SCC

```
oc new-project scc-lab
```

```
oc create sa custom-sa
```

Check:

```
oc get sa
```

SCC Creation:

```yaml
apiVersion: security.openshift.io/v1
kind: SecurityContextConstraints
metadata:
  name: custom-scc
allowHostDirVolumePlugin: false
allowHostIPC: false
allowHostNetwork: false
allowHostPID: false
allowHostPorts: false

readOnlyRootFilesystem: false
runAsUser:
  type: RunAsAny
fsGroup:
  type: RunAsAny
seLinuxContext:
  type: RunAsAny
allowPrivileged: false
allowedCapabilities:
  - NET_BIND_SERVICE
volumes:
```

Apply:

```
oc apply -f custom-scc.yaml
```

Verify:

```
oc get scc | grep custom
```

Show details:

```
oc describe scc custom-scc
```

SCC to service account:

```
oc adm policy add-scc-to-user custom-scc -z custom-sa
```

Verify:

```
oc describe sa custom-sa
oc describe scc custom-scc
```

You should see:

```
Users: system:serviceaccount:scc-lab:custom-sa
```

W/o SCC

File: **test-pod.yaml**

```
apiVersion: v1
kind: Pod
metadata:
  name: test-pod
spec:
  serviceAccountName: custom-sa
  containers:
    - name: app
      image: nginx
      securityContext:
        capabilities:
          add: ["NET_BIND_SERVICE"]
      ports:
        - containerPort: 80
```

Apply:

```
oc apply -f test-pod.yaml
```

If SCC is not correct, you will see:

```
Error: cannot set capabilities
```

But since our SCC **allows `NET_BIND_SERVICE`**, it should run.

Check:

```
oc get pod test-pod
```

SCC Creation:

Edit YAML:

```
securityContext:
  capabilities:
    add: ["SYS_ADMIN"]
```

Apply:

```
oc apply -f test-pod.yaml
```

Expected failure:

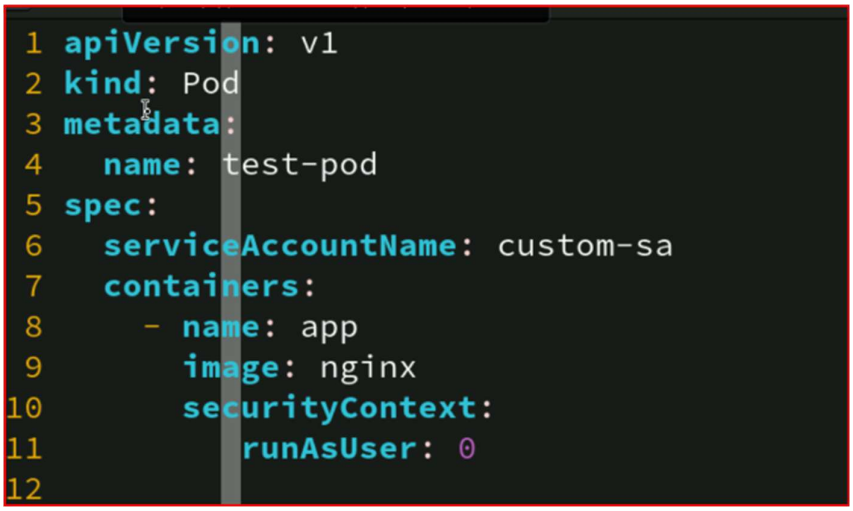
```
Error: capabilities are not allowed: SYS_ADMIN
```

Good — SCC is working.

Running as ROOT

Our SCC allows `runAsUser: RunAsAny`.

Test:



Apply:

```
oc apply -f test-pod.yaml
```

Pod should run successfully.

Assign SCC to all Groups:

Examples:

Assign to all authenticated users:

```
oc adm policy add-scc-to-group custom-scc system:authenticated
```

Assign to all service accounts in the project:

```
oc adm policy add-scc-to-group custom-scc system:serviceaccounts:scc-lab
```

```
[student@workstation ~]$ oc adm policy add-scc-to-group custom-scc system:authen
ticated
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:custom-scc added: "sy
stem:authenticated"
[student@workstation ~]$ oc adm policy add-scc-to-group custom-scc system:servic
eaccounts:scc-lab
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:custom-scc added: "sy
stem:serviceaccounts:scc-lab"
[student@workstation ~]$
```

Final:

Remove SCC from user:

```
oc adm policy remove-scc-from-user custom-scc -z custom-sa
```

Delete SCC:

```
oc delete scc custom-scc
```
