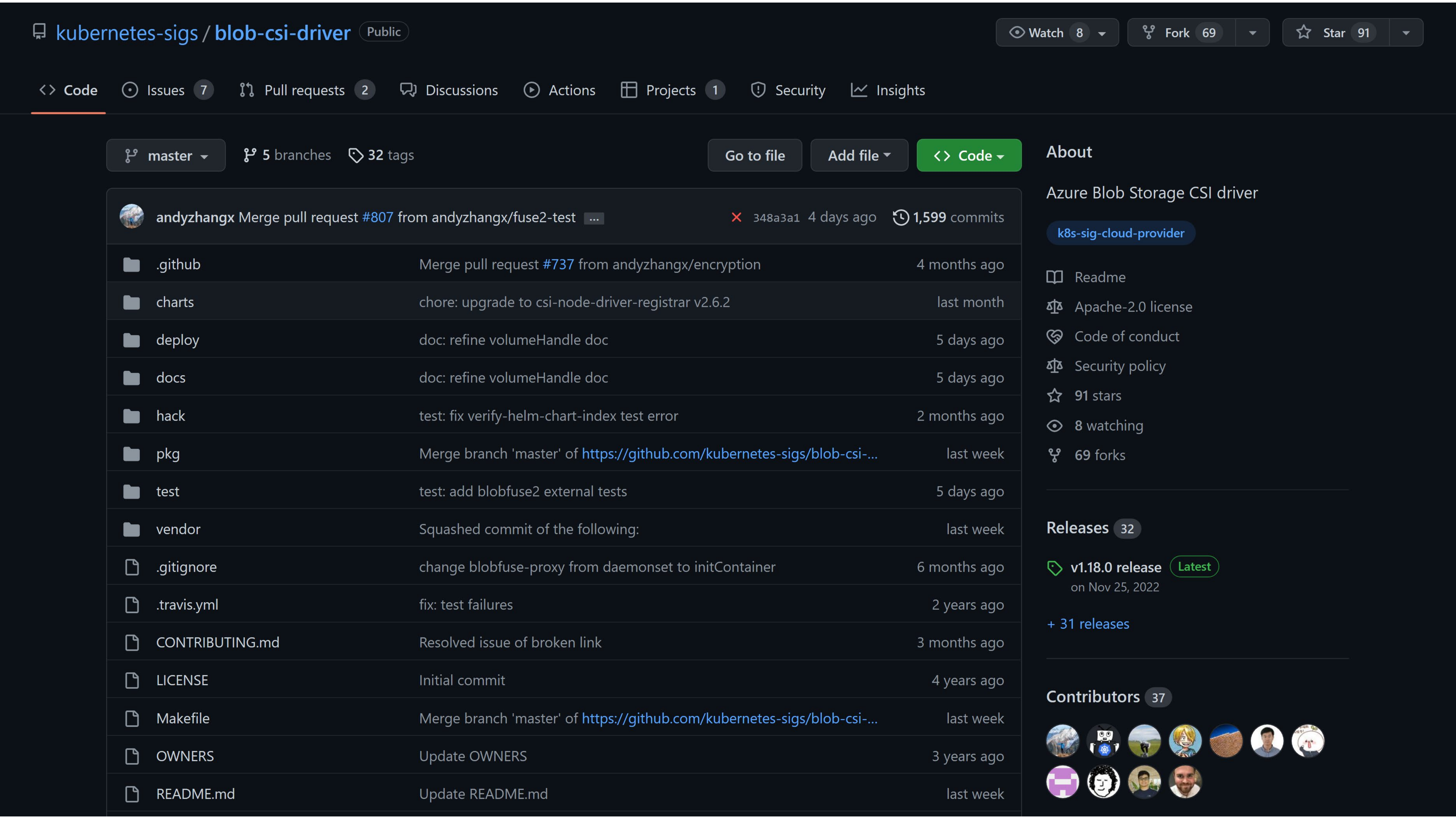
# AKS storage using Azure Blob

Houssem Dellai

# Storage options for AKS

+ Azure Disk
    LRS, ZRS, Shared, Standard, Premium, Ultra
+ Azure File
+ Azure Blob
    NFS v3.0, BlobFuse
+ NetApp Files



andyzhangx Merge pull request #807 from andyzhangx/fuse2-test … ✕ 348a3a1 4 days ago 1,599 commits

| | | |
|---|---|---|
| .github | Merge pull request #737 from andyzhangx/encryption | 4 months ago |
| charts | chore: upgrade to csi-node-driver-registrar v2.6.2 | last month |
| deploy | doc: refine volumeHandle doc | 5 days ago |
| docs | doc: refine volumeHandle doc | 5 days ago |
| hack | test: fix verify-helm-chart-index test error | 2 months ago |
| pkg | Merge branch 'master' of https://github.com/kubernetes-sigs/blob-csi-... | last week |
| test | test: add blobfuse2 external tests | 5 days ago |
| vendor | Squashed commit of the following: | last week |
| .gitignore | change blobfuse-proxy from daemonset to initContainer | 6 months ago |
| .travis.yml | fix: test failures | 2 years ago |
| CONTRIBUTING.md | Resolved issue of broken link | 3 months ago |
| LICENSE | Initial commit | 4 years ago |
| Makefile | Merge branch 'master' of https://github.com/kubernetes-sigs/blob-csi-... | last week |
| OWNERS | Update OWNERS | 3 years ago |
| README.md | Update README.md | last week |

