4. Настройка аутентификации/авторизации

Схема разграничения доступа реализована простая: есть несколько namespace, в каждом из которых есть несколько пользователей с полным доступом. Но сущностей, имеющих отношение к безопасности, достаточно много.

//Здесь будет схема их взаимосвязи.

Создание namespace

Первым делом зайти на мастера и создать namespace:

```
kubectl create namespace sandbox
```

Создание пользователя

Сгенерировать приватный ключ для нового пользователя:

```
openssl genrsa -out sandbox-user.key 2048
```

Создать запрос на сертификат для него:

```
openssl req -new -key sandbox-user.key -out sandbox-user.csr -subj
"/CN=sandbox-user/O=sandbox-group"
```

Сгенерировать сертификат пользователя от CA кубернетеса сроком 1500 дней:

```
sudo openssl x509 -req -in sandbox-user.csr -CA /etc/kubernetes/pki/ca.crt
-CAkey /etc/kubernetes/pki/ca.key -CAcreateserial -out sandbox-user.crt
-days 1500
```

Скопировать файлы ключа и сертификата, и создать новый контекст (связь) для созданных namespace и пользователя. Пути должны быть абсолютными:

```
mv sandbox-user.crt sandbox-user.key ~/.kube/sandbox-user/
kubectl config set-credentials sandbox-user --embed-certs=true
--client-certificate=/home/user/.kube/sandbox-user/sandbox-user.crt
--client-key=/home/user/.kube/sandbox-user/sandbox-user.key
kubectl config set-context sandbox-context --cluster=kubernetes
--namespace=sandbox --user=sandbox-user
```

Наделение пользователя доступом

Теперь есть пользователь, контекст и namespace, но нет прав у пользователя, чтобы кто-то делать в этом namespace. Нужно их создать, для этого создаем такой шаблон ():

```
kind: Role
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  namespace: sandbox
  name: sandbox-manager
rules:
- apiGroups: ["", "extensions", "apps"]
  resources: ["deployments", "replicasets", "pods"]
  verbs: ["get", "list", "watch", "create", "update", "patch", "delete"] #
You can also use ["*"]
---
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: sandbox-manager-binding
  namespace: sandbox
subjects:
- kind: User
  name: sandbox-user
  apiGroup: ""
roleRef:
  kind: Role
  name: sandbox-manager
  apiGroup: ""
```

И применить его.

```
kubectl create -f sandbox-manager.role-and-rolebinding.yaml
```

Выдача доступа пользователю

После создания контекста взять файл ~/.kube/config, удалить оттуда все, что не относится к созданным выше объектам, и отправить его пользователю:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN5RENDQWJDZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpNQjRYRFRFNE1E
Z3dPREV4TWpRd05Gb1hEVEk0TURnd05URXhNalF3TkZvd0ZURVRNQkVHQTFVRQpBeE1LYTNWaV
pYSnVaWFJsY3pDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBT0ty
CncvYUdTcGt0SHlQUGNFSEIxYmNVc2wrb0Z4R1FFUmRWZDBnclNRbmFkaXBpc3V0eFNMSXptTT
EwbHpTWlR1ME8KcUVRcE4rVmZIOXlMZ1E2KzFwY3Y3b2tlL2pTT0dzMGVtb1VlN2F0VVZZNkN5
```

