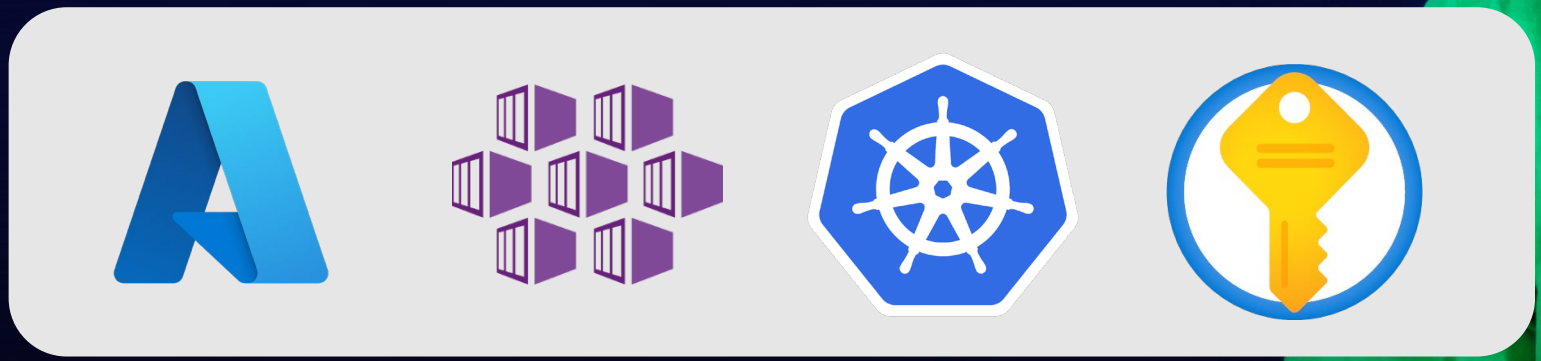
Access to Keyvault using Secret Store CSI & Workload Identity



Houssem Dellai

What is the problem here ?

How a Pod can connect to external secret store providers to retrieve Secrets ?

kubernetes-sigs / secrets-store-csi-driver Public

Watch 20 | Fork 202 | Starred 898

Code | Issues 40 | Pull requests 2 | Actions | Projects 1 | Security | Insights

main | 8 branches | 38 tags | Go to file | Add file | Code

k8s-ci-robot Merge pull request #1109 from aramase/registry.k... 8a38583 17 hours ago 1,119 commits

.github	chore: bump github/codeql-action from 2.1.32 to 2.1.35	2 days ago
.local	chore: remove deprecated `--filtered-watch-secret` flag	13 months ago
apis	release: update manifest and helm charts for v1.2.1	5 months ago
charts/secrets-store-csi-driver	release: update manifest and helm charts for v1.2.4	3 months ago
cmd/secrets-store-csi-driver	chore: update golangci-lint to v1.49.0	3 months ago
config	chore: update tools dependencies and generate manifests	6 months ago
controllers	feat: add token requests client (#805)	10 months ago
deploy	release: update manifest and helm charts for v1.2.4	3 months ago
docker	chore: use kubectl 1.25.4 in driver-crds	27 days ago
docs	Fix typo	17 days ago
hack	chore: bump k8s.io/code-generator from 0.25.3 to 0.25.4 in /h...	23 days ago
img	docs: update readme to reference docs site	2 years ago

About

Secrets Store CSI driver for Kubernetes secrets - Integrates secrets stores with Kubernetes via a CSI volume.

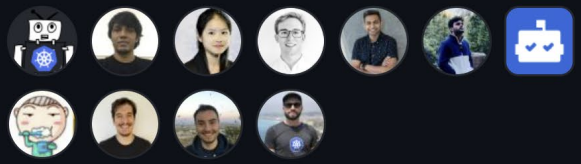
secrets-store-csi-driver.sigs.k8s.io/

Releases 30

v1.2.4 Latest
on Sep 8

+ 29 releases

Contributors 66



+ 55 contributors

Azure / secrets-store-csi-driver-provider-azure Public

Edit Pins | Watch 26 | Fork 170 | Starred 368

Code | Issues 34 | Pull requests 4 | Discussions | Actions | Projects 1 | Security | Insights

master | 10 branches | 27 tags | Go to file | Add file | Code

dependabot[bot] chore: bump github/codeql-action from 2.1.31 t... d2f8e9b 2 days ago 465 commits

.devcontainer	chore: update to go 1.19 (#960)	4 months ago
.github	chore: bump github/codeql-action from 2.1.31 to 2.1.35 (#103...	2 days ago
.pipelines	ci: remove `arc/e2e-test-aks` tests from nightly run (#1023)	8 days ago
arc	chore: update deps (#1005)	last month
charts/csi-secrets-store-provid...	fix: updates template condition for Arc (#973)	2 months ago
cmd	feat: support splitting certs and private key (#1006)	16 days ago
deployment	release: update manifest and helm charts for v1.3.0 (#958)	4 months ago
docs	docs: add keyvault artificats setup for testing (#772)	11 months ago
examples	ci: fix shellcheck file paths (#786)	10 months ago
hack	chore: add cherry_pick_pull script from kubernetes (#661)	15 months ago
images	docs: update readme to reference docs site (#374)	2 years ago
manifest_staging	feat: support splitting certs and private key (#1006)	16 days ago

About

Azure Key Vault provider for Secret Store CSI driver allows you to get secret contents stored in Azure Key Vault instance and use the Secret Store CSI driver interface to mount them into Kubernetes pods.

