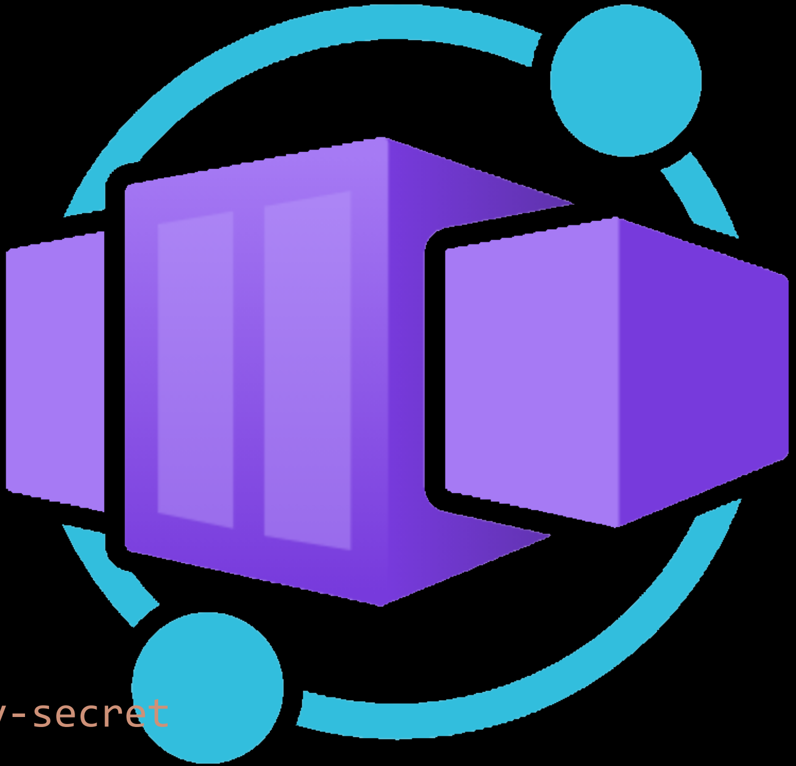
Secure Secrets in Azure Container Apps

```yaml
type: Microsoft.App/app
name: aca-app
properties:
  configuration:
    secrets:
    - name: my-secret-01
      value: MyDatabasePassword
      keyVaultUrl: null
      identity: null
    - name: my-secret-02
      value: null
      keyVaultUrl: https://my.vault.azure.net/secrets/my-secret
      identity: /subscriptions/82f6…
```



Houssem Dellai
Cloud Solution Architect at Microsoft

Why Securing Secrets ?

Store config in the environment : The Twelve-Factor App (12factor.net)

Application configuration should not be hardcoded as constant within the source code.

It should be stored within configuration files (YAML, JSON, XML, .config, etc) or as env variables.

Configurations like background color, app version, backend URL are not sensitive data.

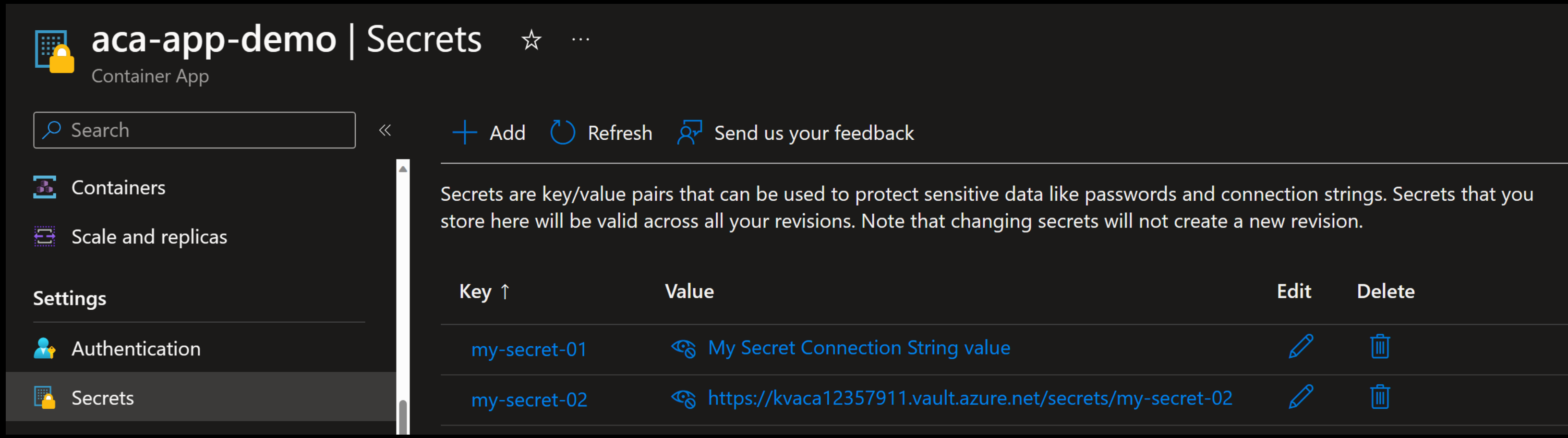
Configurations like API Token, database password or connection string are sensitive data.

