



CHEOPS TECHNOLOGY

The Cloud & Data Centric Company

Arrêtez le Full Admin dans k8s !

Mettez de l'OIDC dans votre vie...



Qui suis-je?



Philippe Durand

Consultant K8S, IA, Performance applicative et infrastructure
@ Cheops Technology



philippe-durand-work

J'accompagne les clients « From Zero to Hero »



Authentification vs Autorisation

Authentification

Le serveur me croit quand je dis être Philippe Durand.



C'est bien
Philippe

Oui, c'est
bien Philippe



Multi Factor Authentication

Authentification vs Autorisation

Autorisation :

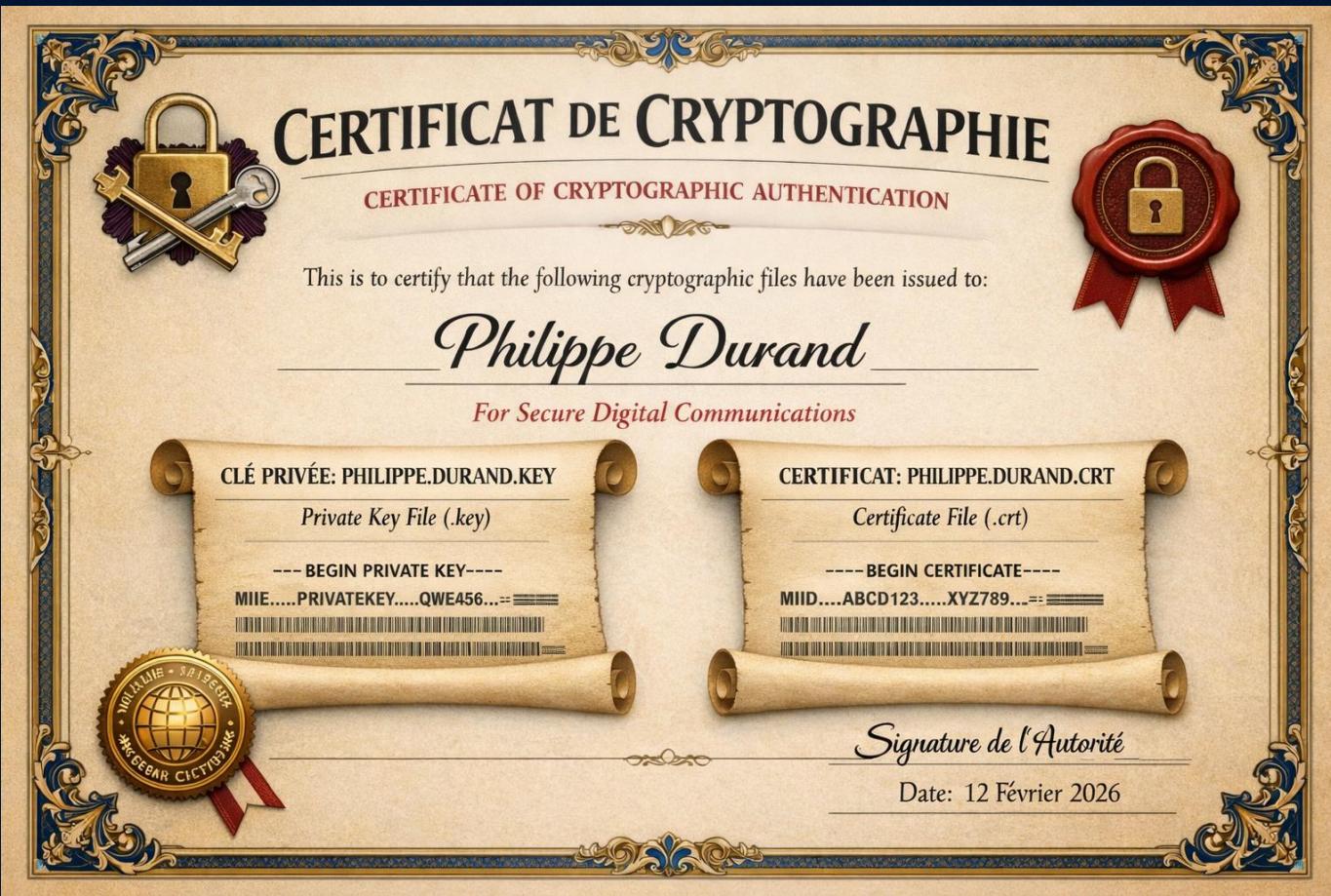
Philippe a le droit de lecture seule.



Role Based Access Control



Accès interdit
aux personnes
non autorisées



Authentification

Avec des certificats

Authentification

Certificats Utilisateur



Terminal

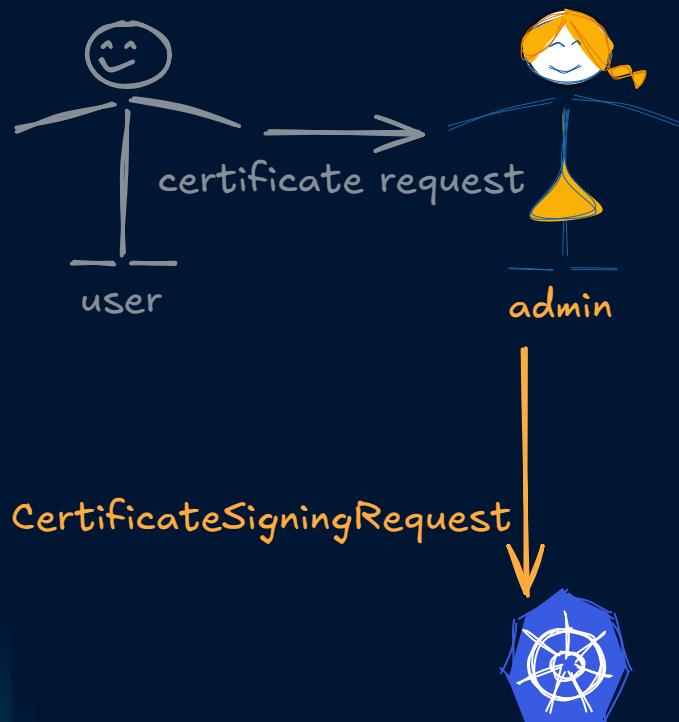
```
$ openssl genrsa -out philippe.key 2048
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC4wn30qxx5J5ir
JFD4fkK+1ul5sXsSYkN5S2RoCq67kbb4ucMJqdjtI6bYzy0WV8cj4AR3/TThCcTh
6pPWZz5BxW+K32xvWJLB+j3R
-----END PRIVATE KEY-----
```



```
$ openssl req -new -key philippe.key -subj "/CN=philippe.durand" -out philippe.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICXzCCAUcCAQAwGjEYMBYGA1UEAwwPcGhpbgLwcGUuZHVsYw5kMIIBIjANBgkq
hkiG9w0BAQEFAOCAQ8AMIIIBCgKCAQEAvMJ9zqsceSeYqyRQ+H5CvtbpebF7EmJD
6oD0dvRnFEYKQNKYvhprihVITKT8g9TMbKJga9SAinc7sdM=
-----END CERTIFICATE REQUEST-----
```

Authentification

Certificats Utilisateur



Terminal

```
$ cat philippe.csr | base64 | tr -d '\n'; echo ;  
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0KTUlJQ1h6Q0NBVWNDQVFBD0dqRVLNQllHQTFVRUF  
3d1BjR2hwYkdsd2NHVXVaSFZ5WVc1a01JSUJJakFOQmdrcQpoa2lHOXcwQkFRRUZBQWluYzdzZE09Ci0tLS0tRU  
5EIENFULRJRkldQVRFIFJFUVVFU1QtLS0tLQo=
```

csr.yaml

```
apiVersion: certificates.k8s.io/v1  
kind: CertificateSigningRequest  
metadata:  
  name: philippe-durand  
spec:  
  request: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSBSRVFVRVNULS0tLS0KTUlJQ1h6Q0NBVWNDQVFBD0dqRVLNQ  
  signerName: kubernetes.io/kube-apiserver-client  
  expirationSeconds: 86400  
  usages:  
    - client auth
```

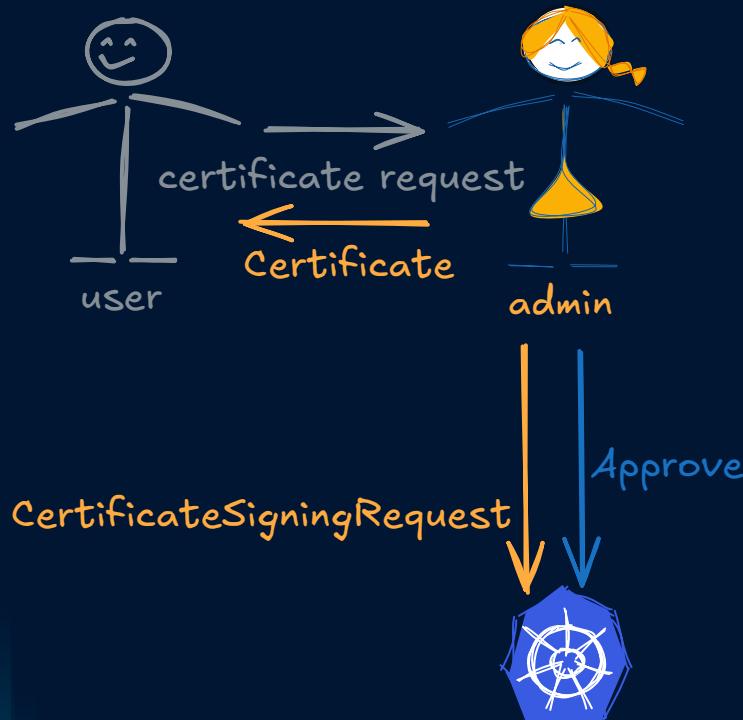
Terminal

```
$ k apply -f csr.yaml  
certificatesigningrequest.certificates.k8s.io/philippe-durand created  
$ k get csr philippe-durand
```

NAME	AGE	SIGNERNAME	REQUESTOR	REQUESTEDDURATION	CONDITION
philippe-durand	68s	kubernetes.io/kube-apiserver-client	admin	24h	Pending

Authentification

Certificats Utilisateur

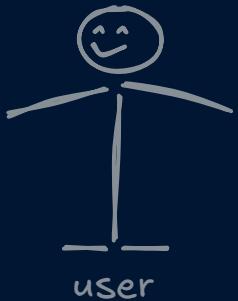


Terminal

```
$ k certificate approve philippe-durand
certificatesigningrequest.certificates.k8s.io/philippe-durand approved
$ k get csr philippe-durand -o jsonpath=".status.certificate"; echo;
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUNQekNDQWVXZ0F3SUJBZ0lSQU0vRW92V0xGN0YwNVpIcZ
2dxaGtqT1BRUURBZ05JQURCRkFpQk52NlNrZjJESephac5c1gydC96SwpyZE5XSS8ydytmRkMvM1JoeWJsMXVB
SWhBTxdUV21u0XB1U1UzTk1qY0Za0VpzQVZ5YlJDQVJFdFhySC9zSVNPKcJNZVAKLS0tLS1FTkQgQ0VSVElGSUN
BVEUtLS0tLQo=
$ k get csr philippe-durand -o jsonpath=".status.certificate" | base64 -d
-----BEGIN CERTIFICATE-----
MIICPzCCAeWgAwIBAgIRAM/EovWL7F05ZeR0e8ltNowCgYIKoZIzj0EAwIwFTET
MBEGA1UEChMKa3ViZXJuZXRLczAeFw0yNjAyMDgwNjU0MTlaFw0yNjAyMDkwNjU0
MTlaMBoxGDAwBgNVBAMTD3BoaWxpCHBLmR1cmFuZDCCASIwDQYJKoZIhvCNQEB
BQADggEPADCCAQoCggEBALjcFc6rHHknmKskUPh+Qr7W6XmxexJiQ3lLZGgKrruR
tvI5wwmp200jptjPi5ZXxyPgBF9NOEJxOGNvFCkmnofupGGmYsi1CmLPS72QJVL
Vm7bCgzMgwJj3zaP0Vnzh+SLAP3ztzM+8wzaxa+Wb3Dv+eGUofSiFFr0VztLhLmP
/7Dyx0ZJb0983poVySVbmSiV3BEf62l07PoCXci6FNqpjHX5llYTdQH+1irQjvcT
VyOHRSgUF0UaoZrdyl973R2RwsNw0/bf1ZZ8Yik5RkEbTYttjL3NvsqMBMp99act
rJv+Yrt0vKaX1VKicmFm5M2wclv3alcggOE2o5T+sXECAwEAAaNGMEQwEwYDVR0l
BAwwCgYIKwYBBQUHawIwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAwB77uHnXAqjD
0zFR0GvObWbtGLcyZTAKBggqhkjOPQQDAGNIADBFAiBNv6Skf2DHJakg9rX2t/zK
rdNWI/2w+FFC/3Rhybl1uAIhAMwTwmn9puSU3NMjcFZ9ZsAVybRCAREtXrH/sISO
BMeP
-----END CERTIFICATE-----
```

