Artigo
Kevin Koloska · Nov. 15, 2022 11min de leitura

Construção de um repositório FHIR + o servidor de autorização/recurso OAuth2 no IRIS for Health - Parte 2

Construção de um repositório FHIR + o servidor de autorização/recurso OAuth2 no IRIS for Health - Parte 2
IRIS para #FHIR #OAuth2 #InterSystems de Saúde
Olá, caros desenvolvedores!
Neste artigo, vamos focar-nos na OAuth2, um protocolo que é cada vez mais utilizado em combinação com o FHIR para realizar permissões.
Nesta parte 1, iniciaremos o contentor Docker para IRIS para a Saúde e Apache, configuraremos a função do servidor de autorização OAuth2 na IRIS for Health, acedemos-lhe a partir da ferramenta de desenvolvimento do Postman REST e obteremos um token de acesso. Além disso, na segunda parte e além, adicionaremos a funcionalidade de repositório FHIR à IRIS for Health, adicionamos a configuração do servidor de recursos OAuth2 e explicaremos como executar consultas de FHIR com fichas de acesso de dentro do Carteiro.

Vários artigos excelentes já foram publicados dentro da comunidade de desenvolvedores para explicar a funcionalidade OAuth2 dos produtos InterSystems; No entanto, gostaria de explicar mais uma vez como criar a versão mais recente.
Implementação do Quadro de Autorização Aberta IRIS InterSystems (Oauth 2.0) - Parte 1
Neste artigo, utilizaremos a versão mais recente da InterSystems IRIS for Health 2020.3 Preview Edition. Se pretender criar um ambiente baseado neste artigo, não se esqueça de utilizar esta ou uma versão posterior do kit. Algumas funcionalidades não estão incluídas em produtos antes desta versão.
Preparativos preliminares
O primeiro passo é fazer os preparativos preliminares. Há muitas coisas para se preparar para construir um ambiente seguro.
IRIS for Health 2020.3 Preview Edition só está disponível como uma versão de recipiente Docker. (InterSystems Docker Hub/IRIS for Health)Para executar a configuração OAuth2, também terá de executar o servidor web e a configuração SSL. Neste artigo, utilizaremos Apache.Quando configurar o SSL em Apache, o certificado de configuração SSL deve corresponder ao nome de anfitrião do servidor. Por favor, tenha isso em conta.

Obtenha ficheiros de amostra do repositório Do GitHub interssistema-jp
O estivador-compose.yml/Dockerfile e outros ficheiros de amostras utilizados nesta configuração estão disponíveis no repositório GitHub para a comunidade de desenvolvedores intersystems.Em primeiro lugar, desaperte este ficheiro no seu ambiente utilizando o seguinte comando. (Também pode fazê-lo a partir do anexo a este artigo.)
Este docker-compose.yml/Dockerfile e outros ficheiros são criados referindo-se à aplicação iris-webgateway-exemplo publicada no OpenExchange.
https://github.com/Intersystems-jp/IRIS4H-OAuth2-handson.git de clone de Git
Alterar a configuração de acordo com o kit utilizado
Neste ficheiro docker-compose.yml, estão configurados dois contentores: o contentor IRIS for Health e o contentor Apache (httpd) serão criados pelo comando de construção de estivadores. O ficheiro docker-compose.yml, disponível no GitHub, refere IRIS for Health Community Edition Preview Edition (2020.3.200.0). A Edição Comunitária pode ser utilizada para a avaliação dos produtos InterSystems.

