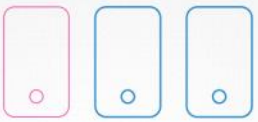
Monday, 24 October 2022 14.10

# SECURITY PRIMITIVES

## Secure Hosts



- Password based authentication disabled
- SSH Key based authentication

## Secure Kubernetes

kube-apiserver

Who can access? | What can they do?

## Authentication

Who can access?

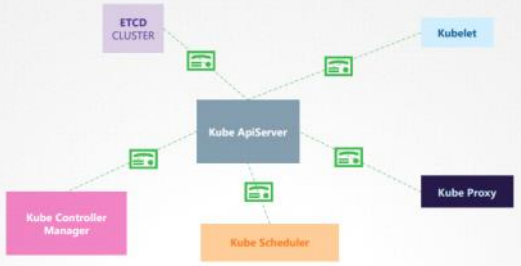
- Files – Username and Passwords
- Files – Username and Tokens
- Certificates
- External Authentication providers - LDAP
- Service Accounts

## Authorization

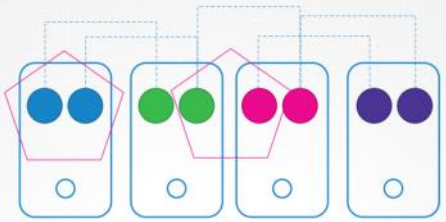
What can they do?

- RBAC Authorization
- ABAC Authorization
- Node Authorization
- Webhook Mode

## TLS Certificates



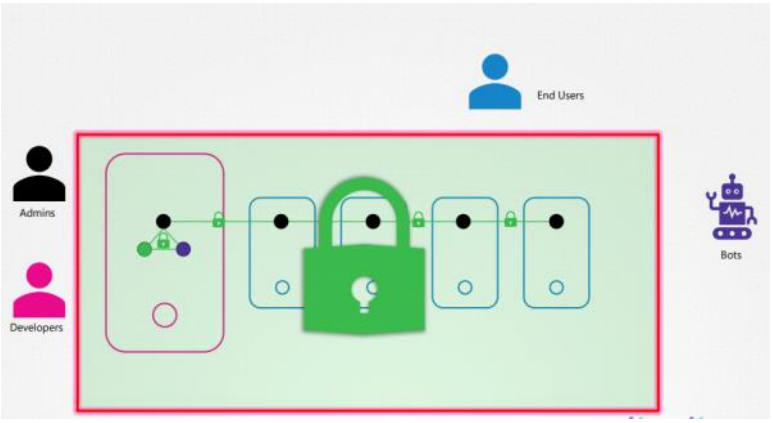

## Network Policies



By default all PODs can access all other PODs within the cluster.

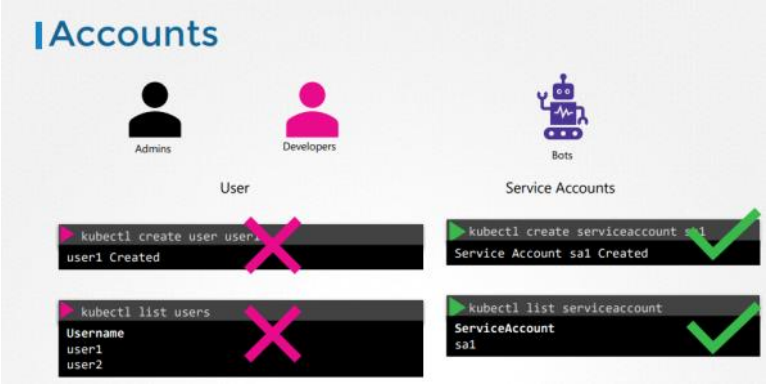
You can restrict access between them using Network Policies.

