axway

Amplify APIM v7.7

Implémentation oauth

3 niveaux d’intégrations

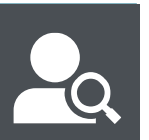
Oauth embarqué

Réaliser l’ensemble des fonctionnalités d’un serveur d’autorisation.

Oauth avec délégation

La gateway Axway d’autorisation délègue l’authentication à un idp externe.

Oauth externe



L’ensemble des fonctionnalité est délégué à l’IDP externe.

Pour consequence, la gestion des applications est réalisée du côté de l’IDP et non dans l’API-Manager

Le portail développeur dispose des fonctionnalités de test via la génération de Token oauth sans authentification de l’utilisateur.

Flow supportés

Amplify API Management propose l'ensemble des fonctionnalités ci-dessous lorsqu'elle est utilisée en tant que serveur d'Autorisations.

- Web-based client application registration
- Generation of authorization codes, access tokens, and refresh tokens
- Support for the following OAuth authentication flows:
  - Authorization code grant (web server)
  - Implicit grant (user agent)
  - Resource owner password credentials
  - Client credentials grant
  - JWT
  - Refresh token
  - Revoke token
  - Token information service
  - SAML assertion

Voir description détaillée dans la documentation Axway

Diagramme de flux « Authorization Code »

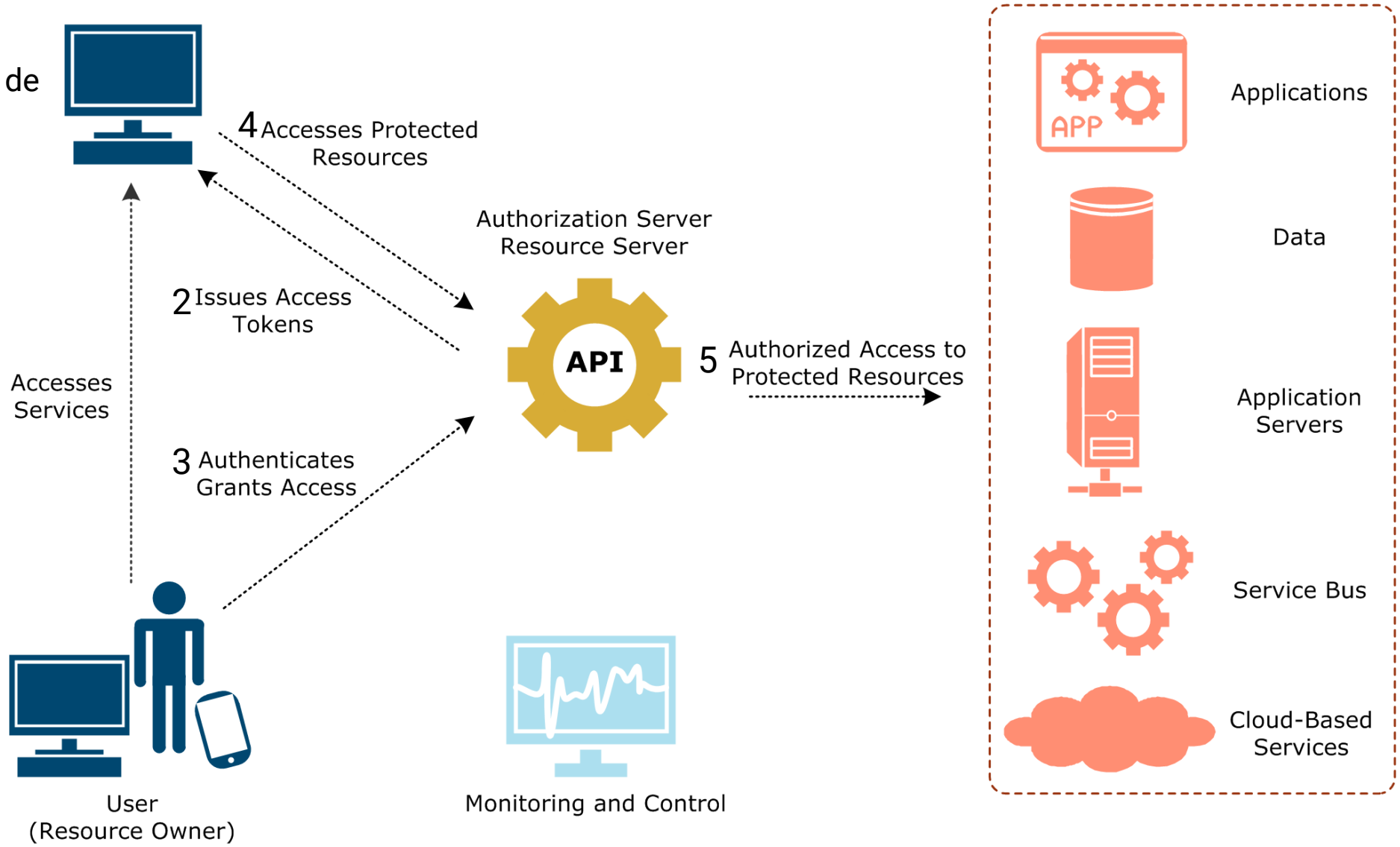
Resource Owner = le propriétaire de la resource

Client = Application réalisant la requête d'accès.

