ArgoCD

Projects, Authentication, Authorization

Projects, Authentication, Authorization

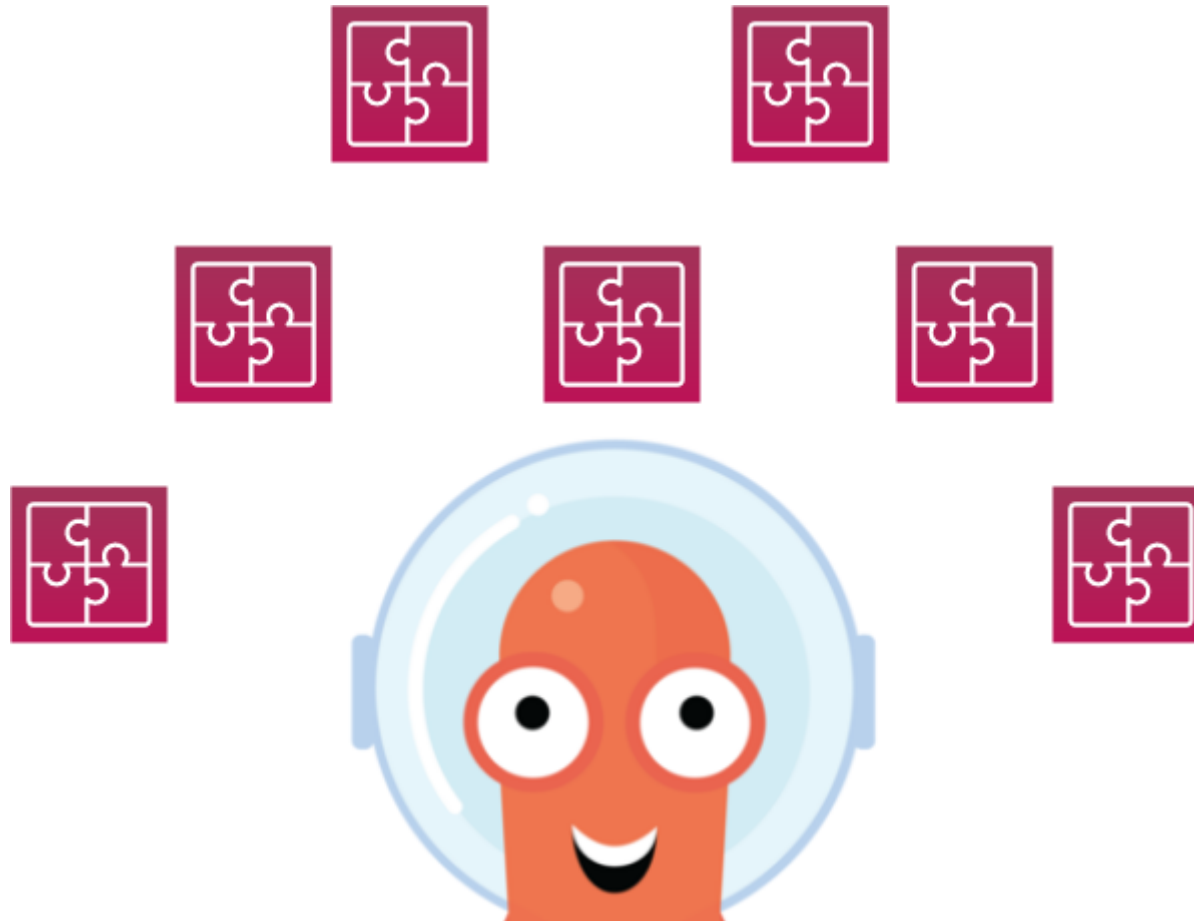¬Applications are collections of Resources