## About

Azure Blob Storage CSI driver

k8s-sig-cloud-provider

- Readme
- Apache-2.0 license
- Code of conduct
- Security policy
- 91 stars
- 8 watching
- 69 forks

## Releases 32

v1.18.0 release Latest
on Nov 25, 2022

+ 31 releases

## Contributors 37

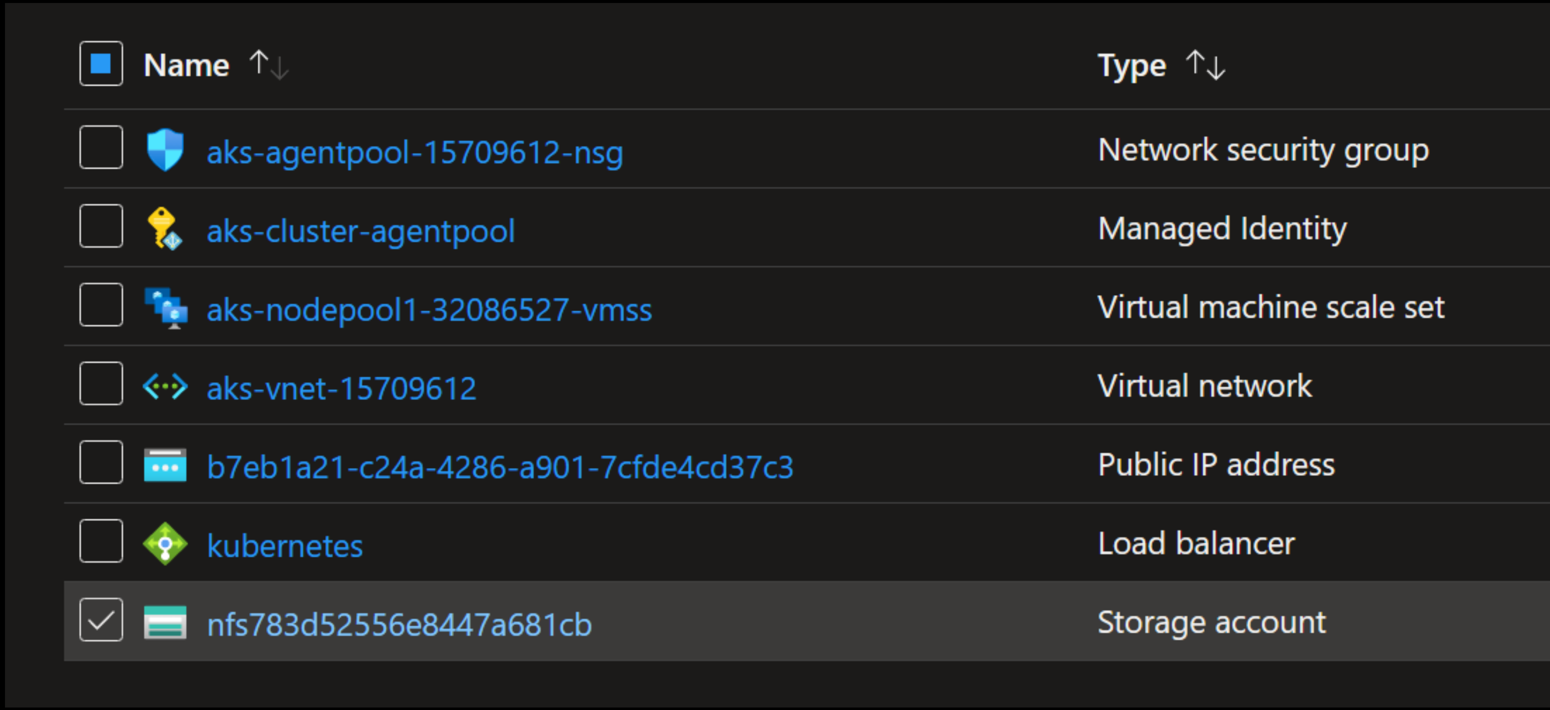
```
$ az aks create --name $AKS_NAME --resource-group $AKS_RG --enable-blob-driver

$ kubectl get pods -n kube-system | grep csi
# NAME                                READY   STATUS    RESTARTS   AGE
# csi-azuredisk-node-8wlc8            3/3     Running   0          100m
# csi-azuredisk-node-9z2wt            3/3     Running   0          100m
# csi-azuredisk-node-q9pwk            3/3     Running   0          100m
# csi-azurefile-node-7tzps            3/3     Running   0          100m
# csi-azurefile-node-8lwrl            3/3     Running   0          100m
# csi-azurefile-node-zdnpn            3/3     Running   0          100m
# csi-blob-node-8spm4                 3/3     Running   0          100m
# csi-blob-node-ctv9c                 3/3     Running   0          100m
# csi-blob-node-jbx9r                 3/3     Running   0          100m

$ kubectl get storageclass
# NAME                     PROVISIONER          RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
# azureblob-fuse-premium   blob.csi.azure.com   Delete          Immediate              true                   6m23s
# azureblob-nfs-premium    blob.csi.azure.com   Delete          Immediate              true                   6m23s
# azurefile                file.csi.azure.com   Delete          Immediate              true                   67m
# azurefile-csi            file.csi.azure.com   Delete          Immediate              true                   67m
# azurefile-csi-premium    file.csi.azure.com   Delete          Immediate              true                   67m
# azurefile-premium        file.csi.azure.com   Delete          Immediate              true                   67m
# default (default)        disk.csi.azure.com   Delete          WaitForFirstConsumer   true                   67m
# managed                  disk.csi.azure.com   Delete          WaitForFirstConsumer   true                   67m
# managed-csi              disk.csi.azure.com   Delete          WaitForFirstConsumer   true                   67m
# managed-csi-premium      disk.csi.azure.com   Delete          WaitForFirstConsumer   true                   67m
# managed-premium          disk.csi.azure.com   Delete          WaitForFirstConsumer   true                   67m
```

