en place tant dans l'organisation que dans les fonctions et taches à prévoir.
De plus cela nécessite d'incorporer à l'equipe en place une compétence IA et un architecte dédié à l'IA. (expert)

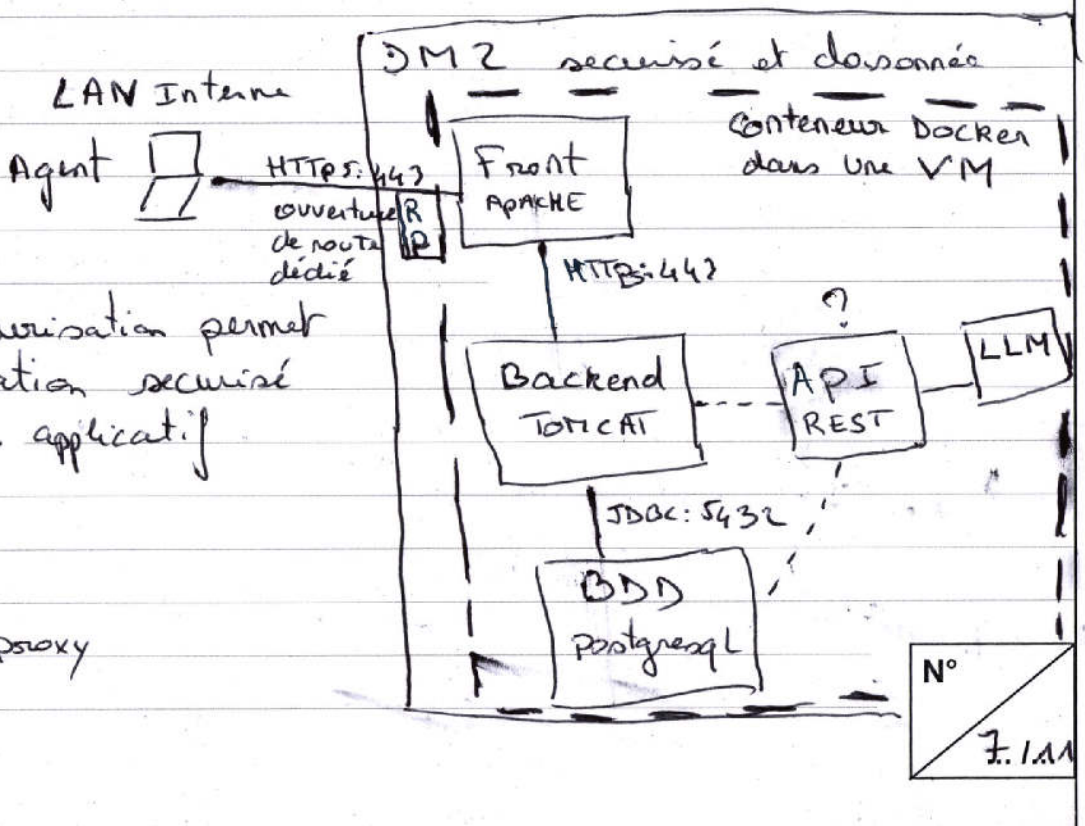
N° 6.1

Etape 3 :

Question 1 :

Il sera possible d'isoler ce service autonome dans une nouvelle DMZ sécurisé. Et de positionner les ressources dans un Conteneurs type Docker.
Nous conserverons l'applications qui ne nécessitera pas un nouveau développement pour eviter la différence de version à gérer. Et il faudra supprimer les autres accès la Base de données.
La Base de donnée sera une nouvelle Base dédiée a ce service autonome.
La question reste à savoir si il faut conserver le LLM sur cette instance. Si oui alors il s'agira d'une nouvelle instance LLM dédiée placer dans le conteneur

L'accès à l'application pourra se faire à travers un système de compte interne à l'application et des ouvertures de route dédiés aux pc des agents. Il pourrait être envisageable de mettre en place un IDP et un annuaire mais cette infra serait lourde pour seulement quelques agent.



