ArgoCon

EUROPE

Mitigating Privilege Escalation in Multi-tenant Argo CD

Principal Software Engineer
@ Red Hat
Member @ Argo Project

ArgoCon
EUROPE

1 April 2025

London, England

Agenda

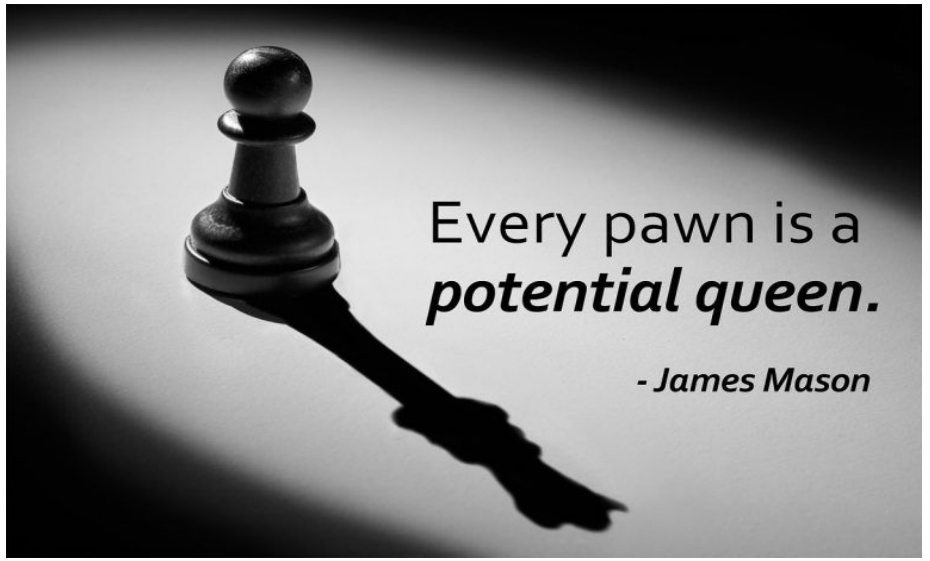
ArgoCon
EUROPE

- What is Privilege escalation ?
- Privilege escalation in Argo CD
- Multi tenant security controls in Argo CD
- Mitigation approaches
  - Policy enforced AppProjects (Classic)
  - App Sync with Impersonation Feature (Recommended way)
- Summary & Key takeaways

What is Privilege Escalation

ArgoCon EUROPE

- Consists of techniques that **adversaries** use to gain **higher-level permissions** on a **system or network**.
- Adversaries can often enter and explore a network with **unprivileged access** but acquire **elevated permissions**.
- Common approaches are to take advantage of **system weaknesses, misconfigurations, and vulnerabilities**.
- Examples of elevated access include:
  - SYSTEM/root level
  - local administrator
  - user account with admin-like access



Types of Privilege Escalation

ArgoCon EUROPE

Vertical
a cybersecurity attack where an attacker exploits vulnerabilities to gain **higher-level privileges** on a system, moving from a lower to a higher access level, like a standard user to an administrator.

Horizontal
occurs when an attacker gains access to resources or data belonging to **another user** with the **same privilege level,** rather than escalating to higher privileges

Multi tenant Security Controls

ArgoCon
EUROPE

RBAC

Includes both Argo CD and Kubernetes Role based access control.