Authentification

Certificats Utilisateur

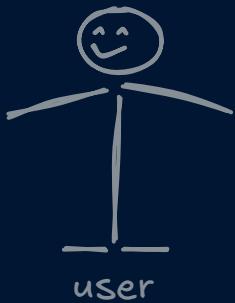


```
~/.kube/config

apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: LS0tLSW8xQXhFblU3RmkrcXhpUzLQUG5UMGpFWEg2M3VQBDRVJUSUZJQ0FURS0tLS0tCg==
    server: https://10.5.0.2:6443
    name: talos-debian-docker
contexts:
- context:
    cluster: talos-debian-docker
    namespace: default
    user: admin@talos-debian-docker
    name: admin@talos-debian-docker
- context:
    cluster: talos-debian-docker
    namespace: default
    user: philippe-durand@talos-debian-docker
    name: philippe-durand@talos-debian-docker
current-context: admin@talos-debian-docker
kind: Config
users:
- name: admin@talos-debian-docker
  user:
    client-certificate-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0mRZbz0kLS0tLS1FTkQgQ0VSVElGSUNBVEutLS0tLQo=
    client-key-data: LS0tLS1CRUdJTiBFQyBQUklwQVRFIetFWS0tLS0tCkKy0tLS1FTkQgRUMgUFJJVkJURSBLRVktLS0tLQo=
- name: philippe-durand@talos-debian-docker
  user:
    client-certificate-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCkVJFdFhySC9zSQ0VSVElGSUNBVEutLS0tLQo=
    client-key-data: LS0tLS1CRUdJTiBQNnBQV1p6NUJ4VLMzJ4dldkTEIrajNSCi0tLS0tRU5E1FBSSVZBVEUgS0VZLS0tLS0K
```

Authentification

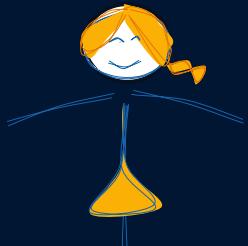
Certificats Utilisateur



user

Terminal

```
$ k --context philippe-durand@talos-debian-docker auth whoami
ATTRIBUTE                                VALUE
Username                               philippe.durand
Groups                                 [system:authenticated]
Extra: authentication.kubernetes.io/credential-id [X509SHA256=f69611bd084675aba59747d756125f98c5c77e03f3c52c79471c2dbab85531a2]
$ k --context philippe-durand@talos-debian-docker auth can-i get pods
no
```



admin

Terminal

```
$ k create clusterrolebinding pdu-view --clusterrole view --user philippe.durand
clusterrolebinding.rbac.authorization.k8s.io/pdu-view created
```



user

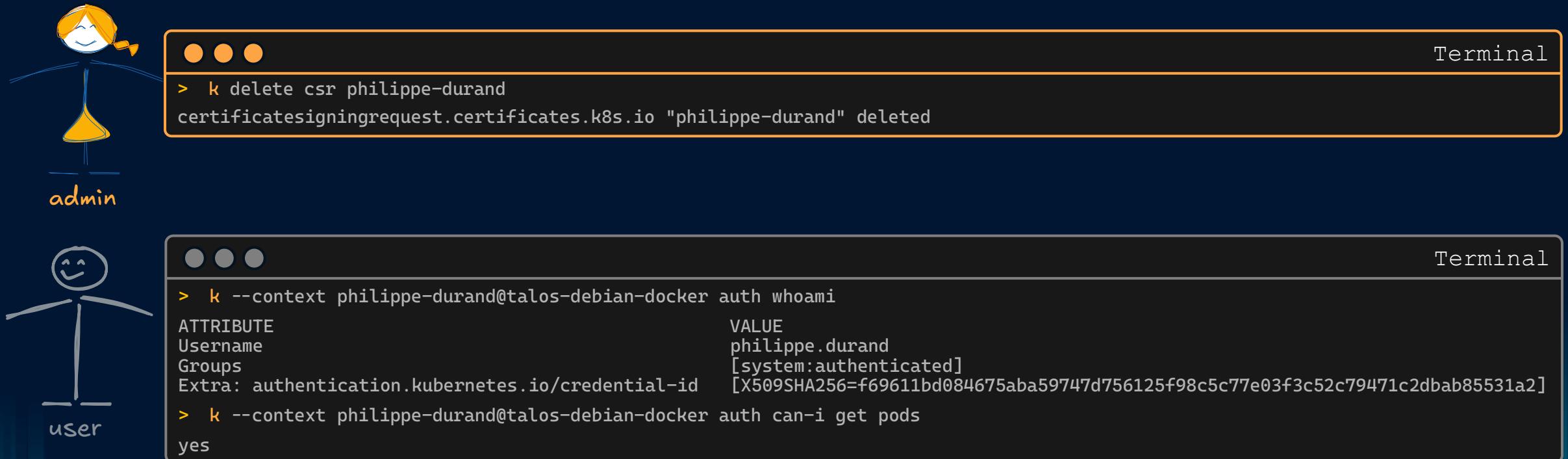
Terminal

```
$ k --context philippe-durand@talos-debian-docker auth can-i get pods
yes
$ k --context philippe-durand@talos-debian-docker auth can-i delete pods
no
```



Authentification

Certificats Utilisateur - révocation





Authentification

Certificats Utilisateur

En pratique

- On ajoute les groupes dans le certificat csr initial

The terminal window shows the command:

```
> openssl req -new -key philippe.key -subj "/CN=philippe.durand/O=devops/O=platform" -out philippe.csr
```

- On fait le RBAC sur les groupes ... c'est quand même plus facile
 - On ne demande pas à un utilisateur
 - de faire tout le travail key / csr / kubeconfig
 - de penser à re-certifier sa clé
- ➔ On va gérer tout ce travail côté admin et produire régulièrement un kubeconfig

Authentification

Résumé

	Certificats
Acteur nominatif	100%
Gestion des groupes	50%
Révocation possible	0%
Simplicité de gestion	20%
Passe les reverse proxy L7 APIServer	0%



Authentification

Avec des Tokens



Authentification

Token

Idée : utiliser les comptes de service (**ServiceAccount**)

- On peut générer plusieurs secrets de type token par compte de service
 - Ces tokens n'expirent pas mais sont révoquables en supprimant le secret
- On peut faire du RBAC pour les comptes de service

Organisation possible

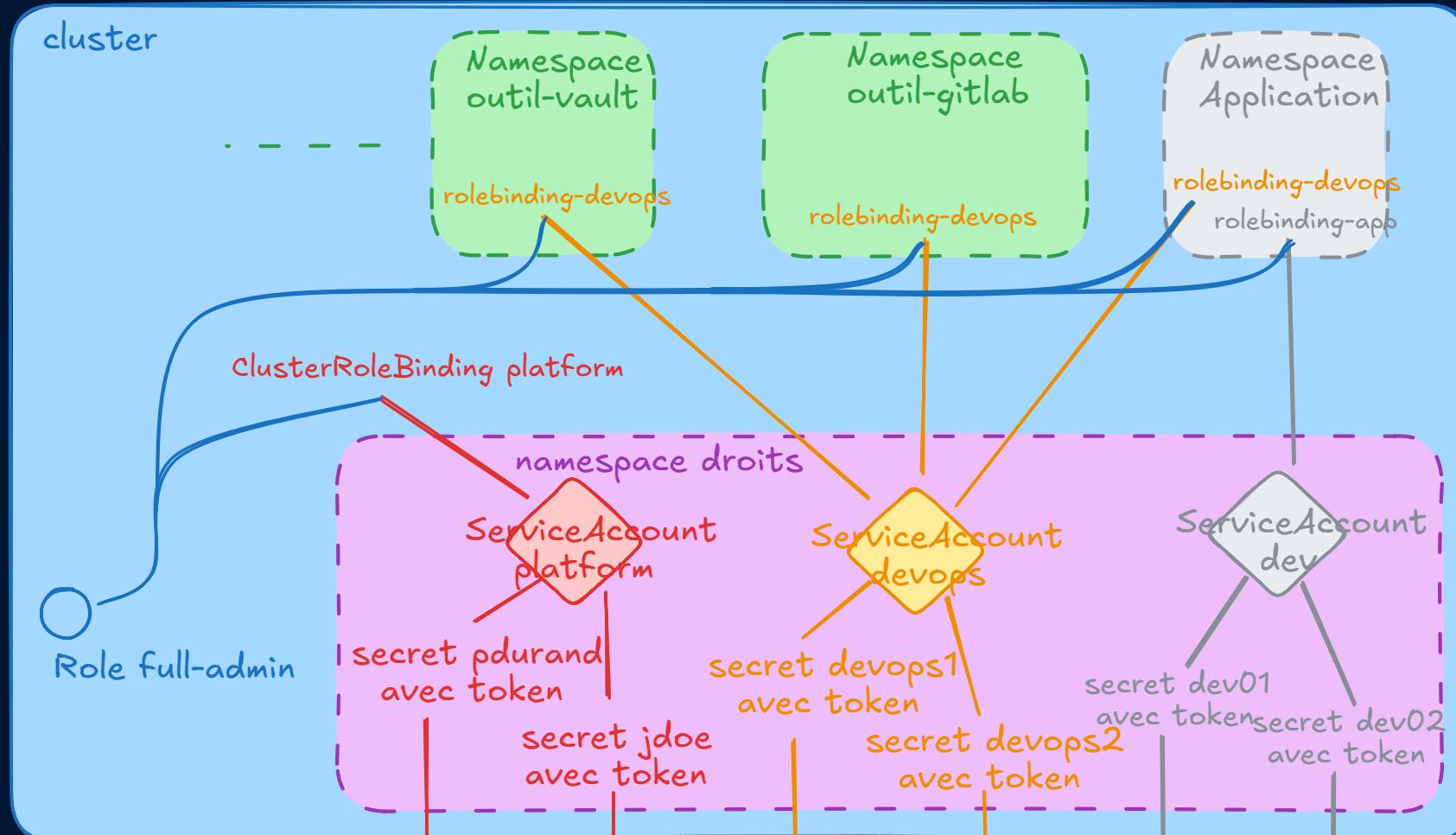
- ServiceAccount == profil métier ➔ plusieurs rôles
- Un token par personne == un identifiant par personne

Industrialisation

- Il est possible d'industrialiser la création / modification des comptes avec des outils comme, par exemple, helm.

Authentification

Token – organisation Démo



Admin global
Pour créer puis maintenir

Authentification

Token : Demo time !



