```
network-policy-deny-imds.yaml - docker-k...
                                                                                                                                                         <u>ເນື່</u> ....
                                                                                                               network-policy-deny-imds.yaml M X
$ kubectl run azure-cli -it --rm --image=mcr.microsoft.com/azure-cli:latest -- bash
                                                                                                                      io.k8s.api.networking.v1.NetworkPolicy (v1@networkpolicy.json)
If you don't see a command prompt, try pressing enter.
                                                                                                                      apiVersion: networking.k8s.io/v1
azure-cli:/#
                                                                                                                      kind: NetworkPolicy # GlobalNetworkPolicy
azure-cli:/# # 4. Get the MSI Kubelet Client ID from the tagsList
azure-cli:/#
                                                                                                                      metadata:
azure-cli:/# MSI_KUBELET_CLIENT_ID="e5dbcd30-9b3d-4041-b791-ac23f9038175"
                                                                                                                        name: deny-metadata-access
azure-cli:/#
                                                                                                                        namespace: default
azure-cli:/# # 5. Get the access token for the MSI Kubelet Client ID
                                                                                                                      spec:
azure-cli:/#
                                                                                                                        podSelector: {}
azure-cli:/# curl -s -H Metadata:true --noproxy "*" \
                                                                                                                        policyTypes:
  "http://169.254.169.254/metadata/identity/oauth2/token?api-version=2021-12-13&resource=https://manag
                                                                                                                        - Egress
ement.azure.com/& http://169.254.169.254/metadata/identity/oauth2/ boken?api-version=2021-12-13&resource=https://
                                                                                                                 10
                                                                                                                        egress:
   jq
                                                                                                                 11
                                                                                                                          - ipBlock:
                                                                                                                 12
  "access_token": "evJ0eXAiOiJKV10iLCJhbGciOiJSUzI1NiIsIng1dCI6Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWkdldyI
sImtpZCI6Ii1LSTNROW50UjdiUm9meG1lWm9YcWJIWkdldyJ9.eyJhdWQi0iJodHRwczovL21hbmFnZW1lbnQuYXp1cmUuY29tLyIs
                                                                                                                 13
                                                                                                                              cidr: 0.0.0.0/0
ImlzcyI6Imh0dHBz0i8vc3RzLndpbmRvd3MubmV0LzE2YjNjMDEzLWQzMDAtNDY4ZC1hYzY0LTdlZGEwODIwYjZkMy8iLCJpYXQi0j
                                                                                                                 14
                                                                                                                              except:
E2Nzc5MTY2NzAsIm5iZiI6MTY3NzkxNjY3MCwiZXhwIjoxNjc4MDAzMzcwLCJhaW8iOiJFMlpnWUtnSWE1aXljZjNhSjVQdVA4NXVy
                                                                                                                 15
                                                                                                                              - 169.254.169.254/32
WFg0RHdBPSIsImFwcGlkIjoiZTVkYmNkMzAtOWIzZC00MDQxLWI3OTEtYWMyM2Y5MDM4MTc1IiwiYXBwaWRhY3IiOiIyIiwiaWRwIj
oiaHROcHM6Ly9zdHMud2luZG93cy5uZXQvMTZiM2MwMTMtZDMwMC00NjhkLWFjNjQtN2VkYTA4MjBiNmQzLyIsImlkdHlwIjoiYXBw
                                                                                                                      apiVersion: networking.k8s.io/v1
Iiwib2lkIjoiNzFlMmVlYTQtNjY0Zi000TQyLThhNzQt0DA3NjE5YjU2MjYwIiwicmqi0iIwLkFBQUFF0EN6RmdEVGpVYXNaSDdhQ0
                                                                                                                      kind: NetworkPolicy
NDMjAwWklmM2tBdXRkUHVrUGF3ZmoyTUJP0EFBQS4iLCJzdWIiOiI3MWUyZWVhNC02NjRmLTQ5NDIt0GE3NC04MDc2MTliNTYyNjAi
                                                                                                                      metadata:
LCJ0aWQi0iIxNmIzYzAxMy1kMzAwLTQ2OGQtYWM2NC03ZWRhMDgyMGI2ZDMiLCJ1dGki0iJ3R3doVGllR0FFT2FjY1dlZmlrbkJBIi
                                                                                                                        name: allow-metadata-access
widmVyIjoiMS4wIiwieG1zX21pcmlkIjoiL3N1YnNjcmlwdGlvbnMvODJmNmQ3NWUtODVmNC00MzRhLWFiNzQtNWRkZGQ5ZmE4OTEw
                                                                                                                 21
                                                                                                                        namespace: default
L3Jlc291cmNlZ3JvdXBzL3JnLXNwb2tlLWFrcy1jbHVzdGVyL3Byb3ZpZGVycy9NaWNyb3NvZnQuTWFuYWdlZElkZW50aXR5L3VzZX
                                                                                                                 22
                                                                                                                      spec:
JBc3NpZ25lZElkZW50aXRpZXMvaWRlbnRpdHkta3ViZWxldCIsInhtc190Y2R0IjoxNjQ1MTM3MjI4fQ.qX4AtJks9hlBs0lYpVCzx
                                                                                                                 23
                                                                                                                        podSelector:
ppLURChLuzs32k4_Q7d8BjJn8zJFsizKx3E4lWjxaEb3xC9euDWyFKzeh5NNrZ8Sq1WQ9nPSPoSU7LDs35R6s5wAHQ69-i3268qZWC
OkOpMipkxwEwhmtj1SV8gLa6Gt3a1Zj6xT69WHVwebehQeE9Jr-XAg4F6geXSKuYv0F9m0kBiriRIMVGFuvJyKsupjN_Niuu0sMJ68
                                                                                                                          matchLabels:
v0897choGr4s7BP84eIeTaVcacjN5D27pUYodAFT5xZUD-j7Vv93Mt_7yTDsqpcb0wpAUYEeFJngTKbr3rpgoysW-vVDsNctxt-jFw
                                                                                                                            app: myapp
maXSP-fsPPn-lTg",
                                                                                                                        policyTypes:
  "client_id": "e5dbcd30-9b3d-4041-b791-ac23f9038175",
                                                                                                                 27
                                                                                                                        - Egress
  "expires_in": "84016",
                                                                                                                        egress:
  "expires_on": "1678003370",
  "ext_expires_in": "86399",
                                                                                                                          - ipBlock:
  "not_before": "1677916670",
                                                                                                                             cidr: 169.254.169.254/32
  "resource": "https://management.azure.com/",
  "token_type": "Bearer"
azure-cli:/# exit
exit
                                                                                                              🥍 main* 🕂 🛇 0 🛆 0 aks-cluster 🚷 default
                                                                                                                                                     - W Prettier 💀
```

connect with boken - APRGW - Database Managed Identity (MSI) L> RBAC role assign.