This data should be accessible by only the application that needs it.

Other applications should not have access.

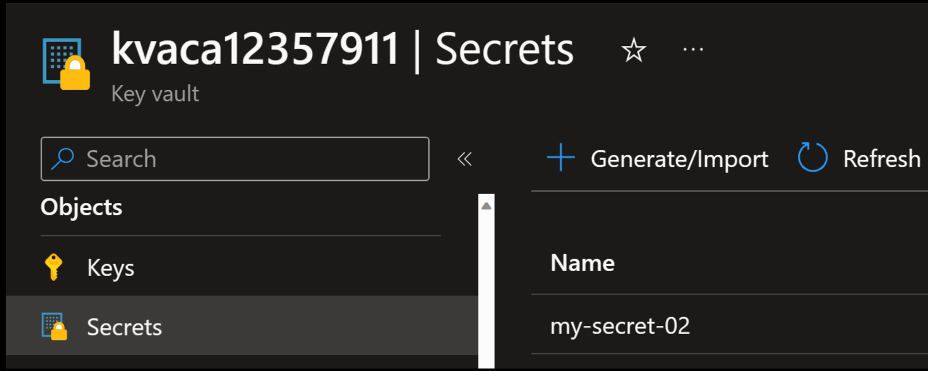
Creating Secrets and reference Key vault (in YAML)

```yaml
type: "Microsoft.App/jobs"
name: "aca-job-processor-wp"
properties:
  configuration:
    secrets:
    - name: my-secret-01
      value: MyDatabasePassword
      keyVaultUrl: null
      identity: null
    - name: my-secret-02
      value: null
      keyVaultUrl: "https://mykv.vault.azure.net/secrets/my-secret-02"
      identity: "/subscriptions/82f6…"
```



Secrets are key/value pairs that can be used to protect sensitive data like passwords and connection strings. Secrets that you store here will be valid across all your revisions. Note that changing secrets will not create a new revision.

Key ↑	Value	Edit	Delete
my-secret-01	My Secret Connection String value		
my-secret-02	https://kvaca12357911.vault.azure.net/secrets/my-secret-02		

