Role Based Access Control

Important term: Authentication, authorization, name space and cluster.

- To properly manage access in k8s it's critical to understand how identity, roles and role bindings interact to control who can do what with resources.
- Identity in Kubernetes:
    - Every request that comes to k8s is associated with some identity, Event a request with no identity is associated with system:unauthenticated group.
    - k8s makes a distinction b/w user identities and service account identities
    - Service accounts are created and managed by k8s itself and are generally associated with components running inside cluster
    - User accounts are all other accounts with actual users of cluster, and often include automation like continuous delivery as a service that runs outside of cluster
    - K8s uses a generic interface for authentication providers
    - k8s supports a number of different authentication providers including
        - HTTP Basic Authentication (Largely deprecated)
        - x509 Client Certificates
        - Static token files on the host
        - Cloud Authentication providers like Azure Active Directory and AWS IAM
        - Authentication Web Hooks
    - While most managed k8s installation configure authentication for you, if you are deploying your own authentication yo will need to configure flags on the k8s API Server appropriately
- Understanding Roles and Role Bindings:
    - Identity is just beginning of authorization in K8s. Once the system knows the identity, it needs to determine if the request is authorized for that user. To achieve this, k8s used the general concept of role and role bindings
    - A role is set of abstract capabilities. For example ability to create Pods, Services etc
    - A role binding is an assignment of a role to one or more identities
- Roles and Role Bindings in K8s
    - In k8s there are two pairs of related resources that represent role and role binding.
    - One pair applies to just a namespace (Role and RoleBinding) and then other applies across the cluster (ClusterRole and ClusterRoleBinding

```
PS C:\Users\qtkha> kubectl get roles --all-namespaces
NAMESPACE     NAME                                             CREATED AT
kube-public   system:controller:bootstrap-signer               2021-07-28T14:39:00Z
kube-system   cloud-provider                                   2021-07-28T14:39:29Z
kube-system   extension-apiserver-authentication-reader        2021-07-28T14:39:00Z
kube-system   gce:cloud-provider                               2021-07-28T14:39:29Z
kube-system   pdcsi-leaderelection                             2021-07-28T14:39:25Z
kube-system   snapshot-controller-leaderelection               2021-07-28T14:39:26Z
kube-system   system::leader-locking-kube-controller-manager   2021-07-28T14:39:00Z
kube-system   system::leader-locking-kube-scheduler            2021-07-28T14:39:00Z
kube-system   system:controller:bootstrap-signer               2021-07-28T14:39:00Z
kube-system   system:controller:cloud-provider                 2021-07-28T14:39:00Z
kube-system   system:controller:glbc                           2021-07-28T14:39:30Z
kube-system   system:controller:token-cleaner                  2021-07-28T14:39:00Z
PS C:\Users\qtkha> kubectl get rolebindings --all-namespaces
NAMESPACE     NAME                                             ROLE                                                          AGE
kube-public   system:controller:bootstrap-signer               Role/system:controller:bootstrap-signer                       23h
kube-system   gce:cloud-provider                               Role/gce:cloud-provider                                       23h
kube-system   gce:podsecuritypolicy:pdcsi-node-sa              ClusterRole/gce:podsecuritypolicy:privileged                  23h
kube-system   metrics-server-auth-reader                       Role/extension-apiserver-authentication-reader                23h
kube-system   pdcsi-leaderelection-binding                     Role/pdcsi-leaderelection                                     23h
kube-system   snapshot-controller-leaderelection               Role/snapshot-controller-leaderelection                       23h
kube-system   system::extension-apiserver-authentication-reader   Role/extension-apiserver-authentication-reader            23h
kube-system   system::leader-locking-kube-controller-manager   Role/system::leader-locking-kube-controller-manager            23h
kube-system   system::leader-locking-kube-scheduler            Role/system::leader-locking-kube-scheduler                     23h
kube-system   system:controller:bootstrap-signer               Role/system:controller:bootstrap-signer                       23h
kube-system   system:controller:cloud-provider                 Role/system:controller:cloud-provider                         23h
kube-system   system:controller:glbc                           Role/system:controller:glbc                                   23h
kube-system   system:controller:token-cleaner                  Role/system:controller:token-cleaner                          23h
PS C:\Users\qtkha>
```

```
PS C:\Users\qtkha> kubectl get clusterroles -A
NAME                                                                   CREATED AT
admin                                                                  2021-07-28T14:38:59Z
cloud-provider                                                         2021-07-28T14:39:29Z
cluster-admin                                                          2021-07-28T14:38:59Z
edit                                                                   2021-07-28T14:38:59Z
external-metrics-reader                                                2021-07-28T14:39:29Z
gce:beta:kubelet-certificate-bootstrap                                 2021-07-28T14:39:30Z
gce:beta:kubelet-certificate-rotation                                  2021-07-28T14:39:30Z
gce:cloud-provider                                                     2021-07-28T14:39:29Z
gke-metrics-agent                                                      2021-07-28T14:39:25Z
kubelet-api-admin                                                      2021-07-28T14:39:30Z
pdcsi-attacher-role                                                    2021-07-28T14:39:25Z
pdcsi-provisioner-role                                                 2021-07-28T14:39:25Z
pdcsi-resizer-role                                                     2021-07-28T14:39:25Z
pdcsi-snapshotter-role                                                 2021-07-28T14:39:25Z
read-updateinfo                                                        2021-07-28T14:39:29Z
snapshot-controller-runner                                             2021-07-28T14:39:26Z
stackdriver:metadata-agent                                             2021-07-28T14:39:21Z
storage-version-migration-crd-creator                                  2021-07-28T14:39:28Z
storage-version-migration-initializer                                  2021-07-28T14:39:28Z
storage-version-migration-trigger                                      2021-07-28T14:39:27Z
system:aggregate-to-admin                                              2021-07-28T14:38:59Z