Admin global



Terminal

```
$ k create clusterrole full-admin --verb='*' --resource='*'  
clusterrole.rbac.authorization.k8s.io/full-admin created  
$ k create ns droits; k create ns ouutil-vault; k create ns ouutil-gitlab; k create ns application  
namespace/droits created  
namespace/outil-vault created  
namespace/outil-gitlab created  
namespace/application created  
$ k -n droits create sa platform; k -n droits create sa devops; k -n droits create sa dev  
serviceaccount/platform created  
serviceaccount/devops created  
serviceaccount/dev created  
$ k create clusterrolebinding platform --clusterrole cluster-admin --serviceaccount droits:platform  
clusterrolebinding.rbac.authorization.k8s.io/platform created  
$ k -n droits apply -f serviceaccount-secret-pdurand.yaml; k -n droits apply -f serviceaccount-secret-jdoe.yaml  
secret/pdurdand created  
secret/jdoe created  
$ k -n droits get secret pdurdand -o jsonpath='{.data.token}' | base64 -d; echo;  
eyJhbGciOiJSUzI1NiIsImtpZCI6IkRsTWhWcnNICi1yVTJxY3VhYXpGUG9WdVNDNHdwTUdzalBSYXh5Nld5YnMifQ.pLlu3LDQuoKGWpZKEzRsqvFSHUmpkcyefM_k0sQv2NH  
2zxSHBan1rM9sCl2IH1lXQNhcplRQoIPh_TMfKIJooyMY2AtWzbhY6SNBYxJ3am7TVyQxkGFj1-rOGGDQTUcO6pbC6sVLmLI
```



serviceaccount-secret-pdurand.yaml

```
apiVersion: v1  
kind: Secret  
metadata:  
  name: pdurand  
  namespace: droits  
  annotations:  
    kubernetes.io/service-account.name: "platform"  
type: kubernetes.io/service-account-token
```

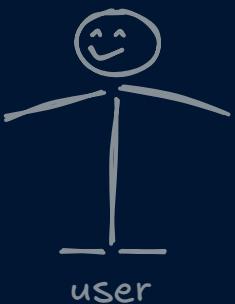


serviceaccount-secret-jdoe.yaml

```
apiVersion: v1  
kind: Secret  
metadata:  
  name: jdoe  
  namespace: droits  
  annotations:  
    kubernetes.io/service-account.name: "platform"  
type: kubernetes.io/service-account-token
```

Authentification

Token : Demo time !



user

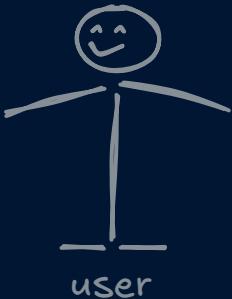
```
~/.kube/config

apiVersion: v1
clusters:
- cluster:
  certificate-authority-data: LS0tLSW8xQXhFblU3RmkrcXhpUzlQUG5UMGpFWEg2M3VQBDRVJUSUZJQ0FURS0tLS0tCg==
  server: https://10.5.0.2:6443
  name: talos-debian-docker
contexts:
...
- context:
  cluster: talos-debian-docker
  namespace: default
  user: philippe-durand@talos-debian-docker
  name: philippe-durand@talos-debian-docker
...
current-context: admin@talos-debian-docker
kind: Config
users:
...
- name: philippe-durand@talos-debian-docker
  user:
    client-certificate-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCkVJFdFhySC9zSQ0VSVElGSUNBVEUtLS0tLQo=
    client-key-data: LS0tLS1CRUdJTiBQNnBQV1p6NUJ4VLMzJ4dldKTEIrajNSCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K
- name: pdurand@talos-debian-docker
  user:
    token: eyJhbGciOiJSUzI1NiIsImtpZCI6IkRsTWhWcnNIci1yVTJxY3VhYXpGUG9WdVNDNHdwTUdza1BSYXh5Nld5YnMifQ.p
- name: jdoe@talos-debian-docker
  user:
    token: eyJhbGciOiJSUzI1NiIsImtpZCI6IkRsTWhWcnNIci1yVTJxY3VhYXpGUG9WdVNDNHdwTUdza1BSYXh5Nld5YnMifQ.e
```



Authentification

Token : Demo time !



Terminal

```
$ k --context pdurand@talos-debian-docker auth whoami
ATTRIBUTE  VALUE
Username    system:serviceaccount:droits:platform
UID        e4027fe1-669f-4e2d-afa7-a16c4dc01c9e
Groups     [system:serviceaccounts system:serviceaccounts:droits system:authenticated]
$ k --context pdurand@talos-debian-docker auth can-i get pods
yes
$ k --context pdurand@talos-debian-docker auth can-i delete ns
yes
```



Terminal

```
$ k -n droits delete secret pdurand
secret "pdurand" deleted from droits namespace
```



Terminal

```
$ k --context pdurand@talos-debian-docker auth whoami
error: You must be logged in to the server (Unauthorized)
$ k --context jdoe@talos-debian-docker auth can-i delete ns
yes
```

Authentification

Il contient quoi ce token ???

The screenshot shows the JSON Web Token (JWT) Debugger interface on jwt.io. At the top, there's a navigation bar with tabs for Debugger, Introduction, Libraries, and Ask. Below the navigation is a header with the title "JSON Web Token (JWT) Debugger". There are two cards at the top: "What is a JWT?" (purple background) and "Warning about using JWTs" (yellow background). The main area contains sections for "ENCODED VALUE" and "DECODED HEADER" on the left, and "DECODED PAYLOAD" on the right. The "ENCODED VALUE" section contains a text input field with a long JWT string and buttons for "COPY" and "CLEAR". The "DECODED HEADER" and "DECODED PAYLOAD" sections each have tabs for "JSON" and "CLAIMS TABLE". The "DECODED HEADER" JSON table shows the following data:

```
{  
  "alg": "RS256",  
  "kid": "D1MhVrsHr-rU2qcuazFPoVuSC4wpMGskPRaxy6Wybs"  
}
```

The "DECODED PAYLOAD" JSON table shows the following data:

```
{  
  "iss": "kubernetes/serviceaccount",  
  "kubernetes.io/serviceaccount/namespace": "droits",  
  "kubernetes.io/serviceaccount/secret.name": "pdurand",  
  "kubernetes.io/serviceaccount/service-account.name": "platform",  
  "kubernetes.io/serviceaccount/service-account.uid": "e4027fe1-669f-4  
e2d-afa7-a16c4dc01c9e",  
  "sub": "system:serviceaccount:droits:platform"  
}
```

Authentification

Résumé

	Certificats	Tokens de SA
Acteur nominatif	100%	0%
Gestion des groupes	50%	80%
Révocation possible	0%	100%
Simplicité de gestion	20%	50%
Passe les reverse proxy L7 APIServer	0%	100%



Authentification

Bilan intermédiaire

C'est complexe, non?

Constat : TROP de clusters

- Sont accédés avec des droits full-admin (le certificat full-admin a été diffusé)
- Sont accessibles par des personnes ne faisant plus partie de l'entreprise
- Voire, sont accessibles en anonymous authent :
 - User : system:anonymous
 - Group : system:unauthenticated





Authentification

Et maintenant?

What if ???

- K8S faisait confiance à une autorité d'authentification externe ?
- Qui fournirait un token JWT contenant user et des groupes externes au cluster ??
- Et que l'on puisse faire le RBAC sur ces groupes ???



Microsoft
Entra ID



Google Cloud



kubernetes

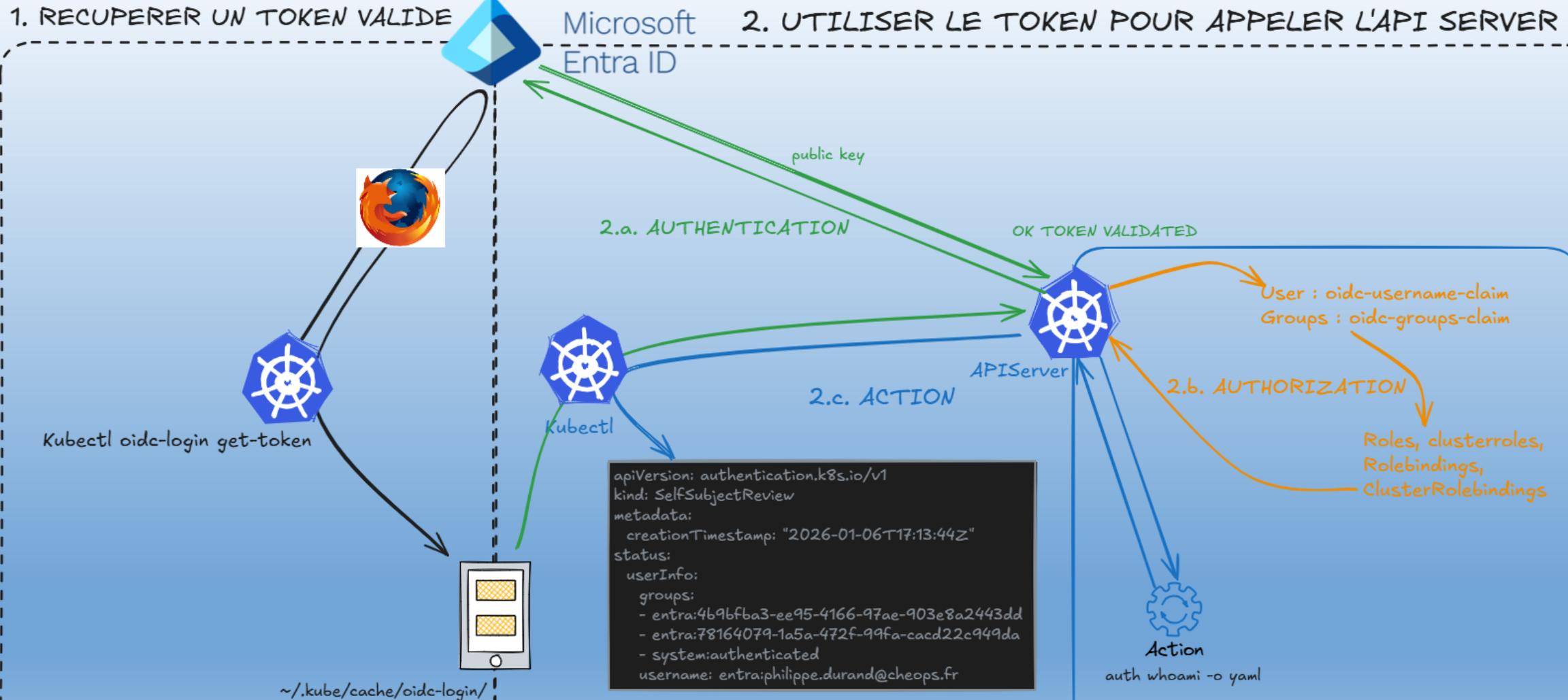
Authentification

OpenID Connect (OIDC)

- Une couche d'identité au-dessus d'OAuth 2.0
- Standard depuis ~2014

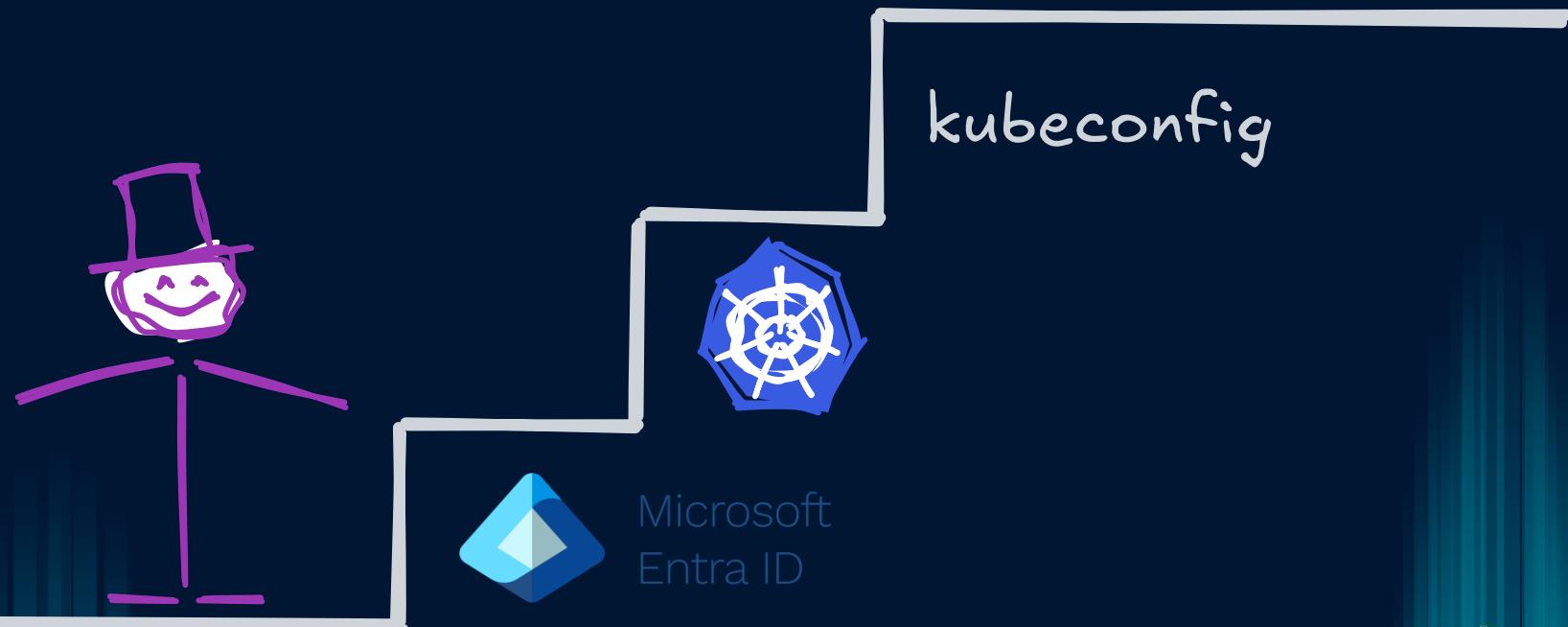
K8S OIDC avec Microsoft Entra

Comment ça fonctionne?



