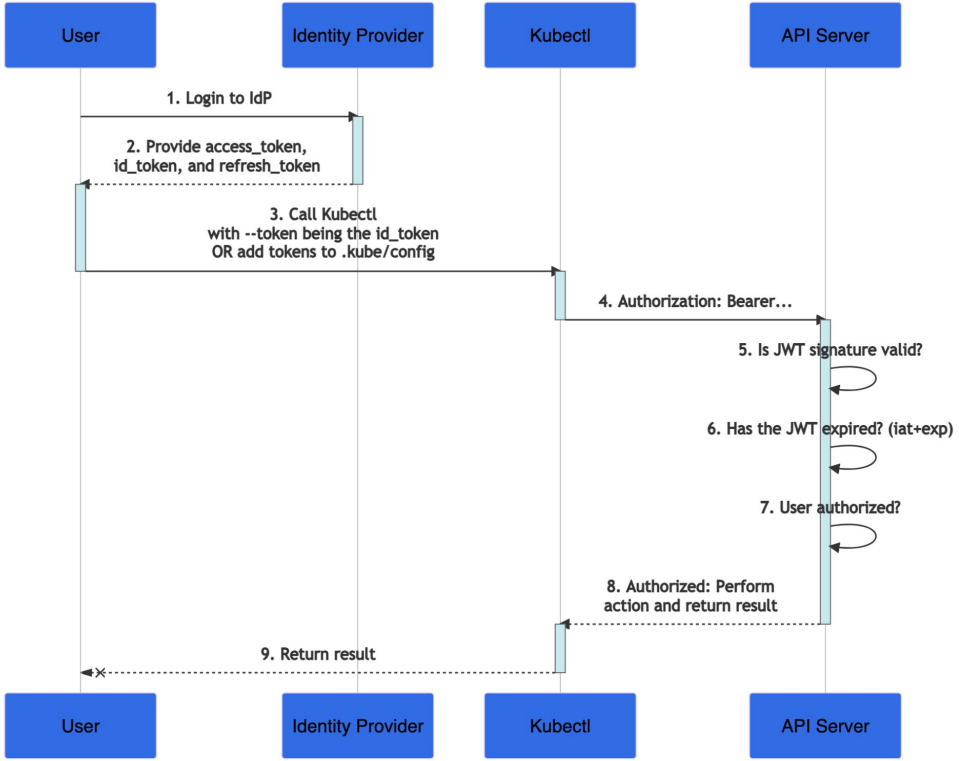
CiLogon tokens in kubernetes

Dima Mishin

SDSC & Calit2/Qualcomm Institute, UCSD

PACIFIC RESEARCH PLATFORM

Kubernetes supports OIDC tokens out of the box



https://kubernetes.io/docs/reference/access-authn-authz/authentication/#openid-connect-tokens

PACIFIC RESEARCH PLATFORM

Using CiLogon for multiple services on Nautilus

- Users authentication in user portal
- Users authentication with the kubernetes API server
- Users authentication in Jupyter hubs
- SSO (NextCloud, GitLab, etc)

PACIFIC RESEARCH PLATFORM

Public client to give to users

Client registration:

◉ Confidential ○ Public

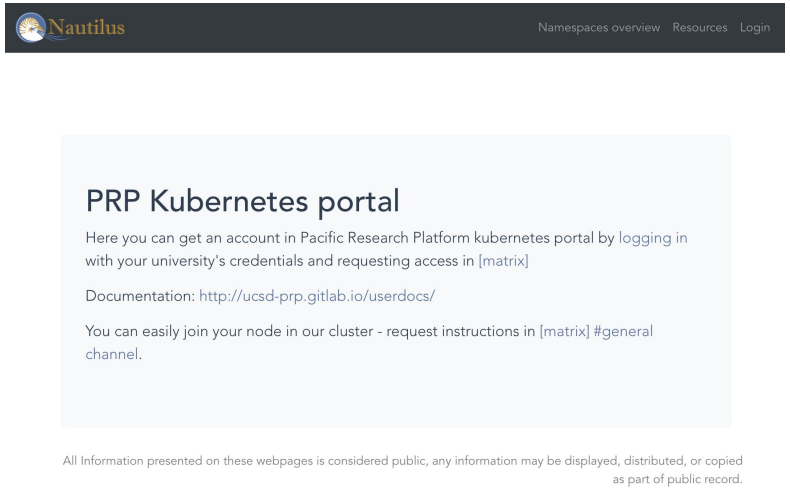
A Public client does not use a client_secret and allows ONLY the "openid" scope.

PRP PACIFIC RESEARCH PLATFORM

it²

Custom made user portal

- Login using CILogon via confidential client
- Get generated kubernetes config file using public client
- Portal sets up user permissions in the cluster based on user ID
- Users are only allowed to create namespaces through the portal
  - Verify the namespace doesn't exist
  - Set up RBAC rules for the user
  - Additional users can be added to namespace by the owner



PACIFIC RESEARCH PLATFORM

With public client kubectl can refresh

kubectl config:

```
- name: <User ID>
  user:
    auth-provider:
      config:
        client-id: <The public client ID>
        client-secret: <The public client secret to refresh the token>
        id-token: <JWT token to access the cluster>
        idp-issuer-url: https://cilogon.org
        refresh-token: <Refresh token>
      name: oidc
```

Kubernetes apiserver config:

```
- --oidc-issuer-url=https://cilogon.org
- --oidc-client-id=<The public client ID>
- --oidc-username-prefix=-
```

PACIFIC RESEARCH PLATFORM

it²

Problem with the auth flow

- Users are authenticated twice: to login and to get the config (different clients)
  - Can use different auth providers => different users => different permissions in the cluster (confusing to users)
    - Example: UCSD AD and Google

PACIFIC RESEARCH PLATFORM

Problem with renewing the token

- Kubectl can be accessed concurrently
  - Several parallel attempts to renew the token => last one doesn't succeed and overwrites the good config
    - Sometimes causes avalanche of requests to CiLogon for unknown reasons

PRP PACIFIC RESEARCH PLATFORM

it²

ACKs

This work was supported in part by
NSF awards CNS-1730158, ACI-1540112, ACI-1541349, OAC-1826967,
The University of California Office of the President,
The University of California San Diego's California Institute for Telecommunications and Information Technology/Qualcomm Institute.
And thanks to CENIC and Internet2 for the 100 Gbps networks

PACIFIC RESEARCH PLATFORM