Cloud Foundry UAA Tutorial

Paulo Jerônimo, 2018-06-06 01:02:09 WEST

Table of Contents

1. UAA local test

Shell 1

```
$ mkdir -p ~/Projects/github.com/cloudfoundry && cd $_
$ [ -d uaa ] || git clone https://github.com/cloudfoundry/uaa
$ cd uaa
$ ./gradlew run
```

Shell 2

```
$ cd
$ type uaac &> /dev/null || sudo gem install cf-uaac
$ rm -f ~/.uaac.yml
```

```
$ uaac target http://localhost:8080/uaa
Unknown key: Max-Age = 86400

Target: http://localhost:8080/uaa

$ cat ~/.uaac.yml
---
http://localhost:8080/uaa:
  current: true
  ca_cert:
```

```
$ uaac token client get admin -s adminsecret
Unknown key: Max-Age = 86400

Successfully fetched token via client credentials grant.
Target: http://localhost:8080/uaa
Context: admin, from client admin

$ cat ~/.uaac.yml
---
http://localhost:8080/uaa:
  current: true
  ca_cert:
  prompts:
    username:
    - text
    - Email
    password:
    - password
    - Password
  contexts:
    admin:
      current: true
      client_id: admin
      access_token:
eyJhbGciOiJIUzI1NiIsImtpZCI6ImxlZ2FjeS10b2tlbi1rZXkiLCJ0eXAiOiJKV1QifQ.eyJqdGGkiOiIzNmR
kYmNiNDM0NmU0MzNiYjQ5NzU5N2I1YjE1YWVjZiIsInN1YiI6ImFkbWluIiwiYXV0aG9yaXRpZXMiOlsiY2xpZ
W50cy5yZWFkIiwiY2xpZW50cy5zZWNyZXQiLCJjbGllbnRzLndyaXRlIiwidWFhLmFkbWluIiwiY2xpZW50cy5
hZG1pbiIsInNjaW0ud3JpdGUiLCJzY2ltLnJlYWQiXSwic2NvcGUiOlsiY2xpZW50cy5yZWFkIiwiY2xpZW50c
y5zZWNyZXQiLCJjbGllbnRzLndyaXRlIiwidWFhLmFkbWluIiwiY2xpZW50cy5hZG1pbiIsInNjaW0ud3JpdGU
iLCJzY2ltLnJlYWQiXSwiY2xpZW50X2lkIjoiYWRtaW4iLCJjaWQiOiJhZG1pbiIsImF6cCI6ImFkbWluIiwiZ
3JhbnRfdHlwZSI6ImNsaWVudF9jcmVkZW50aWFscyIsInJldl9zaWciOiIyYTAyYjE2YyIsImlhdCI6MTUyODI
zMTQyMSwiZXhwIjoxNTI4Mjc0NjIxLCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODAvdWFhL29hdXRoL3Rva
2VuIiwiemlkIjoidWFhIiwiYXVkIjpbInNjaW0iLCJjbGllbnRzIiwidWFhIiwiYWRtaW4iXX0.25Gz3eYy_e-
_0M7jQelWzHQAk8odKH2Uzinqsb1Ggug
      token_type: bearer
      expires_in: 43199
      scope:
      - clients.read
      - clients.secret
      - clients.write
      - uaa.admin
      - clients.admin
      - scim.write
      - scim.read
      jti: 36ddbcb4346e433bb497597b5b15aecf
```

```
$ uaac context

[0]*[http://localhost:8080/uaa]

  [0]*[admin]
      client_id: admin
      access_token:
```
```
eyJhbGciOiJIUzI1NiIsImtpZCI6ImxlZ2FjeS10b2tlbi1rZXkiLCJ0eXAiOiJKV1QifQ.eyJqdGkiOiIzNmR
kYmNiNDM0NmU0MzNiYjQ5NzU5N2I1YjE1YWVjZiIsInN1YiI6ImFkbWluIiwiYXV0aG9yaXRpZXMiOlsiY2xpZ
W50cy5yZWFkIiwiY2xpZW50cy5zZWNyZXQiLCJjbGllbnRzLndyaXRlIiwidWFhLmFkbWluIiwiY2xpZW50cy5
hZG1pbiIsInNjaW0ud3JpdGUiLCJzY2ltLnJlYWQiXSwic2NvcGUiOlsiY2xpZW50cy5yZWFkIiwiY2xpZW50c
