Enhancement - ADFS Scopes

Motivation:

As part of continuous improvement, users would like a improved interaction with the oauth2 process. Currently, users login with their user-id (trp1234) in production, and receive a access-token (see below)

Issue:

* This access-token will contain all user groups for given-user, which can grow to several ten's or hundreds of groups. This translates to several KB http-header, which AWS load-balancers will reject.

Enhancements:

- Use scopes!
  - https://api.dev.awstrp.net/oauth2/token?scope=***aim,katana***
  - ***https://api.dev.awstrp.net/oauth2/authorize?apikey=API_KEY_REDACTED&response_type=code&scope=katana***
- - In the example above, only LDAP groups for "aim" and "katana" will be matched and returned for given users-credentials.
- Obtaining production JWT credentials in non-production environments.

Production-credentials in non-production environments

Use-case: Development teams would like to use production JWT token as the standard to access services that are deployed in higher environment. Example: From DEV use services deployed in STAGE

Implementation: Pass oauth_env=prod or oauth_env=stage to the oauth API, and your credentials will be validated against PROD-ADFS and STAGE-ADFS, respectively. Pass your credentials as you normally would.

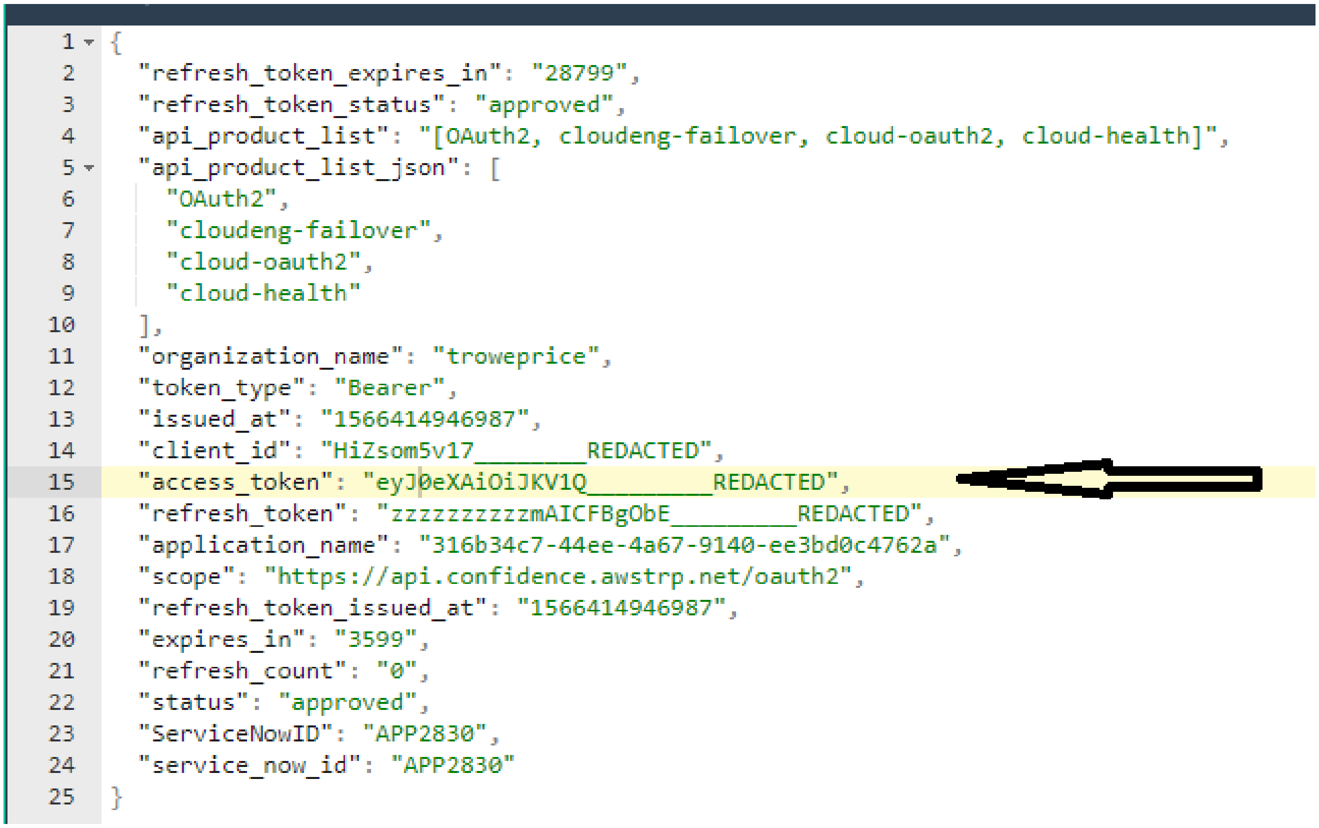
https://api.dev.awstrp.net/oauth2/token?oauth_env=stage