¬ArgoCD instance manages applications

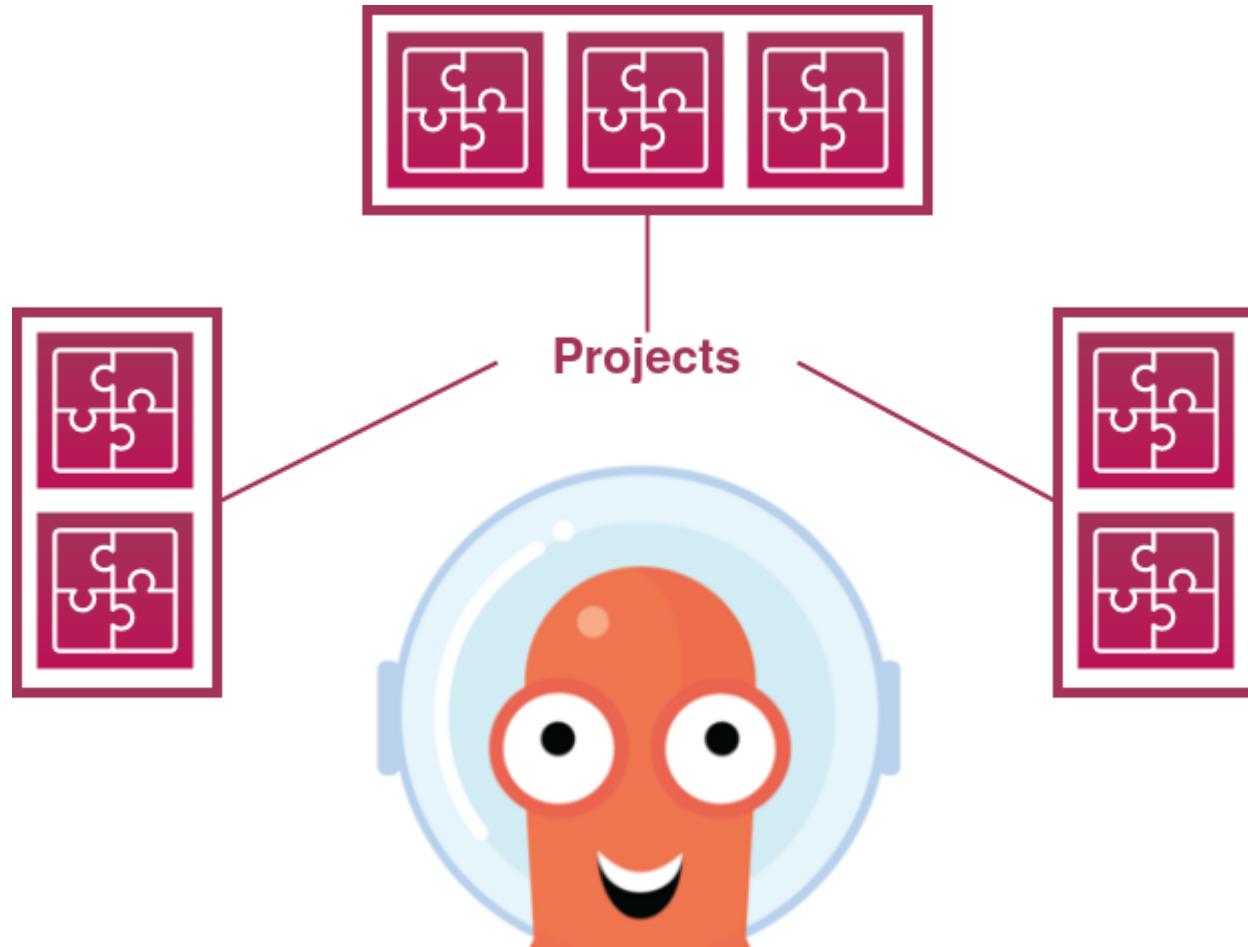¬Multiple Teams working on instance

¬Manage access in Argo

ArgoCD

Projects

ArgoCD
Projects

Projects

Projects

Projects

¬Which repos may be deployed?

¬Where may it be deployed?

¬What kinds of objects?

¬Defining roles (RBAC) for projects.

ArgoCD
Projects

```yaml
apiVersion: argoproj.io/v1alpha1
kind: AppProject
metadata:
  name: my-project
  namespace: argocd
spec:
  description: Example Project
  # Allow manifests to deploy from any Git repos
  sourceRepos:
  - '*'
  # Only permit applications to deploy to the guestbook namespace in the same clus
  destinations:
  - namespace: guestbook
    server: https://kubernetes.default.svc
  # Deny all cluster-scoped resources from being created, except for Namespace
  clusterResourceWhitelist:
  - group: ''
    kind: Namespace
  # Allow all namespaced-scoped resources to be created, except for ResourceQuota,
  namespaceResourceBlacklist:
  - group: ''
    kind: ResourceQuota
  - group: ''
    kind: LimitRange
  - group: ''
    kind: NetworkPolicy
  roles:
  # A role which provides read-only access to all applications in the project
  - name: read-only
    description: Read-only privileges to my-project
    policies:
```

ArgoCD

Authentication

Authentication

¬Authentication exclusive JWT

- Local Admin user

- OAuth2

- Automation Tokens

ArgoCD

Authorization

Authorization

¬User claims groups in JWT

¬Compared against RBAC policies

¬Roles / Policies defined in Argo

Authorization

¬Roles and Policies defined in `argocd-rbac-cm` ConfigMap

¬Create Roles and add Policies to them

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: argocd-rbac-cm
  namespace: argocd
data:
  policy.default: role:readonly
  policy.csv: |
    p, role:org-admin, applications, *, */*, allow
    p, role:org-admin, clusters, get, *, allow
    p, role:org-admin, repositories, get, *, allow
    p, role:org-admin, repositories, create, *, allow
    p, role:org-admin, repositories, update, *, allow
    p, role:org-admin, repositories, delete, *, allow

    g, your-github-org:your-team, role:org-admin
```