Article
Guillaume Rongier · Oct 17, 2022 8m de lecture

Construction d'un référentiel FHIR + le serveur d'autorisation OAuth2/serveur de ressources sur IRIS for Health - Partie 1

Bonjour, chers développeurs !

Dans cet article, je vais vous montrer comment configurer le référentiel FHIR + le serveur d'autorisation OAuth2/serveur de ressources sur IRIS for Health en suivant l'article précédent.

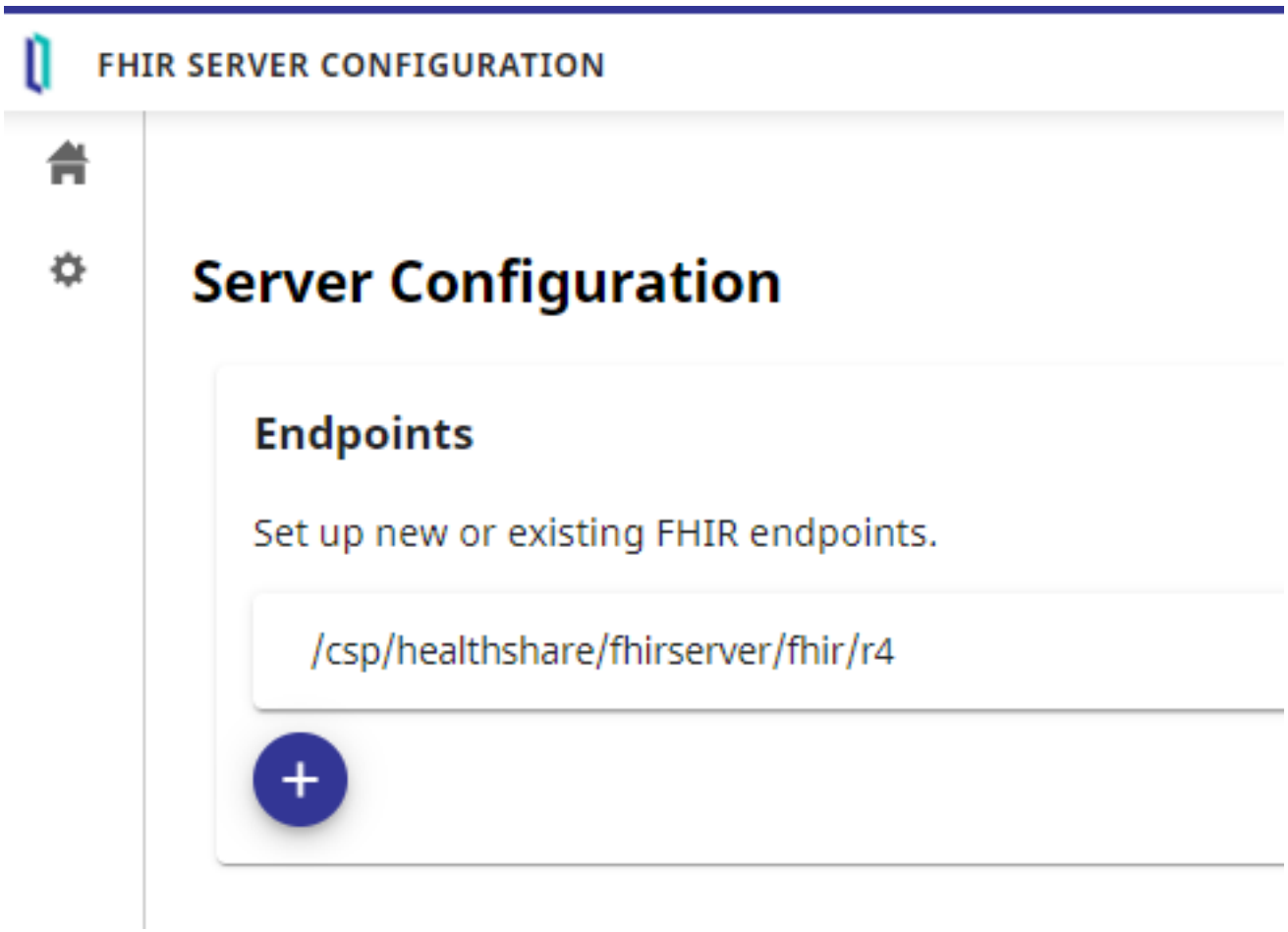
Dans la partie 1, nous vous présentons les préparatifs préliminaires, la configuration du serveur d'autorisation OAuth2 et l'obtention du jeton d'accès.
La partie 2 vous explique comment construire un référentiel FHIR et configurer un client/serveur de ressources OAuth2.