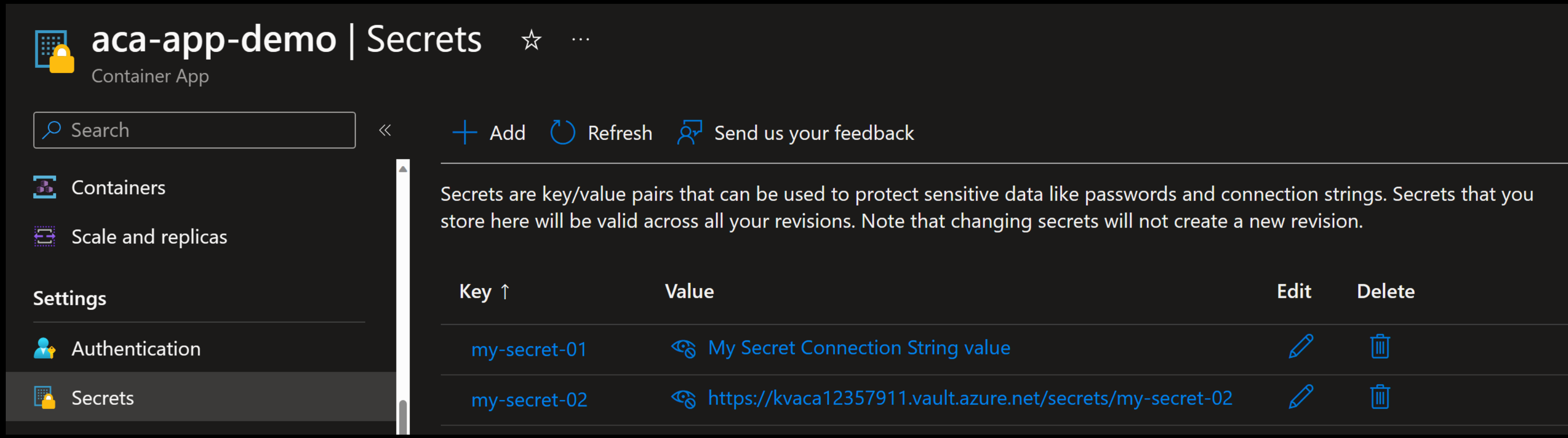


Name
my-secret-02

The Managed Identity will be used to authenticate to Key vault.

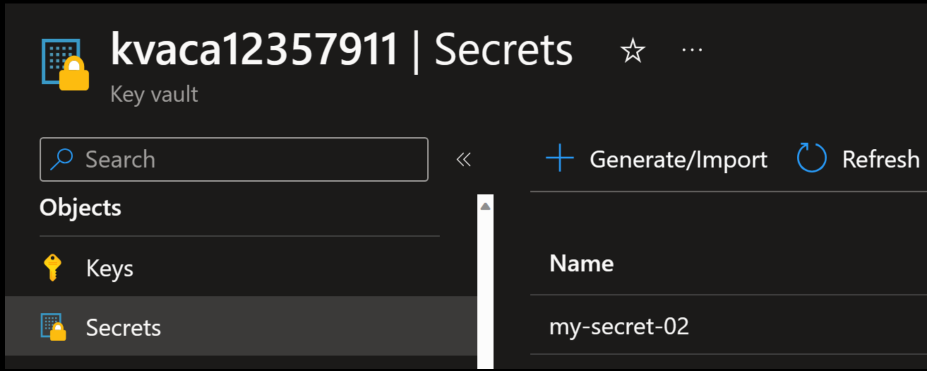
Mount Secrets in environment variables (in YAML)

```yaml
type: "Microsoft.App/jobs"
name: "aca-job-processor-wp"
properties:
  configuration:
    secrets:
    - name: my-secret-01
      value: MyDatabasePassword
      keyVaultUrl: null
      identity: null
    - name: my-secret-02
      value: null
      keyVaultUrl: "https://mykv.vault.azure.net/secrets/my-secret-02"
      identity: "/subscriptions/82f6…"
  template:
    containers:
      env:
      - name: MY_ENV_SECRET_01
        secretRef: my-secret-01
      - name: MY_ENV_SECRET_02
        secretRef: my-secret-02
```



Secrets are key/value pairs that can be used to protect sensitive data like passwords and connection strings. Secrets that you store here will be valid across all your revisions. Note that changing secrets will not create a new revision.