La conteneurisation permet la segmentation sécurisé au niveau applicatif

Rp : Reverse proxy

N° 7.1.11

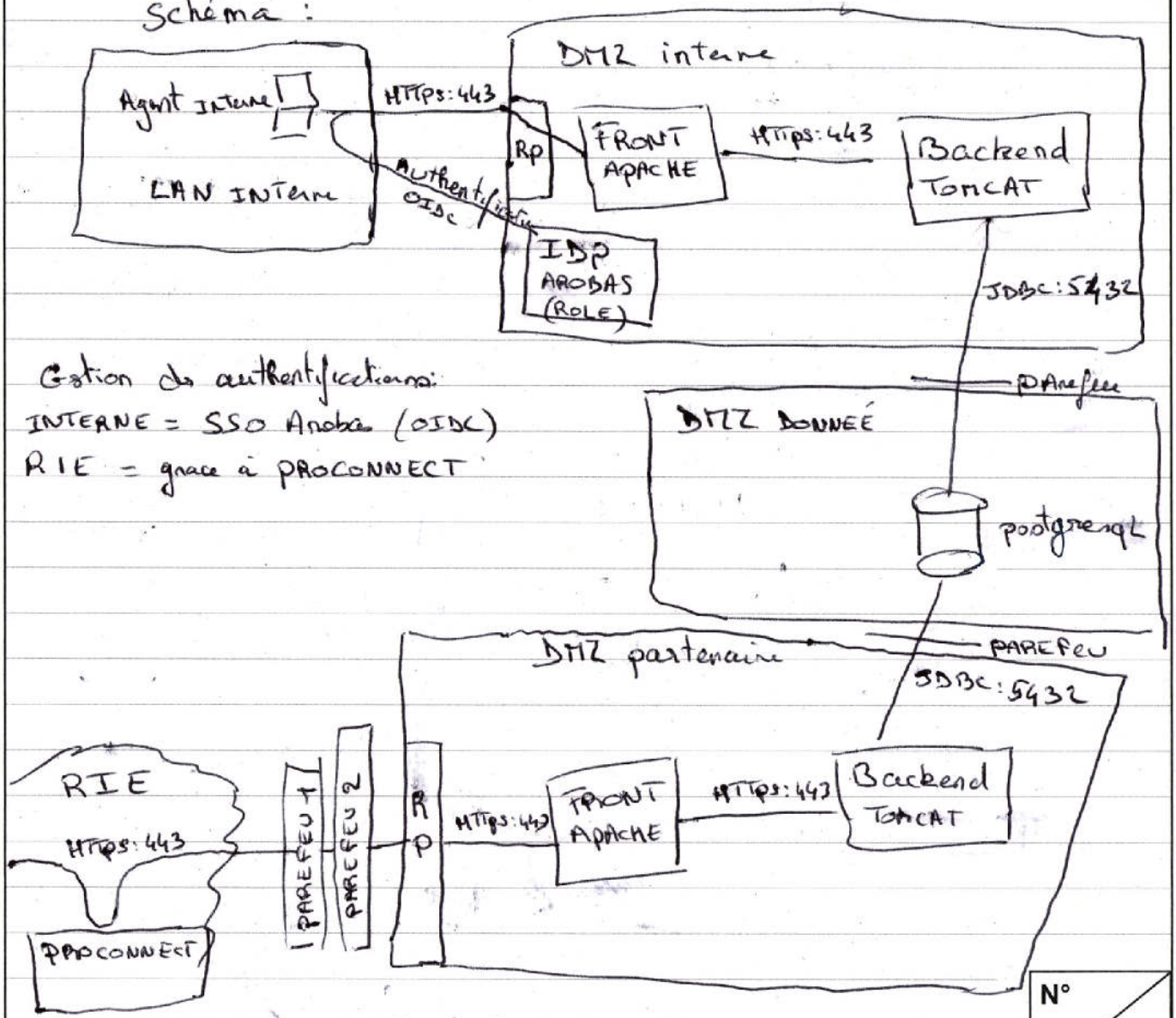
Question 2 :

La conteneurisation permettra de segmenter et cloisonner l'application.

Etape 4 ouverture du service

Question 1 Architecture

Schéma :



Gestion des authentifications :
INTERNE = SSO Arobas (OIDC)
RIE = grace à PROCONNECT

Rp = Reverse proxy

N° 8.111

Intitulé de l'épreuve : Informatique

Nombre de copies : 3

Numérotez chaque page (dans le cadre en bas de la page) et placez les feuilles dans le bon sens.

suite Etape 4

Question 2 :

1) pour les utilisateurs externes, je préconise l'utilisation de la Fédération d'identités PROCONNECT. Celui-ci fait le lien avec les utilisateurs grace à l'adresse Mail professionnelle et le numéro de siret.
Coté application, lors de la premier connexion l'application créera automatiquement le compte utilisateur avec les informations de PROconnect et lui attribuera un Rôle_partenaire en respectant la regle du moindre privilège.

2) La non répudiation des actions des partenaires exteriem et assuré par la complete journalisation des evenements sur l'application. Ainsi un Agent externe verra toute ses actions enregistré dans le fichier de log. De plus si l'authentification proconnect est fait en OIDC, cela garantira que c'est bien cet agent qui s'est connecté et a fait les actions grace à un system de signature electronique dans le protocole OIDC.

N° 9.1.M

Etape 5 :

Question 1 :

Le servica E-NEGO s'inscrit dans la strategie numerique de l'etat qui consiste à partager ou mutualiser les services au niveau interministeriel ou auprès des autres administrations.
Il faudra justifier que tous les critères reglementaire et technique sont validés avant de s'adresser à la DINUM. Pour cela il faudra présenter le dossier d'homologation qui garantira le respect, du service E-NEGO, aux regles RGPD. Il faudra indiquer la stack technique utilisée en cohérence avec notre cadre de cohérence technique CCT. Et montrer que les regles et les bonnes pratiques de conceptions et de developpement ont été appliquées comme le RGAA et les methodes de conception eco-responsable. Nous pourrons alors proposer à la DINUM de deployer cette solution dans le cadre de projet Interministeriel ou dans les autres administration dans un but de partage.
Il sera envisageable de fournir nos ressources et nos livrables.

N° 10/11

Question 2 :

Il faudra vérifier la partie LLM de l'infrastructure de ce service et regarder si le LLM respecte les standards DINUM. Sinon il faudra le faire évoluer pour s'en rapprocher.

Il faudra peut être, éviter de promouvoir le service Hors ligne qui rappelle les anciennes méthodes de travail.

- L'API utilisée devra être basée sur une architecture REST sinon nous risquons de nous éloigner des standards DINUM.

La partie Front de l'application devra être conçu en respectant les normes responsives et respecter au mieux les règles du RGAA pour obtenir une plateforme Inclusive.

Si nous nous écartons trop de ces règles et normes, il faudra alors les retravailler afin d'être cohérent avec la stratégie numérique de l'état.

N°

N°

... /...