External Secrets Operator 和 Secrets Store CSI Driver 之實務比較

Kubernetes Community Days Taipei 2024 – Lighting Talk

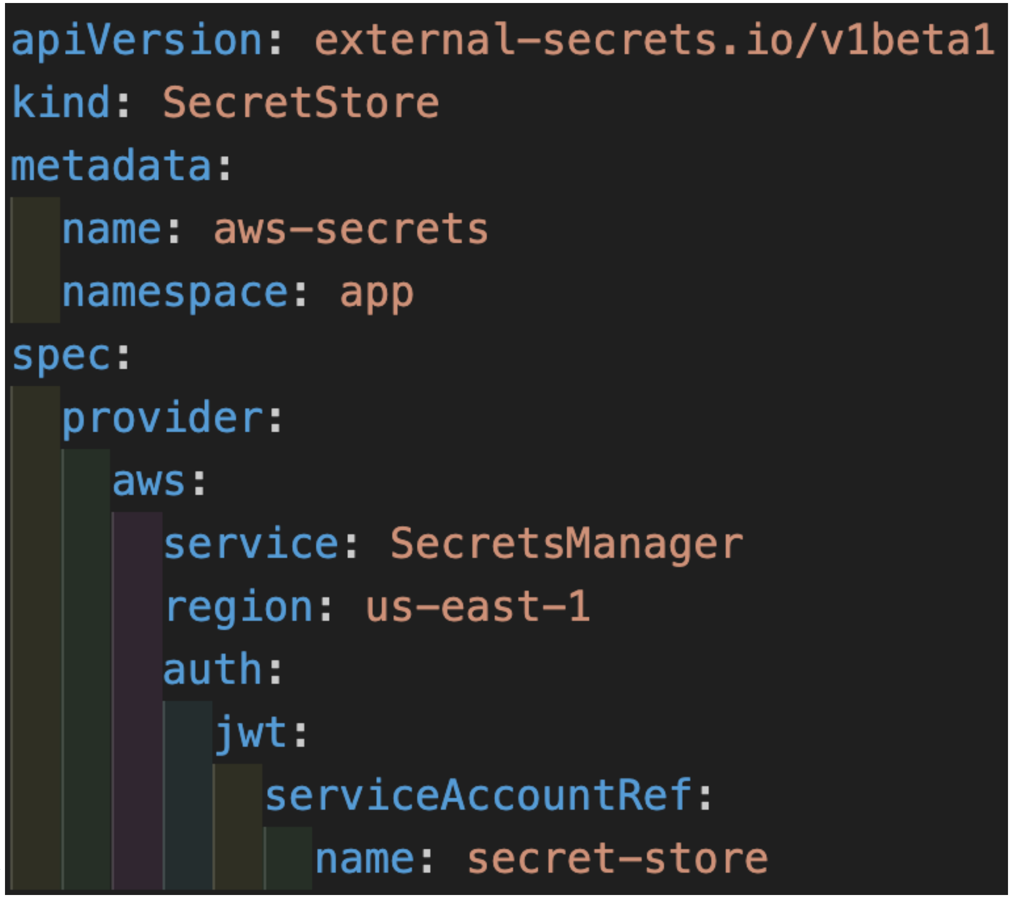
Abby Chuo

A Cloud Architect who assists clients in planning and implementing cloud architectures, leveraging numerous CNCF projects such as Kubernetes. Actively participates in community activities and has served as a co-organizer for PyLadies Taiwan for several years.

透過 **External Secret Operator** 或 **Secrets Store CSI Driver**，可將外部秘密管理系統中的敏感數據自動化同步到 **Kubernetes** 內，供應用程序讀取。