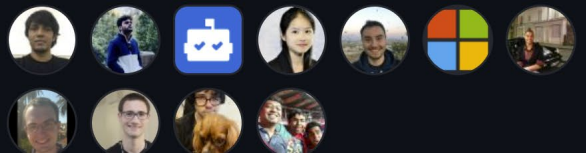
azure.github.io/secrets-store-csi-driver-p...

Releases 21

v1.3.0 Latest
on Aug 12

+ 20 releases

Contributors 53



hashicorp / vault-csi-provider

Public

Watch 35 | Fork 43 | Star 221

Code | Issues 17 | Pull requests 2 | Actions | Projects | Security | Insights

main | 4 branches | 14 tags | Go to file | Add file | Code

tomhjp Update deps (#189) — 2a47fd2 16 days ago — 112 commits

.github/workflows	Update deps (#189)	16 days ago
.release	Updating the release slack channel (#178)	3 months ago
deployment	Deployment: Stop using beta.kubernetes.io/os label (#183)	last month
internal	Update alpine and go.mod dependencies (#176)	3 months ago
manifest_staging/deployment	Deployment: Stop using beta.kubernetes.io/os label (#183)	last month
test/bats	Provide release version at build time, move tests to GitHub Ac...	4 months ago
tools	Update deps (#189)	16 days ago
.gitignore	Use CRT for releases (#128)	11 months ago
.go-version	Update deps (#189)	16 days ago
CHANGELOG.md	Update deps (#189)	16 days ago
CODEOWNERS	add codeowners to protect release dirs (#159)	6 months ago
Dockerfile	Update deps (#189)	16 days ago

About

HashiCorp Vault Provider for Secret Store CSI Driver

kubernetes | vault | secret | provider | csi

Readme

MPL-2.0 license

Code of conduct

Security policy

221 stars

35 watching

43 forks

Releases 10

v1.2.1 Latest

16 days ago

+ 9 releases

GoogleCloudPlatform / secrets-store-csi-driver-provider-gcp Public

Watch 9 | Fork 39 | Star 151

Code | Issues 19 | Pull requests 3 | Actions | Security | Insights

main | 12 branches | 8 tags | Go to file | Add file | Code

sshcherbakov Add Fleet Workload Identity support for pod-adc aut... ... 6e565c5 2 days ago 131 commits

.github	chore: update tests to clear warnings (#179)	3 months ago
auth	Add Fleet Workload Identity support for pod-adc authenticati...	2 days ago
charts/secrets-store-csi-driver-...	chore: add helm template to make it easier to change some v...	2 months ago
config	Define optional per secret file mode (#182)	2 months ago
deploy	v1.1.0: update deploy + changelog (#170) (#171)	7 months ago
docs	Add Fleet Workload Identity support for pod-adc authenticati...	2 days ago
examples	chore: update v1alpha1 -> v1 and recommend 1.0 (#160)	11 months ago
infra	logging: add explicit log levels for debug info (#161)	10 months ago
scripts	Add Fleet Workload Identity support for pod-adc authenticati...	2 days ago
server	Define optional per secret file mode (#182)	2 months ago
test	Add Fleet Workload Identity support for pod-adc authenticati...	2 days ago
tools	chore: update dependencies (#188)	2 months ago

About

Google Secret Manager provider for the Secret Store CSI Driver.

kubernetes | gcp | secrets | google-cloud-platform | csi | gcp-secret-manager

Readme

Apache-2.0 license

Code of conduct

151 stars

9 watching

39 forks

Releases 8

v1.1.0 Latest

on May 17

+ 7 releases

aws / secrets-store-csi-driver-provider-aws Public

Watch 16 | Fork 75 | Star 274

Code | Issues 19 | Pull requests 13 | Discussions | Actions | Projects | Security | Insights

main | 9 branches | 3 tags | Go to file | Add file | Code

danmancuso Add failover region feature. (#151) 84db903 5 days ago 61 commits

.github	Golang update to 1.18 (#115)	3 months ago
auth	secrets store csi driver provider aws initial commit	2 years ago
charts/secrets-store-csi-driver-...	Update Chart.yaml	3 months ago
deployment	Update YAMLs to match Helm chart security context (#129)	2 months ago
examples	Update example secret provider class	2 years ago
provider	Add failover region feature. (#151)	5 days ago
server	Add failover region feature. (#151)	5 days ago
tests	Add failover region feature. (#151)	5 days ago
utils	Add failover region feature. (#151)	5 days ago
.gitignore	Create .gitignore	7 months ago
CODE_OF_CONDUCT.md	Initial commit	2 years ago
CONTRIBUTING.md	Initial commit	2 years ago