K8S OIDC avec Microsoft Entra

Les étapes de paramétrage ...



K8S OIDC avec Microsoft Entra

Paramétrage Entra : Créer une application

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links such as Home, Entra agents, Favorites, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations (which is selected and highlighted in blue), Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview). The main content area is titled "App registrations" and shows a "New registration" button highlighted with a green box. Below it are tabs for "All applications", "Owned applications" (which is selected and underlined in blue), and "Deleted applications". A search bar and a "Add filters" button are also present. A message states, "This account isn't listed as an owner of any applications in this directory.", with a "View all applications in the directory" button. The top right corner shows the user's name (philippe.durand@cheop... DMT-TENANT) and a Copilot icon.

K8S OIDC avec Microsoft Entra

Paramétrage Entra : 1. Créer une application

Register an application - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/CreateApplicationBlade/quickStartType~/null/isMSAApp~/false

Microsoft Entra admin center

Home > Groups | Overview > All groups > Groups | Overview > DMT-Tenant > Groups | Overview > All groups > talos-debian-docker-cluster-view | Members > App registrations > k8s-oidc-meetup-lorient > Microsoft Entra > App registrations

Philippe.Durand@cheop...
DMT-TENANT (M365X03618986...)

Register an application

* Name
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (DMT-Tenant only - Single tenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Web

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the Microsoft Platform Policies [View](#)

Register

K8S OIDC avec Microsoft Entra

Paramétrage Entra : 1. Créer une application

k8s-oidc-meetup-lorient - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Overview/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/7808f3e...

Microsoft Entra admin center

Home > Groups | Overview > All groups > Groups | Overview > DMT-Tenant > Groups | Overview > All groups > talos-debian-docker-cluster-view | Members > App registrations > k8s-oidc-meetup-lorient > Microsoft Entra > App registrations > k8s-oidc-meetup-lorient

philippe.durand@cheop... DMT-TENANT (M365X03618986...)

k8s-oidc-meetup-lorient

Search resources, services, and docs (G+)

Copilot

Endpoints Preview features

Overview Quickstart Integration assistant Diagnose and solve problems

Manage Branding & properties Authentication (Preview) Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest

Get Started Documentation

Display name : k8s-oidc-meetup-lorient Client credentials : Add a certificate or secret Application (client) ID : d2186464-6db9-4750-9883-6bb44cb64004 Redirect URIs : 1 web, 0 spa, 0 public client Object ID : 7808f3e7-fee4-4b6a-b5f4-0e0340335a3d Application ID URI : Add an Application ID URI Directory (tenant) ID : de5169f1-9a13-45fe-a4cf-07feee258b7f Managed application in I... : k8s-oidc-meetup-lorient Supported account types : My organization only

Build your application with the Microsoft identity platform

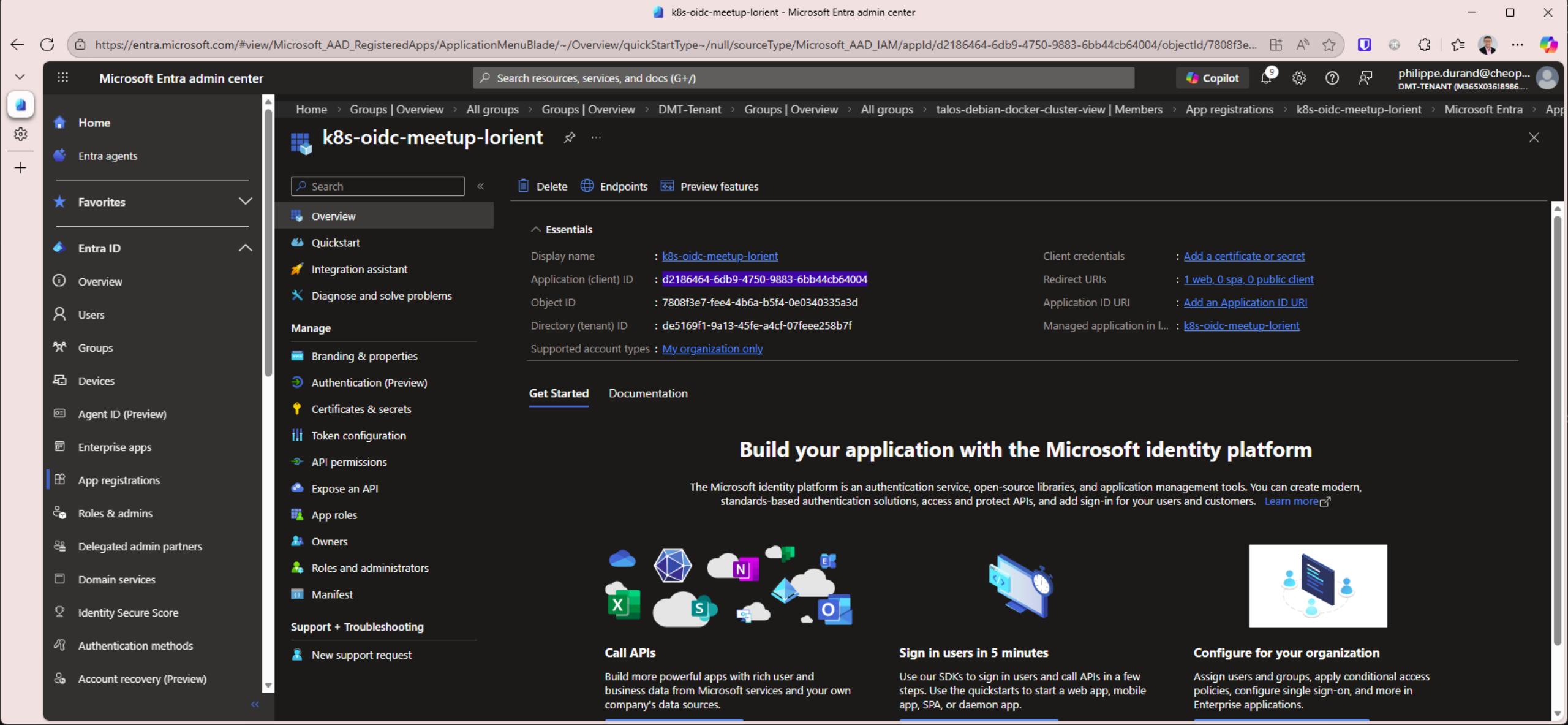
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Call APIs Sign in users in 5 minutes Configure for your organization

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.



K8S OIDC avec Microsoft Entra

Paramétrage Entra : Récupérer les identifiants d'application

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview). The main area displays the 'k8s-oidc-meetup-lorient' application registration. The 'Overview' tab is selected. The 'Essentials' section shows the following details:

Display name	:	k8s-oidc-meetup-lorient
Application (client) ID	:	d2186464-6db9-4750-9883-6bb44cb64004
Object ID	:	7808f3e7-fee4-4b6a-b5f4-0e0340335a3d
Directory (tenant) ID	:	de5169f1-9a13-45fe-a4cf-07feee258b7f
Supported account types	:	My organization only
Client credentials	:	Add a certificate or secret
Redirect URLs	:	1 web, 0 spa, 0 public client
Application ID URI	:	Add an Application ID URI
Managed application in I...	:	k8s-oidc-meetup-lorient

A green arrow points from the 'Object ID' field to a code editor window containing a YAML configuration file named 'Talos-oidc-patch.yaml'. The code in the editor is as follows:

```
cluster:
  apiServer:
    extraArgs:
      oidc-issuer-url: https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0
      oidc-client-id: d2186464-6db9-4750-9883-6bb44cb64004
      oidc-username-claim: email
      oidc-username-prefix: "entra:"
      oidc-groups-claim: groups
      oidc-groups-prefix: "entra:"
```

K8S OIDC avec Microsoft Entra

Paramétrage Entra : Ajouter un secret à l'application

k8s-oidc-meetup-lorient - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Overview/quickStartType~/null/sourceType/Microsoft_AAD_IAM/applId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/7808f3e... Copilot

Microsoft Entra admin center

Home Groups | Overview All groups Groups | Overview DMT-Tenant Groups | Overview All groups talos-debian-docker-cluster-view | Members App registrations k8s-oidc-meetup-lorient Microsoft Entra App

phillippe.durand@cheop... DMT-TENANT (M365X03618986...)

Home Entra agents Favorites Entra ID Overview Integration assistant Diagnose and solve problems Manage Branding & properties Authentication (Preview) Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest Support + Troubleshooting New support request

Search resources, services, and docs (G+)

Overview Quickstart Endpoints Preview features

Display name : k8s-oidc-meetup-lorient Client credentials : Add a certificate or secret Application (client) ID : d2186464-6db9-4750-9883-6bb44cb64004 Redirect URIs : 1 web, 0 spa, 0 public client Object ID : 7808f3e7-fee4-4b6a-b5f4-0e0340335a3d Application ID URI : Add an Application ID URI Directory (tenant) ID : de5169f1-9a13-45fe-a4cf-07feee258b7f Managed application in ... : k8s-oidc-meetup-lorient Supported account types : My organization only

Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Call APIs Sign in users in 5 minutes Configure for your organization

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

Microsoft Entra admin center

Home Groups | Overview All groups Groups | Overview DMT-Tenant Groups | Overview All groups talos-debian-docker-cluster-view | Members App registrations k8s-oidc-meetup-lorient Microsoft Entra App

phillippe.durand@cheop... DMT-TENANT (M365X03618986...)

Home Entra agents Favorites Entra ID Overview Integration assistant Diagnose and solve problems Manage Branding & properties Authentication (Preview) Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest Support + Troubleshooting New support request

Search resources, services, and docs (G+)

Overview Quickstart Endpoints Preview features

Display name : k8s-oidc-meetup-lorient Client credentials : Add a certificate or secret Application (client) ID : d2186464-6db9-4750-9883-6bb44cb64004 Redirect URIs : 1 web, 0 spa, 0 public client Object ID : 7808f3e7-fee4-4b6a-b5f4-0e0340335a3d Application ID URI : Add an Application ID URI Directory (tenant) ID : de5169f1-9a13-45fe-a4cf-07feee258b7f Managed application in ... : k8s-oidc-meetup-lorient Supported account types : My organization only

Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Call APIs Sign in users in 5 minutes Configure for your organization

Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

Use our SDKs to sign in users and call APIs in a few steps. Use the quickstarts to start a web app, mobile app, SPA, or daemon app.

Assign users and groups, apply conditional access policies, configure single sign-on, and more in Enterprise applications.

K8S OIDC avec Microsoft Entra

Paramétrage Entra : Ajouter un secret à l'application

k8s-oidc-meetup-lorient - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Credentials/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/7808f3... Copilot 9 🔍 ⚙️ 🌐 ⚡ 🏷️ philippe.durand@cheop... DMT-TENANT (M365X03618986...)

Microsoft Entra admin center

Home

Entra agents

Favorites

Entra ID

Overview

Users

Groups

Devices

Agent ID (Preview)

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Identity Secure Score

Authentication methods

Account recovery (Preview)

All groups > Groups | Overview > DMT-Tenant > Groups | Overview > All groups > talos-debian-docker-cluster-view | Members >

Search resources, services, and docs (G+)

Copilot 9 🔍 ⚙️ 🌐 ⚡ 🏷️ philippe.durand@cheop... DMT-TENANT (M365X03618986...)

Add a client secret

Description: Kubelogin

Expires: Recommended: 180 days (6 months)

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens (OAuth 2.0). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ
No client secrets have been created for this application.		

