



ArgoCon
NORTH AMERICA

How GitOps Changes Identity and RBAC Management

Alice Jones, Lead DevOps Engineer @ Liatrio

A Brief Review

Permission boundaries across multiple systems are *really* important.



Repo

Repo

Repo

Repo



Application

Application

Application

Application



Namespace

Namespace

Namespace

Namespace

A Brief Review

But they aren't really *easy*.



Repo

Repo

Repo

Repo



Application

Application

Application

Application



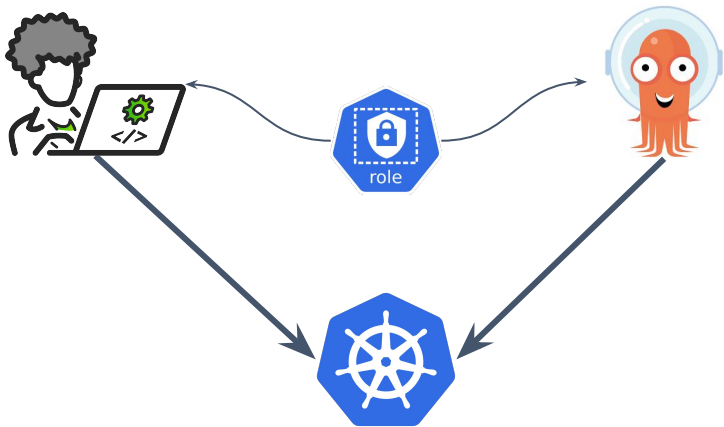
Namespace

Namespace

Namespace

Namespace

Impersonation: A Perfect Tool For Permissions



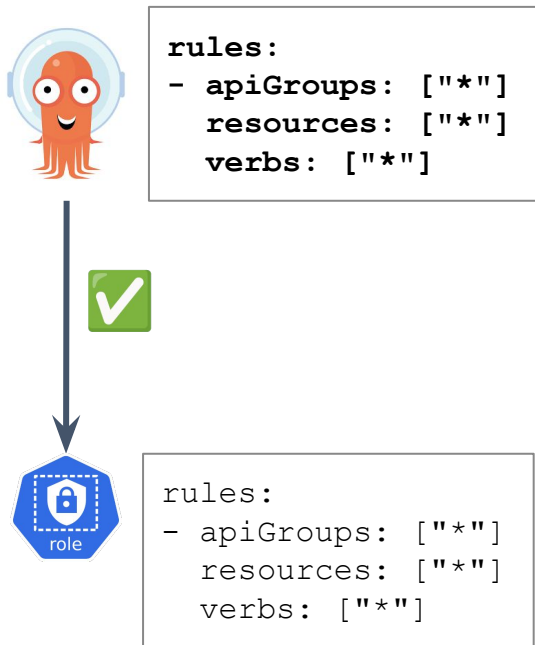
Use the same Role for
ArgoCD and Users!

🚀 New ArgoCD Feature! 🚀

```
kind: AppProject
spec:
  ...
  destinationServiceAccounts:
    - namespace: guestbook
      server: https://kubernetes.default.svc
      defaultServiceAccount: guestbook-deployer
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: guestbook-deployer
subjects:
  - kind: Group
    name: the-a-team
  - kind: ServiceAccount
    name: guestbook-deployer
roleRef:
  kind: Role
  name: guestbook-deployer
```

Impersonation: Kubernetes Native RBAC



Token Exchange: RFC 8693



Dex supports this functionality today!

Shoutout to @seankhliao !

ArgoCD was the motivating example!!!

RFC 8693 OAuth 2.0 Token Exchange #2806

 Merged nabokihms merged 3 commits into [dex:master](#) from [seankhliao:dex-token-exchange](#) on Jul 1, 2023

 Conversation 59  Commits 3  Checks 0  Files changed 14



seankhliao commented on Jan 29, 2023

Contributor ...

What this PR does / why we need it

There are times when we wish to grant machines access to a protected endpoint without using long-lived, static API keys or user/password combinations.

Many modern execution environments can expose short-lived OIDC tokens for the duration of the execution, examples include:

- [Github Actions OIDC](#)
- [CircleCI OIDC](#)
- [Kubernetes Service Accounts](#)

As these are machine users, handling a redirect is not very feasible.

In these cases, clients will have independently authenticated to the upstream IDP (sometimes implicitly by virtue of the IDP integrating with the execution environment) and obtained an ID token.

This PR allows using this prior authentication to be used in obtaining a dex issued token for use with downstream clients.

As a concrete example:

We're running [ArgoCD](#) with dex as the identity provider, connected to Okta for humans.

We want to access the ArgoCD API from our CI environments without keeping around a static key which [may be compromised](#).

Token Exchange: Why Should I Care?