# Using Azure Blob storage

```
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: statefulset-blob-nfs
  labels:
    app: nginx
spec:
  serviceName: statefulset-blob-nfs
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
```

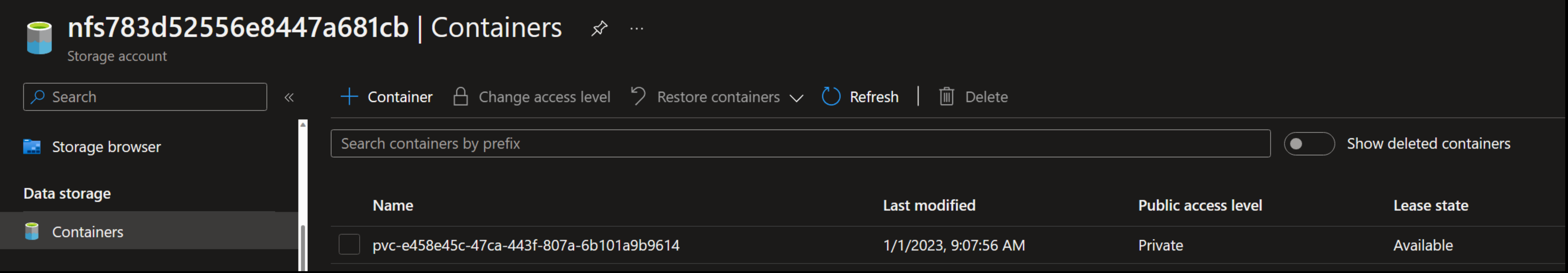
```
  spec:
   containers:
   - name: statefulset-blob-nfs
    image: nginx
    volumeMounts:
    - name: persistent-storage
     mountPath: /mnt/azureblob
 volumeClaimTemplates:
 - metadata:
   name: persistent-storage
   annotations:
    volume.beta.kubernetes.io/storage-class:
azureblob-nfs-premium
  spec:
   accessModes: ["ReadWriteMany"]
   resources:
    requests:
     storage: 100Gi
```

# Created resources



| ■ | Name ↑↓ | Type ↑↓ |
|---|---|---|
| □ | aks-agentpool-15709612-nsg | Network security group |
| □ | aks-cluster-agentpool | Managed Identity |
| □ | aks-nodepool1-32086527-vmss | Virtual machine scale set |
| □ | aks-vnet-15709612 | Virtual network |
| □ | b7eb1a21-c24a-4286-a901-7cfde4cd37c3 | Public IP address |
| □ | kubernetes | Load balancer |
| ☑ | nfs783d52556e8447a681cb | Storage account |

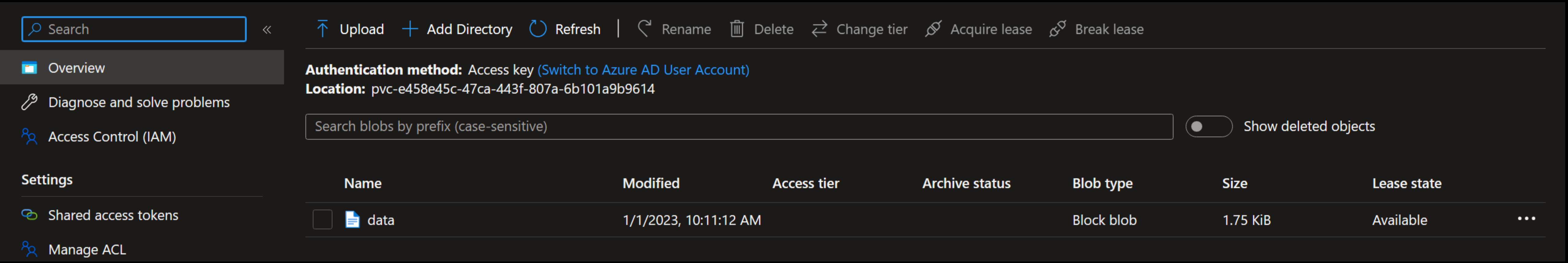
```
kubectl get sts,pods,pvc,pv
# NAME                                   READY   AGE
# statefulset.apps/statefulset-blob-nfs   1/1     49m

# NAME                          READY   STATUS    RESTARTS   AGE
# pod/statefulset-blob-nfs-0    1/1     Running   0          49m

# NAME                                                                STATUS   CAPACITY
# persistentvolumeclaim/persistent-storage-statefulset-blob-nfs-0     Bound    100Gi

# NAME                                                          CAPACITY   ACCESS MODES   RECLAIM POLICY
# persistentvolume/pvc-e458e45c-47ca-443f-807a-6b101a9b9614     100Gi      RWX            Delete
```