Projects

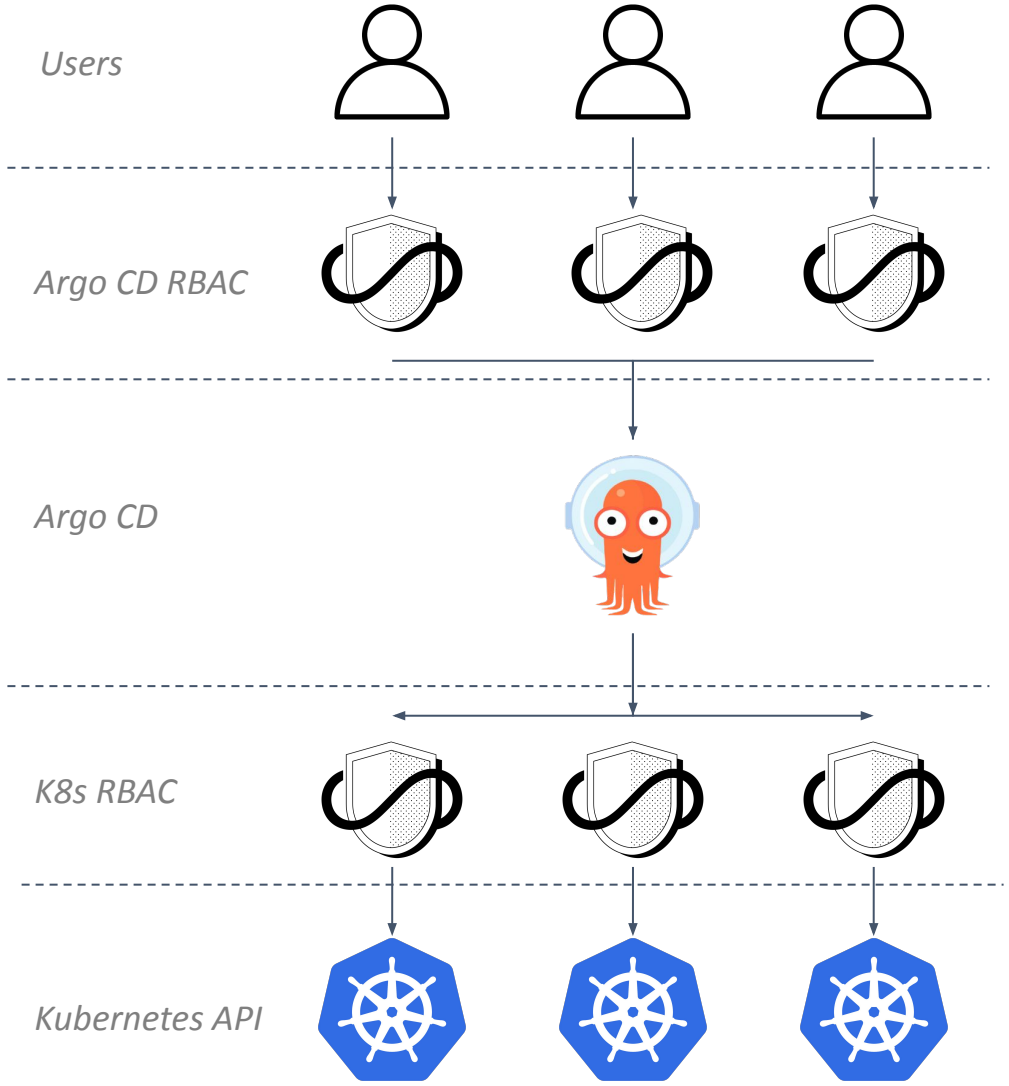
Logical grouping of applications. Often organized along tenant boundaries.

Scope

Scope of Argo CD installation - Cluster or Namespace scoped.