External Secret Operator 使用範例

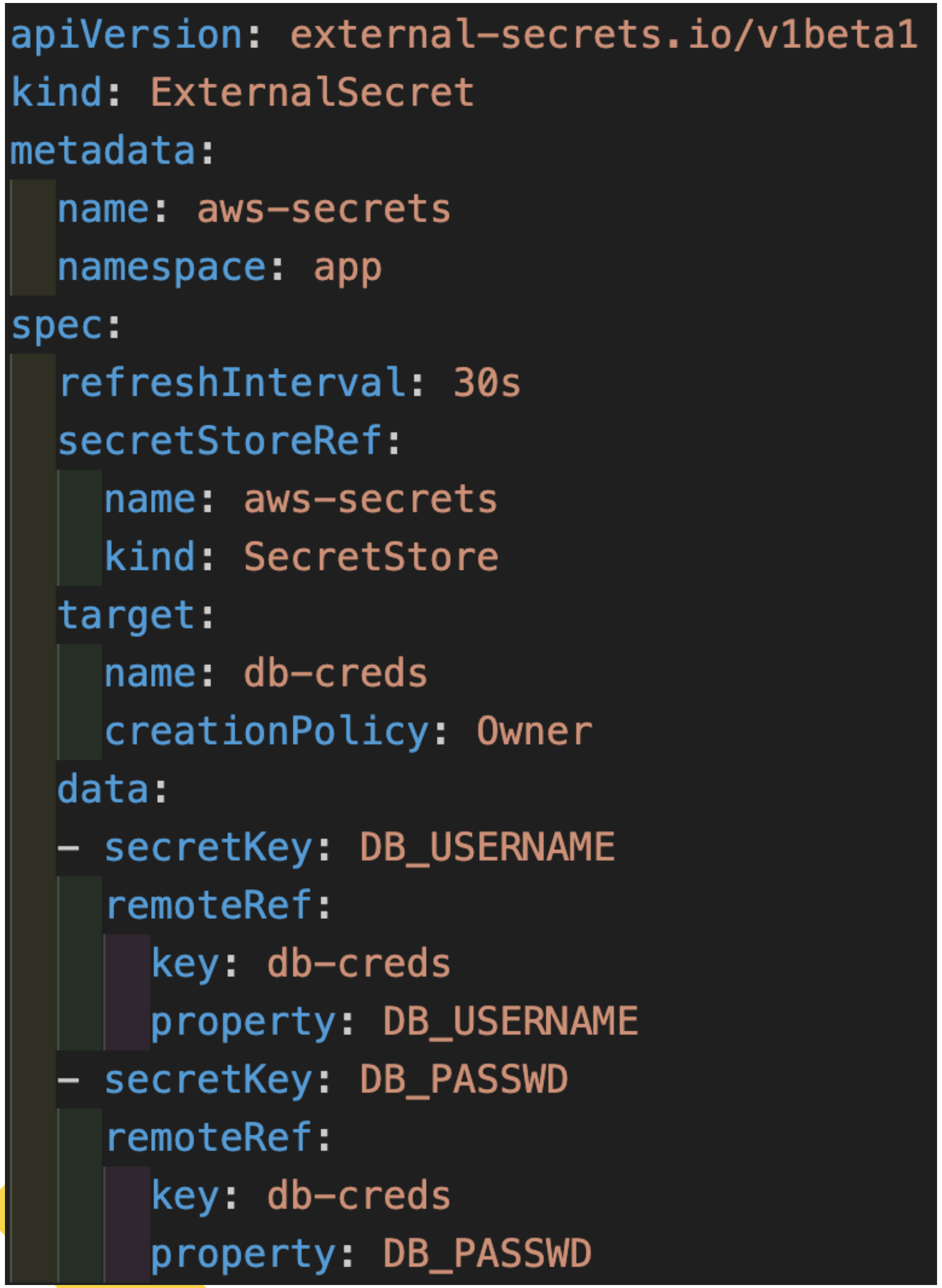
設定 Secret Provider



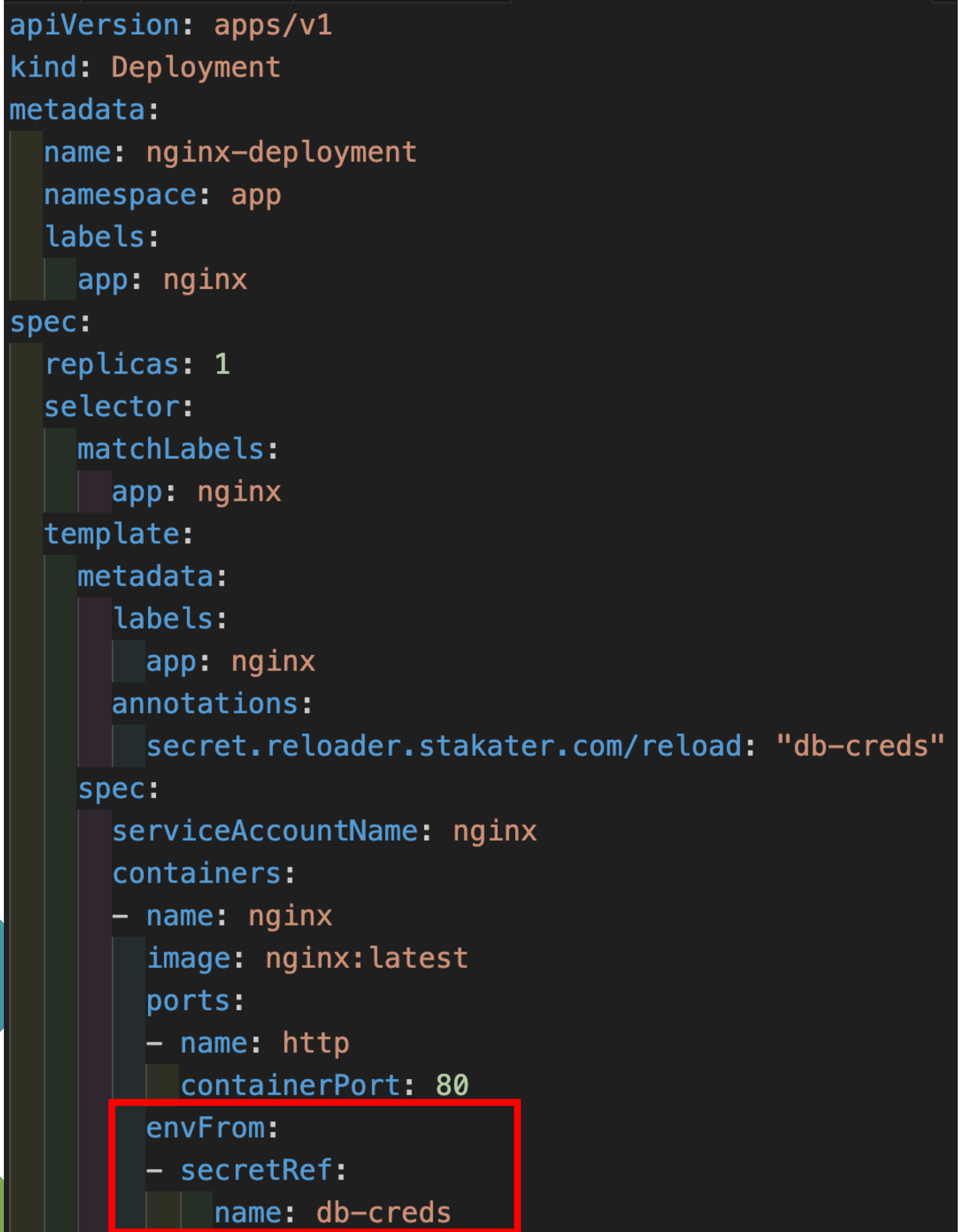
```yaml
apiVersion: external-secrets.io/v1beta1
kind: SecretStore
metadata:
  name: aws-secrets
  namespace: app
spec:
  provider:
    aws:
      service: SecretsManager
      region: us-east-1
      auth:
        jwt:
          serviceAccountRef:
            name: secret-store
```

External Secret Operator 使用範例

指定外部 Secret 來源、產生 K8s Secret



```yaml
apiVersion: external-secrets.io/v1beta1
kind: ExternalSecret
metadata:
  name: aws-secrets
  namespace: app
spec:
  refreshInterval: 30s
  secretStoreRef:
    name: aws-secrets
    kind: SecretStore
  target:
    name: db-creds
    creationPolicy: Owner
  data:
  - secretKey: DB_USERNAME
    remoteRef:
      key: db-creds
      property: DB_USERNAME
  - secretKey: DB_PASSWD
    remoteRef:
      key: db-creds
      property: DB_PASSWD
```