# nfs783d52556e8447a681cb | Containers

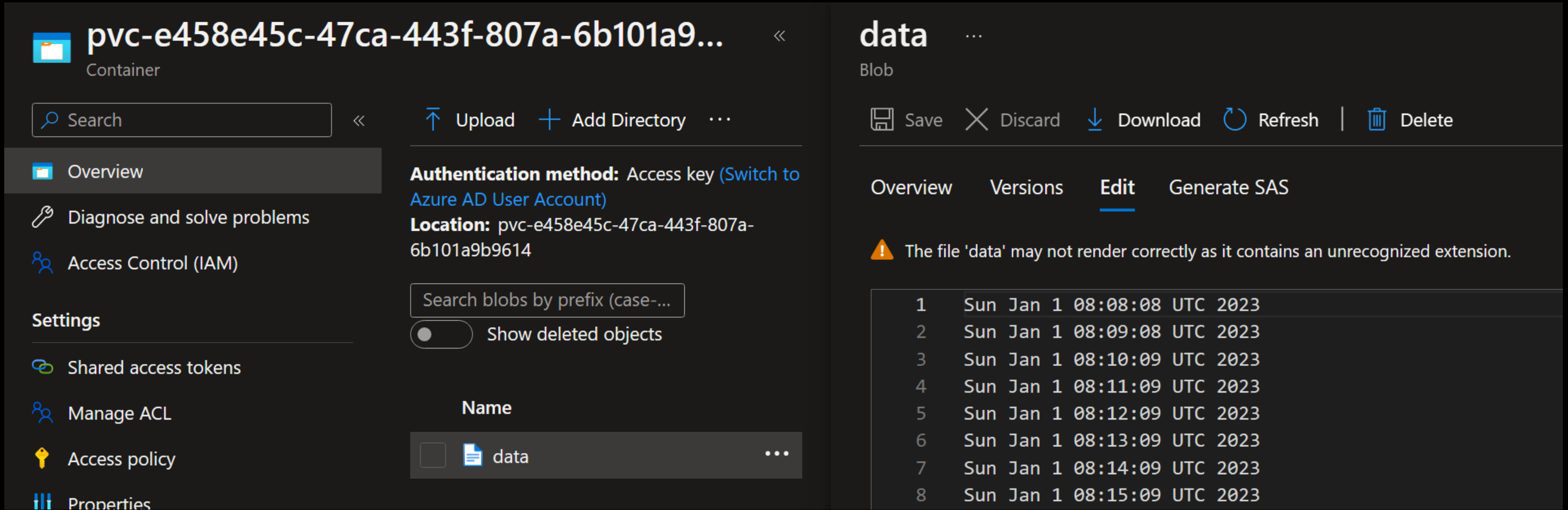
Storage account

| Name | Last modified | Public access level | Lease state |
|---|---|---|---|
| pvc-e458e45c-47ca-443f-807a-6b101a9b9614 | 1/1/2023, 9:07:56 AM | Private | Available |



**Authentication method:** Access key (Switch to Azure AD User Account)
**Location:** pvc-e458e45c-47ca-443f-807a-6b101a9b9614

| Name | Modified | Access tier | Archive status | Blob type | Size | Lease state |
|---|---|---|---|---|---|---|
| data | 1/1/2023, 10:11:12 AM | | | Block blob | 1.75 KiB | Available |