ArgoCon
NORTH AMERICA



Create Applications
List Clusters
Initiate Sync
Configure Sync Policy
Rollback
Update Sync Windows

...



AppProjects: Two Impossible Options



ArgoCon
NORTH AMERICA

```
spec:
  sourceRepos:
  - '*'
  destinations:
  - namespace: '*'
    server: '*'
  clusterResourceWhitelist:
  - group: '*'
    kind: '*'
```

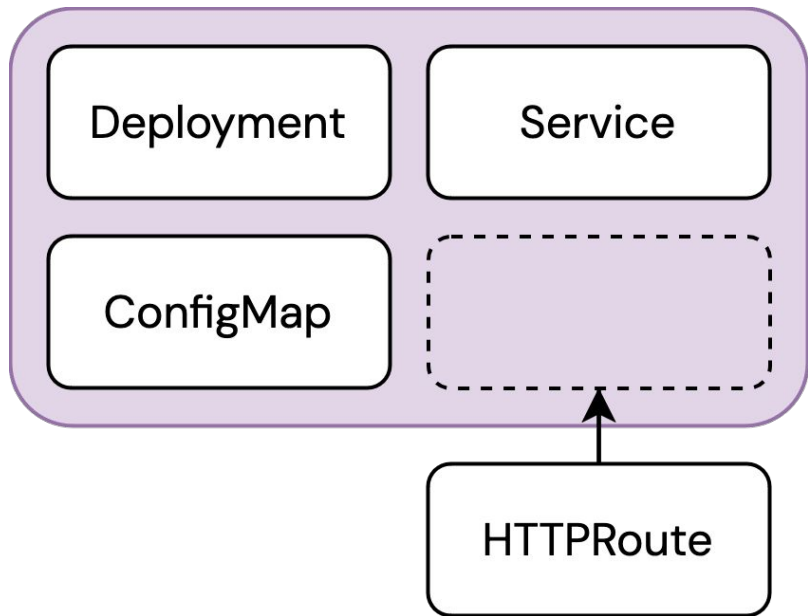
VS

```
spec:
  sourceRepos:
  - 'https://github.com/example/example'
  destinations:
  - namespace: 'default'
    server: 'https://kubernetes.default.svc'
  clusterResourceWhitelist:
  - group: ""
    kind: ConfigMap
  - group: ""
    kind: PersistentVolumeClaim
  - group: ""
    kind: Pod
  - group: ""
    kind: Service
  - group: ""
    kind: ServiceAccount
  - group: apps
    kind: Deployment
  - group: apps
    kind: ReplicaSet
  - group: apps
    kind: StatefulSet
  - group: batch
    kind: CronJob
  - group: batch
    kind: Job
  - group: external-secrets.io
    kind: ExternalSecret
  - group: gateway.networking.k8s.io
    kind: HTTPRoute
```


AppProjects: More Kinds, More Problems



ArgoCon
NORTH AMERICA



```
clusterResourceWhitelist:  
- group: apps  
  kind: Deployment  
- group: ""  
  kind: Service  
- group: ""  
  kind: ConfigMap  
- group: gateway.networking.k8s.io  
  kind: HTTPRoute
```

AppProjects: Automating RBAC Reviews


1	manifests/clusters/dev/tag-01ly/kustomization.yaml	Viewed	...
10	@@ -10,3 +10,4 @@ resources:		
11	- grafana-operator/		
12	- namespaces/		
13	+ - otel-operator/		
13	+ - dash0-operator/		

6	manifests/bootstrap/cluster_dev_project_tag-01ly.yaml	Viewed	...
17	@@ -17,12 +17,16 @@ spec:		
18	kind: ValidatingWebhookConfiguration		
19	- group: apiextensions.k8s.io		
20	kind: CustomResourceDefinition		
21	+ - group: operator.dash0.com		
22	kind: Dash0operatorConfiguration		
23	- group: rbac.authorization.k8s.io		
24	kind: ClusterRole		
25	- group: rbac.authorization.k8s.io		
26	kind: ClusterRoleBinding		
27	description: Platform Project for manifests/clusters/dev/tag-01ly		
28	destinations:		
29	+ - namespace: dash0-system		
30	+ server:		
31	- namespace: github-collector		
32	server:		
33	- namespace: grafana-operator		
49	@@ -49,6 +53,8 @@ spec:		
50	kind: PersistentVolumeClaim		
51	- group: ""		
52	kind: Pod		
53	+ - group: ""		
54	kind: Secret		
55	+ - group: ""		
56	kind: Service		
57	- group: ""		

When a new deployment is added, CI can automatically add permissions for new namespaces and kinds, but...

Permission changes are subject to approval via CODEOWNERS

Reviewers

 **kubernetes-platform-admins** 