íris:
Imagem: loja/intersistemas/irishealth-comunidade:2020.3. 0.200. 0
Se estiver a utilizar uma versão diferente (versão oficial ou mais recente), altere esta parte da especificação.
O recipiente Apache será construído com o conteúdo do Dockerfile, que requer um kit WebGateway para ligar ao IRIS a partir de Apache.Para obter informações sobre como obter este kit, os parceiros da InterSystems podem visitar o site de descarregamento do WRC ou contactar o Centro de Suporte do WRC. Se tiver mais alguma questão, contacte-nos neste endereço.
Modifique as seguintes partes do Dockerfile dependendo do produto que obteve. Independentemente do sistema

operativo da máquina hospedeira (Windows/Ubuntu/CentOS), a plataforma será lnxubuntux64 porque o sistema operativo do recipiente httpd base é Debian.
Versão ARG=2020.3. 0.200. 0
Plataforma ARG =inxubuntux64
ADD WebGateway-${versão}-${plataforma}.tar.gz /tmp/
Preparação de um certificado SSL
No passo seguinte, é preparado um certificado SSL. Ao aceder à autorização OAuth2, o certificado SSL definido no servidor web é verificado para ver se corresponde ao URL a ser acedido. Não é necessário utilizar um certificado oficial; é possível utilizar o OpenSSL, etc. Introduza o nome de anfitrião no campo "Nome Comum" ao criar o certificado.
Além disso, uma vez que o certificado que criou será carregado automaticamente no momento do lançamento, tem de modificar o ficheiro para que este não exija uma palavra-passe. Por favor, consulte o seguinte comando.
$ openssl rsa -in cert.key.org -out cert.key
Coloque os ficheiros CRT e KEY criados no mesmo diretório que o Dockerfile, com os nomes de ficheiros server.crt/servidor.key respectivamente.
Além de o utilizar com o servidor web Apache, precisará de um certificado SSL para a configuração OAuth2. Não precisa de introduzir um nome de anfitrião, etc., mas precisa de criar três conjuntos. (Nas seguintes configurações, aparecem como auth.cer/auth.key , cliente.cer/cliente.key, resserver.cer/resserver.key)
Construindo um estivador e iniciando um contentor de estivadores
Agora está finalmente pronto! Além dos quatro ficheiros que descarregou, tem agora um conjunto de instalações web gateway e dois certificados SSL no seu diretório. Preste atenção às permissões de acesso e execução de cada ficheiro. (Por exemplo, adicionei a permissão de execução a webgateway-entrypoint.sh.)
estiva-composição construção
estiva-composição -d
Uma vez lançado, utilize o comando do PS para verificar se ambos os contentores estão a funcionar.
Nome do recipiente Apache:web
IRIS for Health:store/intersystems/irishealth-community container name:2020.3.0.200.0 (ou outro nome dependendo do conjunto)
Agora tente aceder ao portal de gestão nas seguintes três formas. Se o terceiro método funcionar, a sua configuração SSL através do servidor web Apache é um sucesso!
http://[nome anfitrião]:52773/csp/sys/UtilHome.csp:Este URL é acedido através do Apache Privado no contentor IRIS. Não passa pelo Apache configurado.
http://[hostname]/csp/sys/UtilHome.csp: Este URL fornece acesso ao portal de gestão através do Apache configurado.
https://[hostname]/csp/sys/UtilHome.csp: Este URL fornece acessoao portal de gestão utilizando uma ligação SSL via Apache, que configurae.
Criação de uma configuração SSL
Agora que a IRIS for Health está a funcionar e temos acesso ao portal de gestão, vamos criar a configuração SSL para os preparativos finais.
Aceda ao Portal de Gestão -> Administração do Sistema -> Configuração SSL/TLS de Segurança -> e crie três configurações SSL utilizando os três pares de chaves de certificado que preparou.
Pode escolher o nome que quiser, mas neste artigo utilizaremos SSL4AUTH/SSL4CLIENT/SSL4RESSERVER, de acordo com artigos anteriores sobre AAuth2.

*Sobre a partilha de diretórios entre anfitriões e contentores
Especificar os seguintes volumes no ficheiro de composição de estiva indica a localização atual do diretório de anfitriões = /ISC no recipiente. Utilize este diretório ao especificar o ficheiro do certificado nas definições acima, etc.

```
Volumes:
  - .:/ Isc
```

Este diretório conterá não só ficheiros de ficheiros, mas também ficheiros de base de dados IRIS e ficheiros de configuração. Consulte o documento "Persistente
%SYS for Persistent Instance Data Storage" para obter mais informações.
Configuração OAuth2 na IRIS para a Saúde
Agora é hora de entrar nos detalhes do acesso ao IRIS para a Saúde usando OAuth2!