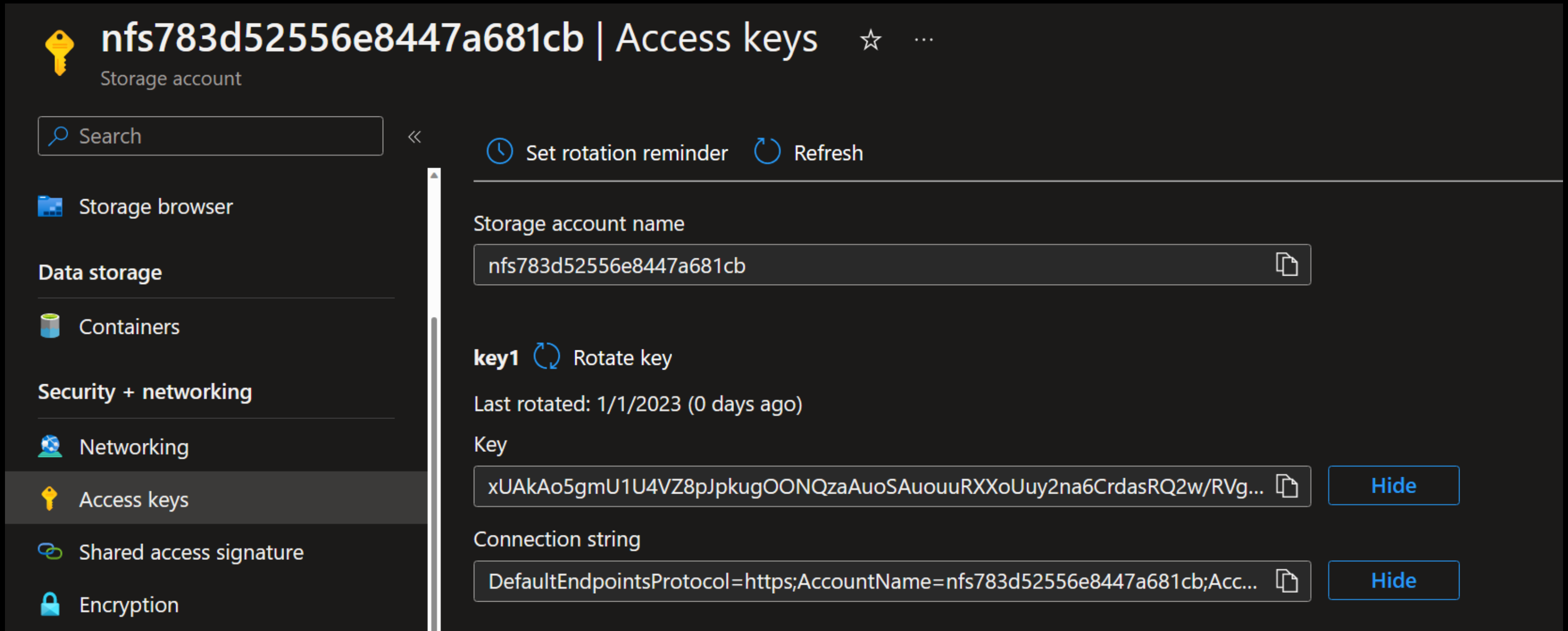
**Authentication method:** Access key (Switch to Azure AD User Account)
**Location:** pvc-e458e45c-47ca-443f-807a-6b101a9b9614

The file 'data' may not render correctly as it contains an unrecognized extension.

```
Sun Jan 1 08:08:08 UTC 2023
Sun Jan 1 08:09:08 UTC 2023
Sun Jan 1 08:10:09 UTC 2023
Sun Jan 1 08:11:09 UTC 2023
Sun Jan 1 08:12:09 UTC 2023
Sun Jan 1 08:13:09 UTC 2023
Sun Jan 1 08:14:09 UTC 2023
Sun Jan 1 08:15:09 UTC 2023
```

# Created resources

```
kubectl get secret
# NAME                                                           TYPE     DATA   AGE
# secret/azure-storage-account-fuse8d87a1d1a8324d7484f-secret   Opaque   2      46m

kubectl get secret azure-storage-account-fuse8d87a1d1a8324d7484f-secret -o yaml
# apiVersion: v1
# data:
#   azurestorageaccountkey: RXk4SHVwUURvZGMydjlnTXJ3THN5YmlGMUpsWjdVaVQrcDE4L2dDFMUmBU3RXd1V5R2c9PQ==
#   azurestorageaccountname: ZnVzZThkODdhMWQxYTgzMjRkNzQ4NGY=
# kind: Secret
```



Storage account name

nfs783d52556e8447a681cb

key1 Rotate key

Last rotated: 1/1/2023 (0 days ago)

