TITRE CONCEPTEUR-DÉVELOPPEUR D'APPLICATIONS (CDA)

BLOC E6.2 – Administration & Conception de Solutions d'Infrastructure

Cahier des Charges de la MSPR « Administrer & sécuriser une solution d'Infrastructure à partir d'un cahier des charges »

COMPÉTENCES ÉVALUÉES :

- Administrer une infrastructure.
- Gérer les accès à une infrastructure.
- Administrer la sécurité de l'infrastructure.
- Maintenir en conditions opérationnelles (Maintenance préventive et corrective).
- Tester et mettre en production des ressources afin d'améliorer une solution d'infrastructure.
- Proposer des scénarios d'évolution et d'amélioration de l'infrastructure.
- Assurer la mise en production de l'infrastructure.
- Installer, configurer et tester l'infrastructure.
- Assurer le support aux utilisateurs et aux équipes techniques.
- Gérer les demandes, les problèmes et les incidents
- Mettre à jour les référentiels de production.
- Résoudre les problèmes techniques.

PHASE 1 : PRÉPARATION DE CETTE MISE EN SITUATION PROFESSIONNELLE RECONSTITUÉE

Durée de préparation : 20 heures

Mise en œuvre : Travail d'équipe constituée de 4 apprenants-candidats (5 maximum si groupe impair)

Résultat attendu :

Réaliser chacune des missions et des corrections demandées en III – Expression des besoins.

PHASE 2 : PRÉSENTATION ORALE COLLECTIVE + ENTRETIEN COLLECTIF

Durée totale par groupe : 30 mn se décomposant comme suit :

- 10 mn de soutenance orale par l'équipe.
- 20 mn d'entretien collectif avec le jury (questionnement complémentaire).
- Objectif : mettre en avant et démontrer que les compétences visées par ce bloc sont bien acquises.

Jury d'évaluation : 2 personnes (binôme d'évaluateurs) par jury – Ces évaluateurs ne sont pas intervenus durant la période de formationet ne connaissent pas les apprenants à évaluer.

I - PRÉSENTATION DE L'ENTREPRISE / CONTEXTE

- Préambule : L'entreprise choisie pour cette MSPR est fictive, les prénoms sont fictifs, toute ressemblance à un cas réel serait purement fortuite.

La clinique LE CHATELET est un Centre de Rééducation et de Réadaptation Fonctionnelles, Clinique de Convalescence Spécialisée, agréée par le ministère de la Santé et des Affaires Sociales.
Elle est conventionnée avec les différents organismes sociaux (toutes les caisses d'Assurances Maladie et les mutuelles).

Sa vocation : la rééducation précoce en traumatologie, chirurgie orthopédique et réparatrice, la réadaptation en rhumatologie, la convalescence spécialisée post-opératoire.

À la suite de la pandémie du COVID-2019, la direction a réalisé qu'il n'y avait aucun moyen mis en place pour permettre à distance aux médecins d'interagir avec les patients et de consulter leur dossier.

Étant donné le nombre de plus en plus important de médecins et de personnel soignant en confinement, la clinique souhaite mettre en place une plate-forme hautement sécurisée permettant dans un premier temps d'accéder aux dossiers médicaux des patients via un portail WEB et dans un second temps de permette de réaliser des consultations à distance.

Ce projet nommé « Résilience 34 » a été lancé mi 2021 et vous avez été choisi en tant que prestataire externe pour le développement du portail d'authentification du service (cursus CDA) et pour la mise en place de l'infrastructure et de sa supervision (cursus ASR).

II – DESCRIPTION DE L'EXISTANT

La gestion des patients au niveau médical est entièrement informatisée par l'intermédiaire d'une application client/serveur développée il y a maintenant une dizaine d'années.
Cette application est une application monolithique s'appuyant sur une base Oracle embarquée.
La connexion s'effectue par l'intermédiaire d'un client lourd.

Le projet résilience prévoit le portage de l'application en mode WEB. Ainsi, que ce soit à distance ou sur site, le personnel pourra accéder aux dossiers médicaux des patients via un navigateur WEB.

Le portail d'authentification sera ouvert à tout Internet, donc hautement critique d'un point de vue de la sécurité.
Au vu des données hébergées, la clinique compte sur votre expertise pour en assurer la sécurité au niveau des accès.
Le contrat que vous avez signé prévoit également que vous accompagniez la Clinique dans sa démarche pour être en règle par rapport aux impératifs légaux concernant ces données sensibles.

