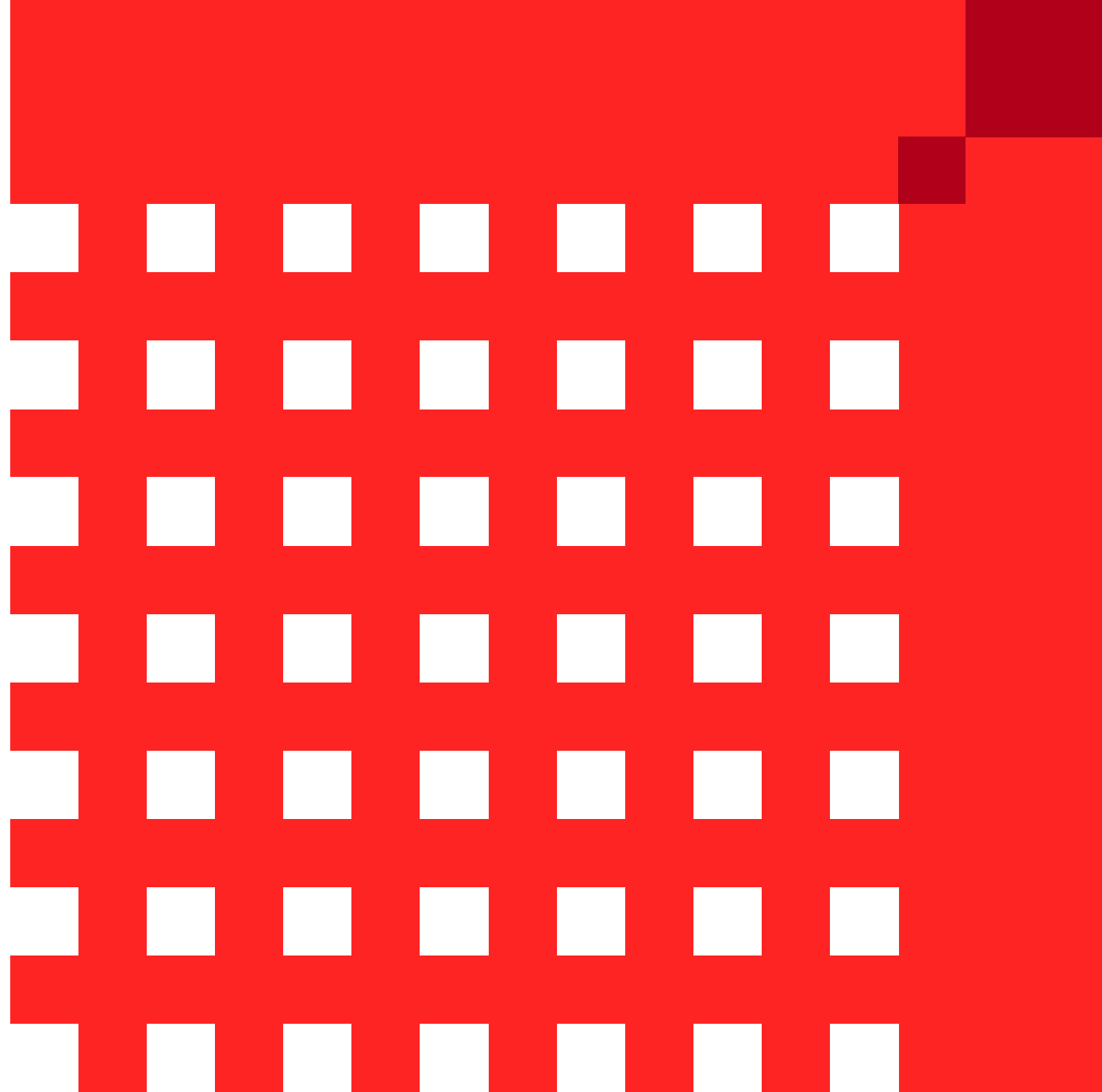


Amplify APIM v7.7

Implémentation oauth



3 niveaux d'intégrations



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 »

