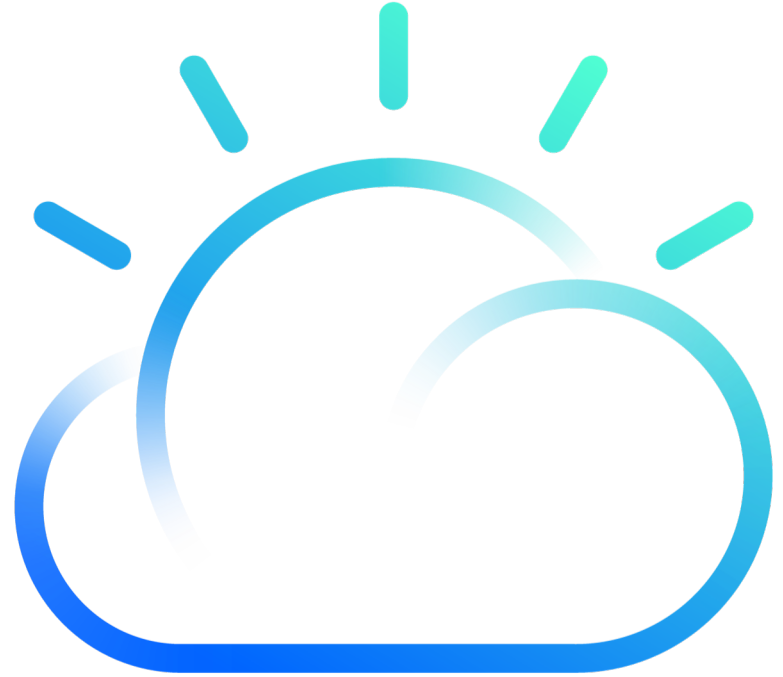


# IBM Cloud private

an innovation accelerator



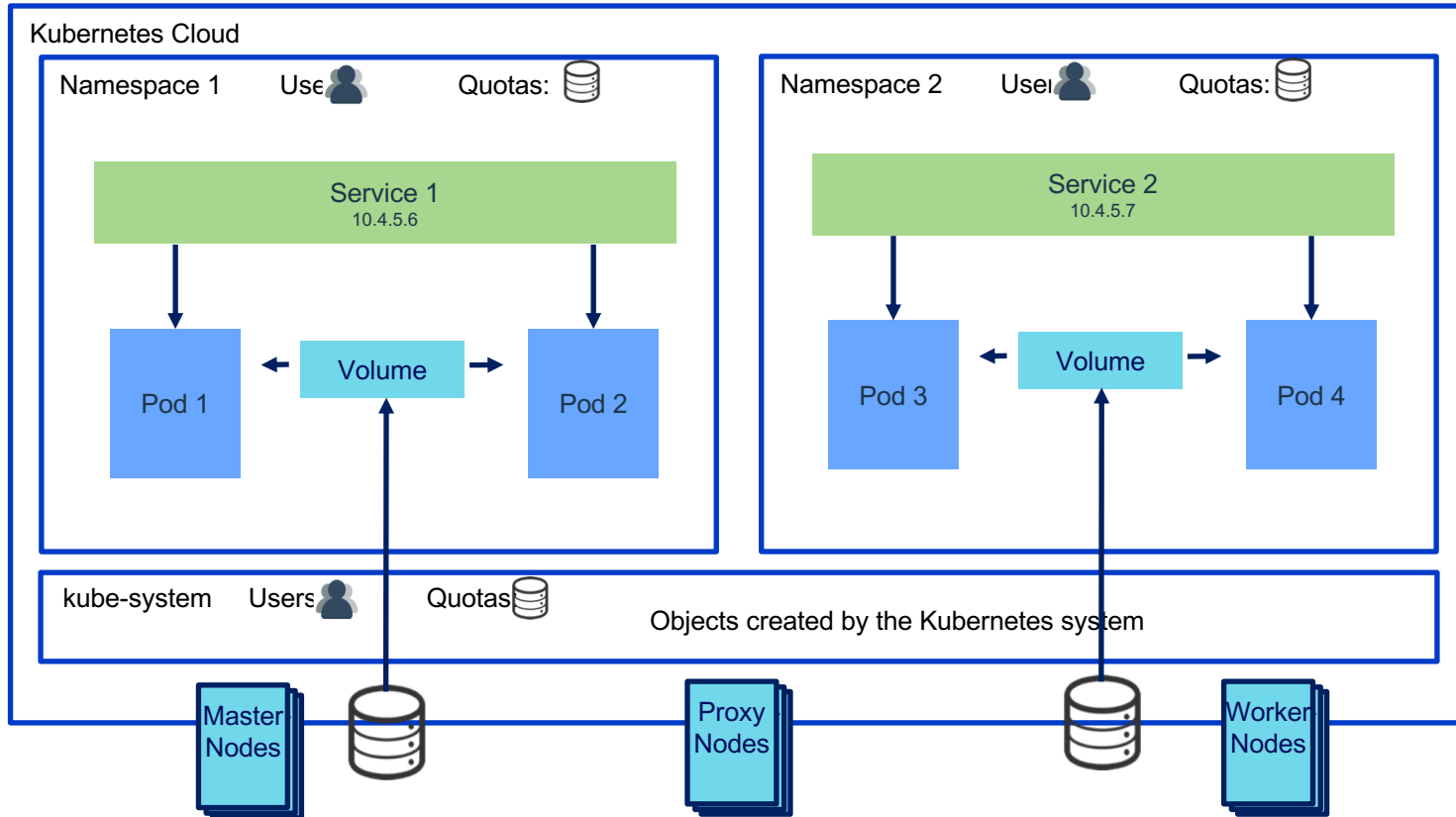
User isolation &  
Role Base Control Access (RBAC)