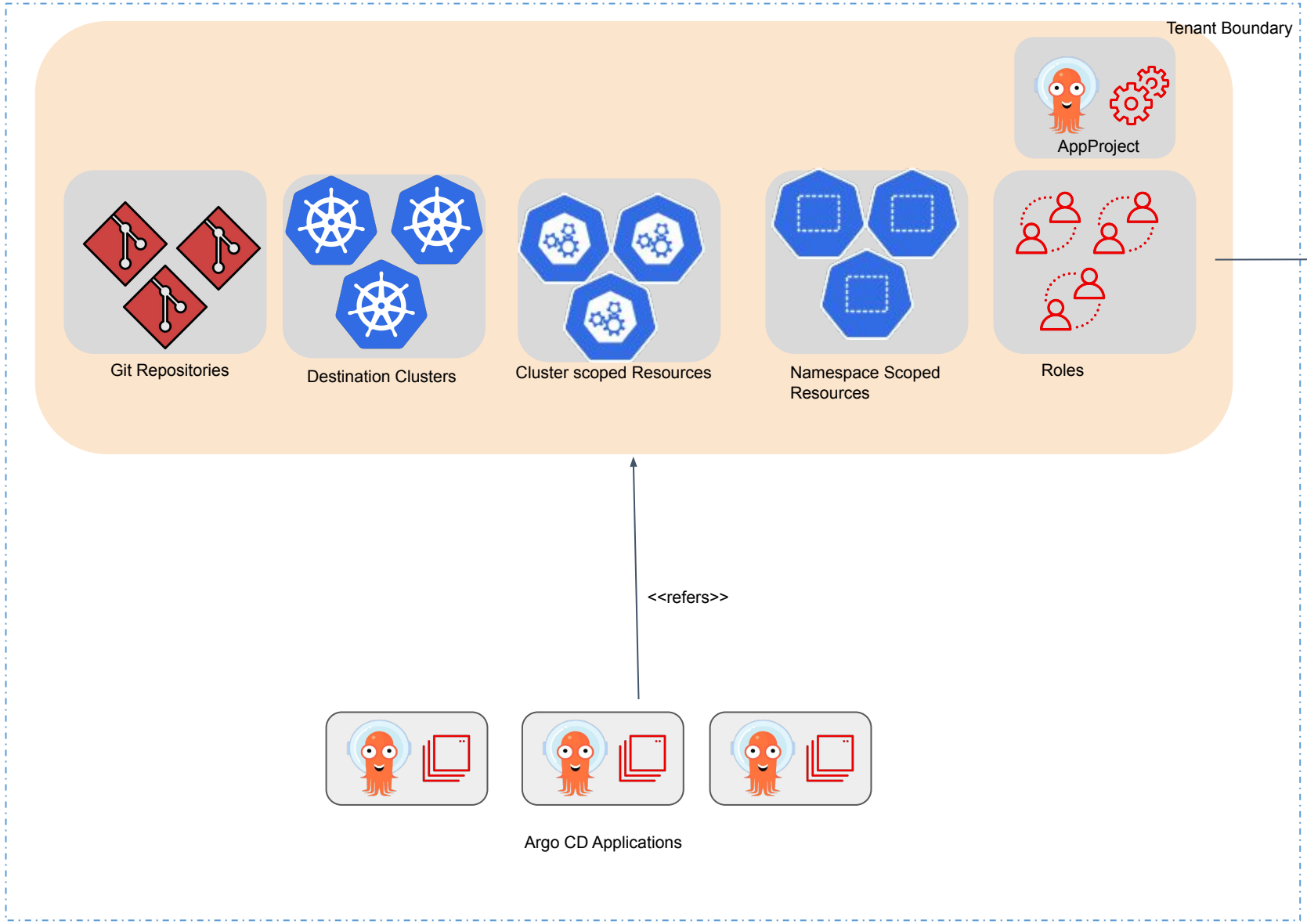
Privilege escalation in Argo CD

- Tenants accessing the same cluster use the **same** Kubernetes **Service Account** for the **sync** operation.
- Different use cases often require vastly **different permissions**
- Argo CD does not support using **different Service Accounts** to the same cluster (*)