Resource Server = Amplify APIM

Authorization Server = Amplify APIM (ou votre IDP si externe)

Description détaillée du fonctionnement avec la gateway Axway sur ce lien.

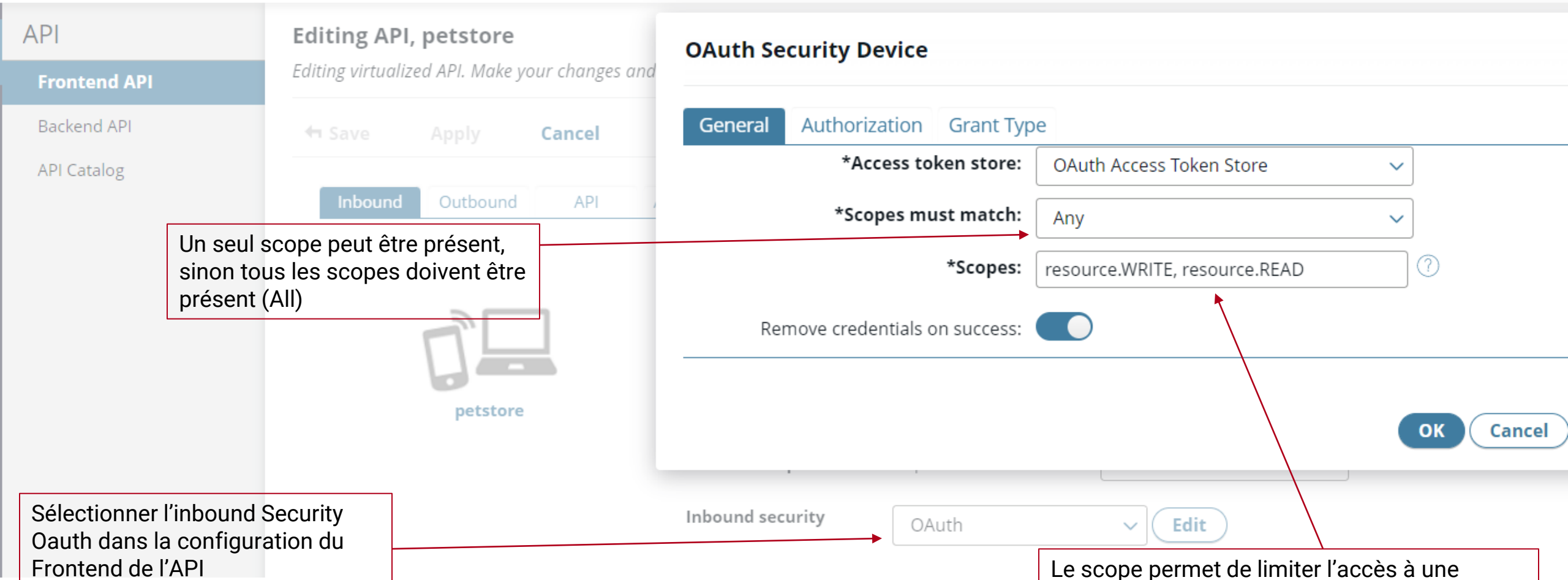


Liste des endpoints

https://docs.axway.com/bundle/axway-open-docs/page/docs/apim_policydev/apigw_oauth/gw_server/index.html

Authorization Endpoint (REST API)	**https://HOST:8089/api/oauth/authorize**
Token Endpoint (REST API)	https://HOST:8089/api/oauth/token
Token Info Endpoint (REST API)	https://HOST:8089/api/oauth/tokeninfo
Revoke Endpoint (REST API)	https://HOST:8089/api/oauth/revoke
Client Application Registry (HTML Interface)	https://HOST:8089
Client Application Registry (REST API)	https://HOST:8089/api/kps/ClientApplicationRegistry

Utilisation Oauth sur un frontend API



Un seul scope peut être présent, sinon tous les scopes doivent être présent (All)

Sélectionner l'inbound Security Oauth dans la configuration du Frontend de l'API

Le scope permet de limiter l'accès à une ressource sur une action, ou une API. Exemple : account.read, account.write, profile.read, transaction.read, etc

Configuration additionnelle

L'onglet « Authorization » définit uniquement la position du token ainsi que le prefix du header.

L'onglet « Grant Type » regroupe la configuration nécessaire pour l'ensembles des flows.

L'exemple ci-contre montre la configuration de « l'authorization code ». A l'exception des URL du serveur oauth, aucune autre modification n'est nécessaire. Celles-ci doivent être utilisées dans les paramètres de de la requête (voir ci-dessous dans Postman).