IUT Nancy-Charlemagne – BUT Informatique S5 – DWM

Développement Web Serveur avancé

TD5 : Authn/Authz basé sur JWT pour l'API Toubeelib

Préliminaires

Récupérer et créer la base de données d'authentification fournie dans Arche. Elle contient des patients (rôle 1), et des praticiens (rôle 10). Le mot de passe est le nom d'utilisateur dans l'adresse mail.

Exercice 1: Service d'Authentification

Créer le service d'authentification qui permet de vérifier les credentials (email, password) d'un utilisateur et retourne un DTO contenant le profil ayant réussi l'authentification : ID, mail et rôle de l'utilisateur.

Exercice 2: Route Signin

Créer le provider d'authentification et implanter la méthode `signin` qui vérifie les credentials en utilisant le service construit dans l'exercice 1, puis crée un DTO d'authentification contenant le profil de l'utilisateur authentifié ainsi qu'un access token et un refresh token.

Créer ensuite la route pour s'authentifier auprès l'API. Choisir la méthode adéquate, puis créer l'action correspondante : elle valide la présence et le type de données d'authentification (email, password), puis utilise le provider pour valider ces credentials et obtenir un couple access token / refresh token. Elle construit enfin une réponse contenant les tokens JWT.

Exercice 3 : Middleware de contrôle d'authentification

Créer un middleware qui vérifie la présence et la validité du token JWT dans la requête. En cas d'erreur, provoque une réponse d'erreur avec le code adapté. Si le token est valide, crée un DTO de profil contenant l'ID, le mail et le rôle de l'utilisateur authentifié. Ce DTO est transmis à l'action suivante dans la requête, il pourra ainsi être utilisé pour les contrôles d'autorisation.

Exercice 4 : Service d'autorisation (Authz) pour les rendez-vous

Construire le service d'autorisation pour contrôler l'accès et la manipulation des rendez-vous. Ce service doit implanter la politique d'autorisation décrite dans le sujet du projet. Le service expose une méthode pour chaque cas. On traite pour l'instant uniquement les cas suivants : - accès à l'agenda d'un praticien, - accès au détail d'un rendez-vous,

Exercice 5 : Contrôle d’autorisation pour les Rendez-vous

Construire le middleware qui vérifie que l’utilisateur authentifié a le droit d’exécuter une opération sur un rendez-vous. Il récupère le DTO de profil de l’utilisateur créé par le middleware d’authentification, puis vérifie le droit d’accès en appelant le service Authz. Il détermine la méthode à appeler dans le service d’autorisation en fonction du nom de la route appelée. En cas d’erreur, provoque une réponse d''erreur avec le code adapté. En cas de succès, passe à l’action suivante.