Jérôme Tarte  
IBM Cloud Adoption Leader  
[jerome.tarte@fr.ibm.com](mailto:jerome.tarte@fr.ibm.com)

**IBM Cloud**

# One cloud, isolation across teams

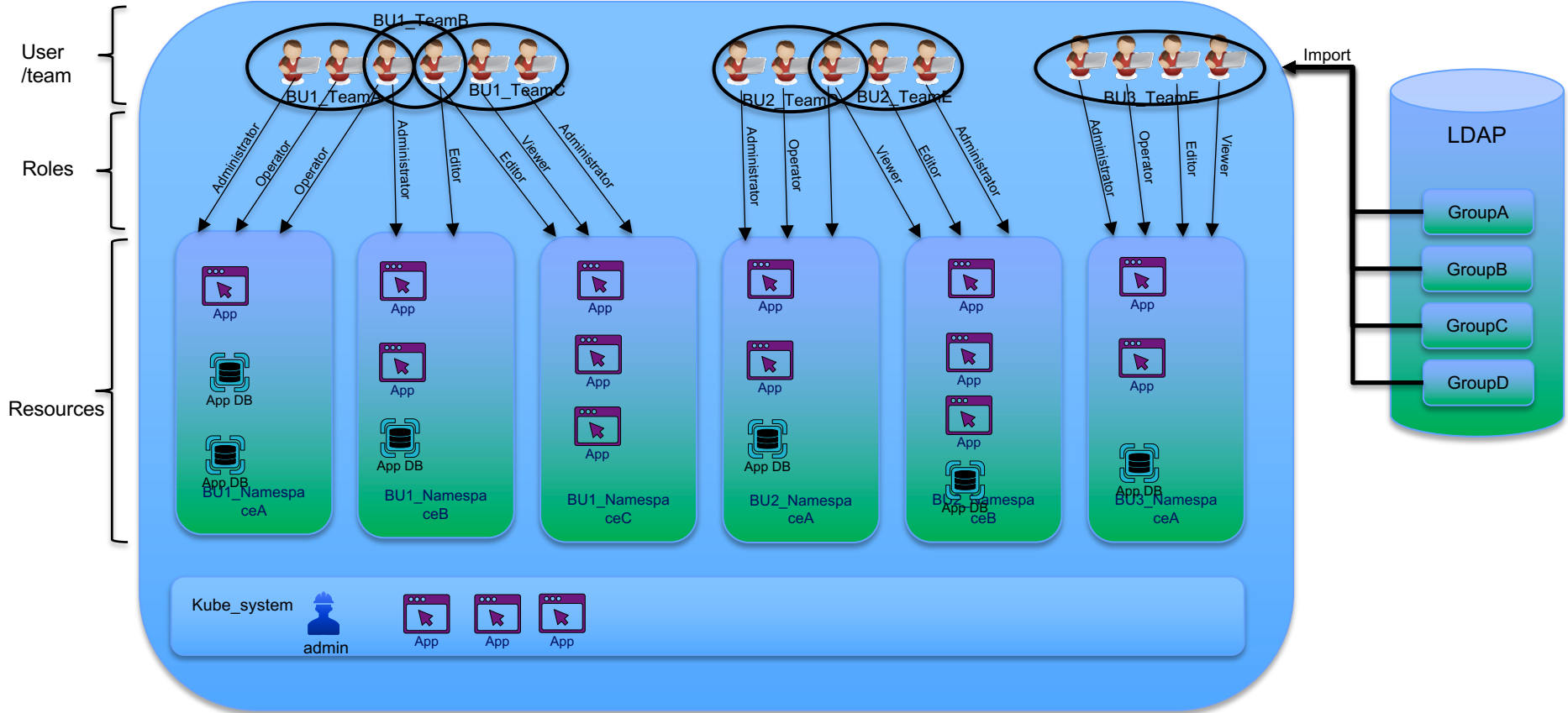


## Quotas

*Categories you can set quotas in a namespace:*

- Compute
- Storage
- Object count (pods, services, pvc, ...)
- Scope

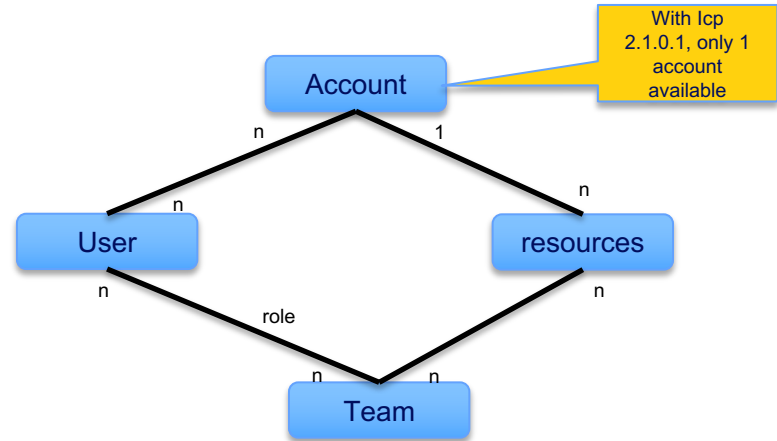
# Team & namespaces isolation on ICP Kubernetes



# Role-Based Access Control (RBAC)

Role	Description	Actions
Viewer	Has read-only access. By default, the Viewer role is assigned to users when they are added to a team.	The Viewer can view information about the team resources.
Editor	Has read and edit access.	The Editor can view and edit team resources.
Operator	Has read, edit, and create access.	The Operator can view, edit, and create team resources.
Administrator	Has add, update, view, and delete access.	The Administrator can create, update, and delete team resources.

- IAM role is assigned to a user when the user is assigned to a team
- Within a team, each user can have only one role.
- If a user is a member of multiple teams, the user can have different roles on each team.
- An IAM role defines the actions that a user can do on the team resources.
- Users are imported from the LDAP



# RBAC and Cluster Administration

Provide cluster administration credentials to some users

- Use of Clusterrolebindings
- Avoid that all administration tasks are made by one generic user *admin*
  - *Improve traceability of actions*

Define credentials at Cluster level

- Credentials could be affined by role
  - Full administration
  - Operator
  - Viewer

Clusterrole and Clusterrolebinding versus Role and Rolebinding

- Clusterrole and Clusterrolebinding are positioned globally
  - Allow the administration of cluster
- Role and Rolebinding are positioned locally
  - Allows the administration of a resource ( namespace)
  - Use to set up team in IBM Cloud private

```
Jeromes-MacBook-Pro:~ jtar$ kubectl get Clusterrolebindings --all-namespaces
```

NAMESPACE	NAME	KIND	SUBJECTS
admin-users	admin-users	ClusterRoleBinding.v1.rbac.authorization.k8s.io	2 item(s)
cluster-admin	cluster-admin	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
default-psp-users	default-psp-users	ClusterRoleBinding.v1.rbac.authorization.k8s.io	2 item(s)
oidc-admin-binding	oidc-admin-binding	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
privileged-psp-users	privileged-psp-users	ClusterRoleBinding.v1.rbac.authorization.k8s.io	6 item(s)
servicecatalog.k8s.io:apiserver	servicecatalog.k8s.io:apiserver	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
servicecatalog.k8s.io:apiserver-auth-delegator	servicecatalog.k8s.io:apiserver-auth-delegator	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
servicecatalog.k8s.io:controller-manager	servicecatalog.k8s.io:controller-manager	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:basic-user	system:basic-user	ClusterRoleBinding.v1.rbac.authorization.k8s.io	2 item(s)