Key

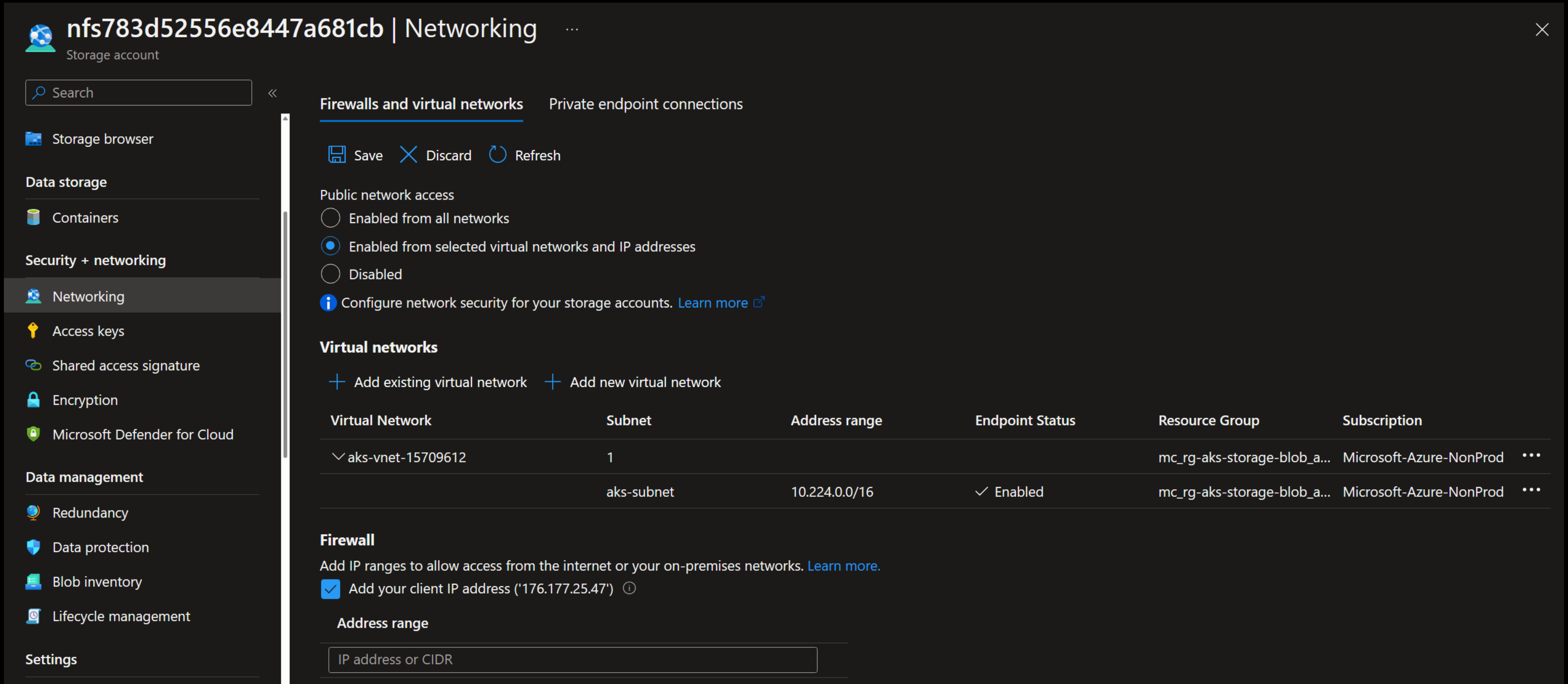
xUAkAo5gmU1U4VZ8pJpkugOONQzaAuoSAuouuRXXoUuy2na6CrdasRQ2w/RVg...

Connection string

DefaultEndpointsProtocol=https;AccountName=nfs783d52556e8447a681cb;Acc...

# Access to Storage Account

```
Mounting blobfuse requires account key. Link.

Mounting blob storage NFSv3 does not need account key.
Select Enabled from selected virtual networks and IP addresses with same vnet as agent node.
```



nfs783d52556e8447a681cb | Networking

Storage account

Public network access

○ Enabled from all networks

● Enabled from selected virtual networks and IP addresses

○ Disabled

Configure network security for your storage accounts. Learn more

**Virtual networks**

| Virtual Network | Subnet | Address range | Endpoint Status | Resource Group | Subscription |
|---|---|---|---|---|---|
| aks-vnet-15709612 | 1 | | | mc_rg-aks-storage-blob_a... | Microsoft-Azure-NonProd |
| | aks-subnet | 10.224.0.0/16 | ✓ Enabled | mc_rg-aks-storage-blob_a... | Microsoft-Azure-NonProd |

**Firewall**

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

☑ Add your client IP address ('176.177.25.47')