y5zZWNyZXQiLCJjbGllbnRzLndyaXRlIiwidWFhLmFkbWluIiwiY2xpZW50cy5hZG1pbiIsInNjaW0ud3JpdGU
iLCJzY2ltLnJlYWQiXSwiY2xpZW50X2lkIjoiYWRtaW4iLCJjaWQiOiJhZG1pbiIsImF6cCI6ImFkbWluIiwiZ
3JhbnRfdHlwZSI6ImNsaWVudF9jcmVkZW50aWFscyIsInJldl9zaWciOiIyYTAyYjE2YyIsImlhdCI6MTUyODI
zMTQyMSwiZXhwIjoxNTI4Mjc0NjIxLCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODAvdWFhL29hdXRoL3Rva
2VuIiwiemlkIjoidWFhIiwiYXVkIjpbInNjaW0iLCJjbGllbnRzIiwidWFhIiwiYWRtaW4iXX0.25Gz3eYy_e-
_0M7jQelWzHQAk8odKH2Uzinqsb1Ggug
```
```
      token_type: bearer
      expires_in: 43199
      scope: clients.read clients.secret clients.write uaa.admin clients.admin
scim.write scim.read
      jti: 36ddbcb4346e433bb497597b5b15aecf
```

```
$ uaac token decode

Note: no key given to validate token signature

  jti: 36ddbcb4346e433bb497597b5b15aecf
  sub: admin
  authorities: clients.read clients.secret clients.write uaa.admin clients.admin
scim.write scim.read
  scope: clients.read clients.secret clients.write uaa.admin clients.admin scim.write
scim.read
  client_id: admin
  cid: admin
  azp: admin
  grant_type: client_credentials
  rev_sig: 2a02b16c
  iat: 1528231421
  exp: 1528274621
  iss: http://localhost:8080/uaa/oauth/token
  zid: uaa
  aud: scim clients uaa admin
```

```
$ uaac user add smokeuser --given_name smokeuser --family_name smokeuser --emails
smokeuser@mail.com --password smokepassword
user account successfully added
```

```
$ uaac users | grep smokeuser
      familyname: smokeuser
      givenname: smokeuser
      value: smokeuser2@mail.com
    username: smokeuser
```

```
$ uaac group add "smoke.extinguish"
  id: fa615872-4ec7-4e76-8420-18054ab92a6b
  meta
    version: 0
    created: 2018-06-05T23:57:20.091Z
    lastmodified: 2018-06-05T23:57:20.091Z
  members:
  schemas: urn:scim:schemas:core:1.0
  displayname: smoke.extinguish
  zoneid: uaa

$ uaac member add smoke.extinguish smokeuser
success
```

```
$ uaac client add smoke --name smoke --scope "smoke.extinguish"
--authorized_grant_types "password" -s "smokesecret"
  scope: smoke.extinguish
  client_id: smoke
  resource_ids: none
  authorized_grant_types: password refresh_token
  autoapprove:
  authorities: uaa.none
  name: smoke
  required_user_groups:
  lastmodified: 1528239527414
  id: smoke
```

```
$ uaac token owner get smoke smokeuser -s smokesecret -p smokepassword

Successfully fetched token via owner password grant.
Target: http://localhost:8080/uaa
Context: smokeuser, from client smoke
```

```
$ uaac context

[0]*[http://localhost:8080/uaa]