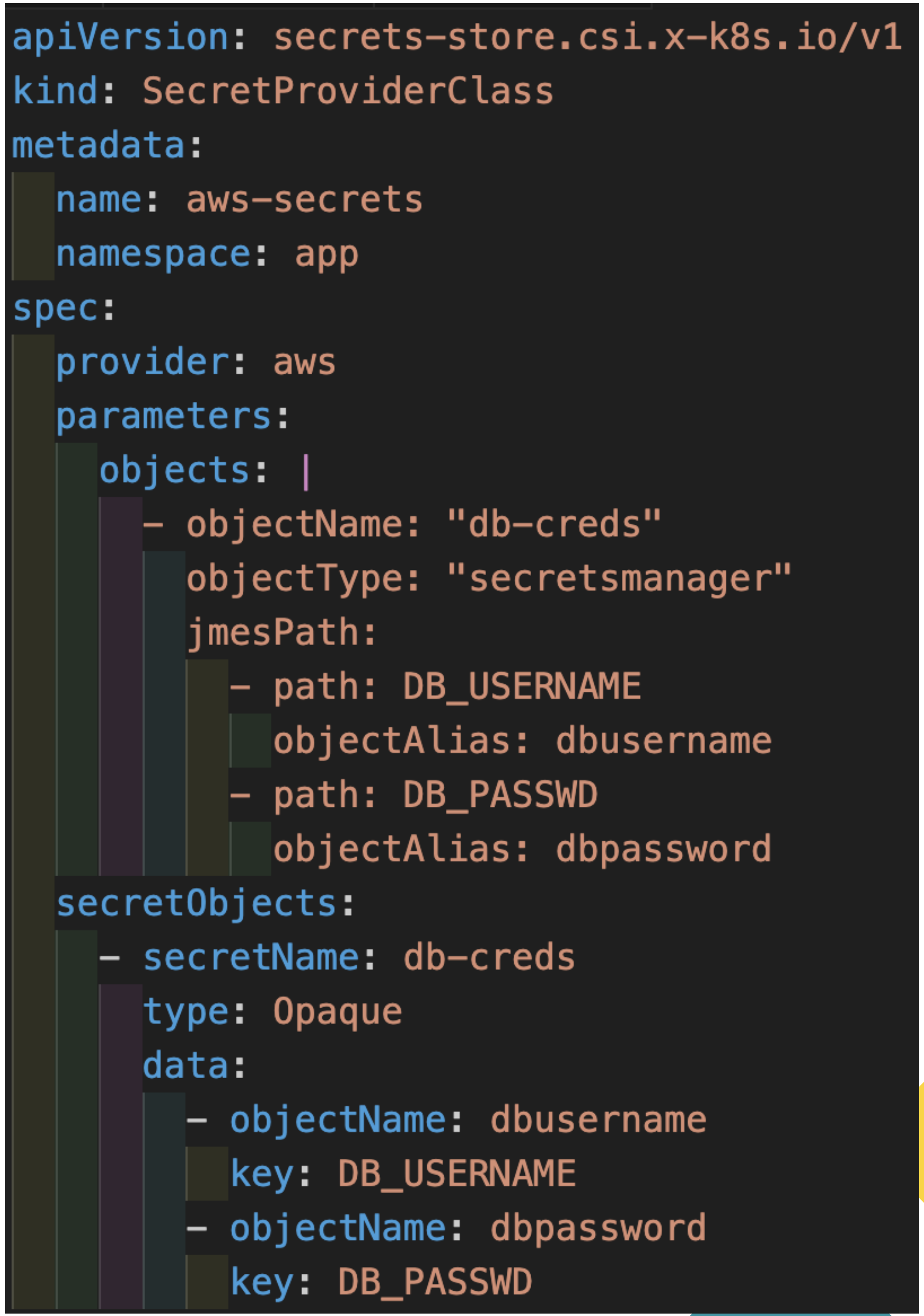
```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  namespace: app
  labels:
    app: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
      annotations:
        secret.reloader.stakater.com/reload: "db-creds"
    spec:
      serviceAccountName: nginx
      containers:
      - name: nginx
        image: nginx:latest
        ports:
        - name: http
          containerPort: 80
        envFrom:
        - secretRef:
            name: db-creds
```