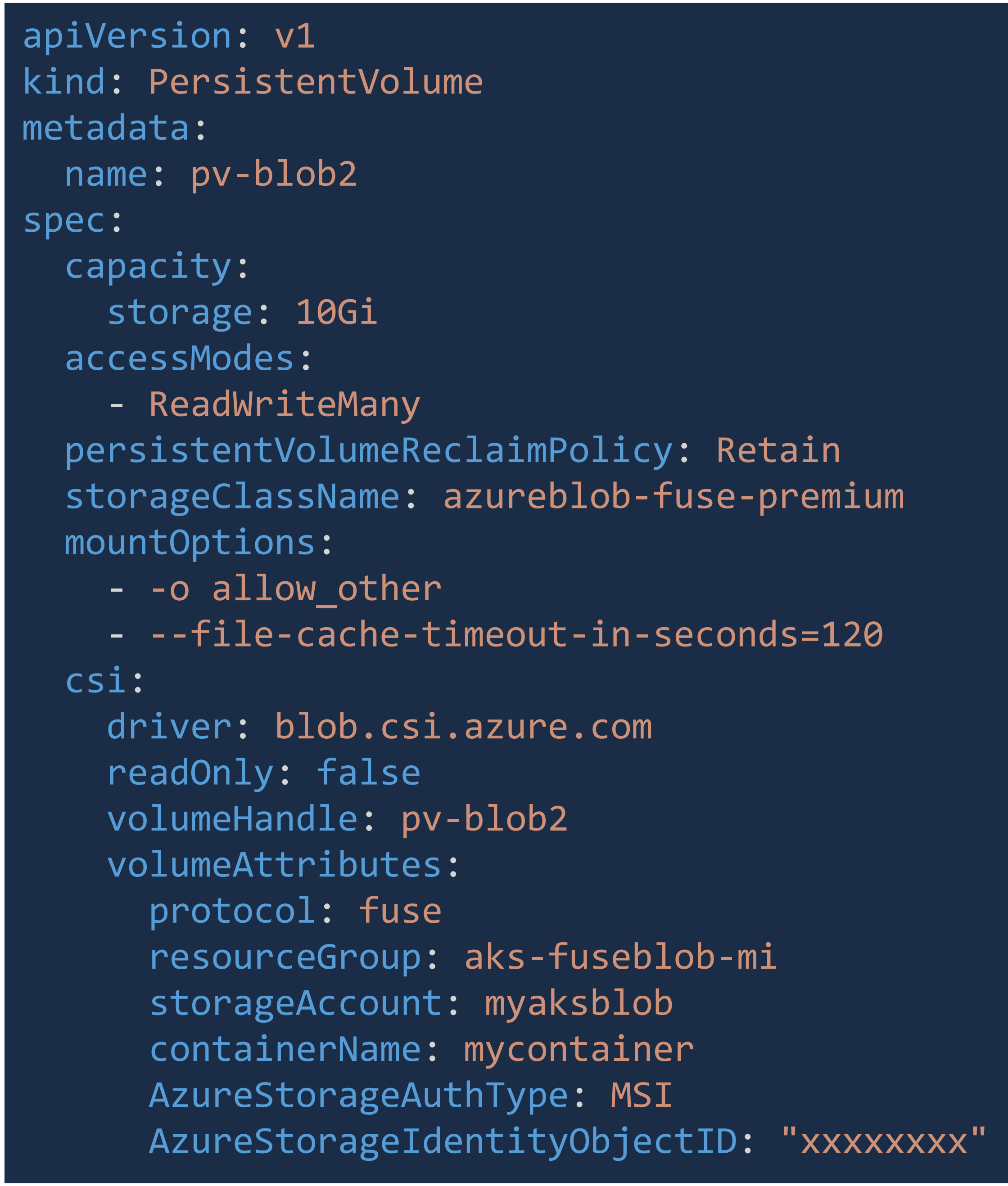
Address range

IP address or CIDR

# Blob with User Identity

Supports authentication using Azure Managed Identity.

More details:
https://github.com/qxsch/Azure-Aks/tree/master/aks-blobfuse-mi



```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-blob2
spec:
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteMany
  persistentVolumeReclaimPolicy: Retain
  storageClassName: azureblob-fuse-premium
  mountOptions:
    - -o allow_other
    - --file-cache-timeout-in-seconds=120
  csi:
    driver: blob.csi.azure.com
    readOnly: false
    volumeHandle: pv-blob2
    volumeAttributes:
      protocol: fuse
      resourceGroup: aks-fuseblob-mi
      storageAccount: myaksblob
      containerName: mycontainer
      AzureStorageAuthType: MSI
      AzureStorageIdentityObjectID: "xxxxxxxx"
```