  [1]*[smokeuser]
      user_id: 3b2dda2c-a859-461a-b32e-633c76a3684c
      client_id: smoke
      access_token:
```
```
eyJhbGciOiJIUzI1NiIsImtpZCI6ImxlZ2FjeS10b2tlbi1rZXkiLCJ0eXAiOiJKV1QifQ.eyJqdGkiOiIzMDc
yNTdmY2E2Yzg0ZTY5OTdlZGI5NzVhNmExMTcxMSIsInN1YiI6IjNiMmRkYTJjLWE4NTktNDYxYS1iMzJlLTYzM
2M3NmEzNjg0YyIsInNjb3BlIjpbInNtb2tlLmV4dGluZ3Vpc2giXSwiY2xpZW50X2lkIjoic21va2UiLCJjaWQ
iOiJzbW9rZSIsImF6cCI6InNtb2tlIiwiZ3JhbnRfdHlwZSI6InBhc3N3b3JkIiwidXNlcl9pZCI6IjNiMmRkY
TJjLWE4NTktNDYxYS1iMzJlLTYzM2M3NmEzNjg0YyIsIm9yaWdpbiI6InVhYSIsInVzZXJfbmFtZSI6InNtb2t
ldXNlciIsImVtYWlsIjoic21va2V1c2VyMkBtYWlsLmNvbSIsImF1dGhfdGltZSI6MTUyODIzOTYwOCwicmV2X
3NpZyI6IjhhYjBhMDg3IiwiaWF0IjoxNTI4MjM5NjA4LCJleHAiOjE1MjgyODI4MDgsImlzcyI6Imh0dHA6Ly9
sb2NhbGhvc3Q6ODA4MC91YWEvb2F1dGgvdG9rZW4iLCJ6aWQiOiJ1YWEiLCJhdWQiOlsic21va2UiXX0.4u-
RJcdg76Rk4MPIV6SM4jTwy_8zFcnBErRBKIWIE6Y
```
```
      token_type: bearer
      refresh_token:
```
```
eyJhbGciOiJIUzI1NiIsImtpZCI6ImxlZ2FjeS10b2tlbi1rZXkiLCJ0eXAiOiJKV1QifQ.eyJqdGkiOiIyMTF
iMGZlNzkzNmM0Y2NkYmRjMDdlNWFhMTIzOGIyNC1yIiwic3ViIjoiM2IyZGRhMmMtYTg1OS00NjFhLWIzMmUtN
jMzYzc2YTM2ODRjIiwic2NvcGUiOlsic21va2UuZXh0aW5ndWlzaCJdLCJpYXQiOjE1MjgyMzk2MDgsImV4cCI
6MTUzMDgzMTYwOCwiY2lkIjoic21va2UiLCJjbGllbnRfaWQiOiJzbW9rZSIsImlzcyI6Imh0dHA6Ly9sb2Nhb
Ghvc3Q6ODA4MC91YWEvb2F1dGgvdG9rZW4iLCJ6aWQiOiJ1YWEiLCJncmFudF90eXBlIjoicGFzc3dvcmQiLCJ
1c2VyX25hbWUiOiJzbW9rZXVzZXIiLCJvcmlnaW4iOiJ1YWEiLCJ1c2VyX2lkIjoiM2IyZGRhMmMtYTg1OS00N
jFhLWIzMmUtNjMzYzc2YTM2ODRjIiwicmV2X3NpZyI6IjhhYjBhMDg3IiwiYXVkIjpbInNtb2tlIl19.fMW6fY
qf7AeT7vxe2-4eioPq1WXhRp_iKU3pm3KrRVg
```
```
      expires_in: 43199
      scope: smoke.extinguish
      jti: 307257fca6c84e6997edb975a6a11711
```

2. References

- https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2

- https://docs.run.pivotal.io/concepts/architecture/uaa.html

- https://docs.cloudfoundry.org/concepts/high-availability.html

- https://docs.cloudfoundry.org/uaa/uaa-user-management.html

- https://github.com/cloudfoundry/uaa/blob/master/docs/UAA-Security.md

- http://www.java-allandsundry.com/2017/02/using-uaa-oauth2-authorization-server.html

    - https://github.com/bijukunjummen/oauth-uaa-sample

- http://www.java-allandsundry.com/2017/02/bootstrapping-oauth2-authorization.html

- https://www.jhipster.tech/using-uaa/#jhipster-uaa

- https://ronaldwildenberg.com/cloudfoundry/2017/12/01/run-local-uaa.html

- https://downey.io/notes/dev/create-cloud-foundry-read-only-admin/

- https://sks.gitbooks.io/my-road-2-industrial-applications/content/en/Security/registering_client_in_uaa.html