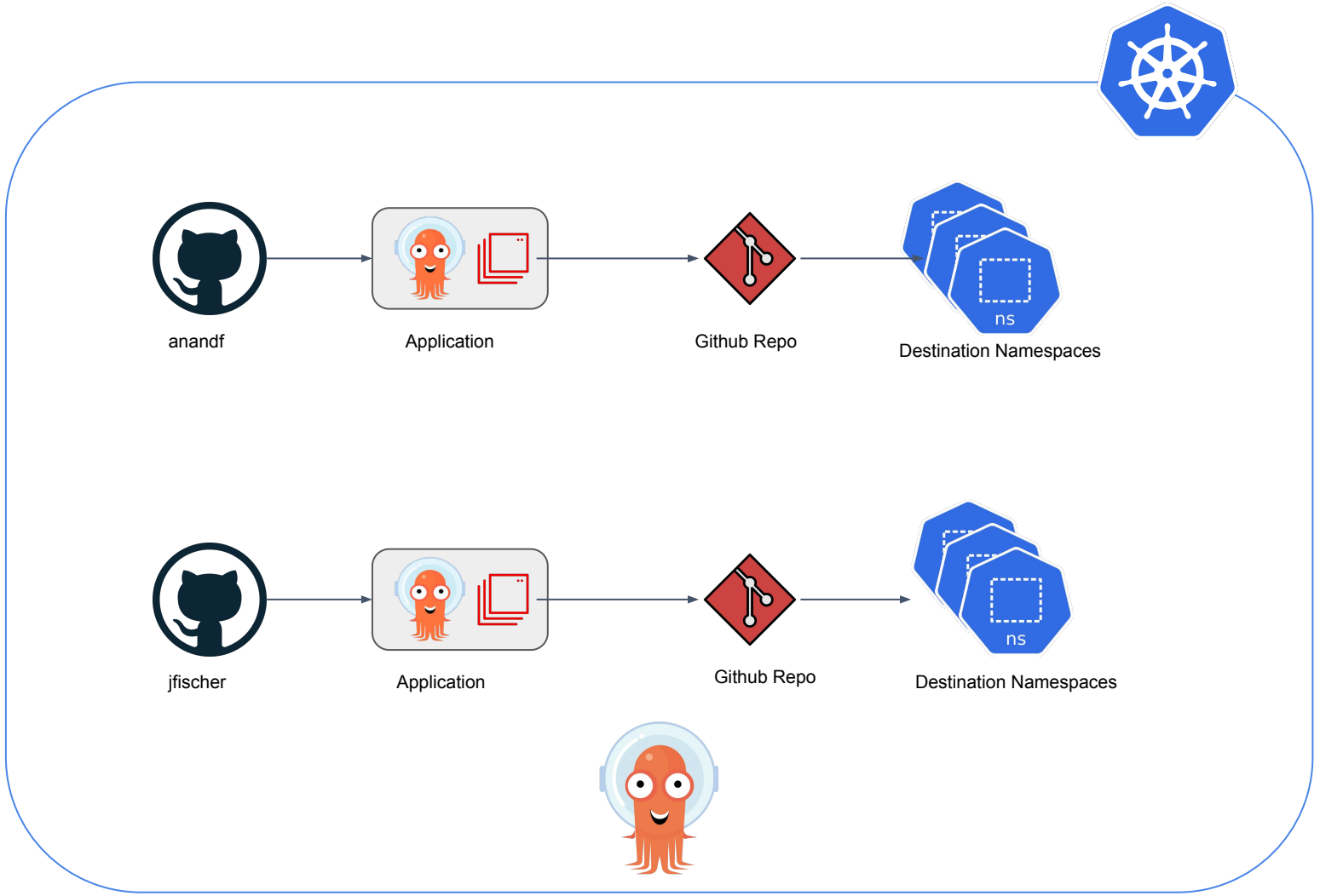


TLDR; Service Account must have privileges that meet the needs of all tenants use cases!