La configuration du référentiel FHIR et le serveur client/ressource OAuth2 que nous allons configurer aujourd'hui peuvent être utilisés séparément de l'instance IRIS du serveur d'autorisation OAuth2 que nous avons configuré dans la partie 1 précédente, ou ils peuvent être co-localisés dans la même instance.
Dans cet article, nous allons le configurer dans la même instance que le précédent.

Construction du référentiel FHIR et spécification du nom du client OAuth

La construction d'un référentiel FHIR est décrite dans le document "Installer et configurer un serveur FHIR" .

Dans l'écran suivant, après l'avoir construit, cliquez sur l'URL du point de terminaison /csp/healthshare/fhirserver/fhir/r4 pour ouvrir l'écran de configuration.



Sur l'écran de configuration, saisissez le nom de configuration client OAuth2 que vous allez créer dans le champ **Nom du client OAuth**.
Si vous avez déjà configuré un client OAuth2, veuillez faire correspondre son nom.

Dans cet exemple, nous allons utiliser la chaîne "FHIRResource". Pour la modifier, cliquez sur le bouton "Modifier" dans l'écran ci-dessus, puis sur le bouton "Mettre à jour" pour enregistrer les modifications.

Configuration client OAuth2

Dans ce qui suit, nous allons créer la configuration client OAuth2.

Accédez à **Administration du système → Sécurité → OAuth2.0** dans le portail de gestion et sélectionnez **"Client "** au lieu de **"Serveur "**, contrairement à la partie précédente 1.

Sur l'écran suivant, cliquez sur **"Creation de la Description du Serveur"** pour créer la configuration de la connexion au serveur d'autorisation OAuth2.

Pour le point de terminaison de l'émetteur, la page Description du serveur indique le point de terminaison du serveur d'autorisation configuré dans la partie 1.

Voici l'écran de configuration du serveur d'autorisation OAuth2 configuré dans la partie 1.

Pour la configuration SSL/TLS, entrez la configuration SSL/TLS "SSL4CLIENT" que vous avez créée lors de la préparation de la Partie 1.

Après avoir saisi les éléments, exécutez **" Découvrir et sauvegarder "** pour obtenir les informations du serveur d'autorisation OAuth2 !

Si l'accès est réussi, les informations obtenues s'afficheront, comme indiqué ci-dessous.
Veuillez noter qu'une erreur peut se produire au cours de ce processus si le certificat SSL spécifiant le nom d'hôte que vous avez préparé précédemment dans la préparation de la partie 1 n'est pas créé correctement et reconnu.

Attention: Même si vous utilisez le fichier docker-container DL dans la partie 1 de cette série, vous pouvez avoir des difficultés à accéder au conteneur IRIS -> conteneur Apache en spécifiant le nom d'hôte. Dans ce cas, vous pouvez résoudre le problème en entrant le nom d'hôte et l'adresse IP de votre machine dans le fichier docker-compose.yml en tant que extrahosts, comme indiqué ci-dessous.

```
extra_hosts:
  - <yourhostname>:<your ip address>
```

Une fois que vous avez enregistré la configuration, cliquez sur **" Sauvegarder "** pour revenir à la page suivante, puis sélectionnez **" Configuration client "** pour créer la configuration du référentiel FHIR.

Ajout d'une configuration client au client OAuth2

C'est un titre compliqué, mais l'étape suivante consiste à ajouter la configuration client (informations sur le référentiel FHIR spécifique, l'application CSP, etc. que vous souhaitez connecter au serveur d'autorisation OAuth2 en tant que client OAuth2) à la configuration client OAuth2 que vous venez de créer (avec des informations sur le serveur d'autorisation OAuth2 auquel se connecter).

Sur l'écran suivant, cliquez sur **" Créer une configuration client "** pour afficher l'écran suivant et régler les éléments nécessaires.

Si vous sélectionnez d'abord le type de client = Serveur de ressources, l'écran de saisie sera le même que ci-dessous.

Nom d'application	FHIRResource: Saisissez la valeur que vous avez entrée pour " Nom du client OAuth " dans la configuration du référentiel FHIR.
Nom du client	Il s'agit du nom du client qui sera enregistré auprès du serveur d'autorisation OAuth2. Il peut être identique au nom de l'application ; cependant, nous avons choisi un nom différent ici.
Description	Saisissez une description pour cette configuration.
Type du client	Sélectionnez " Serveur de ressources ".
Configuration SSL/TLS	Spécifiez la configuration SSL/TLS que vous avez préparée précédemment lors de la préparation de la partie 1.

Après avoir rempli le formulaire, cliquez sur le bouton **" Enregistrement dynamique et sauvegarde "** pour sauvegarder et enregistrer le fichier sur le serveur.
C'est un peu confus, mais lorsque le bouton passe de " Enregistrement dynamique et sauvegarde " à **" Obtenir les métadonnées de mise à jour et sauvegarder "**, l'enregistrement a réussi.