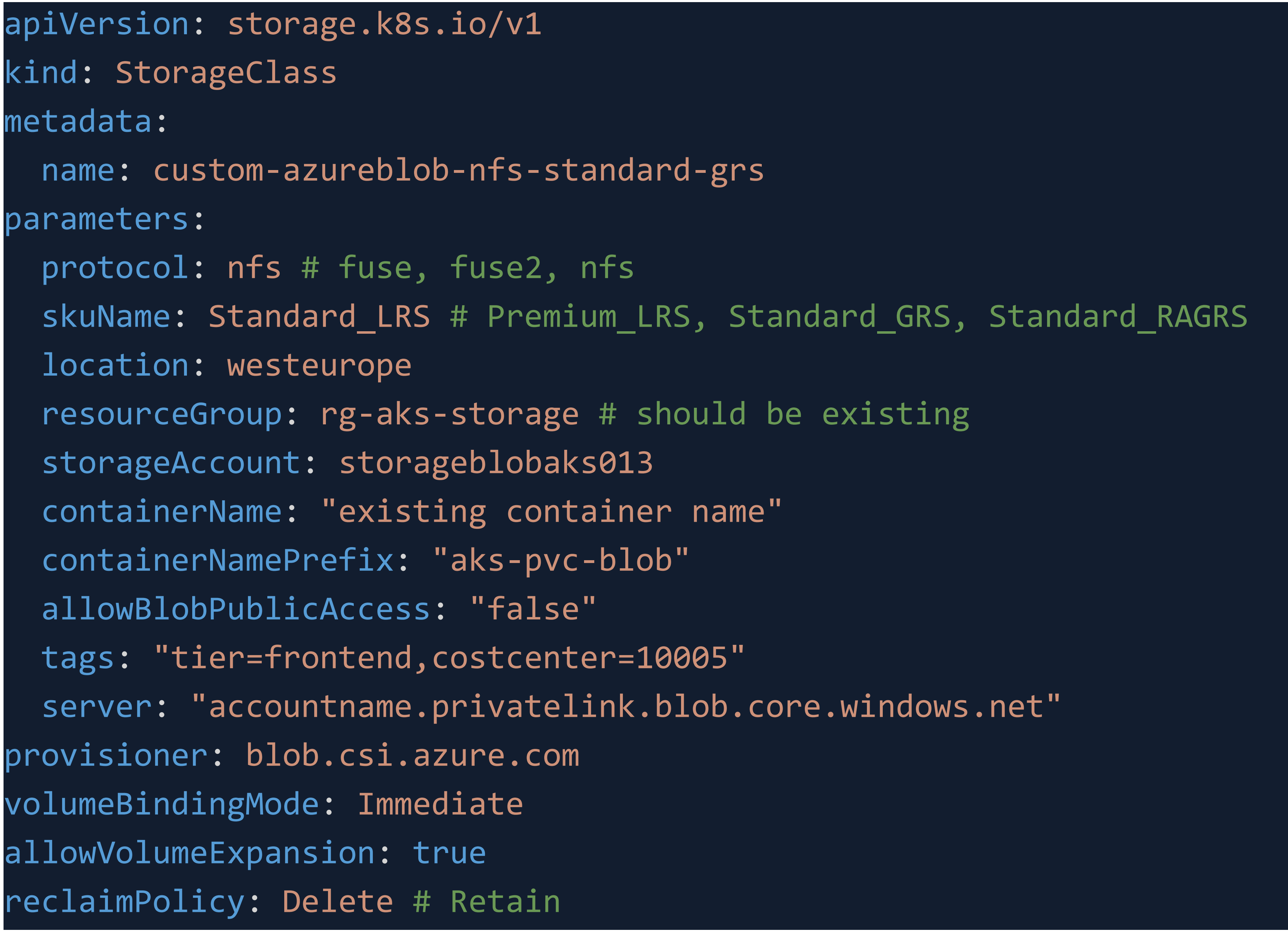
# Bring your own existing storage account

```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: blob-fuse
provisioner: blob.csi.azure.com
parameters:
  resourceGroup: EXISTING_RESOURCE_GROUP_NAME
  storageAccount: EXISTING_STORAGE_ACCOUNT_NAME # cross subscription not supported
  containerName: EXISTING_CONTAINER_NAME
reclaimPolicy: Retain
volumeBindingMode: Immediate
```

More details: [https://github.com/kubernetes-sigs/blob-csi-driver/blob/master/deploy/example/e2e_usage.md#option2-bring-your-own-storage-account](https://github.com/kubernetes-sigs/blob-csi-driver/blob/master/deploy/example/e2e_usage.md#option2-bring-your-own-storage-account)

# More options with Azure Blob

More details:
https://github.com/kubernetes-sigs/blob-csi-driver/blob/master/docs/driver-parameters.md



```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: custom-azureblob-nfs-standard-grs
parameters:
  protocol: nfs # fuse, fuse2, nfs
  skuName: Standard_LRS # Premium_LRS, Standard_GRS, Standard_RAGRS
  location: westeurope
  resourceGroup: rg-aks-storage # should be existing
  storageAccount: storageblobaks013
  containerName: "existing container name"
  containerNamePrefix: "aks-pvc-blob"
  allowBlobPublicAccess: "false"
  tags: "tier=frontend,costcenter=10005"
  server: "accountname.privatelink.blob.core.windows.net"
provisioner: blob.csi.azure.com
volumeBindingMode: Immediate
allowVolumeExpansion: true
reclaimPolicy: Delete # Retain
```

# Save secret in Azure Keyvault

More details: https://github.com/kubernetes-sigs/blob-csi-driver/blob/master/docs/read-from-keyvault.md

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-blob-keyvault
spec:
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteMany
  persistentVolumeReclaimPolicy: Retain
  storageClassName: blob-fuse
  csi:
    driver: blob.csi.azure.com
    readOnly: false
    volumeHandle: unique-volumeid
    volumeAttributes:
      containerName: EXISTING_CONTAINER_NAME
      storageAccountName: EXISTING_STORAGE_ACCOUNT_NAME
      keyVaultURL: https://xxx.vault.azure.net/
      keyVaultSecretName: xxx
```

# Limitations of Azure Blob

Although Blob CSI Driver allows ReadWriteMany access mode to be used, its functionality is limited by the underlying volume-mounting technology.

If azure-storage-fuse is being used to mount a Blob storage container, multiple nodes are allowed to mount the same container, but for just read-only scenarios.

It means, you can still use ReadWriteMany mode to claim a volume, but you should carefully avoid writing to one single file from multiple nodes as there will be data corruption.

NFSv3, in the contrast, fully supports ReadWriteMany access mode.

More details: https://github.com/kubernetes-sigs/blob-csi-driver/blob/master/docs/limitations.md