Argo CD Projects



Use Case - Argo CD



Approach 1 : Policy enforced AppProjects

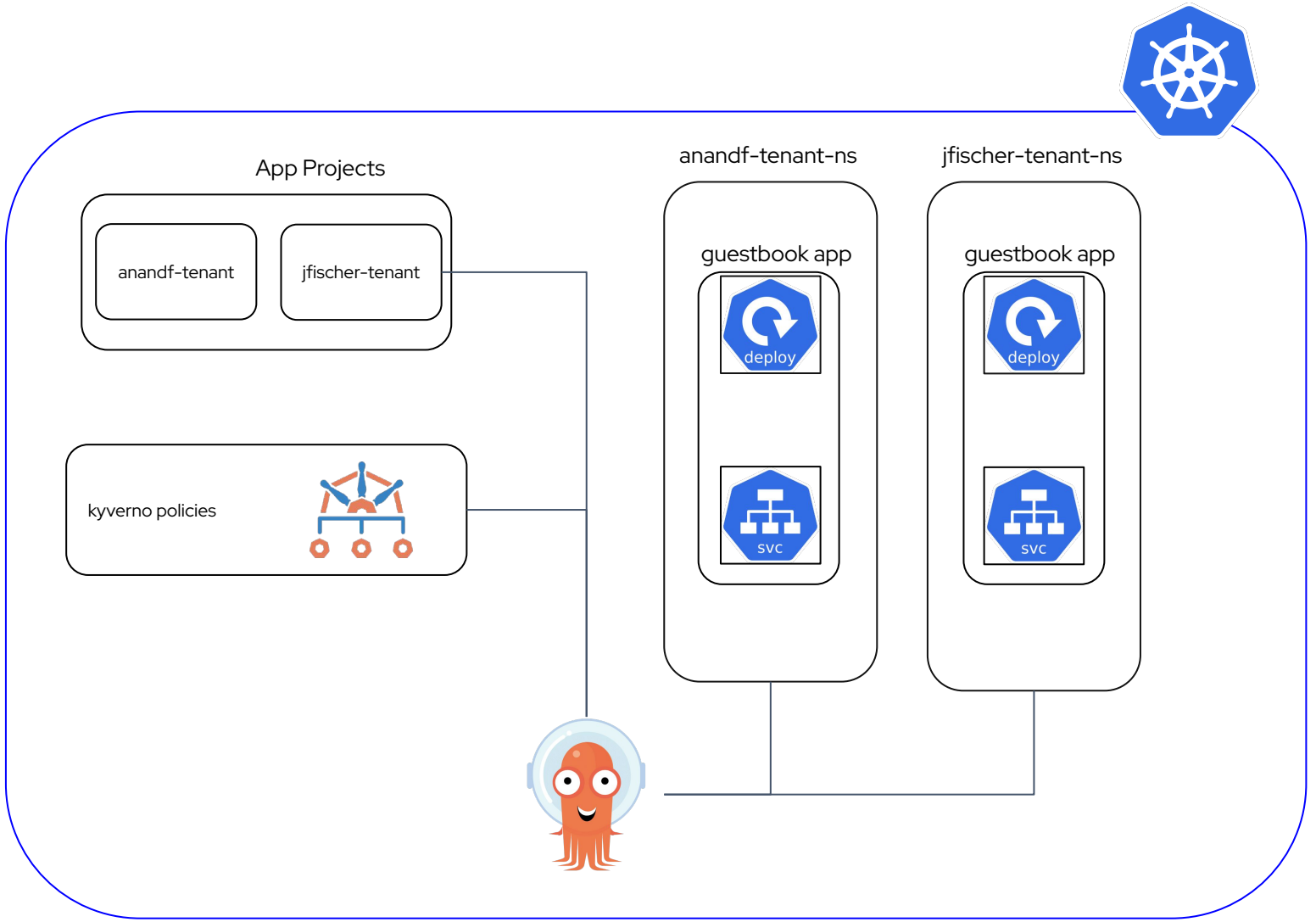
ArgoCon EUROPE

- In this approach we ensure that all the security posture remains same between AppProjects and k8s RBAC.

- Kyverno (or) Open Policy Agent (OPA) can be used for enforcing policies.