About

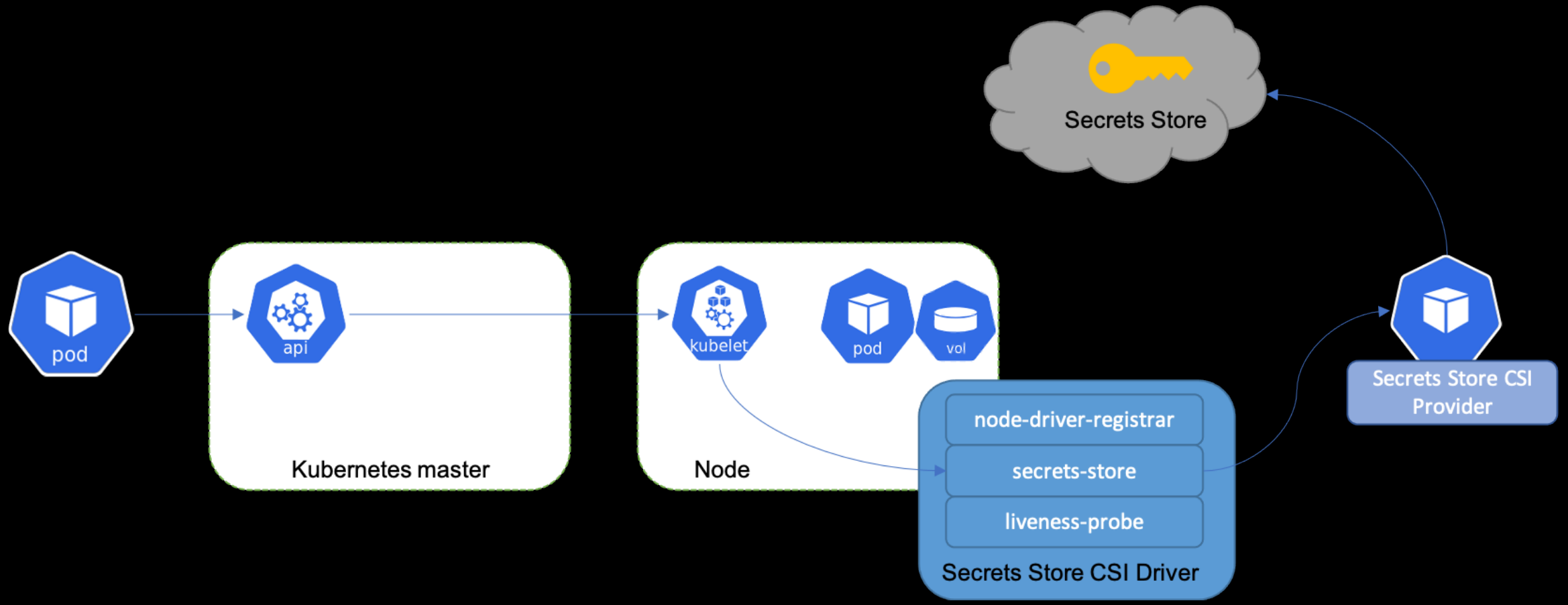
The AWS provider for the Secrets Store CSI Driver allows you to fetch secrets from AWS Secrets Manager and AWS Systems Manager Parameter Store, and mount them into Kubernetes pods.

Readme
Apache-2.0 license
Code of conduct
Security policy
274 stars
16 watching
75 forks

Releases 1

secrets-store-csi-driver-provider... Latest
on Sep 24

Secrets Store CSI architecture



Secret Store CSI in AKS - authentication options

1. **Service Principal (SPN)**
   Works for any kubernetes cluster, but SPN credentials are stored in k8s