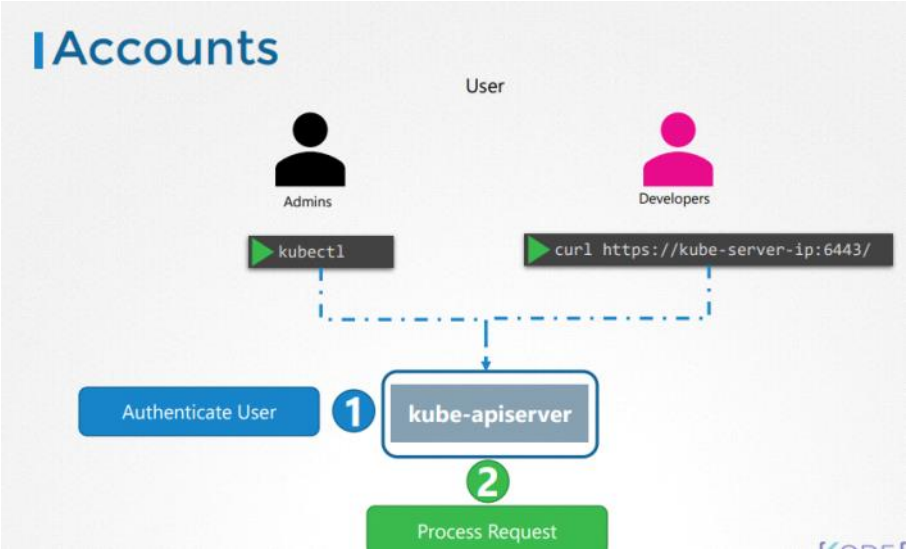
# AUTHENTICATION



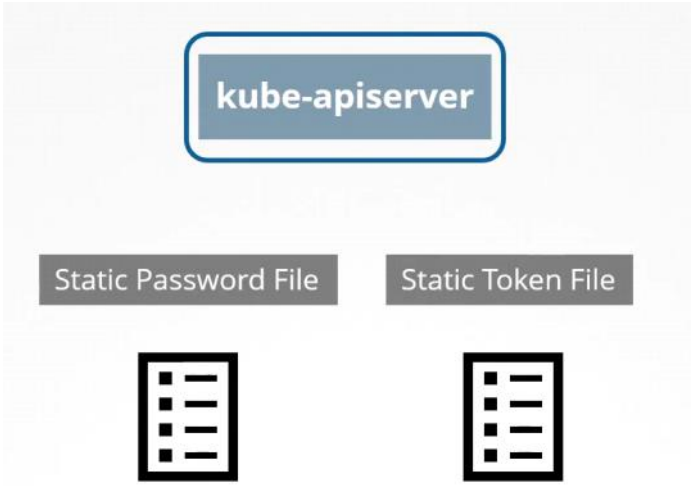


Admins
Developers
Bots
User
Service Accounts


Accounts
Admins
Developers
Bots
User
Service Accounts
kubectl create user user1
user1 Created
kubectl create serviceaccount sa1
Service Account sa1 Created
kubectl list users
Username
user1
user2
kubectl list serviceaccount
ServiceAccount
sa1


Accounts
User
Admins
Developers
kubectl
curl https://kube-server-ip:6443/
Authenticate User
1
kube-apiserver
2
Process Request


Auth Mechanisms
kube-apiserver
Static Password File
Static Token File
Certificates
Identity Services




# Auth Mechanisms - Basic

kube-apiserver

--basic-auth-file=user-details.csv

user-details.csv

```
password123,user1,u0001
password123,user2,u0002
password123,user3,u0003
password123,user4,u0004
password123,user5,u0005
```

kube-apiserver.service

```
ExecStart=/usr/local/bin/kube-apiserver \\
  --advertise-address=${INTERNAL_IP} \\
  --allow-privileged=true \\
  --apiserver-count=3 \\
  --authorization-mode=Node,RBAC \\
  --bind-address=0.0.0.0 \\
  --enable-swagger-ui=true \\
  --etcd-servers=https://127.0.0.1:2379 \\
  --event-ttl=1h \\
  --runtime-config=api/all \\
  --service-cluster-ip-range=10.32.0.0/24 \\
  --service-node-port-range=30000-32767 \\
  --v=2
  --basic-auth-file=user-details.csv
```

# Kube-api Server Configuration

kube-apiserver.service

```
ExecStart=/usr/local/bin/kube-apiserver \\
  --advertise-address=${INTERNAL_IP} \\
  --allow-privileged=true \\
  --apiserver-count=3 \\
  --authorization-mode=Node,RBAC \\
  --bind-address=0.0.0.0 \\
  --enable-swagger-ui=true \\
  --etcd-servers=https://127.0.0.1:2379 \\
  --event-ttl=1h \\
  --runtime-config=api/all \\
  --service-cluster-ip-range=10.32.0.0/24 \\
  --service-node-port-range=30000-32767 \\
  --v=2
  --basic-auth-file=user-details.csv
```

/etc/kubernetes/manifests/kube-apiserver.yaml

```
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: null
  name: kube-apiserver
  namespace: kube-system
spec:
  containers:
  - command:
    - kube-apiserver
    - --authorization-mode=Node,RBAC
    - --advertise-address=172.17.0.107
    - --allow-privileged=true
    - --enable-admission-plugins=NodeRestriction
    - --enable-bootstrap-token-auth=true
    - --basic-auth-file=user-details.csv
    image: k8s.gcr.io/kube-apiserver-amd64:v1.11.3
    name: kube-apiserver
```

# Authenticate User

```
curl -v -k https://master-node-ip:6443/api/v1/pods -u "user1:password123"
{
  "kind": "PodList",
  "apiVersion": "v1",
  "metadata": {
    "selfLink": "/api/v1/pods",
    "resourceVersion": "3594"
  },
  "items": [
    {
      "metadata": {
        "name": "nginx-64f497f8fd-krkg6",
        "generateName": "nginx-64f497f8fd-",
        "namespace": "default",
        "selfLink": "/api/v1/namespaces/default/pods/nginx-64f497f8fd-krkg6",
        "uid": "77dd7dfb-2914-11e9-b468-0242ac11006b",
        "resourceVersion": "3569",
        "creationTimestamp": "2019-02-05T07:05:49Z",
        "labels": {
          "pod-template-hash": "2090539498",
          "run": "nginx"
```

# Auth Mechanisms - Basic

Static Password File

user-details.csv

```
password123,user1,u0001,group1
password123,user2,u0002,group1
password123,user3,u0003,group2
password123,user4,u0004,group2
password123,user5,u0005,group2
```

Static Token File

user-token-details.csv

```
KpjCVbI7rCFAHYPkBzRb7gu1cUc4B,user10,u0010,group1
rJjncHmvtXHc6MlWQddhtvHyyhgTdxSC,user11,u0011,group1
mjpOFIELFOkL9toikaRNtt59ePtczZSq,user12,u0012,group2
PG4lIXhs7QjqwWkmBkvgGT9glOyUqZij,user13,u0013,group2
```

```
--token-auth-file=user-details.csv
```

```
curl -v -k https://master-node-ip:6443/api/v1/pods --header "Authorization: Bearer KpjCVbI7rCFAHYPkBzRb7gu1cUc4B"
```

# Note

- This is not a recommended authentication mechanism
- Consider volume mount while providing the auth file in a kubeadm setup
- Setup Role Based Authorization for the new users