Guide technique Local OIDC Server

Points de terminaison

Le serveur local/oidcserver utilise quatre points de terminaison pour répondre aux sollicitations des clients Oauth :

- authorize_endpoint : <wwwroot>/local/oidcserver/endpoints/authorize.php
- token_endpoint : <wwwroot>/local/oidcserver/endpoints/token.php
- userinfo_endpoint : <wwwroot>/local/oidcserver/endpoints/userinfo.php
- revoke_endpoint : <wwwroot>/local/oidcserver/endpoints/revoke.php
- logout_endpoint : <wwwroot>/local/oidcserver/endpoints/logout.php
- jwks : <wwwroot>/local/oidcserver/endpoints/jwks.php
- config : <wwwroot>/local/oidcserver/endpoints/config.php

Cinématiques

Point de terminaison d'autorisation

Ce point de terminaison reçoit les demandes d'autorisation émise par les clients, et délivre un jeton temporaire d'autorisation si le client a été reconnu dans la configuration du serveur. La demande d'autorisation est envoyée par un agent utilisateur à partir du poste de l'utilisateur final.

Le serveur d'autorisation vérifie si une session est déjà active, provenant de l'utilisateur final (sur la base du cookie de session associé au serveur d'authentification).

Si aucune session n'est détectée, le serveur d'autorisation redirige l'utilisateur final vers sa séquence de connexion. La demande d'autorisation est mémorisée pendant cet échange, pour pouvoir être traitée par la fin du processus. L'utilisateur se connecte sur le serveur d'autorisation, qui crée une session, et vérifie les conditions d'admissibilité de l'utilisateur (droits à se faire autoriser pour ce client). La dernière étape est déclenchée.

Si une session a été détectée, l'utilisateur est considéré comme déjà connecté et l'étape suivante est automatiquement déclenchée.

En fin de traitement, le serveur d'autorisation renvoie l'agent utilisateur vers une entrée du serveur de ressource capable de traiter le jeton d'autorisation et poursuivre les échanges d'authentification.

Point de terminaison du jeton d'accès

Ce point de terminaison répond à un serveur de ressources pour valider l'accès, en vérifiant l'intégrité

et la “sincérité” du jeton d'autorisation que lui envoie l'agent utilisateur en rebond de la demande d'autorisation.

Le token d'autorisation est porté par une en-tête `Authorize:`, sous la forme d'un token “Bearer <crypted_token>”.

Le serveur d'autorisation confirme l'accès en renvoyant un jeton d'accès (Oauth2). Le server local/oidcserver prend en charge la couche supplémentaire OIDC en envoyant les “scopes” requis par une transmission d'identité OIDC.

Point de terminaison des infos utilisateur

Ce point de terminaison fournit une fiche de métadonnées étendue sur l'utilisateur, en fonction des règles de divulgation configurées dans le serveur d'autorisation, et/ou les “acceptations” de transmission de l'utilisateur propriétaire des données.

Point de terminaison de révocation (revoke)

Ce point de terminaison est utilisé par un client pour se déconnecter de la session Oauth2 et forcer la perte de validité de son token d'autorisation associé. La révocation, à elle seule ne constitue pas un acte de déconnexion de la fédération. D'autres sessions d'outils liés à la fédération peuvent rester connecté, ainsi que la session principale du fournisseur d'identité.

Point de terminaison de déconnexion fédéré (logout)

Ce point de terminaison reçoit une demande de déconnexion provenant du serveur de ressources, lorsque l'utilisateur final se déconnecte localement de ce dernier. La session présente sur le serveur d'autorisation est détruite. La reconnaissance de l'utilisateur concerné se fait sur la valeur du champ d'en-tête `Authorize:` qui doit porter le token d'accès.

Le serveur d'autorisation conserve la mémoire des token d'accès “actifs”. si lors d'une demande de déconnexion, d'autres tokens actifs sont identifiés pour l'utilisateur, alors le serveur local/oidcserver émettra des demandes de logout sur les points de terminaison de déconnexion des serveurs de ressources clients.

La demande de déconnexion cliente portera également le token d'accès (Bearer) dans le champ d'en-tête `Authorize:`

Point de terminaison de configuration (config)

Ce point de terminaison permet une lecture sans authentification de la configuration “publique” du serveur.

Point de terminaison de configuration JWKS

Ce point de terminaison permet une lecture sans authentification de la configuration du format JWKS (JSON Web Key Set). Il permet entre autre à n'importe quel tiers de récupérer les clefs publiques permettant de dialoguer avec le serveur de manière sécurisée.

Sommaire du plugin - Index des plugins - Accueil du catalogue