Examinons les informations de configuration de l'autorisation OAuth2 côté serveur et vérifions si elle est enregistrée.

Sur la page **Portail de gestion→Administration du système→Gestion de la sécurité→OAuth2.0→Serveur**, cliquez sur **"Description du client",** et vous verrez qu'il est enregistré comme indiqué ci-dessous.

Confirmez que le nom est celui que vous avez spécifié dans le nom du client.

Dans la première partie, lorsque nous avons testé l'accès à partir de Postman, nous avons copié manuellement l'ID client et la clé privée qui s'affichent plus bas dans l'écran du descripteur client. Cependant, cette fois-ci, ces informations sont transmises au côté client pendant le processus d'enregistrement dynamique.

Accès au référentiel FHIR à partir de Postman en utilisant un jeton d'accès OAuth2

Et enfin, il est temps d'y accéder depuis Postman !

Tout d'abord, nous devons obtenir un jeton d'accès. La méthode de base est la même que celle utilisée à la fin de la partie 1, mais nous devons ajouter un paramètre audience pour indiquer où le jeton d'accès sera émis.

```
aud=https://[hostname]/csp/healthshare/fhirserver/fhir/r4
```

Pour l'ajouter spécifiquement dans Postman, ajoutez-le comme paramètre à l'URL du point de terminaison du code d'autorisation comme suit :
(A cause des limitations de l'écran de Postman, vous ne pouvez pas voir tous les paramètres, mais veuillez inclure tous les éléments ci-dessus aud=https://[hostname]/csp/healthshare/fhirserver/fhir/r4)

Attention : **Vous n'avez pas besoin de changer** l'ID client et le Secret client que vous entrez dans Postman pour ceux émis dans l'enregistrement dynamique du serveur de ressources plus tôt. Utilisez l'ID et la clé secrète du client émis pour Postman que vous avez ajouté dans la partie 1.

Après avoir obtenu le jeton d'accès, veuillez copier son contenu.

Dans Postman, si vous laissez le TYPE d'autorisation comme OAuth2, vous disposez d'une fonction pour envoyer le jeton d'accès. Toutefois, dans le référentiel FHIR d'IRIS for Health, il est également nécessaire d'envoyer les informations relatives à l'utilisateur et au mot de passe de l'autorisation de base.

À cette fin, lors d'un accès à partir de Postman, le TYPE d'Autorisation (qui est un peu difficile) doit être Basic Auth, le nom d'utilisateur et le mot de passe doivent être saisis, et le jeton d'accès doit être envoyé comme paramètre dans la demande REST au référentiel FHIR.

En détail : tout d'abord, saisissez le nom d'utilisateur et le mot de passe comme indiqué dans l'écran suivant. Ces informations d'utilisateur seront vérifiées pour voir si elles correspondent aux informations d'utilisateur dans le sous jeton d'accès ; il doit donc s'agir du même utilisateur que celui que vous avez saisi lorsque vous avez obtenu le jeton d'accès.

Dans l'onglet Params, pour accesstoken, entrez la valeur du jeton d'accès que vous venez de saisir pour le paramètre.

Si vous venez de construire le référentiel FHIR, il n'y a pas de données dans le référentiel, mais vous pouvez demander les données du patient !

Pour l'URL de la demande, entrez https://[hostname]/csp/healthshare/fhirserver/fhir/r4/Patient, et sélectionnez GET comme méthode HTTP (comme indiqué dans la figure ci-dessus).

Appuyez sur le bouton "Envoyer" pour soumettre la demande ! Si vous obtenez le Paquet FHIR comme indiqué ci-dessous, vous avez réussi à accéder au référentiel FHIR en utilisant le jeton d'accès !

Pour plus d'informations sur la manière d'enregistrer et de rechercher des données dans le référentiel FHIR, veuillez consulter la documentation et les articles de la communauté IRIS for Health.

Documentation d'IRIS pour la santé 2020.3 Dépôt de ressources

Comment avez-vous réussi à accéder au référentiel FHIR ?

La configuration décrite dans cette série est la plus simple. Dans un projet FHIR réel, le contenu des données à renvoyer dépendra du contenu approuvé par l'utilisateur, ce qui devra être pris en compte et mis en œuvre.

Nous continuerons à tenir la communauté des développeurs informée de FHIR.

#FHIR #OAuth2 #InterSystems IRIS for Health

URL de la source:https://fr.community.intersystems.com/post/construction-dun-r%C3%A9f%C3%A9rentiel-fhir-le-serveur-dautorisation-oauth2serveur-de-ressources-sur-iris