```
eEt2MlRCYWtDRkthYSs5azJVVApyalhwSVBocHltTVN3WnRRMnlma1ZIUXA4K0QxazY0Mlp2WU
JtTGl2L2RTbU45d20yYUlNeU5mYW0zMUV5cHJKCnZ4NkNJbWx2M1FUMU1tR2EwdXI0VEl0OTdH
TXczSkpCWENKZFVMZlBmMnFCYldaWTBxOXlZaTZrMXI5eUdKUHYKRUZWblRuYnFlcE5nVkgyMD
NrN0llWGN1SDVsbHJXZDExd1BJUWZBQkkvcGVySHFLc0xtMHR6bmdMc0J4V2hlNwpITTVPbXhz
UWw2VjJiWDlvT0IwQ0F3RUFBYU1qTUNFd0RnWURWUjBQQVFIL0JBUURBZ0trTUE4R0ExVWRFd0
VCCi93UUZNQU1CQWY4d0RRWUpLb1pJaHZjTkFRRUxCUUFEZ2dFQkFGTkpKUUp5OW5tM1E5Y0tr
UkdaZU1qMnl6WVcKazMvU3FRZ1pHWktMNEs1MWdYd2VUeFA2akg0MW10YUF5UHk2RnJOYUJYVG
ZnWUx4ejBsYUFLSWwvaXlPWUw2MQpxc2xVemMwZHJMU2UrUlR3cU9razRPZWtheThyZTF5MDJ0
a3pVMmVpS0JLb05yZjFnU1lqcnEyYWlZN0ZlZzVuCktaUHQzNGRmaVo5dTdPaXRwTmM3YVVtSl
dHaWtBVEFLY3VKRnNKYXg0QjI3aEVKNkRqL1pqeUlRNk1OK2dlcEIKUVRKc09OWU1XL0dNd3Yv
MWhBbXVSU1FrTUF2UlNKNy93U25vRWkveG8ycytmMzNYSEo5UHRWeEZFUUcrUzZTQQpWcXJ2YV
lWNm1RN1g3N0dQRHdHYmxEV3NMeWRJMXZtcE1jbmtDdUpEclhuM2pNZFJnQ2JvekRpaVhXcz0K
LS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQo=
    server: https://192.168.66.206:6443
  name: kubernetes
contexts:
- context:
    cluster: kubernetes
    namespace: sandbox
    user: sandbox-user
  name: sandbox-context
current-context: sandbox-context
kind: Config
preferences: {}
users:
- name: sandbox-user
  user:
    client-certificate-data:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUN3RENDQWFnQ0NRQzFVMlpiK0hXUVdUQU
5CZ2txaGtpRzl3MEJBUXNGQURBVk1STXdFUVlEVlFREV3cHIKZFdKbGNtNWxkR1Z6TUI0WERU
RTRNRGd5TXpFeE1EY3pPVm9YRFRJeU1UQXdNVEV4TURjek9Wb3dMekVWTUJNRwpBMVVFQXd3TW
MyRnVaR0p2ZUMxMWMyVnlNUll3RkFZRFZRUUtEQTF6WVc1a1ltOTRMV2R5YjNWd01JSUJJakFO
CkJna3Foa2lHOXcwQkFRUZBQU9DQVE4QU1JSUJDZ0tDQVFFQXVMamh0bUROQmpKUVQwaGJOWm
hiYzlyemxFcDQKR3ZlS1dOU1pBOXNTSVhQYUVFOGlEUDJyOGlOb0xpUjZhaFd0cllxcnVicUpu
dEtEZnVpVkIrcjBCV3dHemN6bwp5OW0rdkpxQWo1M0VkU0xMWVdZQndrUkZEQ3U2MFBHZGNzRF
hHRElrMENEQ2xTUzRYc0xkaFJoWU40aDl0Z0RZCkc3VThsZUZtdjBRNjVBcnMxS1ArZEt3UUJS
dk53Nm9VWEdEcVhBRTB1WUpXTjZHM3pzb0xINWdOUElNcWhaK28KWnVhYjFrT1B3SjVaZ0lIWD
VSMWlIWi8xZWdYRW90Z0RZalgvRXE0MzNmaXBaV2toYkpCZnBsVDlubGZqWWxtUQpObWV6OEpn
eTJ3dTVMeGY5clhld2JVRVpnWExXYzRicXROOHlwaHU5SXl1SkRlTFhoaThtTnRWYzBRSURBUU
FCCk1BMEdDU3FHU0liM0RRRUJDd1VBQTRJQkFRQVFVenRTdUViZnhjR3BlVDU5U1VJTjN0Qmw4
bzM0SVFHVTBlVDQKN3hYSkhiOE9VdDhOQkRydGVPa0dIeE9ia2FaY1VpYnBVRWxUNXNGd3I1aS
tpR3gzMXZJMUljellqOGVaNE9xOQpOYmMwRTF5Y0szK1NTM2JzcXNNQ09ZcWY5NmlLVUx6SWlo
ay9jQ1BOdGpOdTNmR3lncysvSlA2dWF1UlNUZFgyCkhSRkFqaFNRWDNaS1M1MmRzMktZUmxaNk
NyRXcyTy9zMVFKcUxJYW9ITEwxdW1NMXVhNGViYktwV3h6ZjE2bTEKaDRaclVLRnpucHBSaXVm
eDUrR2treDZyZGpMLzRYVzZKK1NyT3M5d21FT0Y0Qm1PUXlKMTV4YnlPMkFWM3JGQQpxb1k5RF
Q3Y1ZrYWdwZFVoYjlwS2hXSENRbzJMQlJQVGd1Z1EyWnNFRjM0bWtmdjEKLS0tLS1FTkQgQ0VS