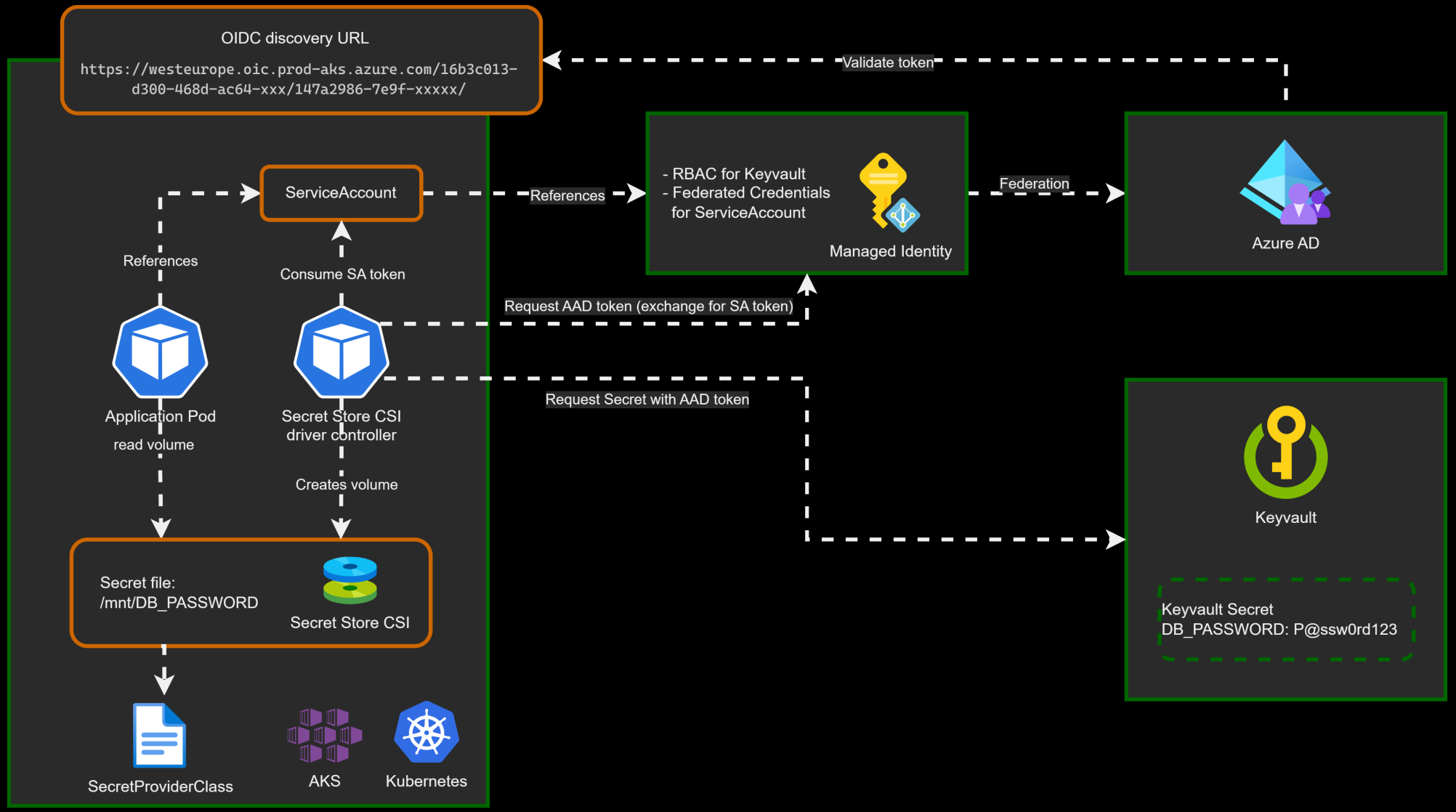
2. **System Managed Identity attached to the VMSS (Nodepool)**
   Uses one single Identity that is available to all Pods and all Nodes

3. **User Managed Identity attached to the VMSS (Nodepool)**
   Identity is available to all Pods and all Nodes

4. **User Managed Identity attached to the VMSS with Pod Identity**
   Pod Identity intercepts calls to IMDS/Identity

5. **Workload Identity with Service Account**
   Works for any kubernetes cluster, no credentials, native to kubernetes

Secrets Store CSI & Workload Identity together

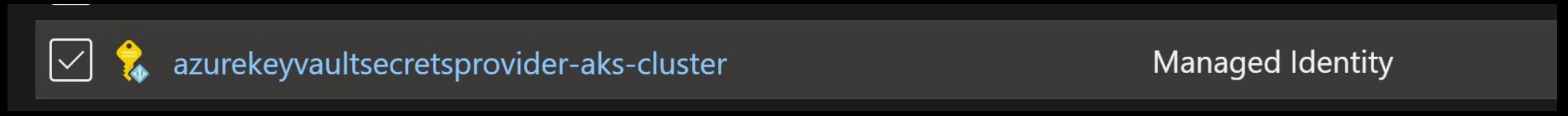


Create AKS cluster with Secrets Store CSI & Workload Identity

```
$ az group create -n aks_rg -l westeurope

$ az aks create -g aks_rg -n aks_cluster `
                --enable-addons azure-keyvault-secrets-provider `
                --enable-secret-rotation `
                --rotation-poll-interval 5m `
                --enable-oidc-issuer `
                --enable-workload-identity

$ az aks update… # also possible (doesn’t need to recreate the cluster)
```