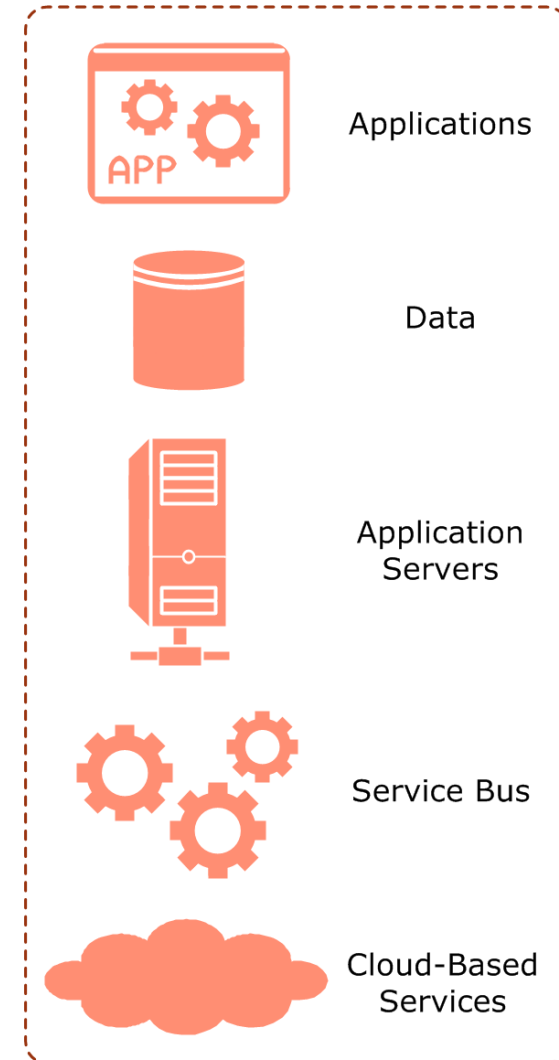
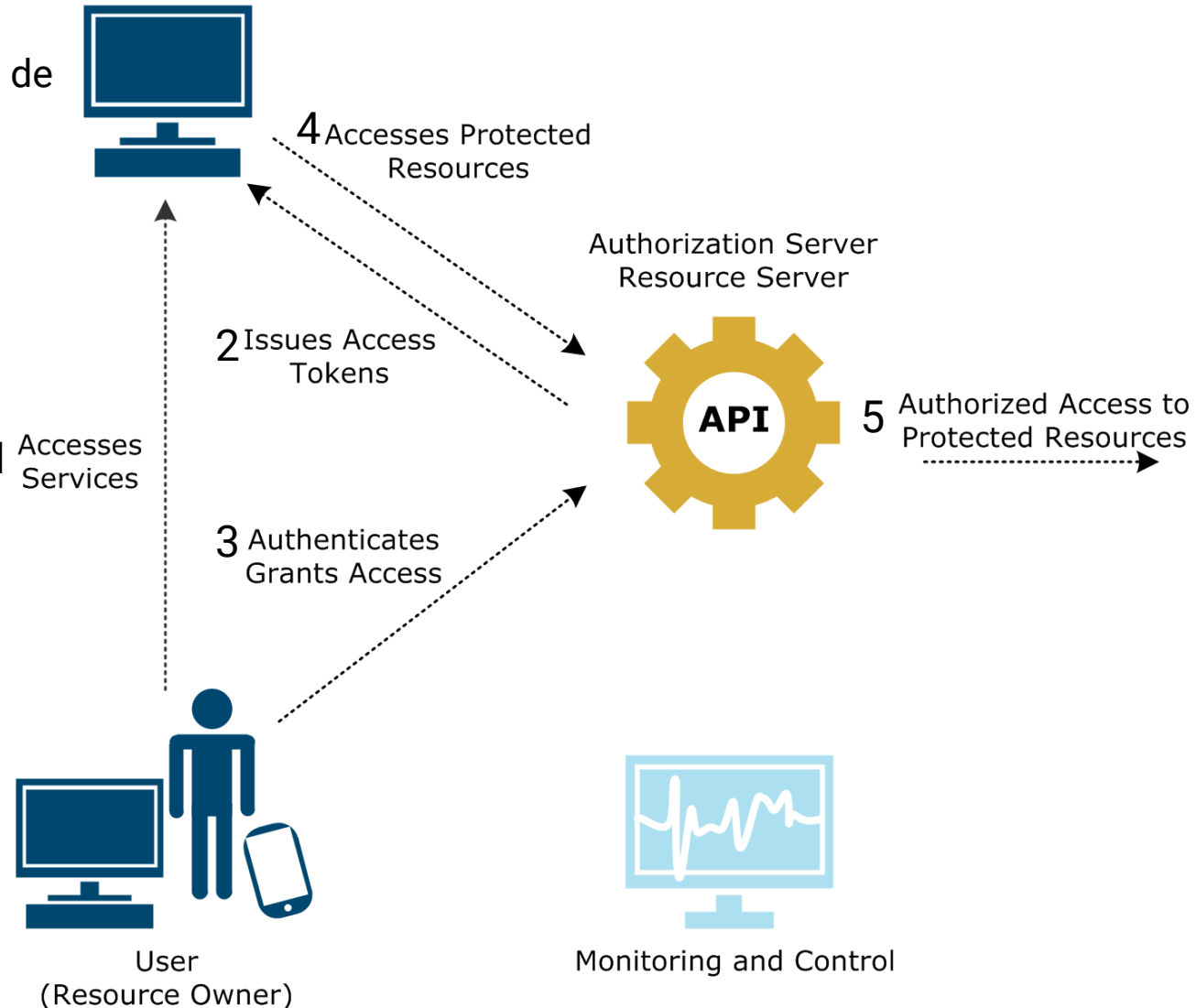
Resource Owner = le propriétaire de la ressource