L'authentification obéira à des règles strictes de reconnaissance des utilisateurs et de modalités d'authentification.

Le portail sera interfacé avec la base des utilisateurs qui se trouve être le serveur Active Directory du domaine de la Clinique.

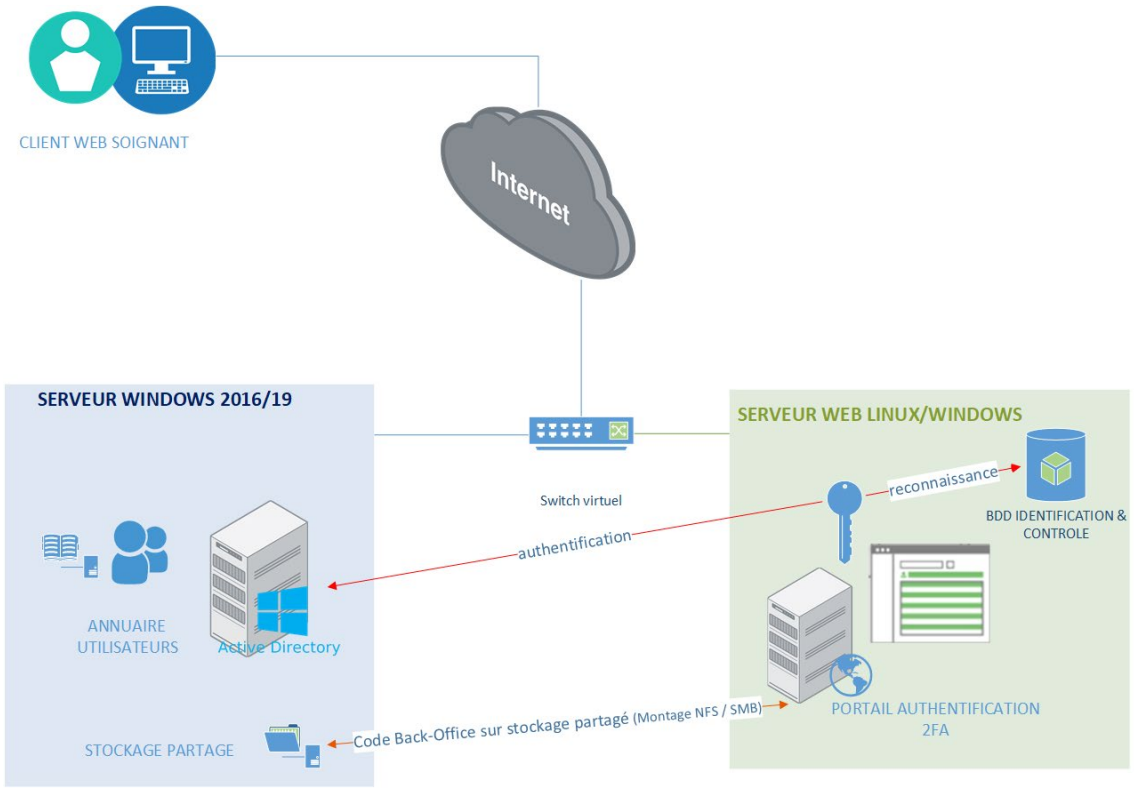
Étant obligé de reprendre l'existant, le portail devra établir l'authentification du soignant selon la présence de son compte dans cet annuaire Active Directory.

III – EXPRESSION GLOBALE DES BESOINS

Votre tâche consiste à réaliser les missions suivantes :

- Mission M1 : Développement de la page WEB d'authentification renforcée dont un mécanisme d'authentification à 2 facteurs
- Mission M2 : Hébergement de l'application WEB sur un serveur LINUX paramétré par votre équipe
- Mission M3 : Authentification via une base utilisateurs qui repose sur un annuaire Active Directory
- Mission M4 : Rédaction des livrables (cf section « livrables attendus ») et préparation de la soutenance

- Voici un schéma global de la solution à mettre en œuvre :



IV – CAHIER DES CHARGES DÉTAILLÉ PAR MISSION :

Mission M1 : Développement de la page WEB d'authentification renforcée dont un mécanisme d'authentification à deux facteurs

Dans la phase d'avant-projet, la réflexion doit se porter sur le choix du langage à utiliser qui est complétement libre.
Une réflexion doit ensuite avoir lieu sur la méthode de travail au sein du groupe, sur l'organisation et devra déboucher sur un listing précis des tâches ainsi qu'une planification.