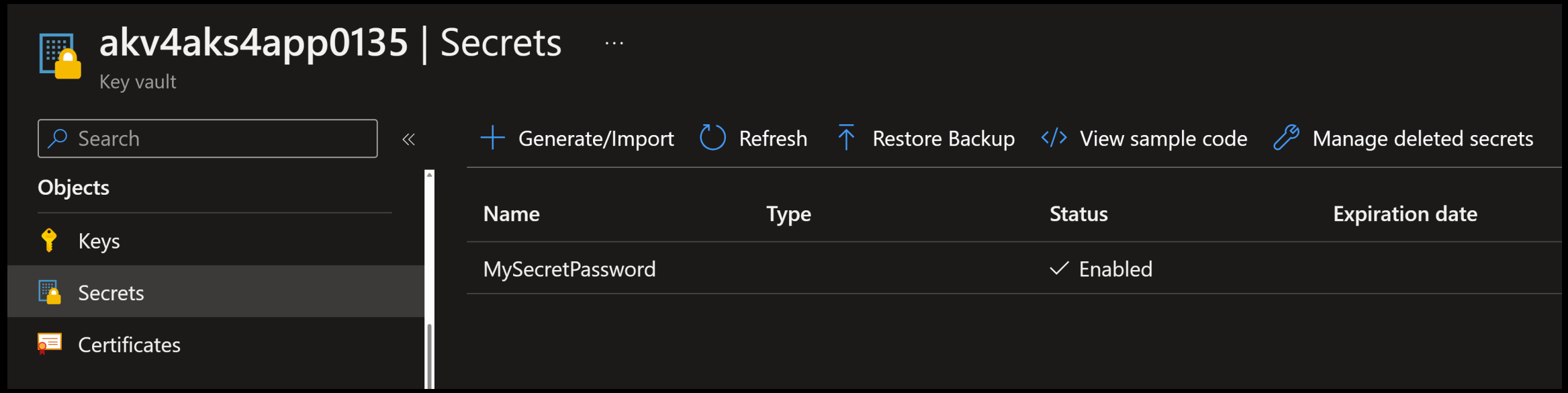
What will be created ?

```
$ az aks show -n $AKS_NAME -g $AKS_RG --query "oidcIssuerProfile.issuerUrl" -otsv
//https://westeurope.oic.prod-aks.azure.com/16b3c013-d300-468d-ac64-
7eda0820b6d3/147a2986-7e9f-4357-8e76-76d2c293a35d/
$
$ kubectl get pods -n kube-system `
          -l 'app in (secrets-store-csi-driver, secrets-store-provider-azure)'
NAME                                     READY   STATUS    RESTARTS   AGE
aks-secrets-store-csi-driver-fdbgq       3/3     Running   0          106s
aks-secrets-store-csi-driver-g85p5       3/3     Running   0          111s
aks-secrets-store-provider-azure-6dphc   1/1     Running   0          106s
aks-secrets-store-provider-azure-f6xcb   1/1     Running   0          111s
$
$ az aks show -n $AKS_NAME -g $AKS_RG -o tsv `
     --query addonProfiles.azureKeyvaultSecretsProvider.identity.clientId
//6c082379-0f2c-4dce-b41f-c3b53d83caed
```



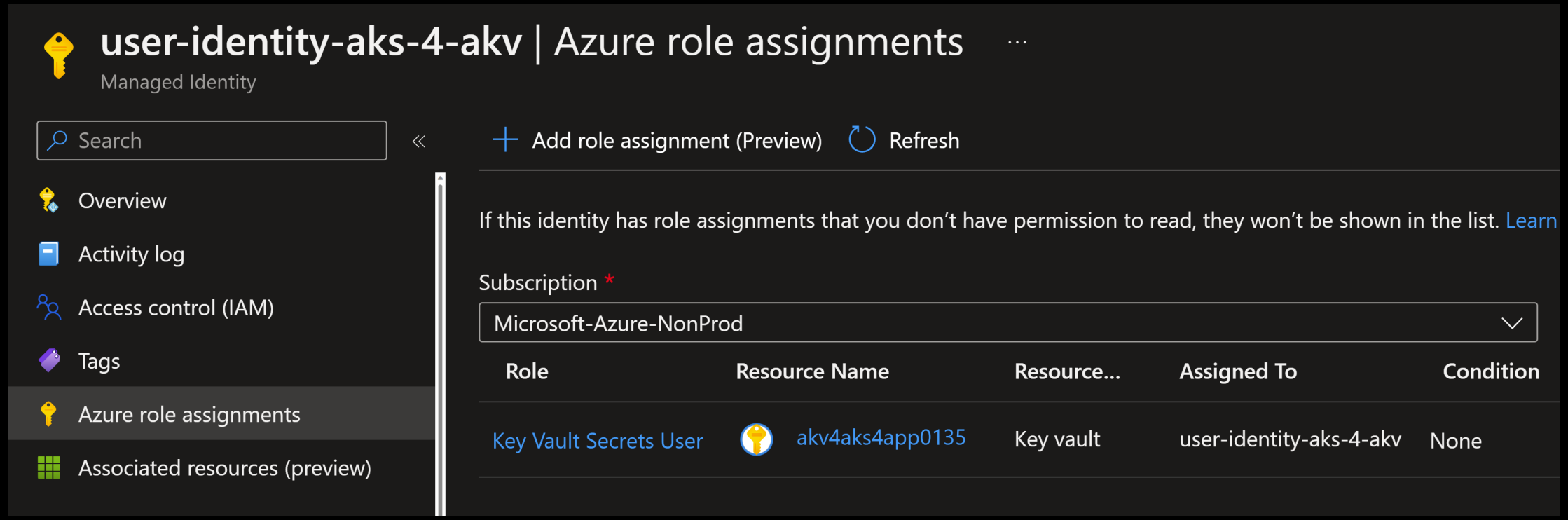
Create Azure Keyvault and Secret

```
$ az keyvault create -n $AKV_NAME -g $AKS_RG --enable-rbac-authorization

$ az keyvault secret set --vault-name $AKV_NAME --name $AKV_SECRET_NAME `
            --value "P@ssw0rd123!"
```