- Some of the policies
  - Do not refer the ***default*** AppProject in any Application.
  - Enforce all AppProjects inherit from the ***global*** AppProject.
  - Enforce all AppProjects are bound to only its tenant's namespace.
  - Enforce all AppProjects allow destinations that are allowed for its tenant.
  - Keep every resources **blacklisted** and **whitelist** it explicitly per tenant.

Demo Setup

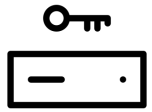

App Projects
anandf-tenant
jfischer-tenant
kyverno policies
anandf-tenant-ns
guestbook app
deploy
svc
jfischer-tenant-ns
guestbook app
deploy
svc

Approach 2: App Sync with Impersonation

New enhancement
introduced in Argo CD v2.13

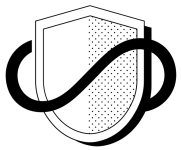
Aimed for improving
multi-tenancy user experience in
Argo CD

Experimental feature
Maturity : Alpha

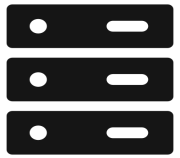


Only Administrators can
configure the service account to
be used for the sync operation

Disabled by default.
Can be enabled by setting
`application.sync.impersonation.enabled: true`



Improves the security posture of
Argo CD



Can only be enabled/disabled at
system level and not per application
or project

How to use this feature

ArgoCon EUROPE

- Enable the feature by running the following command

```
kubectl patch configmap argocd-cm -n argocd \
 -p '{"data": {"application.sync.impersonation.enabled": "true"}}'
```

- (Optional) Add support for apps in any namespace by running the following command.

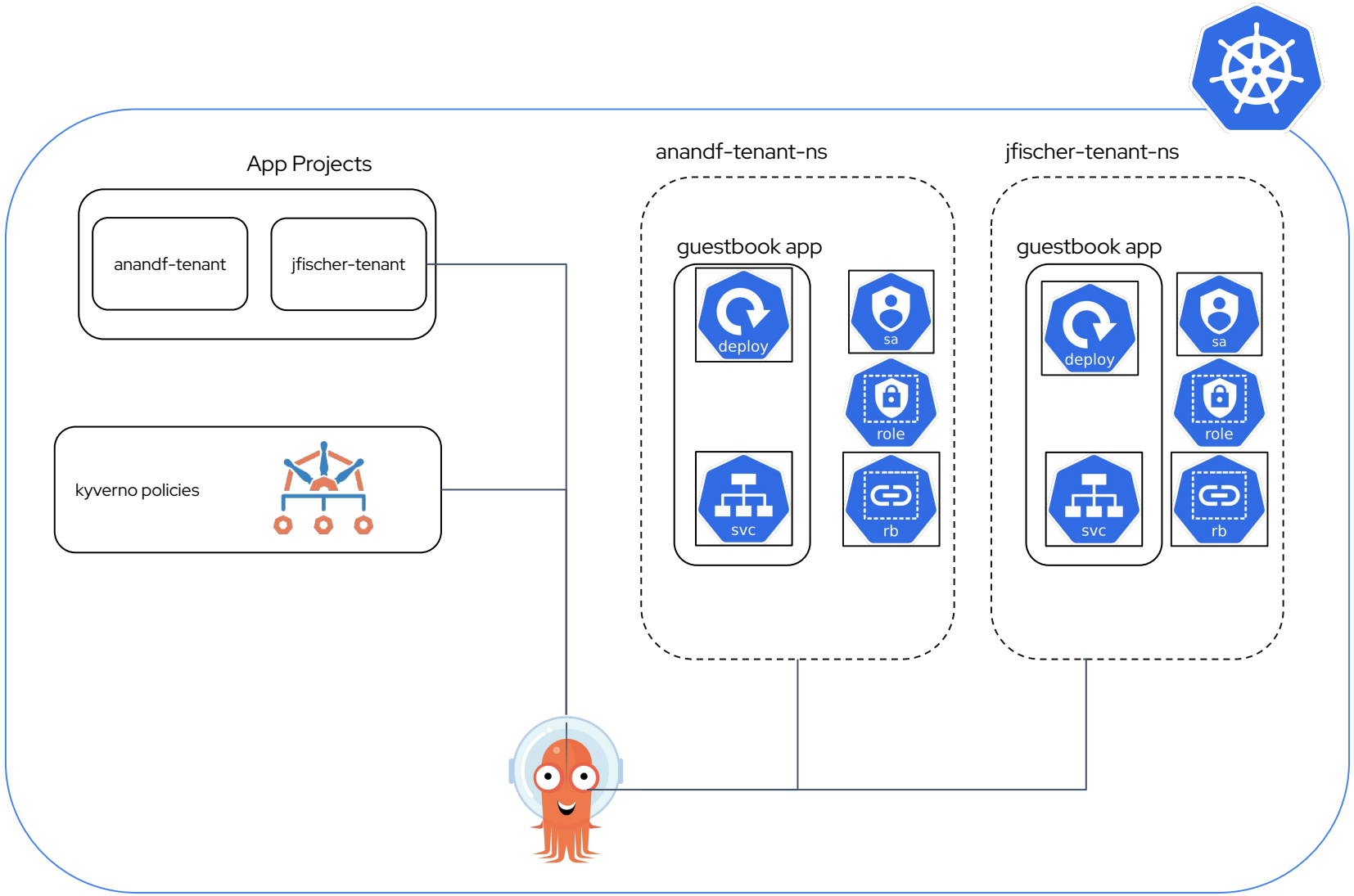
```
kubectl patch cm argocd-cmd-params-cm -n argocd \
  -p '{"data": {"application.namespaces": "tenant-*"}}'
```