system:aggregate-to-edit                                               2021-07-28T14:38:59Z
system:aggregate-to-view                                               2021-07-28T14:38:59Z
system:auth-delegator                                                  2021-07-28T14:38:59Z
system:basic-user                                                      2021-07-28T14:38:59Z
system:certificates.k8s.io:certificatesigningrequests:nodeclient       2021-07-28T14:38:59Z
system:certificates.k8s.io:certificatesigningrequests:selfnodeclient   2021-07-28T14:38:59Z
system:certificates.k8s.io:kube-apiserver-client-approver              2021-07-28T14:38:59Z
system:certificates.k8s.io:kube-apiserver-client-kubelet-approver      2021-07-28T14:38:59Z
system:certificates.k8s.io:kubelet-serving-approver                    2021-07-28T14:38:59Z
system:certificates.k8s.io:legacy-unknown-approver                     2021-07-28T14:38:59Z
system:clustermetrics                                                  2021-07-28T14:39:24Z
system:controller:attachdetach-controller                              2021-07-28T14:38:59Z
system:controller:certificate-controller                               2021-07-28T14:38:59Z
system:controller:clusterrole-aggregation-controller                   2021-07-28T14:38:59Z
system:controller:cronjob-controller                                   2021-07-28T14:38:59Z
system:controller:daemon-set-controller                                2021-07-28T14:38:59Z
```

```
PS C:\Users\qtkha> kubectl get clusterrolebindings -A
NAME                                                   ROLE                                                                          AGE
cluster-admin                                          ClusterRole/cluster-admin                                                     23h
cluster-autoscaler-updateinfo                          ClusterRole/read-updateinfo                                                   23h
event-exporter-rb                                      ClusterRole/view                                                              23h
gce:beta:kubelet-certificate-bootstrap                 ClusterRole/gce:beta:kubelet-certificate-bootstrap                            23h
gce:beta:kubelet-certificate-rotation                  ClusterRole/gce:beta:kubelet-certificate-rotation                             23h
gce:cloud-provider                                     ClusterRole/gce:cloud-provider                                                23h
gke-metrics-agent                                      ClusterRole/gke-metrics-agent                                                 23h
kube-apiserver-kubelet-api-admin                       ClusterRole/kubelet-api-admin                                                 23h
kubelet-bootstrap                                      ClusterRole/system:node-bootstrapper                                          23h
kubelet-bootstrap-certificate-bootstrap                ClusterRole/gce:beta:kubelet-certificate-bootstrap                            23h
kubelet-bootstrap-node-bootstrapper                    ClusterRole/system:node-bootstrapper                                          23h
kubelet-cluster-admin                                  ClusterRole/system:node                                                       23h
kubelet-user-npd-binding                               ClusterRole/system:node-problem-detector                                      23h
master-monitoring-role-binding                         ClusterRole/system:master-monitoring-role                                     23h
metrics-server:system:auth-delegator                   ClusterRole/system:auth-delegator                                             23h
npd-binding                                            ClusterRole/system:node-problem-detector                                      23h
pdcsi-controller-attacher-binding                      ClusterRole/pdcsi-attacher-role                                               23h
pdcsi-controller-provisioner-binding                   ClusterRole/pdcsi-provisioner-role                                            23h
pdcsi-controller-resizer-binding                       ClusterRole/pdcsi-resizer-role                                                23h
pdcsi-snapshotter-binding                              ClusterRole/pdcsi-snapshotter-role                                            23h
snapshot-controller-role                               ClusterRole/snapshot-controller-runner                                        23h
stackdriver:metadata-agent                             ClusterRole/stackdriver:metadata-agent                                        23h
storage-version-migration-crd-creator                  ClusterRole/storage-version-migration-crd-creator                             23h
storage-version-migration-initializer                  ClusterRole/storage-version-migration-initializer                             23h
storage-version-migration-migrator-v2                  ClusterRole/cluster-admin                                                     23h
storage-version-migration-trigger                      ClusterRole/storage-version-migration-trigger                                 23h
system:basic-user                                      ClusterRole/system:basic-user                                                 23h
system:clustermetrics                                  ClusterRole/system:clustermetrics                                             23h
system:controller:attachdetach-controller              ClusterRole/system:controller:attachdetach-controller                         23h
system:controller:certificate-controller               ClusterRole/system:controller:certificate-controller                          23h
system:controller:clusterrole-aggregation-controller   ClusterRole/system:controller:clusterrole-aggregation-controller               23h
system:controller:cronjob-controller                   ClusterRole/system:controller:cronjob-controller                              23h
system:controller:daemon-set-controller                ClusterRole/system:controller:daemon-set-controller                           23h
system:controller:deployment-controller                ClusterRole/system:controller:deployment-controller                           23h
system:controller:disruption-controller                ClusterRole/system:controller:disruption-controller                           23h
system:controller:endpoint-controller                  ClusterRole/system:controller:endpoint-controller                             23h
system:controller:endpointslice-controller             ClusterRole/system:controller:endpointslice-controller                        23h
```

```
verbs: ["create", "delete", "get", "list", "patch", "update", "watch"]

Sample Role Binding in YAML
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
namespace: default
name: pods-and-services
subjects:
- apiGroup: "rbac.authorization.k8s.io"
    kind: User
    name: tonystark
- apiGroup: "rbac.authorization.k8s.io"
    kind: Group
    name: avengers
roleRef:
apiGroup: "rbac.authorization.k8s.io"
kind: Role
name: pod-and-services
Verbs for k8s roles
```