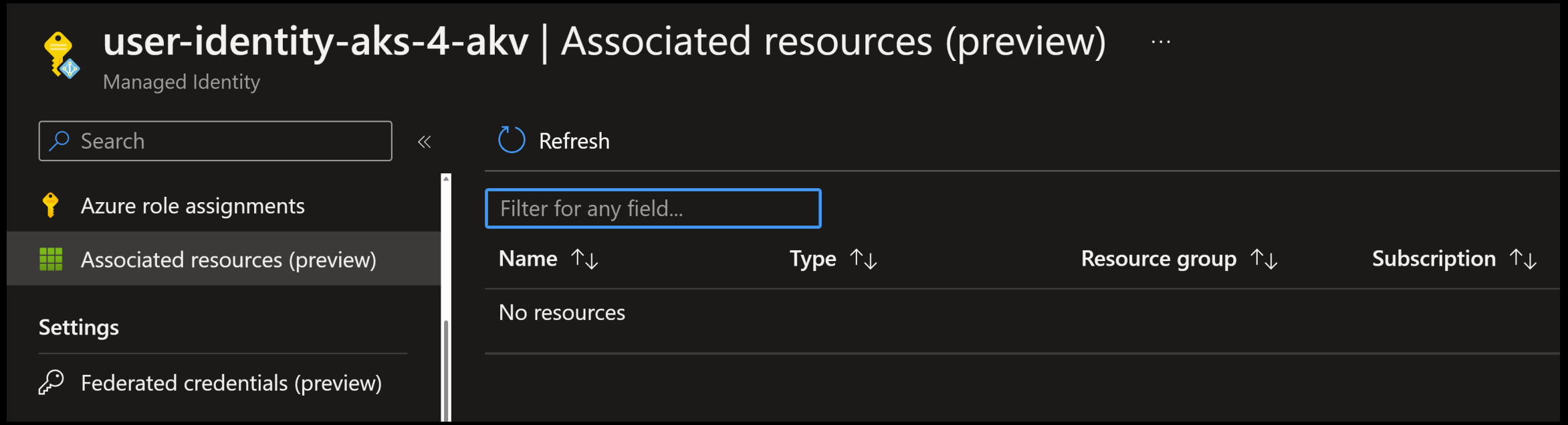


Create User Assigned Managed Identity

```
$ az identity create -g $AKS_RG -n $IDENTITY_NAME

$ az role assignment create --assignee $IDENTITY_CLIENT_ID `
        --role "Key Vault Secrets User" `
        --scope $AKV_ID
```