Add Cancel

... > > All groups > Groups | Overview > DMT-Tenant > Groups | Overview > All groups > talos-debian-docker-cluster-view | Members >

Search Got feedback?

Overview Quickstart Integration assistant Diagnose and solve problems

Manage

Branding & properties Authentication (Preview) Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest

Support + Troubleshooting

New support request

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Récupérer le secret

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, and the main content area displays the 'Certificates & secrets' page for the application 'k8s-oidc-meetup-lorient'. The 'Client secrets (1)' tab is selected, showing one entry:

Description	Expires	Value	Secret ID
Kubelogin	09/08/2026	X6j8Q~7pc2~6ONWyHT15gdPa8j~rvt26...	980f8a2d-9be8-4850-8067-c770bd574008

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage du token

k8s-oidc-meetup-lorient - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/TokenConfiguration/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/

Microsoft Entra admin center

Home

Entra agents

Favorites

Entra ID

Overview

Users

Groups

Devices

Agent ID (Preview)

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Identity Secure Score

Authentication methods

Account recovery (Preview)

All groups > Groups | Overview > DMT-Tenant > Groups | Overview > All groups > talos-debian-docker-cluster-view | Members > A

k8s-oidc-meetup-lorient | Token configuration

Search

Got feedback?

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. Learn more

+ Add optional claim + Add groups claim

Claim ↑ Description

No results.

Edit groups claim

Adding the groups claim applies to Access, ID, and SAML token types. Learn more

Select group types to include in Access, ID, and SAML tokens.

Security groups

Directory roles

All groups (includes 3 group types: security groups, directory roles, and distribution lists)

Groups assigned to the application (recommended for large enterprise companies to avoid exceeding the limit on the number of groups a token can emit)

Customize token properties by type

↓ ID

↓ Access

↓ SAML

Add Cancel

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage du token

Microsoft Entra admin center - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/TokenConfiguration/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/

Philippe.Durand@cheop... DMT-TENANT (M365X03618986...)

k8s-oidc-meetup-lorient | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑	Description
groups	Optional formatting for group claims

Add optional claim

Some of these claims (email) require OpenID Connect scopes to be configured through the API permissions page or by checking the box below. [Learn more](#)

Turn on the Microsoft Graph email permission (required for claims to appear in token).

ID
 Access
 SAML

Claim ↑	Description
acct	User's account status in tenant
acrs	Auth Context IDs of the operations the bearer is eligible...
auth_time	Time when the user last authenticated; See OpenID Con...
ctry	User's country/region
<input checked="" type="checkbox"/> email	The addressable email for this user, if the user has one
family_name	Provides the last name, surname, or family name of the ...
fwd	IP address
given_name	Provides the first or "given" name of the user, as set on ...
in_corp	Signals if the client is logging in from the corporate net...
ipaddr	The IP address the client logged in from
login_hint	Login hint

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage du token

k8s-oidc-meetup-lorient - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/TokenConfiguration/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/

Microsoft Entra admin center

Home

Entra agents

Favorites

Entra ID

Overview

Users

Groups

Devices

Agent ID (Preview)

Enterprise apps

App registrations

Roles & admins

Delegated admin partners

Domain services

Identity Secure Score

Authentication methods

Account recovery (Preview)

All groups > Groups | Overview > DMT-Tenant > Groups | Overview > All groups > talos-debian-docker-cluster-view | Members > App registrations > k8s-oidc-meetup-lorient > Microsoft Entra > App registrations > k8s-oidc-meetup-lorient | Token configuration

Search resources, services, and docs (G+)

Copilot

Philippe.Durand@cheop...

DMT-TENANT (M365X03618986...)

k8s-oidc-meetup-lorient | Token configuration

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑	Description	Token type ↑	Optional settings
email	The addressable email for this user, if the user has one	ID	-
groups	Optional formatting for group claims	ID, Access, SAML	Default

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appld/d2186464-6db9-4750-9883-6bb44cb64004/objectId/7808f3e... Copilot 13 🔍 🚧 ? 🔍 philippe.durand@cheop... DMT-TENANT (M365X0361896...)

k8s-oidc-meetup-lorient - Microsoft Entra admin center

k8s-oidc-meetup-lorient | API permissions

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

API / Permissions name	Type	Description
Microsoft Graph (2)		
email	Delegated	View users' email add
User.Read	Delegated	Sign in and read user

Configured permissions

Applications are authorized to call APIs when they are granted permissions all the permissions the application needs. [Learn more about permissions](#)

+ Add a permission ✓ Grant admin consent for DMT-Tenant

To view and manage consented permissions for individual apps, as well as

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Rights Management Services
Allow validated users to read and write protected content

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Dynamics CRM
Access the capabilities of CRM business software and ERP systems

Intune
Programmatic access to Intune data

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Microsoft Entra ID activity logs

OneNote
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

Power Automate
Embed flow templates and manage flows

Power BI Service
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

Home Entra agents Favorites Entra ID Overview Users Groups Devices Agent ID (Preview) Enterprise apps App registrations Roles & admins Delegated admin partners Domain services Identity Secure Score Authentication methods Account recovery (Preview)

Search Refresh Got feedback?

Overview Quickstart Integration assistant Diagnose and solve problems Branding & properties Authentication (Preview) Certificates & secrets Token configuration API permissions Expose an API App roles Owners Roles and administrators Manifest New support request

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

Request API permissions - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/7808f3e... Copilot 13 🔍 ⚙️ 🌐 🗃️ 🗺️ philippe.durand@cheop... DMT-TENANT (M365X03618986...)

Microsoft Entra admin center

k8s-oidc-meetup-lorient | API permissions

Search resources, services, and docs (G+)

Home Entra agents Favorites Entra ID Overview Users Groups Devices Agent ID (Preview) Enterprise apps App registrations Roles & admins Delegated admin partners Domain services Identity Secure Score Authentication methods Account recovery (Preview)

All groups Groups | Overview DMT-Tenant Groups | Overview All groups talos

Overview Quickstart Integration assistant Diagnose and solve problems

Add a permission Grant admin consent for DMT-Tenant

API / Permissions name	Type	Description
Microsoft Graph (2)		
email	Delegated	View users' email address
User.Read	Delegated	Sign in and read user profile information

Configured permissions

Applications are authorized to call APIs when they are granted permission to all the permissions the application needs. [Learn more about permissions](#)

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.

Application permissions Your application runs as a background service or daemon without a signed-in user.

Select permissions

Start typing a permission to filter these results

Permission	Admin consent required
OpenId permissions (2)	
<input checked="" type="checkbox"/> email View users' email address	No
<input type="checkbox"/> offline_access Maintain access to data you have given it access to	No
<input checked="" type="checkbox"/> openid Sign users in	No

Add permissions Discard

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links such as Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview). The main content area is titled "k8s-oidc-meetup-lorient | API permissions". It displays a warning message: "You are editing permission(s) to your application, users will have to consent even if they've already done so previously." Below this, there is a section titled "Configured permissions" with a table listing API permissions. The table has columns for "API / Permissions name", "Type", "Description", "Admin consent requ...", and "Status". Three permissions are listed under "Microsoft Graph (3)": "email" (Delegated, View users' email address, No), "openid" (Delegated, Sign users in, No), and "User.Read" (Delegated, Sign in and read user profile, No). A button labeled "Grant admin consent for DMT-Tenant" is visible above the table. At the bottom, a note says "To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications."

API / Permissions name	Type	Description	Admin consent requ...	Status
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	...
User.Read	Delegated	Sign in and read user profile	No	...

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled "Microsoft Entra admin center" and includes sections for Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview). The "App registrations" section is currently selected.

The main content area is titled "k8s-oidc-meetup-lorient | API permissions". It displays a message: "Successfully granted admin consent for the requested permissions." Below this, there is a section titled "Configured permissions" with the following description: "Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs." A link to "Learn more about permissions and consent" is provided.

A table lists the configured permissions:

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
email	Delegated	View users' email address	No	Granted for DMT-Tenant
openid	Delegated	Sign users in	No	Granted for DMT-Tenant
User.Read	Delegated	Sign in and read user profile	No	Granted for DMT-Tenant

At the bottom right of the table, there are two buttons: "Remove permission" and "Revoke admin consent". The "Revoke admin consent" button is highlighted with a green box.

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

k8s-oidc-meetup-lorient - Microsoft Entra admin center

https://entra.microsoft.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/CallAnAPI/quickStartType~/null/sourceType/Microsoft_AAD_IAM/appId/d2186464-6db9-4750-9883-6bb44cb64004/objectId/7808f3e... Copilot 16 🔍 ⚙️ 🌐 ⚡ 🗑️ 🗃️ 🗃️ philippe.durand@cheop... DMT-TENANT (M365X03618986...)

Microsoft Entra admin center

Home Entra agents Favorites Entra ID Overview Users Groups Devices Agent ID (Preview) Enterprise apps App registrations Roles & admins Delegated admin partners Domain services Identity Secure Score Authentication methods Account recovery (Preview)

All groups Groups | Overview DMT-Tenant Groups | Overview All groups talos-debian-docker-cluster-view | Members App registrations k8s-oidc-meetup-lorient Microsoft Entra App registrations k8s-oidc-meetup-lorient API permissions

Search resources, services, and docs (G+)

k8s-oidc-meetup-lorient | API permissions

Search Refresh Got feedback?

Revoke admin consent

Are you sure you want to revoke admin consent for Microsoft Graph – email for k8s-oidc-meetup-lorient?

Yes, remove Cancel

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

Add a permission Grant admin consent for DMT-Tenant

API / Permissions name	Type	Description	Admin consent requ...	Status	...
email	Delegated	View users' email address	No	Granted for DMT-Tenant	...
openid	Delegated	Sign users in	No	Granted for DMT-Tenant	...
User.Read	Delegated	Sign in and read user profile	No	Granted for DMT-Tenant	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links such as Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview). The main content area is titled "k8s-oidc-meetup-lorient | API permissions". It displays a message: "Successfully granted admin consent for the requested permissions." Below this, there is a section titled "Configured permissions" with a table listing API permissions. The table has columns for "API / Permissions name", "Type", "Description", "Admin consent requ...", and "Status". Three entries under "Microsoft Graph (3)" are listed:

API / Permissions name	Type	Description	Admin consent requ...	Status
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	Granted for DMT-Tenant
User.Read	Delegated	Sign in and read user profile	No	Granted for DMT-Tenant

At the bottom, a note says: "To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications."

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Paramétrage de l'api

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links such as Home, Entra agents, Favorites, Entra ID, Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview). The main content area is titled "k8s-oidc-meetup-lorient | API permissions". It displays a message: "Successfully granted admin consent for the requested permissions." Below this, there is a section titled "Configured permissions" with a table showing three permissions for Microsoft Graph:

API / Permissions name	Type	Description	Admin consent requ...	Status
email	Delegated	View users' email address	No	...
openid	Delegated	Sign users in	No	Granted for DMT-Tenant
User.Read	Delegated	Sign in and read user profile	No	...

At the bottom, a note says: "To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications."