External Secret Operator 使用範例

透過環境變數讓應用程式讀取 Secret

Secrets Store CSI Driver 使用範例

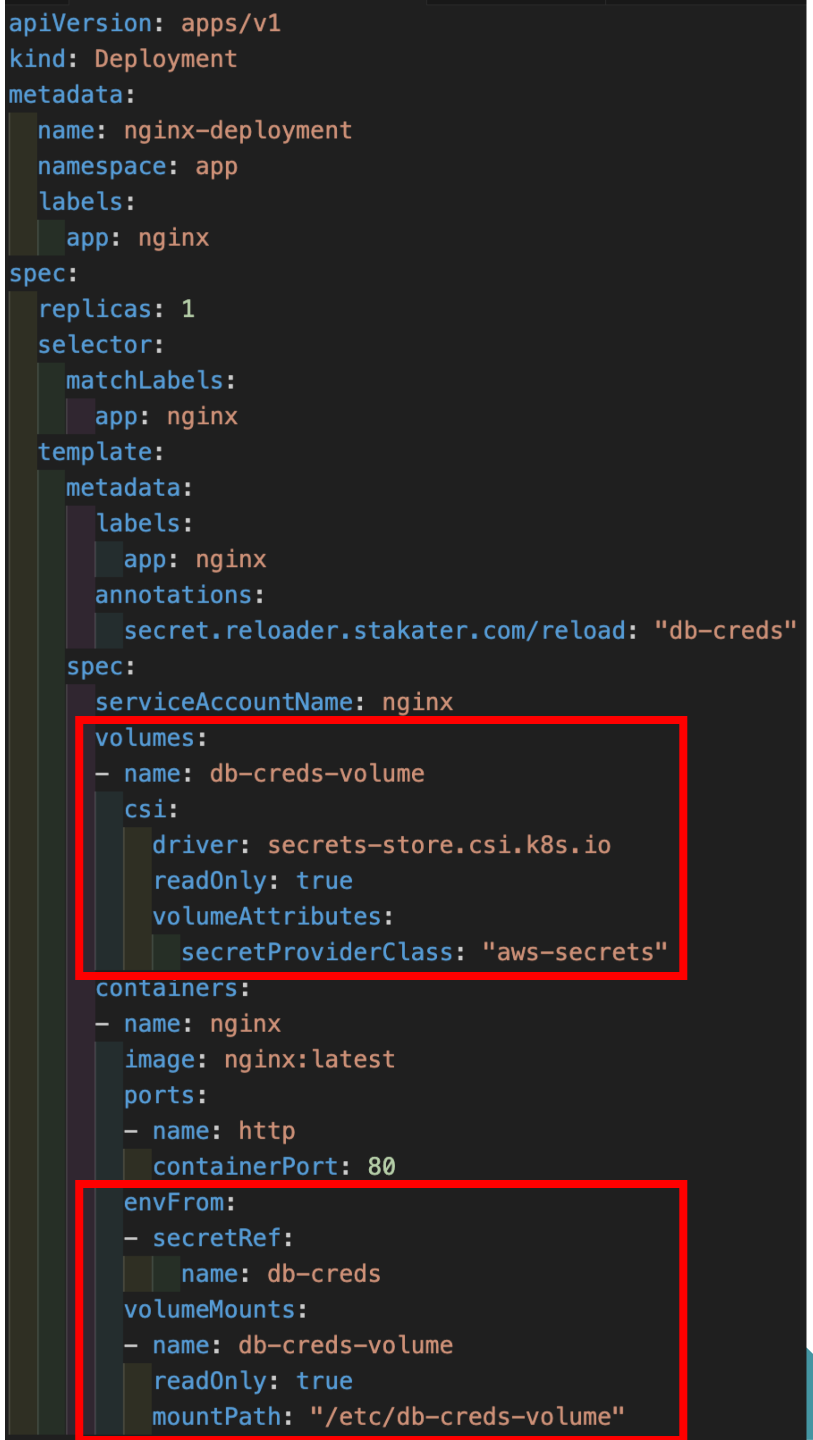
設定 Secret Provider、 指定外部 Secret 來源、指定 K8s Secret 內容 (並不會直接產生 K8s Secret)



```yaml
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: aws-secrets
  namespace: app
spec:
  provider: aws
  parameters:
    objects: |
      - objectName: "db-creds"
        objectType: "secretsmanager"
        jmesPath:
          - path: DB_USERNAME
            objectAlias: dbusername
          - path: DB_PASSWD
            objectAlias: dbpassword
  secretObjects:
    - secretName: db-creds
      type: Opaque
      data:
        - objectName: dbusername
          key: DB_USERNAME
        - objectName: dbpassword
          key: DB_PASSWD
```

Secrets Store CSI Driver 使用範例

透過環境變數讓應用程式讀取 Secret (必須掛載 Volume，K8s Secret 才會產生出來)



```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  namespace: app
  labels:
    app: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
      annotations:
        secret.reloader.stakater.com/reload: "db-creds"
    spec:
      serviceAccountName: nginx
      volumes:
      - name: db-creds-volume
        csi:
          driver: secrets-store.csi.k8s.io
          readOnly: true
          volumeAttributes:
            secretProviderClass: "aws-secrets"
      containers:
      - name: nginx
        image: nginx:latest
        ports:
        - name: http
          containerPort: 80
        envFrom:
        - secretRef:
            name: db-creds
        volumeMounts:
        - name: db-creds-volume
          readOnly: true
          mountPath: "/etc/db-creds-volume"
```

兩者差異

	Type	**Installation Complexity**	**Sync as Volume**	**Sync as K8s Secret**	**Secret Auto Rotation**	**Permission Grant on**	**Community Engagement**
External Secret Operator	Pod	Low	N	Y	Enabled by default	SecretStore	Medium
Secrets Store CSI Driver	DaemonSet	Low	Y	Disabled by default	Disabled by default (Alpha)	Pod (App)	Low

Thank you