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

Utilisation Oauth sur un frontend API

The screenshot shows the 'Editing API, petstore' interface. On the left, a sidebar lists 'API', 'Frontend API' (selected), 'Backend API', and 'API Catalog'. The main area has tabs for 'Inbound', 'Outbound', and 'API'. The 'Inbound' tab is active, showing 'Inbound security' with a dropdown set to 'OAuth' and an 'Edit' button. A modal window titled 'OAuth Security Device' is open, showing the 'General' tab. It contains fields for '*Access token store:' (set to 'OAuth Access Token Store'), '*Scopes must match:' (set to 'Any'), and '*Scopes:' (set to 'resource.WRITE, resource.READ'). A toggle for 'Remove credentials on success:' is also visible. Red arrows point from text boxes to these specific configuration elements.

API

Frontend API

Backend API

API Catalog

Editing API, petstore

Editing virtualized API. Make your changes and

Save Apply Cancel

Inbound Outbound API

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

petstore

Inbound security OAuth Edit

OAuth Security Device

General Authorization Grant Type

*Access token store: OAuth Access Token Store

*Scopes must match: Any

*Scopes: resource.WRITE, resource.READ

Remove credentials on success: ☒

OK Cancel

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'autorization 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).

Token Name

access_token

Grant Type

Authorization Code

Callback URL ⓘ

https://oauth.pstmn.io/v1/callback

☒ Authorize using browser

Auth URL ⓘ

https://[redacted]:8089/api/oauth/author...

Access Token URL ⓘ

https://[redacted]:8089/api/oauth/token

Client ID ⓘ

42d57305-f4ee-4dcb-bcae-15f0a5449C... ⚠

Client Secret ⓘ

66344864-b2ee-4020-b00f-84f8afb4c11f ⚠

Scope ⓘ

resource.READ

General

Authorization

Grant Type

Implicit

Authorization Code

Client Credentials

The authorization code is obtained by using an authorization server as an intermediary between the cli and resource owner.

The authorization code grant type cannot be configured here, the OAuth Authorization Server is responsible for configuring the authorization code grant type.

You can publish the currently configured authorization code grant type information below to the API Catalog. Doing so will advertise these details to clients of this API so that they can successfully retrieve : access token, and subsequently supply the access token for verification by this security device when invoking this API.

Publish to API Catalog:

☒

*Request endpoint URL:

https://[redacted]:8089/api/oauth/auth

*Request client ID name:

client_id

*Request client secret name:

client_secret

*Token URL:

https://[redacted]:8089/api/oauth/toke

*Token name:

access_code