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Groupes et affectations groupes ↔ users

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation links for Home, Entra agents, Favorites (Overview, Users, Groups, Devices, Agent ID (Preview), Enterprise apps, App registrations, Roles & admins, Delegated admin partners, Domain services, Identity Secure Score, Authentication methods, and Account recovery (Preview)). The main content area is titled "All groups" and displays a list of 6 groups found. The columns are Name, Object Id, Group type, Membership type, Email, and Source. Two groups are listed:

Name	Object Id	Group type	Membership type	Email	Source
talos-debian-docker-cluster-admin	921b8d0f-a256-4a59-8baa-65c90ec581ac	Security	Assigned		Cloud
talos-debian-docker-cluster-view	c23b7510-9d24-4c94-882c-2aff5be1562	Security	Assigned		Cloud

K8S OIDC avec Microsoft Entra

Paramétrage Entra – Groupes et RBAC K8S

All groups

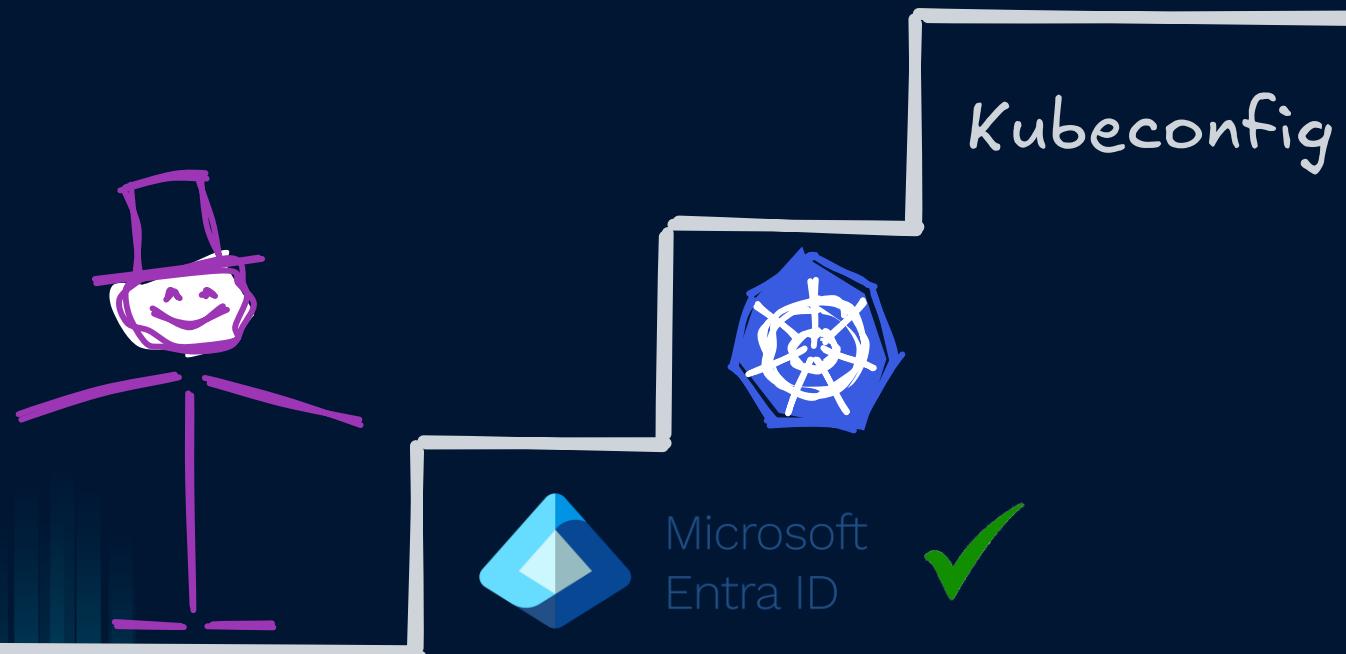
Name ↑	Object Id	Group type	Membership type	Email	Source
T talos-debian-docker-cluster-admin	921b8d0f-a256-4a59-8baa-65c90ec581ac	Security			Cloud
T talos-debian-docker-cluster-view	c23b7510-9d24-4c94-882c-2afff5be1562	Security			Cloud



```
$ k create clusterrolebinding entra-admin --clusterrole cluster-admin --group entra:921b8d0f-a256-4a59-8baa-65c90ec581ac
clusterrolebinding.rbac.authorization.k8s.io/entra-admin created
$ k create clusterrolebinding entra-view --clusterrole view --group entra:c23b7510-9d24-4c94-882c-2afff5be1562
clusterrolebinding.rbac.authorization.k8s.io/entra-view created
```

K8S OIDC avec Microsoft Entra

Le paramétrage ... avance.



K8S OIDC avec Microsoft Entra

Paramétrage K8S



Talos-oidc-patch.yaml

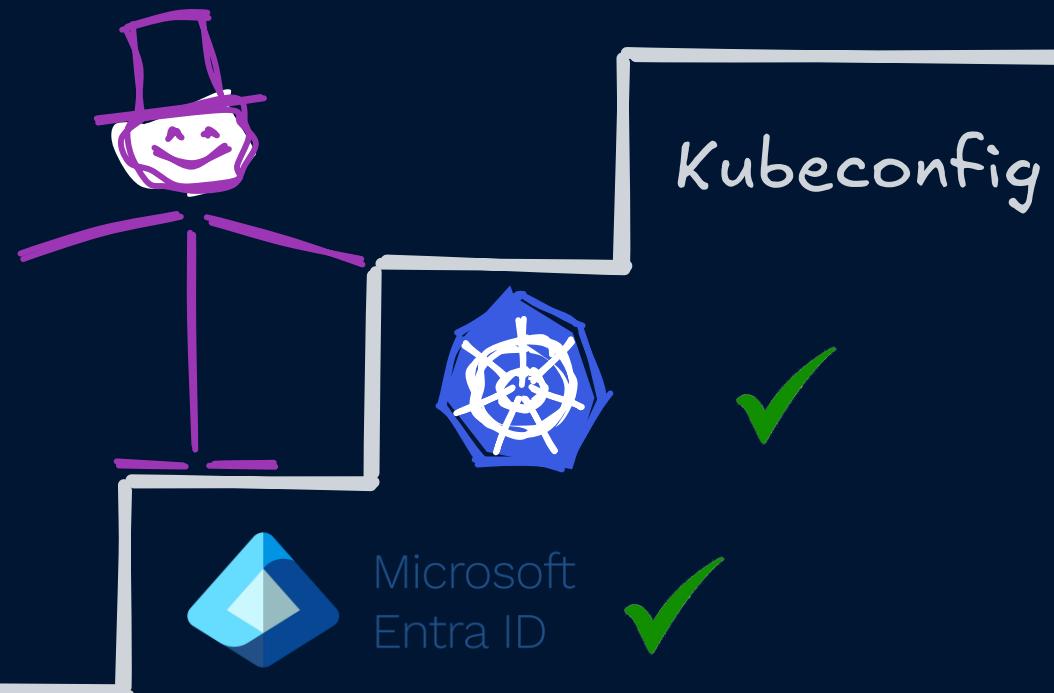
```
cluster:
  apiServer:
    extraArgs:
      oidc-issuer-url: https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0
      oidc-client-id: d2186464-6db9-4750-9883-6bb44cb64004
      oidc-username-claim: email
      oidc-username-prefix: "entra:"
      oidc-groups-claim: groups
      oidc-groups-prefix: "entra:"
```

Terminal

```
$ talosctl edit machineconfig --nodes 10.5.0.2
Applied configuration without a reboot
$ docker restart talos-debian-docker-controlplane-1
talos-debian-docker-controlplane-1
```

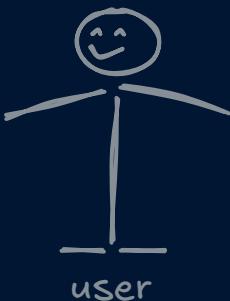
K8S OIDC avec Microsoft Entra

Le paramétrage ... on y est presque!



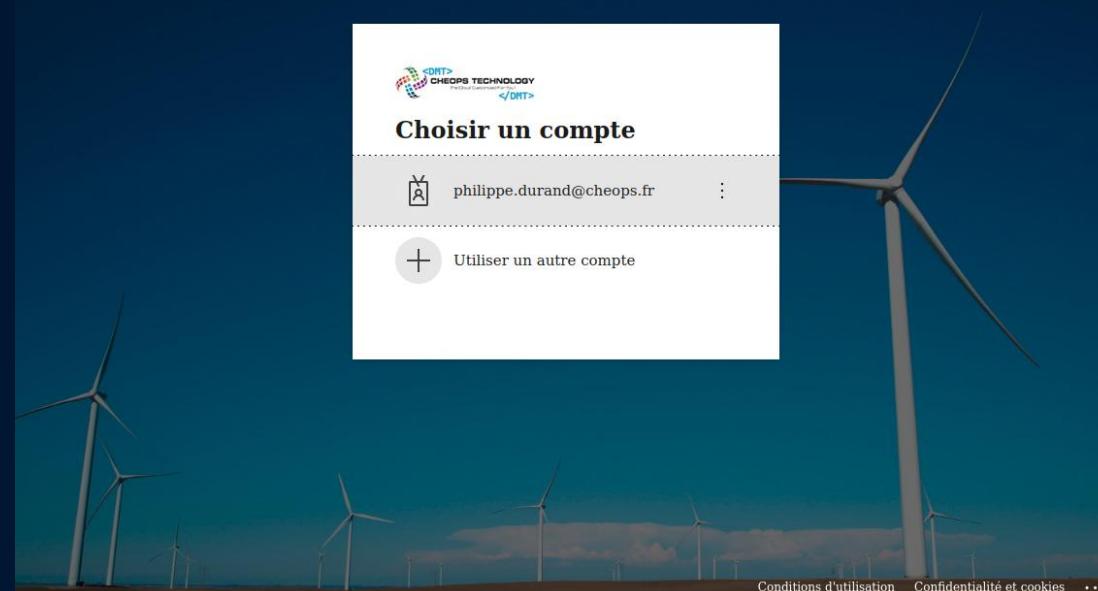
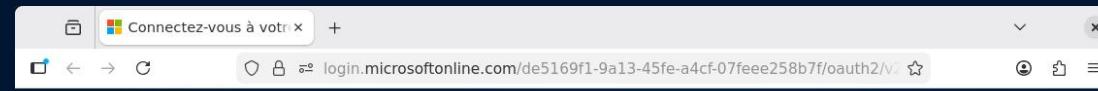
K8S OIDC avec Microsoft Entra

Paramétrage kubectl



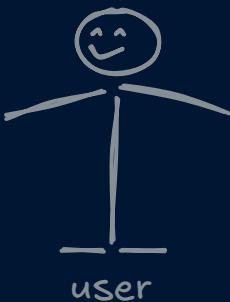
Terminal

```
$ brew install int128/kubelogin/kubelogin
$ kubelogin get-token --oidc-issuer-url https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0 --oidc-client-id d2186464-6db9-4750-9883-6bb44cb64004 --oidc-client-secret X6j8Q~7pc2~60NWyHT15gdPa8j~rvrt26NGGKhacB
```



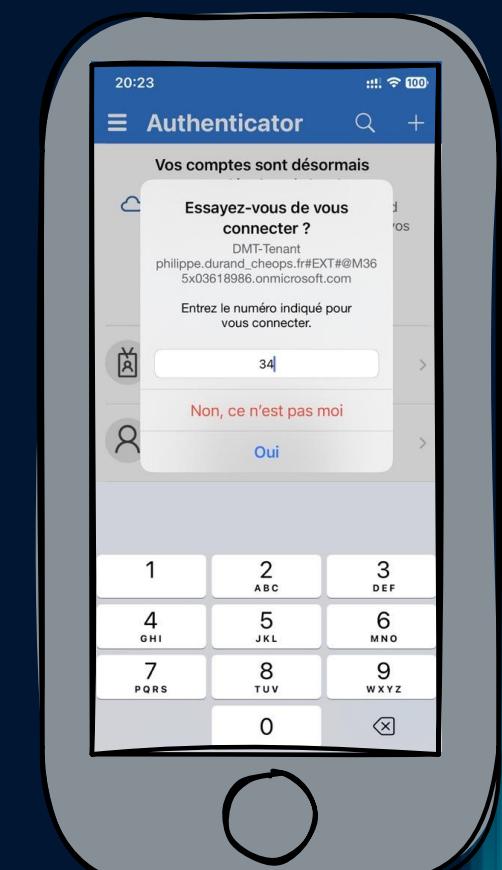
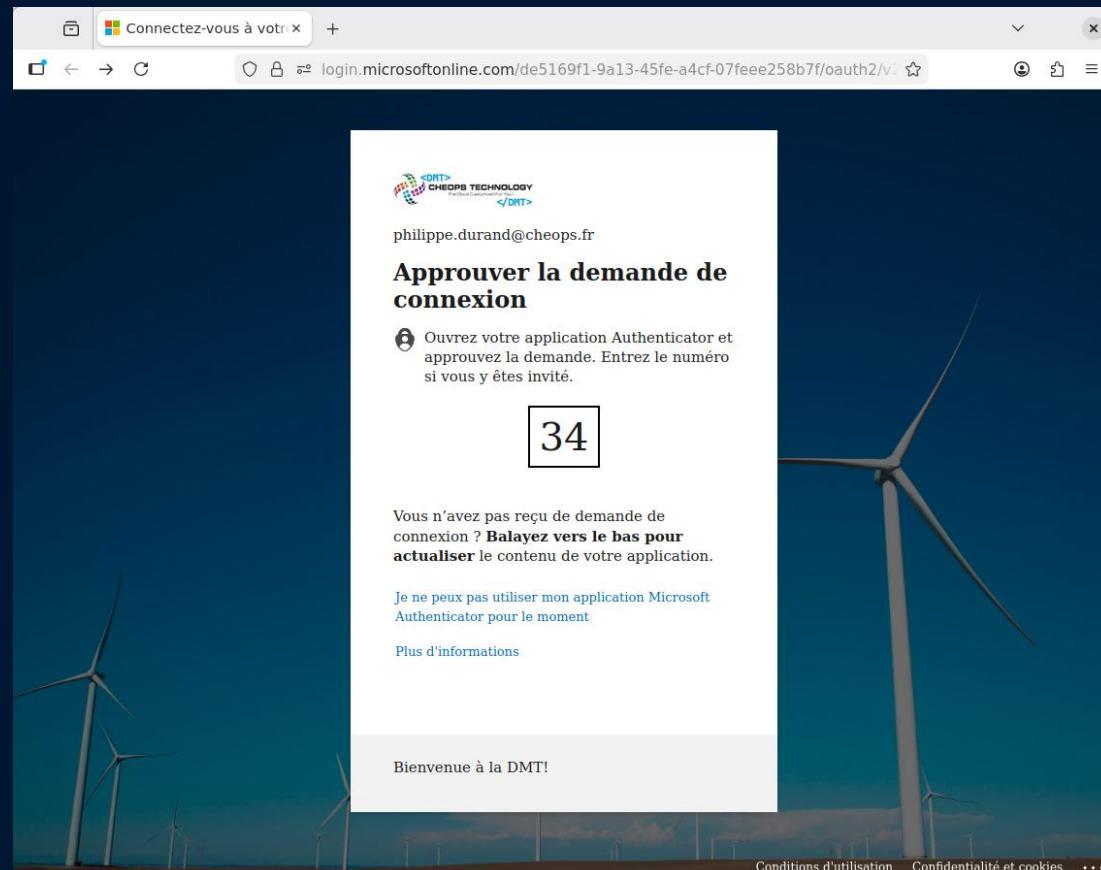
K8S OIDC avec Microsoft Entra