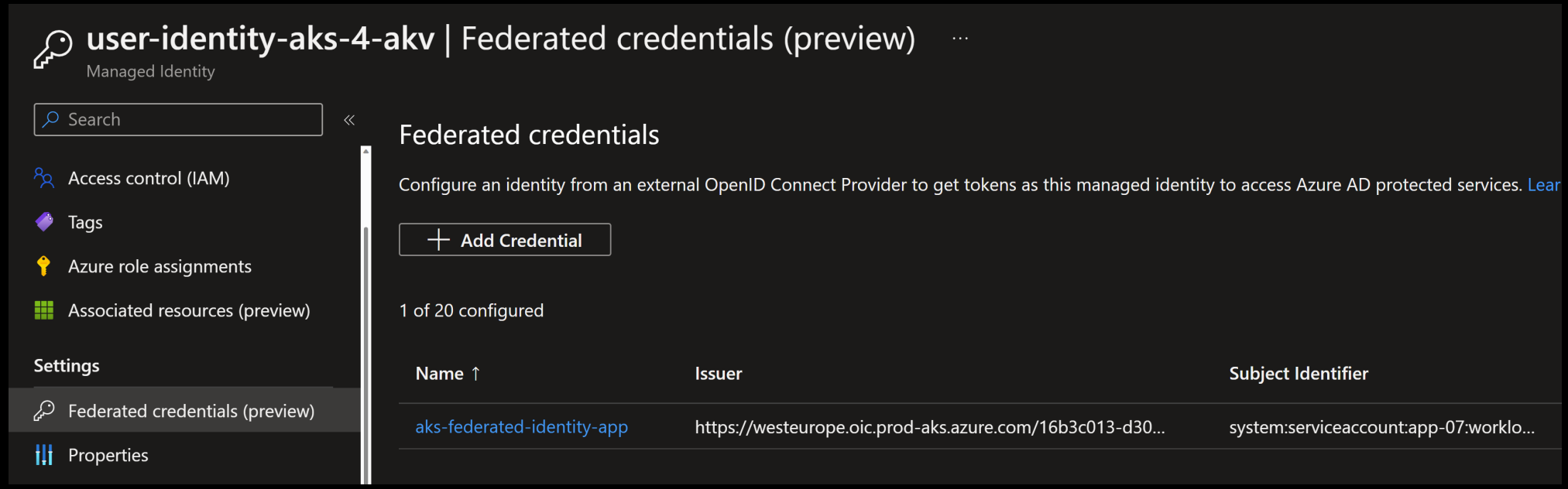


Managed Identity is not attached to the VMSS/Nodepool



Configure federated credentials for Managed Identity

```
$ az identity create -g $AKS_RG -n $IDENTITY_NAME

$ az identity federated-credential create -n $FEDERATED_IDENTITY_NAME `
            -g $AKS_RG `
            --identity-name $IDENTITY_NAME `
            --issuer $AKS_OIDC_ISSUER `
            --subject system:serviceaccount:${NAMESPACE_APP}:${SERVICE_ACCOUNT_NAME}
```



Edit Federated Credential ...

Configure an identity from an external OpenID Connect Provider to get tokens as this managed identity to access Azure AD protected services.

Federated credential scenario * ⓘ

Configure a Kubernetes service account to get tokens as this application and access Azure resou...

Configuration guide for Kubernetes identities

Connect your Kubernetes cluster

Please enter the details of the Kubernetes cluster that you want to connect to Azure Active Directory. These values will be used by Azure AD to validate the connection and should match your Kubernetes OIDC configuration.

Cluster Issuer URL * ⓘ

https://westeurope.oic.prod-aks.azure.com/16b3c013-d300-468d-ac64-7eda0820b6d3/cb981066-d...

Namespace * ⓘ

app-07

Service Account * ⓘ

workload-identity-sa

Subject identifier * ⓘ

system:serviceaccount:app-07:workload-identity-sa

This value is generated based on the Kubernetes account details provided.Edit (optional)

Credential details

Enter and review the details for this credential. The credential name cannot be edited after creation.

Name * ⓘ

aks-federated-identity-app

Audience * ⓘ

api://AzureADTokenExchange

Edit (optional)

How it works: SecretProviderClass

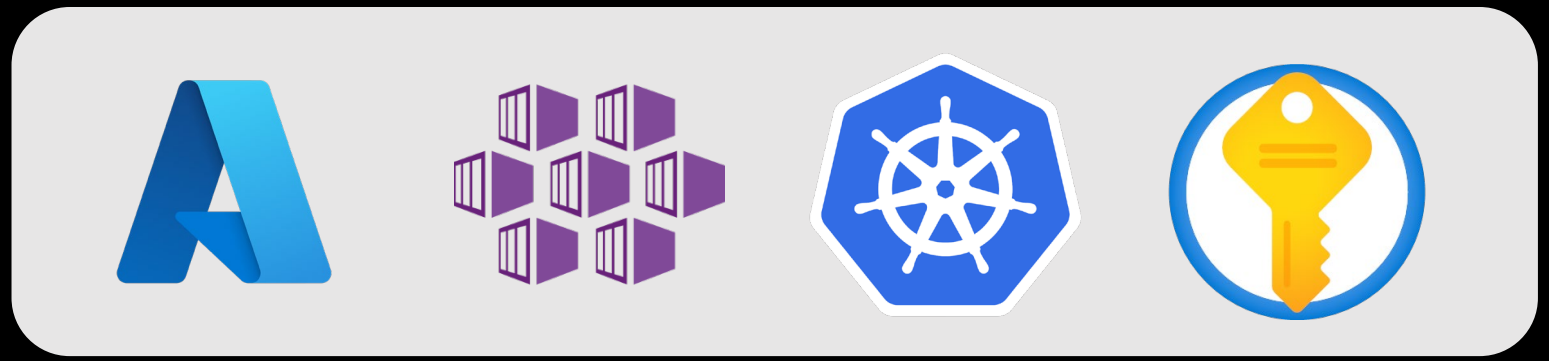
```yaml
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: akv-spc-app # needs to be unique per namespace
spec:
  provider: azure # accepted provider options: azure or vault or gcp
  parameters:
    usePodIdentity: "false"
    useVMManagedIdentity: "false"
    clientID: "b7d9e3a0-116c-40e8-988e-4e899d41b2e5" # uses workload identity
    keyvaultName: akv4aks4app0179          # Set to the name of your key vault
    cloudName: "AzurePublicCloud"
    objects:  |
      array:
        - |
          objectName: MySecretPassword
          objectType: secret  # object types: secret, key, or cert
          objectVersion: ""   # [OPTIONAL] object versions, default to latest if empty
    tenantId: "16b3c013-xxxx-468d-ac64-7eda0820b6d3"  # The tenant ID of the key vault
```