Pour cette mission M1, il est attendu que soit développé une page WEB d'authentification selon les critères suivants :

- Mise en place d'une authentification forte à double facteur de votre choix : jeton, OTP (one time password), validation mail etc…
- Construire une Base de données applicative permettant de gérer les mécanismes de reconnaissance de navigateur et d'adresse IP des utilisateurs.
  - Le mécanisme de reconnaissance doit être capable de détecter le navigateur habituel utilisé par le soignant et si ce n'est pas le cas, le soignant devra confirmer par mail sa connexion via un mail généré par le système.
  - Le mécanisme de reconnaissance d'adresse IP devra se déclencher si l'adresse IP publique utilisée

par le soignant n'est pas habituelle. Dans ce cas-là, il devra générer un mail de signalement au soignant pour lui faire part d'une activité inhabituelle mais ne bloquera pas la connexion sauf si l'adresse IP n'est pas française.

- Mise en place d'un mécanisme anti-brute force : les tentatives de login trop nombreuses en peu de temps doivent entrainer le blocage de l'utilisateur selon sa provenance et selon des critères à définir. Un script permettant de tester ce système devra être fourni.
- La page doit être accessible dans un premier temps via le réseau local de la clinique puis via Internet (ou un réseau externe au LAN comme le réseau local de l'EPSI ou tout autre réseau virtuel).

Ressources & Exemples :

Authentification 2FA :
https://fr.wikipedia.org/wiki/Authentification_forte
https://fr.wikipedia.org/wiki/Google_Authenticator

Identification du client WEB :
https://developer.mozilla.org/fr/docs/Web/HTTP/Browser_detection_using_the_user_agent

Identification d'une adresse IP :
https://db-ip.com/
https://lite.ip2location.com/ip2location-lite

Anti Brute-Force :
https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
https://predatech.co.uk/protecting-your-web-app-brute-force-login-attacks/
https://doc.ubuntu-fr.org/fail2ban

Mission M2 : Hébergement de l'application WEB sur un serveur LINUX paramétré par votre équipe

Vous devez mettre en place le serveur WEB sur un serveur de type Linux (avec support LTS). Le serveur WEB répondra aux requêtes des utilisateurs en exécutant ou interprétant votre code qui sera lui stocké physiquement sur un serveur Windows ou Linux dédié au stockage.

Afin d'économiser des ressources, vous pouvez choisir d'attribuer ce rôle au serveur Active directory, au lieu de créer un autre serveur.

Une solution à base de conteneurs au niveau serveur WEB est parfaitement envisageable.

Vous devez impérativement mettre en place HTTPS sur le site WEB, si vous avez enregistré votre nom de domaine, vous pouvez utiliser Let's Encrypt en tant que CA. https://letsencrypt.org/fr/, sinon il faudra utiliser des certificats autogénérés.

NOTE :
Il est possible d'envisager l'hébergement de l'infrastructure sur la plate-forme étudiante AZURE en ce qui concerne l'annuaire utilisateur mais ce choix entraine l'adaptation du code de votre portail et n'est donc pas anodin. Il faudra veiller également à ce que le compte étudiant utilisé possède suffisamment de crédits pour la durée du projet.

Ressources & Exemples :

HTTPS :
https://doc.ubuntu-fr.org/tutoriel/securiser_apache2_avec_ssl
https://developers.google.com/web/fundamentals/security/encrypt-in-transit/enable-https

Stockage partagé :
https://doc.ubuntu-fr.org/tutoriel/un_simple_partage_nfs
https://doc.ubuntu-fr.org/samba
https://www.freenas.org/

Mission M3 : Authentification via une base utilisateurs qui repose sur un Annuaire Active Directory

Le serveur Active directory contient la liste des comptes utilisateurs autorisés à se connecter à l'application.

Votre portail WEB doit s'appuyer sur cet annuaire Active directory.

Active Directory est un service installé sur un O.S de type Windows server.
C'est en réalité un annuaire LDAP un peu modifié qu'il est parfaitement possible d'interroger via des requêtes LDAP à partir de votre application.

Il vous faudra donc monter un serveur Active Directory avec Windows 2016 ou 2019, y créer un domaine (par exemple chatelet.local) et y ajouter des utilisateurs (les comptes des soignants).