Paramétrage kubectl



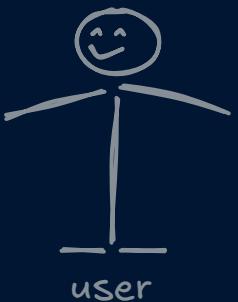
Terminal

```
$ brew install int128/kubelogin/kubelogin
$ kubelogin get-token --oidc-issuer-url https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0 --oidc-client-id d2186464-6db9-4750-9883-6bb44cb64004 --oidc-client-secret X6j8Q~7pc2~60NWyHT15gdPa8j~rvrt26NGGKhacB
```

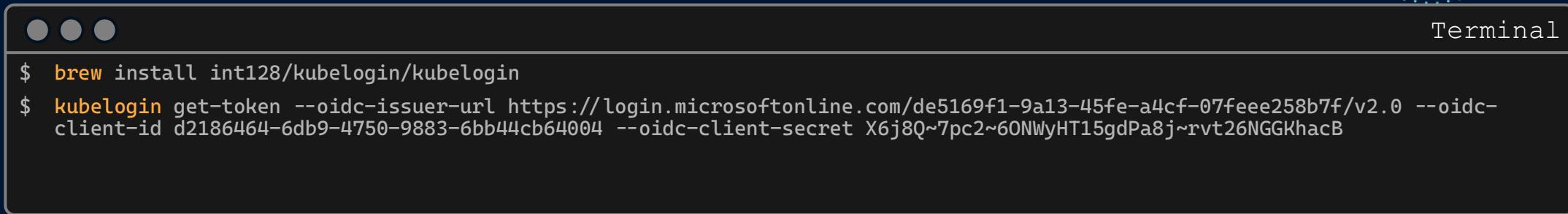


K8S OIDC avec Microsoft Entra

Paramétrage kubectl

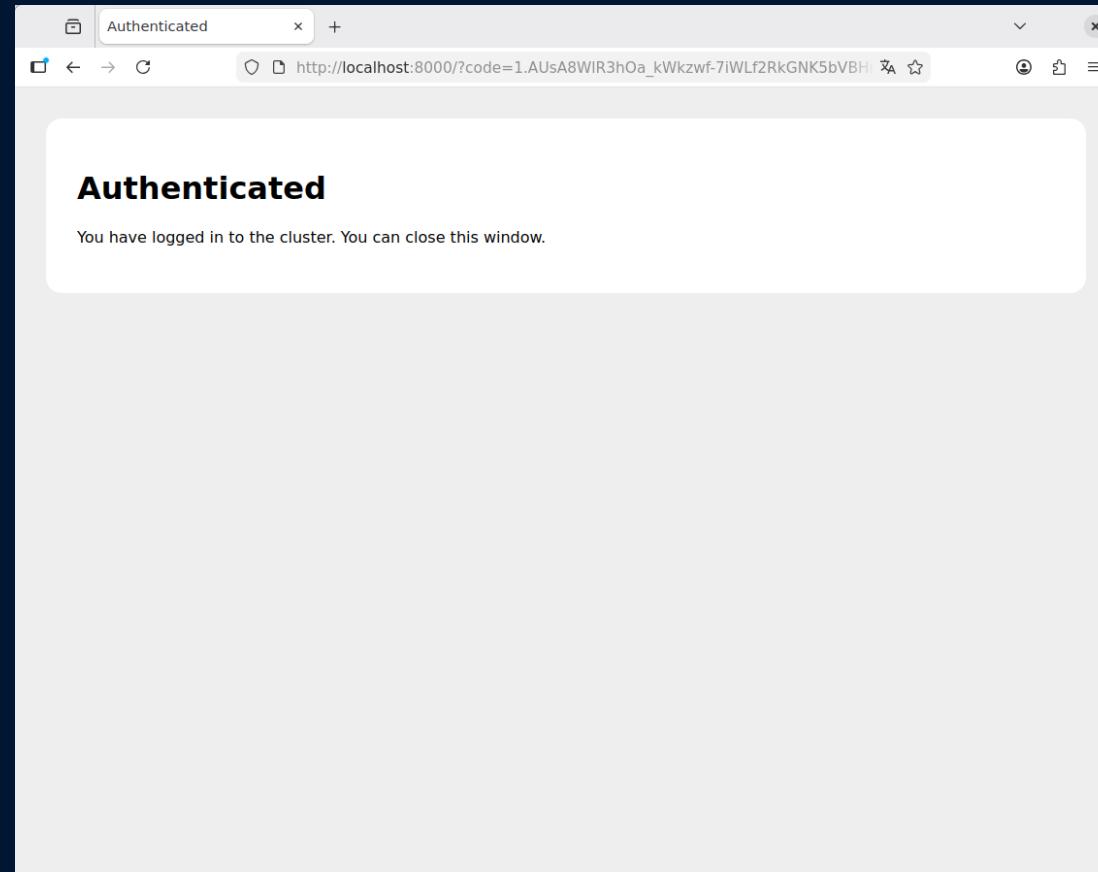


user



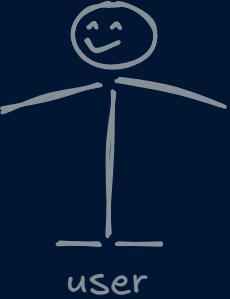
A terminal window titled "Terminal" showing the execution of the kubelogin command. The command installs the kubelogin package and then retrieves a token from Microsoft Entra using the specified issuer URL, client ID, and client secret.

```
$ brew install int128/kubelogin/kubelogin
$ kubelogin get-token --oidc-issuer-url https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0 --oidc-client-id d2186464-6db9-4750-9883-6bb44cb64004 --oidc-client-secret X6j8Q~7pc2~60NWyHT15gdPa8j~rvr26NGGKhacB
```



K8S OIDC avec Microsoft Entra

Paramétrage kubectl



user

```
$ brew install int128/kubelogin/kubelogin
$ kubelogin get-token --oidc-issuer-url https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0 --oidc-client-id d2186464-6db9-4750-9883-6bb44cb64004 --oidc-client-secret X6j8Q~7pc2~60NWyHT15gdPa8j~rvt26NGGKhacB
{"kind": "ExecCredential", "apiVersion": "client.authentication.k8s.io/v1beta1", "spec": {"interactive": false}, "status": {"expirationTimestamp": "2026-02-10T20:23:13Z", "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IlBjWDk4R1g0MjBUMVg2c0JEa3poUW1xZ3dNVSJ9.eyJhdWQiOiJkMjE4NjQ2NC02ZGI5LTQ3NTAtOTg4My02YmI0NGNInjQwMDQjLCJpc3MiOiJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vZGU1MTY5ZjEtOWExMy00NWZlLWE0Y2YtMDdmZWVLMjU4YjdmL3YyLjAiLCJpYXQiOjE3NzA3NTewOTMsIm5iZiI6MTc3MDc1MTA5MywiZXhwIjoxNzcwNzU00TkzLCJlbWFpbCI6InBoawxpCHBLlR1cmFuZEBjaGVvcHMuZnIiLCJncm91cHMiOlzsINGI5YmZiYTMTzWU5NS00MTY2LTk3YWUtOTAzzThhMjQ0M2RkIiwiZjViNmY3MGMTzDY4YS00NGI4LWIxNDgtNjVkjyjgyNWU5ZjkxIiwiOTIxYjhkMGYtYTI1Ni00YTU5LThiYWEtNjVjOTBLYzU4MWFjIiwiYzIzYjc1MTAtOWQyNC00Yzk0LTg4MmMtMmFmZmY1YmUxNTYyIiwiNzgxNjQwNzktMWE1YS00NzJmLTk5ZmEtY2FjZDIyYzk0OWRhIiwiNWQyN2VkZWetNjBhZS00YWJkLThhZGMtYzI5MjgzNthjYjNkIl0sImlkCI6Imh0dHBzOi8vc3RzLndpbmRvd3MubmV0LzY0ZjE5OGIzLTA2MzQtNGU3MS1hNjJmLTBmYjZjYWU4YWNLzI8iLCJub25jZSI6IlJjZmFYbVk4SENYbEFkNk1LZ1dfTkx0WnF2NkE1UXM3MjlnRmVSR3VUb0UiLCJyaCI6IjEuQVVzQThXbFIzaE9hX2tXa3p3Zi03aVdMZjJsA0dOSzViVKJIBuLoCnRFeTJRQVJHQWFSTEFBLiIsInN1YiI6Ii16cFRpRi1lsjJFaG56c3pjU1YyWXlySnk1UmtvUWF6aGVsb0xzVC04R3MiLCJ0aWQjOiJkZTUxNjlmMS05YTEzLTQ1ZmUtYTRjZi0wN2ZLZWUyNThiN2YiLCJ1dGkiOijXM2NpU0p0VGVVNllCdEZFZkFFVUFBIiwidmVyIjoimI4wn0.F-Jy5InwUNTx2UgZQdwPihDGnc6V8gvzIRo-4NjVbDkJZLxpFUGAGlTquVnlaME4S5sr2jQTPlqTId-QwYJC4qxvcvxYrv7shzjFWgX3lTe6mv3l6tz0kcmz79W1YyWIIVretqUX2uRd0oewwReCZecgaJnVv-BBYhCjxkXV8s-PLlWI7SGvjLgQDd_UdfjWVAZcgNAyFR8NR5rZtX0JialZguxe0tzj45dxZj4oRWFc1IZLHc7Fq-4Yitq4WhFYEDYK-IofQ14lR2nDVM3Y29Qw9XELgNWAXcx8CymLJCSJ2DbEftdqVzEJ5K4K3BmnH2F5T2h1cg4s5EdGOf9w"}}
$ export TOKEN=$(kubelogin get-token \
    --oidc-issuer-url https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0 \
    --oidc-client-id d2186464-6db9-4750-9883-6bb44cb64004 \
    --oidc-client-secret X6j8Q~7pc2~60NWyHT15gdPa8j~rvt26NGGKhacB \
    | jq -r '.status.token')
$ KUBECONFIG=/dev/null k --server=https://10.5.0.2:6443 --insecure-skip-tls-verify --token="$TOKEN" auth whoami
ATTRIBUTE      VALUE
Username        entra:philippe.durand@cheops.fr
Groups          [entra:4b9bfba3-ee95-4166-97ae-903e8a2443dd entra:78164079-1a5a-472f-99fa-cacd22c949da entra:5d27edea-60ae-4abd-8adc-c2928358cb3d entra:921b8d0f-a256-4a59-8baa-65c90ec581ac entra:c23b7510-9d24-4c94-882c-2afff5be1562 entra:f5b6f70c-d68a-44b8-b148-65db825e9f91 system:authenticated]
$ KUBECONFIG=/dev/null k --server=https://10.5.0.2:6443 --insecure-skip-tls-verify --token="$TOKEN" auth can-i delete ns
yes
```