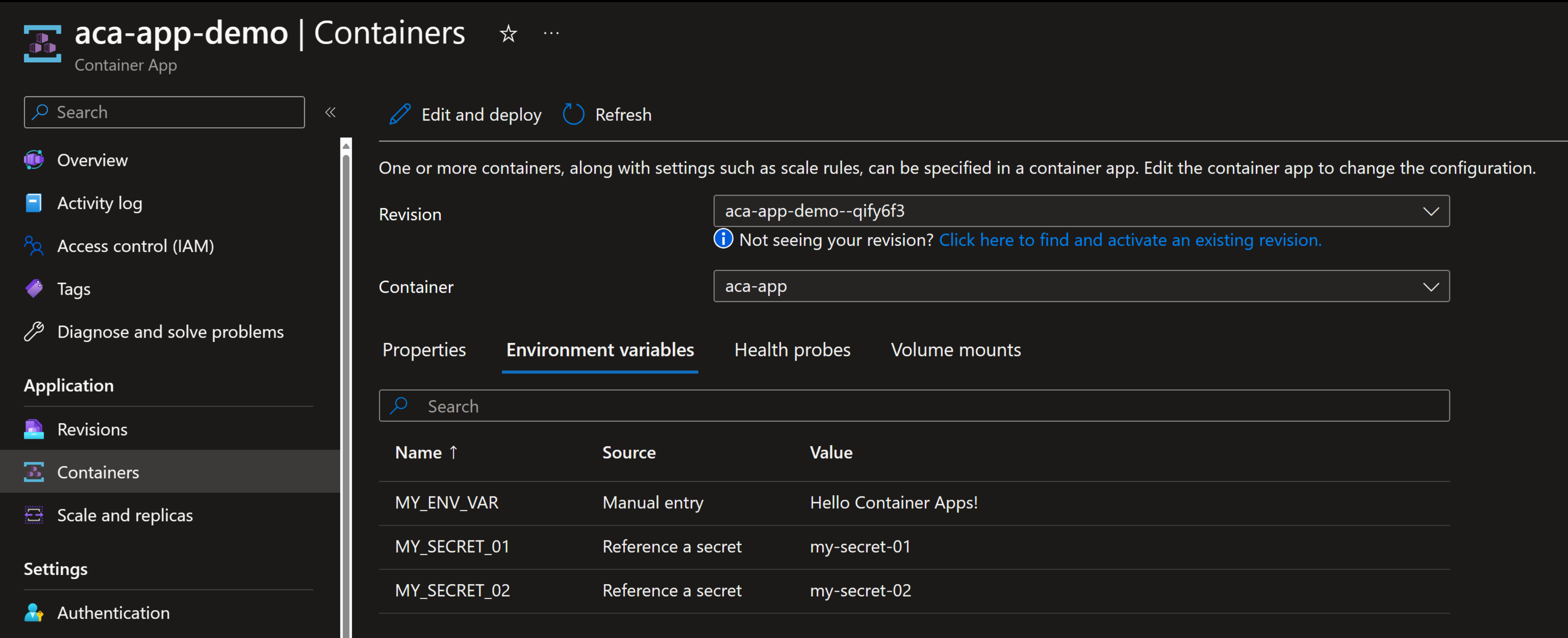
Key ↑	Value	Edit	Delete
my-secret-01	My Secret Connection String value	✎	🗑
my-secret-02	https://kvaca12357911.vault.azure.net/secrets/my-secret-02	✎	🗑



Name
my-secret-02

```python
My_secret = os.getenv("MY-ENV-SECRET_01")
My_env_secret_kv= os.getenv("MY_ENV_SECRET_02")
```

Mount Secrets in environment variables (in YAML)



One or more containers, along with settings such as scale rules, can be specified in a container app. Edit the container app to change the configuration.