Étant donné que dans la réalité, on s'appuie sur un serveur existant, il ne faut pas que votre application ait accès à l'AD en écriture mais simplement en lecture pour valider ou non le compte lors de l'authentification.

Si vous n'avez pas de connaissances en serveur WINDOWS et Active directory, l'installation du service se fait entièrement via une interface graphique à base de « wizard ».
Il n'y a pas de subtilité mise à part le fait que vous puissiez être bloqué par défaut par le firewall intégré à Windows.

Ressources & Exemples :

http://www.linux-france.org/prj/edu/archinet/systeme/ch56s05.html
https://www.jmdoudoux.fr/java/dej/chap-jndi.htm#jndi-6
https://theitbros.com/ldap-query-examples-active-directory/

Mission M4 : Rédaction des livrables et préparation de la soutenance

Voici la liste des livrables attendus :

- Une démonstration de votre portail sécurisé aura lieu lors de la soutenance orale dont la date vous sera communiquée dans les meilleurs délais.
  Vous devez démontrer que vous remplissez l'ensemble des fonctions et des contraintes décrites précédemment dans le document lors de cette démonstration, elle demande donc de la préparation et un fil conducteur.
- Un guide à l'usage des utilisateurs concernant l'authentification forte
- Un organigramme « flow chart » du processus complet d'authentification à l'usage du technicien / développeur

V – CONTRAINTES ET MOYENS :

5.1 Langage de programmation & O.S

Le langage est totalement libre de choix à partir du moment où vous répondez au cahier des charges.

5.2 Mise en place des serveurs

Il n'y a pas de ressources spécifiques matérielles allouées à votre MSPR.
Vous devez donc virtualiser le serveur WEB et le serveur AD avec une application de virtualisation type VMWARE WORKSTATION PRO ou VIRTUAL BOX

On conseille fortement de stocker les machines virtuelles sur un disque de type SSD.

Il est cependant possible à titre d'exception et pour des cas particuliers d'allouer des ressources matérielles.

5.3 Travail en groupe

Les groupes doivent être formés de 4 apprenants maximum et constitués dès le début de la première séance. Ils seront par la suite immuables.

- Établir en début de projet un planning prévisionnel précisant les tâches à accomplir, leur durée estimée et leur affectation.
- Certaines tâches sont dépendantes des autres, n'hésitez pas à créer des services temporaires pour tester votre code : par exemple le code peut fonctionner en http dans un premier temps, puis dans un

second temps seulement on ajoutera la couche HTTPS).

- L'intégration de l'annuaire Active Directory nécessite presque obligatoirement de se documenter sur les annuaires LDAP et les protocoles sous-jacents.

- Les outils de virtualisation permettent d'exécuter des VMS sur n'importe quel poste, la copie des VMS est facile (il suffit de copier le répertoire), il est possible de faire des clones.
  Comme vous travaillez à plusieurs, rien n'empêche d'utiliser chacun sa propre VM pour des tests et des développements.
  De plus, l'utilisation d'outils collaboratifs comme GitHub semble ici tout à fait adéquate.

5.4 Suivi

À l'issue de chaque séance, un compte rendu d'avancement devra être rédigé.

Il devra indiquer le travail effectué sur la séance ainsi que la planification du contenu de la prochaine séance.

Il peut se résumer à un ensemble des tâches accomplies, un récapitulatif des tâches à accomplir (et leur priorisation) ainsi que les problèmes rencontrés.

À noter que c'est votre intervenant qui précisera les modalités et la fréquence des rendus.

➢ Compétences évaluées :

Vous aurez à démontrer les compétences suivantes :

- Administrer une infrastructure.
- Gérer les accès à une infrastructure.
- Administrer la sécurité de l'infrastructure.
- Maintenir en conditions opérationnelles (Maintenance préventive et corrective).
- Tester et mettre en production des ressources afin d'améliorer une solution d'infrastructure.
- Proposer des scénarios d'évolution et d'amélioration de l'infrastructure.
- Assurer la mise en production de l'infrastructure.
- Installer, configurer et tester l'infrastructure.
- Assurer le support aux utilisateurs et aux équipes techniques.
- Gérer les demandes, les problèmes et les incidents
- Mettre à jour les référentiels de production.
- Résoudre les problèmes techniques.