K8S OIDC avec Microsoft Entra

Paramétrage kubectl

JSON Web Tokens - jwt.io

Get up-to-speed with JSON Web Tokens. Get the JWT Handbook for free ↗

JWT Debugger

Debugger Introduction Libraries Ask

JSON WEB TOKEN (JWT)

Valid JWT
Signature Verified

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IlBjWDk4R1g0MjBUMVg2c0JEa3poUW1xZ3dNVSJ9.eyJhdWQioiJkMjE4NjQ2NC02ZGI5LTQ3NTAtOTg4My02YmI0NGNiJQwMDQilCJpc3MiOijodHRwcovL2xvZ2luLm1pY3Jvc29mdg9ubgluZ55jb20vZGU1MTY5ZjEtOWExMy00NWZLLWE0Y2YTM DdmZW1MjU4ydmL3YyLja1lCJpyXQI0je3Nza3NTV5MTVsIm5iZi16MTc3Mdc1NjkxNiwiZXhwIjo xNzcwNzYwODE2LCJ1bWFpbCI6InBoaWxpchBlLmR1cmFuZEBjaGVvcHMuZnIiLCJnc91cHMiOlslNGI5YmZiYT MtZwUSN00MTY2Ltk3YWUtOTA2ZThMjQ0M2RkIiwiNzgxNjQwnZktMW1Y500NzJmlTk5ZmEtY2FjZDiyZk00WRhIiwiNwQyN2VkZWEtNjBhZ500YWjkLThhZGMtYz15MjgzNThjYjNkIiwi0TixYjhkMGYtYTI1Ni00YTU5LThiYWEtNjVjOTB1YzU4MWFjIiwiYzIzYjic1MTAt0WQyNC00Yzk0LTg4MmMtMfmZmY1YmUxNTYyIiwiZjViNmY3MGmtZDY4Y500NGI4LWIxNDgtNjVkjgyNWU5ZjkxI10sImlkCCI6Imh0dBzoi8vc3RzLndpbmRvd3MubmV8LzY0ZjE5OGIzLTA2MzQtNGU3MS1hNjJmlTBmVjZjYWU4YWNIzI8iLCJub25jZSI6IjZPNnxwS18zNXZQTUV2d1I0dwVfd1FFLXR4bFBrdm9ZRpNUUs5M21WRmMiLCJyaCI6IjEuQVzQThKbFIzaE9hx2tXa3p3Zi03aVdMZjjsa0d05zViVkJibUlOcnRFETJRQVJHQWFSTEFBLIIsInN1YiI6Ii16cFRpRi1lsjJFaG56c3pjU1YyNxlySnk1UmtvUWF6aGVsb0xZVC04R3MiLCJ0aWQioiJkZTUxNjlmMS05YTEzLTQ1ZmUtYTrjZi0wN2ZlZWUyNThiN2YiLCJ1dGkiOjLcW9panIybFhrMndYNlxUGtpUkFBiwidmVyIjoiMi4wIn0.AYQspPQBQmOCMzl_Qp6qcrXooUbWnqhKoXbggfz2gdybssYSU06gBoWYN2uKI7vuhLh132hu8j1YWB-7CJG3vCKjOs6Bwix9U_aeooyzkG0gWwBZPYIw05NXZGAhq9SnCwyFcHiUGH9X-MxeHOfHMiAmiA3Get5kAK2jDJC148ROYj9ChNq1Y-lvP-gldOBWupWYthcLInda4sx3nJDAP4-S9wVfw6q8XTqt1DUnZ6AbniINSqhYZ3k_s_2j_Ls3SyU_D41Pu0PGAG4zEAZ0qqkmGAXMMtytjv9yMgy9cqdf5FdYiqVHhsVRqrhzirMY3UELROC9SLZdtKDmA
```

DECODED PAYLOAD

JSON CLAIMS TABLE

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "PcX98GX420T1X6sBDkzhQmqgwMU"
}
```

JSON CLAIMS TABLE

```
{
  "aud": "d2186464-6db9-4750-9883-6bb44cb64004",
  "iss": "https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07fee258b7f/v2.0",
  "iat": 1770756916,
  "nbf": 1770756916,
  "exp": 1770760816,
  "email": "philippe.durand@cheops.fr",
  "groups": [
    "4b9bfbfa3-ee95-4166-97ae-903e8a2443dd",
    "78164079-1a5a-472f-99fa-cacd22c949da",
    "5d27edea-60ae-4abd-8adc-c2928358cb3d",
    "921b8d0f-a256-4a59-8baa-65c90ec581ac",
    "c23b7510-9d24-4c94-882c-2afff5be1562",
    "f5b6f70c-d68a-44b8-b148-65db825e9f91"
  ],
  "idp": "https://sts.windows.net/64f198b3-0634-4e71-a62f-0fb6cae8acef/",
  "nonce": "6051pJ_35vPMEvvR4ue_wQ_-tx1PkvoYfjMQK93mVFc",
```

K8S OIDC avec Microsoft Entra

Paramétrage kubectl



```
~/.kube/config

apiVersion: v1
clusters:
- cluster:
  certificate-authority-data: LS0tLSW8xQXhFblU3RmkrcXhpUzlQUG5UMGpFWEg2M3VQBDRVJUSUZJQ0FURS0tLS0tCg==
  server: https://10.5.0.2:6443
  name: talos-debian-docker
contexts:
...
- context:
  cluster: talos-debian-docker
  namespace: default
  user: philippe-durand@talos-debian-docker
  name: philippe-durand@talos-debian-docker
...
current-context: admin@talos-debian-docker
kind: Config
users:
...
- name: philippe-durand@talos-debian-docker
  user:
    client-certificate-data: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCkVJFdFhySC9zSQ0VSVElGSUNBVEUtLS0tLQo=
    client-key-data: LS0tLS1CRUdJTiBQNnBQV1p6NUJ4VLMzJ4dldKTEIrajNSCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K
- name: entra@talos-debian-docker
  user:
    token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IlBjWDk4R1g0MjbUMVg2c0JEa3poUW1xZ3dNVSJ9.eyJhdWQ
```

K8S OIDC avec Microsoft Entra



Paramétrage kubectl

Terminal

```
$ k --context entra@talos-debian-docker auth can-i delete ns
yes

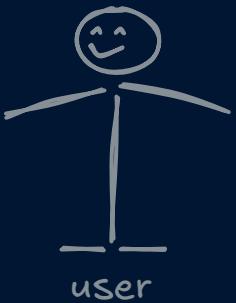
$ k config set-credentials oidc \
--exec-api-version=client.authentication.k8s.io/v1 \
--exec-interactive-mode=Never \
--exec-command=kubectl \
--exec-arg=oidc-login \
--exec-arg=get-token \
--exec-arg="--oidc-issuer-url=https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0" \
--exec-arg="--oidc-client-id=d2186464-6db9-4750-9883-6bb44cb64004" \
--exec-arg="--oidc-client-secret=X6j8Q~7pc2~60NWyHT15gdPa8j~rvt26NGGKhacB"
User "oidc" set.
```

~/.kube/config

```
...
current-context: admin@talos-debian-docker
kind: Config
users:
...
- name: oidc
  user:
    exec:
      apiVersion: client.authentication.k8s.io/v1
      args:
      - oidc-login
      - get-token
      - --oidc-issuer-url=https://login.microsoftonline.com/de5169f1-9a13-45fe-a4cf-07feee258b7f/v2.0
      - --oidc-client-id=d2186464-6db9-4750-9883-6bb44cb64004
      - --oidc-client-secret=X6j8Q~7pc2~60NWyHT15gdPa8j~rvt26NGGKhacB
      command: kubectl
      env: null
      interactiveMode: Never
      provideClusterInfo: false
```

K8S OIDC avec Microsoft Entra

Paramétrage kubectl



user

Terminal

```
$ k --context oidc auth can-i delete ns
yes
$ k --context oidc auth whoami
ATTRIBUTE VALUE
Username entra:philippe.durand@cheops.fr
Groups [entra:4b9bfba3-ee95-4166-97ae-903e8a2443dd entra:78164079-1a5a-472f-99fa-cacd22c949da entra:5d27edea-60ae-4abd-8adc-c2928358cb3d entra:921b8d0f-a256-4a59-8baa-65c90ec581ac entra:c23b7510-9d24-4c94-882c-2afff5be1562 entra:f5b6f70c-d68a-44b8-b148-65db825e9f91 system:authenticated]
```



Admin global

<input type="checkbox"/>	T talos-debian-docker-cluster-admin	921b8d0f-a256-4a59-8baa-65c90ec581ac	Security	Assigned	Cloud
<input type="checkbox"/>	T talos-debian-docker-cluster-view	c23b7510-9d24-4c94-882c-2afff5be1562	Security	Assigned	Cloud

DP

DURAND Philippe



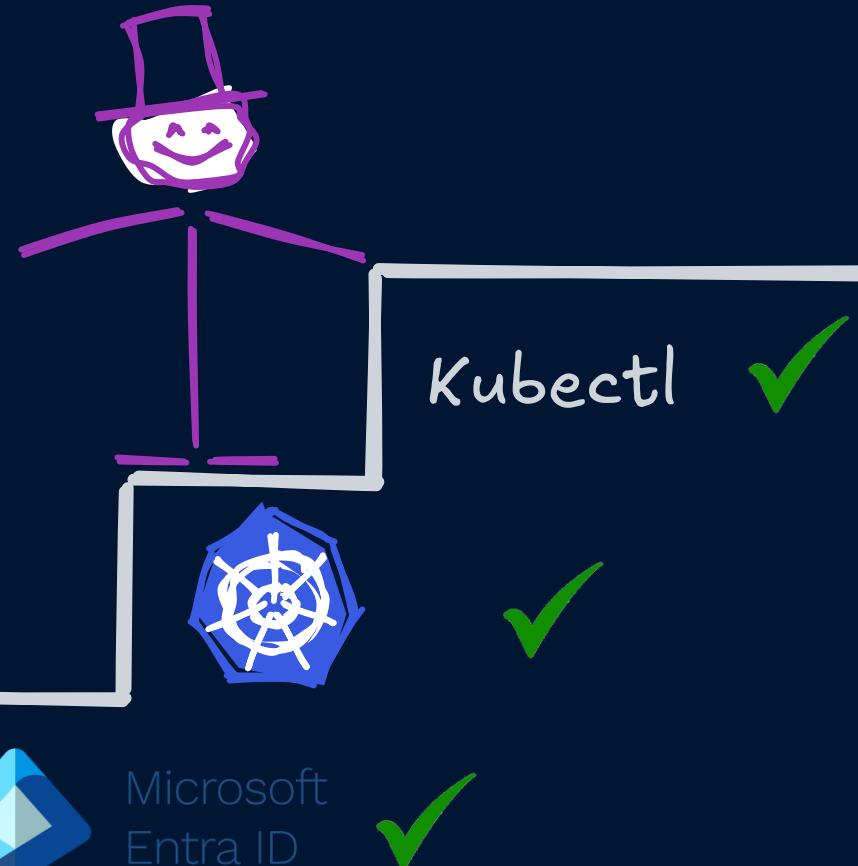
user

Terminal

```
$ rm ~/.kube/cache/oidc-login/*
$ k --context oidc auth can-i get pods
yes
$ k --context oidc auth can-i delete ns
no
```

K8S OIDC avec Microsoft Entra

Le paramétrage ... est fini!



Authentification

Résumé

	Certificats	Tokens de SA	OIDC
Acteur nominatif	100%	0%	100%
Gestion des groupes	50%	80%	100%
Révocation possible	0%	100%	100%
Simplicité de gestion	20%	50%	90%
Passe les reverse proxy L7 APIServer	0%	100%	100%

Authenfication

Alors ... convaincu?



Certificats,
Tokens



OIDC!

Questions Réponses



philippe-durand-work