Revision: aca-app-demo--qify6f3

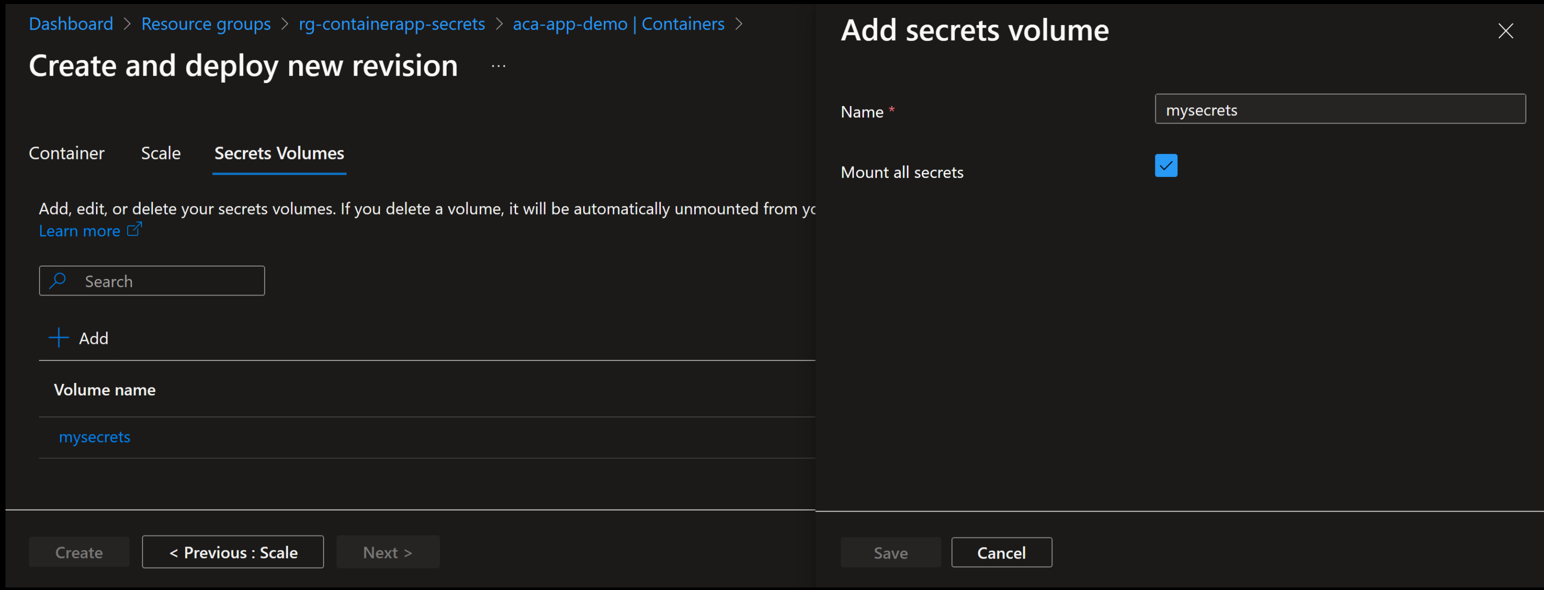
Not seeing your revision? Click here to find and activate an existing revision.

Container: aca-app

Name ↑	Source	Value
MY_ENV_VAR	Manual entry	Hello Container Apps!
MY_SECRET_01	Reference a secret	my-secret-01
MY_SECRET_02	Reference a secret	my-secret-02

Container App mount Secrets as Volume (ARM/Bicep)

```
"template": {
    "containers": [
        {
            "image": "myregistry/myQueueApp:v1",
            "name": "myQueueApp",
            "volumeMounts": [
                {
                    "name": "mysecrets",
                    "mountPath": "/mnt/secrets"
                }
            ]
        }
    ],
    "volumes": [
        {
            "name": "mysecrets",
            "storageType": "Secret"
        }
    ]
}
```



Dashboard > Resource groups > rg-containerapp-secrets > aca-app-demo | Containers >

Create and deploy new revision ···

Add, edit, or delete your secrets volumes. If you delete a volume, it will be automatically unmounted from yo
Learn more

Volume name
mysecrets

Add secrets volume

Name *: mysecrets

Mount all secrets: ☑

Accessing Secrets from env variables and volume

```
az containerapp exec -n aca-app-demo -g rg-containerapp-secrets --command bash


root@aca-app-demo--qify6f3-5c6f44d5f-blvh8:/app# printenv | grep MY_SECRET
MY_SECRET_01=My Secret Connection String value
MY_SECRET_02=P@ssw0rd123!


root@aca-app-demo--qify6f3-5c6f44d5f-svszm:/app# ls /mnt/secrets/
my-secret-01 my-secret-02

root@aca-app-demo--qify6f3-5c6f44d5f-svszm:/app# cat /mnt/secrets/my-secret-01
My Secret Connection String value

root@aca-app-demo--qify6f3-5c6f44d5f-svszm:/app# cat /mnt/secrets/my-secret-02
P@ssw0rd123!
```