Verb	HTTP Method	Description
create	POST	Create a new resources
delete	DELETE	Delete an existing resource
get	GET	Get a resource
list	GET	List a collection of resources
patch	PATCH	Modify an existing resource via a partial change
update	PUT	Modify an existing resource via a complete object
watch	GET	Watch for streaming updates to a resource

Verb	HTTP Method	Description
proxy	GET	Connect to resource via streaming WebSocket Proxy

- Using built-in roles: K8s has a large number of built-in cluster roles kubectl get clusterroles
  - While most of the built-in-roles are for system utilities, four are designed for generic end users
  - The cluster-admin role provides the complete access to the entire cluster
  - The admin role proved complete access to a complete namespace
  - The edit role allows an end user to modify things in a namespace
  - The view role allows for read-only access to a namespace
- Testing Authorization with can-i:
  - This tool is very useful for testing if a particular user can do particular action
- Note: Fix for inventory Service issue

```
FROM python:3-alpine3.13
LABEL author="khaja"
LABEL organization="qualitythought"
ARG HOME_DIR='/inventory-service'
ADD . ${HOME_DIR}
ENV MYSQL_USERNAME='qtdevops'
ENV MYSQL_PASSWORD='qtdevops'
ENV MYSQL_SERVER='localhost'
ENV MYSQL_DATABASE='qtinvsrv'
EXPOSE 8080
WORKDIR ${HOME_DIR}
RUN apk add build-base
RUN apk add --update py-pip
RUN apk add py-cryptography
RUN apk add gcc musl-dev python3-dev libffi-dev libressl-dev cargo
RUN pip install cryptography
RUN pip install -r requirements.txt
ENTRYPOINT [ "python", "app.py" ]
```