https://api.dev.awstrp.net/oauth2/token?oauth_env=prod

Getting Started

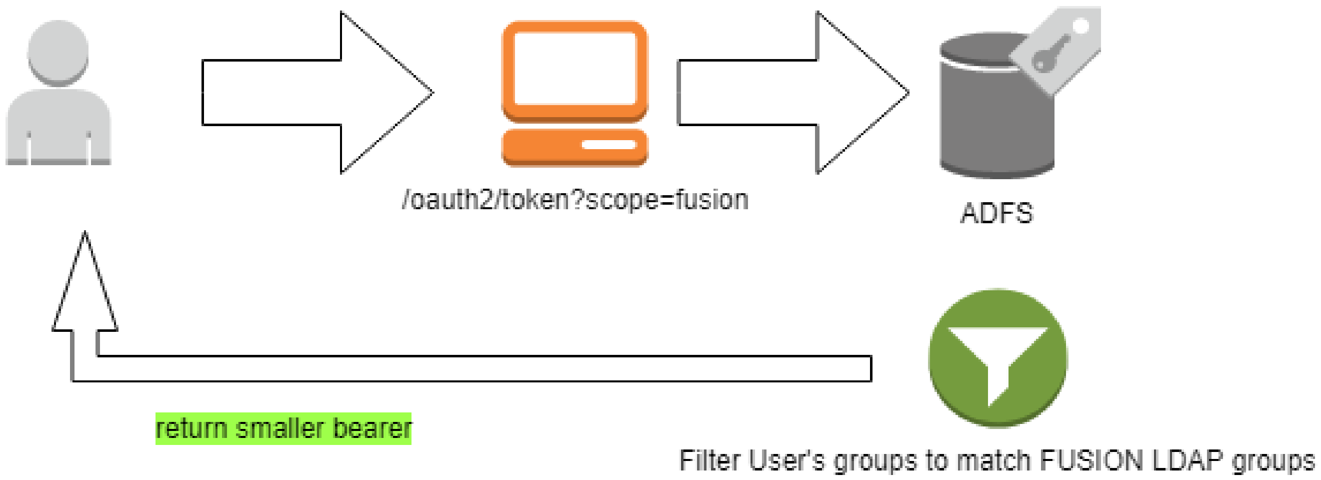
- Onboard your scope and desired LDAP-groups here - https://gitlab.awstrp.net/coretech-oauth/scopes
- Once you receive confirmation from LDAP-team, you should able to get started.

Thanks - Erik Sheely Steven Nakhla



```
{
  "refresh_token_expires_in": "28799",
  "refresh_token_status": "approved",
  "api_product_list": "[OAuth2, cloudeng-failover, cloud-oauth2, cloud-health]",
  "api_product_list_json": [
    "OAuth2",
    "cloudeng-failover",
    "cloud-oauth2",
    "cloud-health"
  ],
  "organization_name": "troweprice",
  "token_type": "Bearer",
  "issued_at": "1566414946987",
  "client_id": "HiZsom5v17________REDACTED",
  "access_token": "eyJ0eXAiOiJKV1Q_________REDACTED",
  "refresh_token": "zzzzzzzzzzmAICFBgObE_________REDACTED",
  "application_name": "316b34c7-44ee-4a67-9140-ee3bd0c4762a",
  "scope": "https://api.confidence.awstrp.net/oauth2",
  "refresh_token_issued_at": "1566414946987",
  "expires_in": "3599",
  "refresh_count": "0",
  "status": "approved",
  "ServiceNowID": "APP2830",
  "service_now_id": "APP2830"
}
```

Enhancement - ADFS Scopes


/oauth2/token?scope=fusion
ADFS
return smaller bearer
Filter User's groups to match FUSION LDAP groups