VElGSUNBVEUtLS0tLQo=
    client-key-data:
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFcEFJQkFBS0NBUUVBdUxqaHRtRE
5CakpRVDBoYk5aaGJjOXJ6bEVwNEd2ZUtXTlNaQTlzU0lYUGFFRThpCkRQMnI4aU5vTGlSNmFo
V3RyWXFydWJxSm50S0RmdWlWQityMEJXd0d6Y3pveTltK3ZKcUFqNTNFZFNMTFlXWUIKd2tSRk
RDdTYwUEdkY3NEWEdESWswQ0RDbFNTNFhzTGRoUmhZTjRoOXRnRFlHN1U4bGVGbXYwUTY1QXJz
MUtQKwpkS3dRQlJ2Tnc2b1VYR0RxWEFFMHVZSldONkczenNvTEg1Z05QSU1xaForb1p1YWIxa0
```

9Qd0o1WmdJSFg1UjFpCkhaLzFlZ1hFb3RnRFlqWC9FcTQzM2ZpcFpXa2hiSkJmcGxUOW5sZmpZ
bG1RTm1lejhKZ3kyd3U1THhmOXJYZXcKYlVFWmdYTFdjNGJxdE44eXBodTlJeXVKRGVMWGhpOG
1OdFZjMFFJREFRQUJBb0lCQVFDdzlQdlZPUHB2bXpkdwpIQUswWHhZTThJMHpXL3VlNmRCd3RJ
azVObDR5Q2NlMm8vZ2N0YzVJa2o2MUpXRFh5NWlyalJKaFJCK2VORkNmCi9MTDMrTTUzZXpzeF
g4RUx0N2FPK3Z0NW1VdWdZd3F1YllmMTBHek04Zjl2Tm1iOGpWd0E0OWg4UVVYbWxsekEKK3JB
M1ZsRDhNaGNyaWJkOUk2dThjVWQ2cHlRN1c5TkRiZ2F5K2JrOWpxTllQNUlsaFk1YmJkeCtWVz
VOSzdrVgo4aXdOV005RmdWWWlJRWtCQjZkWFJ2V3UvVUQ5Nk5VajMzZ0RKMk9hRGdwNytzUkta
R3JON01Fb2orUkVpYnVaCjVHL3Z5T2haQ0tha0hYV1FSamFxNDE2ME1MU05IUXJudXJUK2kwVE
N0SEpvdS9jRW5DbmFKZ1k3cXI0Y0RiVXUKc3g1dUU5RWhBb0dCQU54SEk2VkV4MEY5V3dyZXFn
MXlnL1VyWWZmT1pJY3NYT2tWck5oRlp2TlBtM2pHclI0VApZanoxaC9ZZTd6VTV0S2hLMnA0Z1
MzR2NMWDBMUFA5NHJOejZ1U1hpRXV2Q0dIaGtWZUVWS20ydjl2YVZITWNYCmNlUnU5TVpEV3pv
a1JyVlcxZGJ6SUpqb2VwMTRWbkVTQUw0ckZaT3lIUTFVcDIvMU5mYWcrVHRkQW9HQkFOYXQKcE
5lblpmNFI1UHVveDBITVBJbUpoM2RDakhiUmplYk1jZVlLV0VLUjFWclFTSjgvUTloYW5vZnpp
THNUN2hpWQpDQzNYY1lsUkI4Z1J0MmtkRlBNREgyQUI4YjNwMlhTQmlYaFgvcTIwdi9lU1ZQM1
liVDl5eVovMHI0WFQvL2lWCjVNcnFPQnM0WmlBdlFDcXhCWVpTcUFSRGFHMk9BcDFscXdOK1ZN
UUZBb0dBZkl5ODJ2WEl0SDdzdTNpckxtOVIKclk2YUZrUGRFNUZCOTRrSjhqOUx0c2VNWVAzMV
pNd1EvK2JVdVpWRUxCUTAwZk9CS1dlWlFPUE4xS1pHRnkxawprSTR6b2ZmeU90dkVlazVCUU1O
MitnNUUxYWY2WFpna0RjV3ZJV3QwYWF1WlQyK0orYi8rN25hRTNnVHMyNElTCmFYUnkvcy8zSF
ZLQVdnMk1OYWRQUlFFQ2dZRUF0K01McFhJTmltRTNuRjJKT0pKQ2RLbHFjVHgrNXpRKzhhakUK
RTRGZThyN0tXN3kzeURpLzI2NWJ4eVpUUTdRaHFjMW9qQ1BVYkFRTnYxRjFvc00zYzZXRUZZLz
B5M0ZwUkVQRgpSbUZSbE9lVDIvUHJlM2tNczJHVzFiNFpMM0JWL1ZBZ0o3UVRGVFh0UExwY28z
VDR2NE5EeWtzWFEyaDJVdTZJCld6aTJVU1VDZ1lCcGppOXBIVUFNV3dGbjE1NW9sdlFRY3g1M1
F0MWdVRWZuMWh6VEZLak51bVhMc1prOTYxelMKU2QzeDZ5NzQ5QlhkSHl6QXUxZGlKVTZ3dCsy

```
TXczM3FJZllMUjl2SG1DVTEveHdpblhXZi9WVUtVVWhVVncrUwpmSndQam9SK3hsdU9rUTMvRV
lyMWdkR0lkZWFpcFFoV1ZWaXFQaXo1MTRBZ2dRQmlsc3dGOWc9PQotLS0tLUVORCBSU0EgUFJJ
VkFURSBLRVktLS0tLQo=
```

Источники

- https://docs.bitnami.com/kubernetes/how-to/configure-rbac-in-your-kubernetes-cluster/
- www.youtube.com/watch?v=CgCLPYJRxbU&t=1406s
- https://dev-ops-notes.ru/cloud/kubernetes-1-7-%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0-rbac/