Configurar o servidor de autorização OAuth2
Primeiro, vamos configurar o servidor de autorização OAuth2! Vá ao Portal de Gestão → Administração do Sistema → Segurança → OAuth 2.0 → Server.
Siga as instruções abaixo para configurar as definições.
Definições no separador "Geral"
Ponto final do transmissor: Nome anfitrião Insira o nome de anfitrião.
Ponto final do transmissor: Prefixo Pode introduzir o valor da sua escolha, mas aqui definimo-lo como "authserver".
Tipos de subvenções apoiadas Neste artigo, só usaremos o "Código de Autorização", mas se quiser testar outros "Tipos de subvenções", por favor adicione uma marca de verificação. Adicione também uma marca de verificação à "Autorização JWT"
SSL/TLS de configuração Especifique a configuração SSL que acabou de adicionar.

No separador "Âmbitos", clique em "Adicionar um âmbito suportado" para os adicionar. Mais tarde, o ecrã de início de sessão de código de autorização apresentará a "descrição" que escreveu aqui.

Não altere o separador "Intervalos" a partir do valor predefinido. No separador "Definições JWT", vamos selecionar "RS512" como algoritmo de assinatura.

No último separador "Personalização", altere a especificação "Token Class Generation" para %OAuth2.Server.JWT.

Uma vez introduzido a informação, clique no botão "Guardar" para guardar a configuração.
Agora que tem a configuração necessária para que a IRIS for Health funcione como um servidor de autorização OAuth2, está pronto para tentar! Vamos tentar aceder-lhe do Carteiro e ver se conseguimos um sinal de acesso! No entanto, antes de o fazermos, temos de realizar duas outras configurações.
Adicionar uma descrição do cliente
Primeiro, adicione a informação do Carteiro a que pretende aceder como cliente OAuth2. O registo do cliente OAuth2 pode ser adicionado através de registo dinâmico ou outros métodos.
Clique em "Descrição do Cliente" na página de configuração do servidor para continuar.

Clique em "Criar descrição do cliente" para adicionar uma entrada.
Siga as instruções abaixo para criar uma subscrição do cliente.
Definições no separador "Geral"
Nome Insira um nome à sua escolha. Neste caso, escolhemos "carteiro".
Tipo de Cliente Selecione "Confidencial"
Redirecionamento de URL Clique no botão "Adicionar URL" para adicionar um URL de redirecionamento para o Carteiro. https://www.getpostman.com/oauth2/callback como URL de redirecionamento para carteiro.
Tipos de subvenções apoiadas Especifique o mesmo "Código de Autorização" que foi configurado nas definições do servidor de autorização OAuth2. (Predefinição) Adicione um controlo se quiser testar outros tipos de bolsas também. No entanto, as definições devem ser as mesmas que a configuração do servidor de autorização.
Verifique também a caixa "Autorização JWT". Especificar aqui
Algoritmo de assinatura autenticado Verifique "autorização JWT" ao abrigo de tipos de subvenção suportados para poder selecioná-la. Selecione "RS512".

Uma vez inserida a informação, clique no botão "Guardar" para guardar a descrição do cliente.
Clique no separador "Referências ao Cliente" para ver o ID do cliente e a chave privada do cliente para esta entrada. Você vai precisar desta identificação e chave privada quando fizer testes do POSTMAN.

Adicionar uma aplicação web
Deve ser adicionado outro parâmetro importante antes de aceder ao mesmo a partir do POSTMAN. O ecrã de configuração do servidor de autorização OAuth2 determinou que o ponto final para esta configuração é https:///authserver/oauth2. Para que o acesso a este ponto final seja tratado corretamente pela IRIS, precisamos de adicionar uma aplicação web para esta rota URL.

Vá à Administração do Sistema→SSecurity →Applicações→Web Applications, e clique em "Criaruma nova aplicação Web".