- Destination service accounts can be added to the AppProject under .spec.destinationServiceAccounts

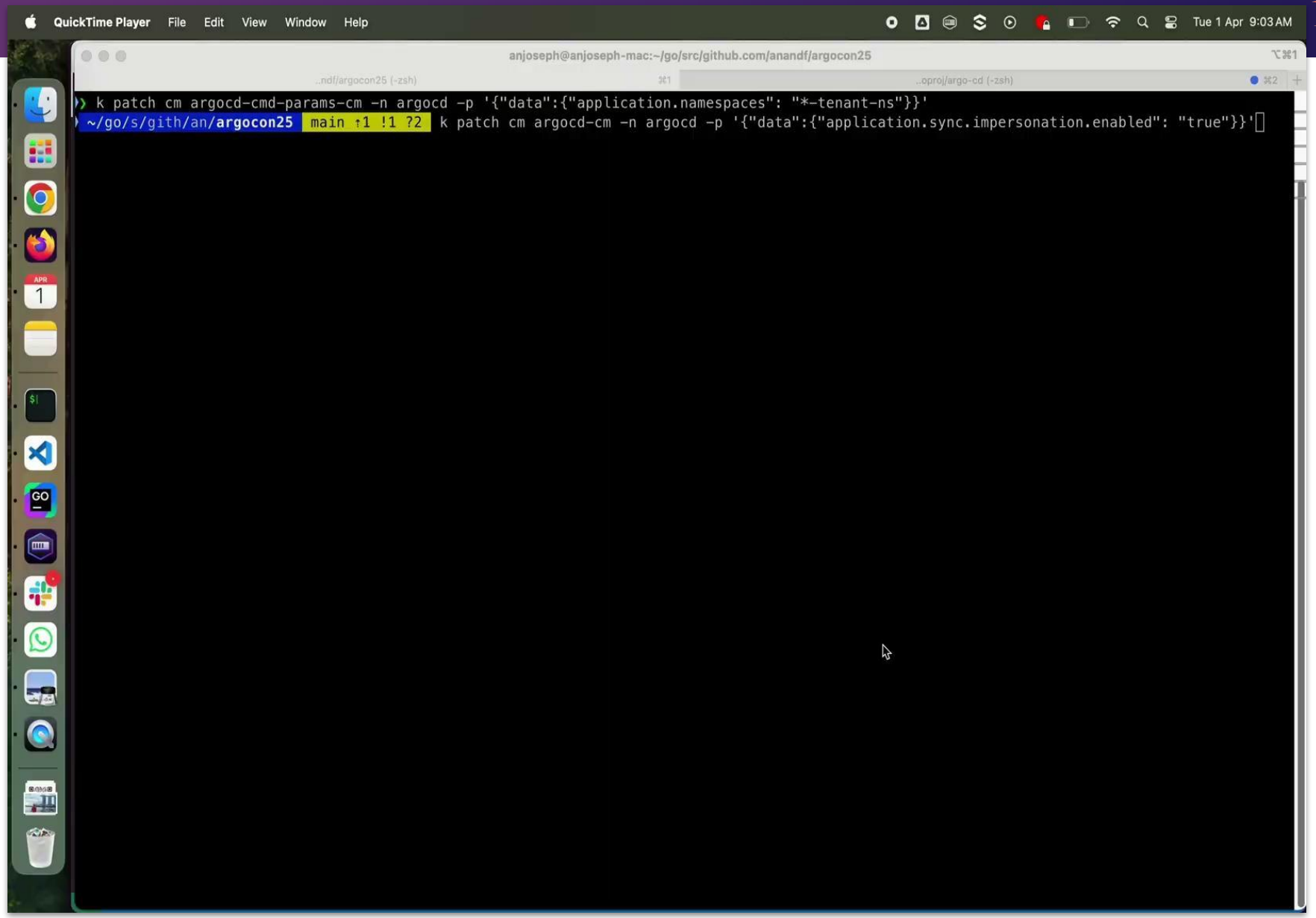
- One or more Destination ServiceAccounts can be configured in an AppProject, each pointing to target server and namespace combination

```
destinationServiceAccounts:
 - server: https://kubernetes.default.svc
   namespace: guestbook
   defaultServiceAccount: guestbook-deployer
 - server: https://kubernetes.default.svc
   namespace: guestbook-dev
   defaultServiceAccount: guestbook-dev-deployer
 - server: https://kubernetes.default.svc
```

