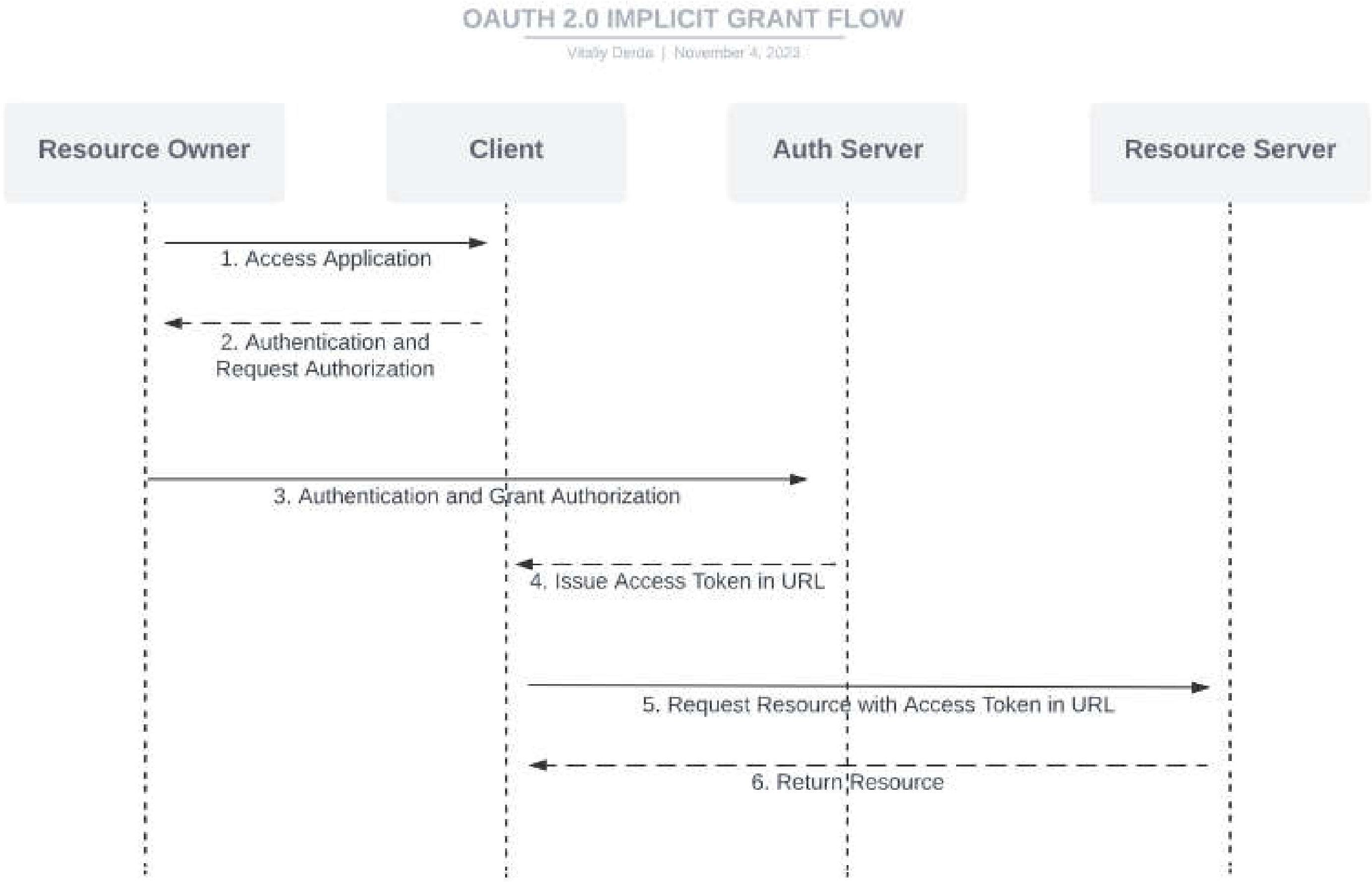
OAUTH 2.0. IMPLICIT GRANT FLOW

The following diagram shows the flow for the Implict grant type:


OAUTH 2.0 IMPLICIT GRANT FLOW
Vitaliy Derda | November 4, 2023
Resource Owner
Client
Auth Server
Resource Server
1. Access Application
2. Authentication and Request Authorization
3. Authentication and Grant Authorization
4. Issue Access Token in URL
5. Request Resource with Access Token in URL
6. Return Resource

The flow of the Implicit grant type is:

1. **Access Application**: The user accesses the app and triggers authentication and authorization.
2. **Authentication and Request Authorization**: The app prompts the user for their username and password. The first time the user goes through this flow for the app, the user sees an approval page. On this page, the user can choose permissions to authorize the app to access resources on their behalf.
3. **Authentication and Grant Authorization**: The authorization server receives the authentication and authorization grant.
4. **Issue Access Token**: The authorization server validates the authorization code and returns an access token with the redirect URL.
5. **Request Resource w/ Access Token in**: The app attempts to access the resource from the resource server by presenting the access token in the URL.
6. **Return Resource**: If the access token is valid, the resource server returns the resources that the user authorized the app to receive.

The resource server runs in TAS for VMs under a given space and org. Developers set the permissions for the resource server API endpoints. To do this, they create resources that correspond to API endpoints secured by Single Sign-On. apps can then access these resources on behalf of users.