Pod using Secret Store

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations:
    azure.workload.identity/client-id:
b7d9e3a0-116c-40e8-988e-4e899d41b2e5
  labels:
    azure.workload.identity/use: "true"
  name: workload-identity-sa
```

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deploy
spec:
<code removed>
    spec:
      serviceAccountName: workload-identity-sa
      containers:
      - image: nginx
        name: nginx
        volumeMounts:
        - name: secrets-store-inline
          mountPath: "/mnt/secrets-store"
          readOnly: true
      volumes:
        - name: secrets-store-inline
          csi:
            driver: secrets-store.csi.k8s.io
            readOnly: true
            volumeAttributes:
              secretProviderClass: akv-spc-app
```

```
$ kubectl exec -it $POD_NAME -n $NS_APP -- cat /mnt/secrets-store/$AKV_SECRET_NAME
P@ssw0rd123!
```



DEMO

Secret Store CSI – features

The plugin can retrieve Secrets, Keys and Certificates from Keyvault
Works with both Keyvault RBAC and Policy Assignment mode

Auto rotation feature with poll interval
If secrets are updated in Keyvault, the plugin will sync (restart pod with Reloader)
The plugin checks for new updates each 2 minutes by default, but could be changed

Used also to retrieve TLS certificates for Ingress Controller or app pods

Supports mounting multiple secrets store objects as a single volume

Features \ Providers	Azure	GCP	AWS	Vault
Sync as Kubernetes secret	Yes	Yes	Yes	Yes
Rotation	Yes	Yes	Yes	Yes
Windows	Yes	No	No	No
Helm Chart	Yes	No	No	Yes

https://secrets-store-csi-driver.sigs.k8s.io/providers.html

Set Secret as environment variable

https://secrets-store-csi-driver.sigs.k8s.io/topics/set-as-env-var.html

```yaml
kind: Pod
apiVersion: v1
metadata:
  name: secrets-store-inline
spec:
  containers:
  - name: busybox
    image: k8s.gcr.io/e2e-test-images/busybox:1.29
    command:
    - "/bin/sleep"
    - "10000"
    volumeMounts:
    - name: secrets-store01-inline
      mountPath: "/mnt/secrets-store"
      readOnly: true
    env:
    - name: SECRET_USERNAME
      valueFrom:
        secretKeyRef:
          name: foosecret
          key: username
  volumes:
  - name: secrets-store01-inline
    csi:
      driver: secrets-store.csi.k8s.io
      readOnly: true
      volumeAttributes:
        secretProviderClass: "azure-sync"
```

```yaml
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: azure-sync
spec:
  provider: azure
  secretObjects:
  - secretName: foosecret
    type: Opaque
    labels:
      environment: "test"
    data:
    - objectName: secretalias
      key: username
  parameters:
    usePodIdentity: "false"
    keyvaultName: "$KEYVAULT_NAME"
    objects: |
      array:
        - |
          objectName: $SECRET_NAME
          objectType: secret
          objectAlias: secretalias
          objectVersion: $SECRET_VERSION
        - |
          objectName: $KEY_NAME
          objectType: key
          objectVersion: $KEY_VERSION
    tenantId: "tid"
```

SecretProviderClassPodStatus

Contains details about the current object versions that have been loaded in the pod mount.

https://secrets-store-csi-driver.sigs.k8s.io/concepts.html

```yaml
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClassPodStatus
metadata:
  creationTimestamp: "2021-01-21T19:20:11Z"
  generation: 1
  labels:
    internal.secrets-store.csi.k8s.io/node-name: kind-control-plane
    manager: secrets-store-csi
    operation: Update
    time: "2021-01-21T19:20:11Z"
  name: nginx-secrets-store-inline-crd-dev-azure-spc
  namespace: dev
  ownerReferences:
  - apiVersion: v1
    kind: Pod
    name: nginx-secrets-store-inline-crd
    uid: 10f3e31c-d20b-4e46-921a-39e4cace6db2
  resourceVersion: "1638459"
  selfLink: /apis/secrets-store.csi.x-k8s.io/v1/namespaces/dev/secretproviderclasspodstat
  uid: 1d078ad7-c363-4147-a7e1-234d4b9e0d53
status:
  mounted: true
  objects:
  - id: secret/secret1
    version: c55925c29c6743dcb9bb4bf091be03b0
  - id: secret/secret2
    version: 7521273d0e6e427dbda34e033558027a
  podName: nginx-secrets-store-inline-crd
  secretProviderClassName: azure-spc
  targetPath: /var/lib/kubelet/pods/10f3e31c-d20b-4e46-921a-39e4cace6db2/volumes/kubernet
```

Best practices for Secret Store CSI

Use 1 User Managed Identity per application

Ideally,each application would have its own Keyvault, secrets and SecretProviderClass.

Deploy the driver and providers into the kube-system or a separate dedicated namespace

On pod delete, the corresponding volume is cleaned up and deleted.

https://secrets-store-csi-driver.sigs.k8s.io/topics/best-practices.html

Resources

Secrets Store CSI driver
https://secrets-store-csi-driver.sigs.k8s.io/

Azure Key Vault provider for Secret Store CSI driver
https://github.com/Azure/secrets-store-csi-driver-provider-azure

Demo with code
https://github.com/HoussemDellai/docker-kubernetes-course/tree/main/40_secret_store_csi_keyvault