Demo Setup


App Projects
anandf-tenant
jfischer-tenant
kyverno policies
anandf-tenant-ns
guestbook app
deploy
sa
role
svc
rb
jfischer-tenant-ns
guestbook app
deploy
sa
role
svc
rb

Demo


QuickTime Player File Edit View Window Help
Tue 1 Apr 9:03 AM
anjoseph@anjoseph-mac:~/go/src/github.com/anandf/argocon25
k patch cm argocd-cmd-params-cm -n argocd -p '{"data":{"application.namespaces": "*-tenant-ns"}}'
~/go/s/gith/an/argocon25 main ↑1 !1 ?2 k patch cm argocd-cm -n argocd -p '{"data":{"application.sync.impersonation.enabled": "true"}}'

Benefits

ArgoCon
EUROPE

- Prevent privilege escalation (issue#9606)
- Possibility of having multiple destination clusters with same server URL (issue#15027).
- Support for avoiding accidental deletion of resources (issue#11227) (Work In progress)

Additional Resources

ArgoCon
EUROPE

Feature Documentation

- https://argo-cd.readthedocs.io/en/stable/operator-manual/app-sync-using-impersonation/
- https://argo-cd.readthedocs.io/en/stable/proposals/decouple-application-sync-user-using-impersonation/

Demo Materials

https://github.com/anandf/ArgoConEU2025

Summary & Key Takeaway

ArgoCon
EUROPE

- App sync with impersonation is a powerful feature to use existing Kubernetes RBAC to decouple the sync process for multiple tenants.
- It allows platform admins to follow the principle of assigning least privileges that is required for each tenant.
- It works directly with k8s RBAC and can avoid privilege escalations caused due to misconfigurations.
- Having policies to enforce the best practices can greatly improve the security posture of Argo CD.