É fornecido um modelo de aplicação web OAuth2, por isso selecione primeiro "/oauth2" em "Copy from".
Definições de "Editar aplicações web"

Cópia de "/oauth2": Selecione sempre este primeiro na lista de drop-down.
Nome /authserver/oauth2
Ativação Verifique o botão de rádio "REST".

Depois de introduzir cada valor, guarde-o.

Teste OAuth2 do POSTMAN
Vamos testá-lo do CARTMAN. Os testes também podem ser feitos a partir de outras ferramentas ou do próprio programa. A explicação detalhada do POSTMAN está fora do âmbito deste artigo, mas um ponto a notar é que a verificação do certificado SSL deve ser alterada para OFF nas definições do POSTMAN.

Depois de criar um novo pedido no POSTMAN, selecione "OAuth 2.0" no separador TIPO DE PERMISSÃO e clique em "Obter Novo Token de Acesso".

No ecrã seguinte, insira os valores da seguinte forma.
Configurações「GET NOVO TOKEN DE ACESSO」
Nome simbólico Insira um nome à sua escolha.
Tipo de subvenção Escolha "Código de Autorização".
URL de retorno https://www.getpostman.com/oauth2/callback

Auth URL https:///authserver/oauth2/authorize Insira o valor do ponto final +/authorize. Ao adicionar ?uilocales=ja, pode exibir o ecrã de login em japonês.
Auth Token URL https:///authserver/oauth2/token. Introduza o valor do ponto final +/token.
ID do cliente Introduza o ID do cliente apresentado no separador Referências ao Cliente depois de guardar a descrição do cliente.
Segredo do Cliente Introduza a chave privada do cliente, que é apresentada no separador Referências ao Cliente depois de guardar a descrição do cliente.
Campo Introduza o âmbito guardado na configuração do servidor de autorização, por exemplo "scope1". Também pode especificar vários campos separados por espaços.
Estado Introduza o parâmetro de estado "Estado", que é utilizado para contramedidas contra o CSRF. Não é explicitamente usado, mas não pode ser deixado vazio, por isso entramos numa corda arbitrária.

Depois de introduzir as definições e clicar no botão "Request Token", verá o ecrã de login como mostrado abaixo.

Tente iniciar sedução com a informação do utilizador (por exemplo, SYSTEM) que tem acesso ao portal de gestão.
No ecrã seguinte após o início de sessão, pode decidir conceder permissões a esta aplicação. Depois de clicar em "Permitir", se o token de acesso for apresentado no ecrã seguinte, como mostrado abaixo, o teste de aquisição de token de acesso é bem sucedido!

Teste OpenID Connect
IRIS for Health pode realizar o processamento de autorização OAuth2, bem como o processamento de autenticação compatível OpenID Connect.Para mais detalhes consulte este documento.
Nesta configuração, o OpenID Connect está ativado, por isso vamos testar se também conseguimos obter o token OpenID Connect ID!
É fácil de implementar. No ecrã GET NEW ACCESS TOKEN, adicione "openid" ao seu âmbito e faça um pedido.

O OpenID Connect também será apresentado na página de pedido de permissão. Depois de iniciar sessão e dar as suas permissões, certifique-se de que também obtém um token de identificação (idtoken) quando vir o ecrã seguinte. (Pode ser necessário rolar.)

Conseguiu o sinal de acesso e idtoken?
Embora alguns preparativos, como certificados, exijam um pouco de tempo e esforço, poderíamos construir um servidor de autorização OAuth2 com tal simplicidade usando IRIS para a Saúde, uma plataforma de base de dados.
Na próxima parte desta série, vou finalmente mostrar-lhe como construir um repositório FHIR, registar o repositório FHIR como um servidor de recursos OAuth2, e mostrar-lhe como descansar o repositório FHIR usando um token de acesso OAuth2 da POSTMAN.
Ir para a publicação inicial escrita por @Shintaro Kaminaka

#FHIR #OAuth2 #InterSystems IRIS for Health

URL de origem:https://pt.community.intersystems.com/post/constru%C3%A7%C3%A3o-de-um-reposit%C3%B3rio-fhir-o-servidor-de-autoriza%C3%A7%C3%A3orecurso-oauth2-no-iris-health-parte