system:controller:attachdetach-controller	system:controller:attachdetach-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:certificate-controller	system:controller:certificate-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:cronjob-controller	system:controller:cronjob-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:daemon-set-controller	system:controller:daemon-set-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:deployment-controller	system:controller:deployment-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:disruption-controller	system:controller:disruption-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:endpoint-controller	system:controller:endpoint-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:generic-garbage-collector	system:controller:generic-garbage-collector	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:horizontal-pod-autoscaler	system:controller:horizontal-pod-autoscaler	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:job-controller	system:controller:job-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:namespace-controller	system:controller:namespace-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:node-controller	system:controller:node-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:persistent-volume-binder	system:controller:persistent-volume-binder	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:pod-garbage-collector	system:controller:pod-garbage-collector	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:replication-controller	system:controller:replication-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:resourcequota-controller	system:controller:resourcequota-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:route-controller	system:controller:route-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:service-account-controller	system:controller:service-account-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:service-controller	system:controller:service-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:statefulset-controller	system:controller:statefulset-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:controller:tll-controller	system:controller:tll-controller	ClusterRoleBinding.v1.rbac.authorization.k8s.io	2 item(s)
system:discovery	system:discovery	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:kube-controller-manager	system:kube-controller-manager	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:kube-dns	system:kube-dns	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:kube-scheduler	system:kube-scheduler	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:node	system:node	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)
system:node-proxier	system:node-proxier	ClusterRoleBinding.v1.rbac.authorization.k8s.io	1 item(s)

```
Jeromes-MacBook-Pro:~ jtar$
```

# Demonstration

