KubeCon | CloudNativeCon

Europe 2019

Secrets Store CSI Driver

Bring Your Own Enterprise Secrets Store to Kubernetes

Rita Zhang (@ritazzhang, Microsoft)
Anubhav Mishra (@anubhavm, HashiCorp)

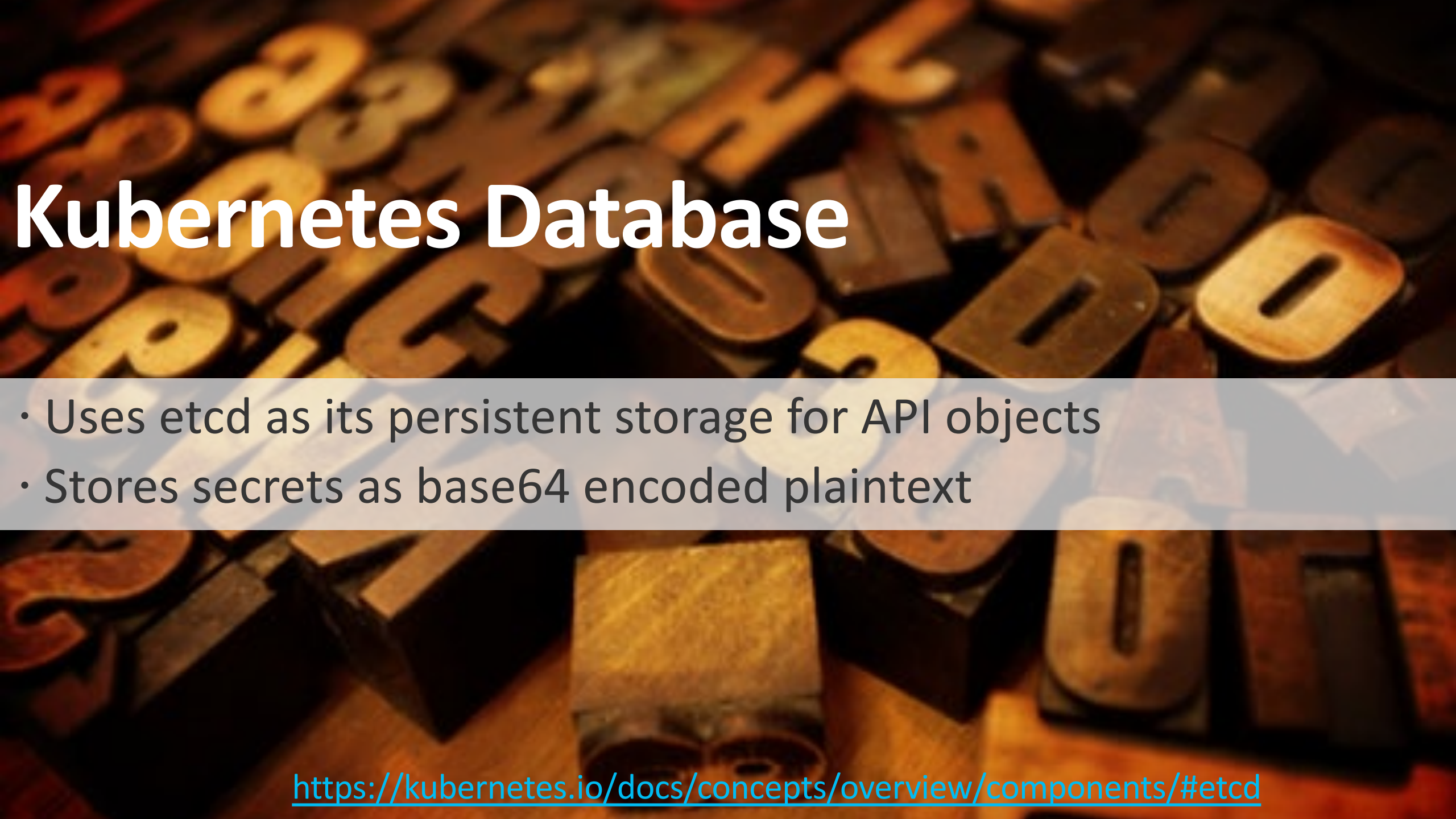
Rita Zhang

- Software engineer, Microsoft, San Francisco
- Container upstream team, Azure Kubernetes Service
- Maintainer for secrets-store-csi-driver, keyvault-flexvolume, Open Policy Agent Gatekeeper

@ritazzhang

Anubhav Mishra

- Team Lead, Developer Advocacy, HashiCorp, Vancouver.
- Provider Maintainer, Virtual Kubelet, Helm
- Provider Maintainer, secrets-stores-csi-driver



Kubernetes Database

- Uses etcd as its persistent storage for API objects
- Stores secrets as base64 encoded plaintext

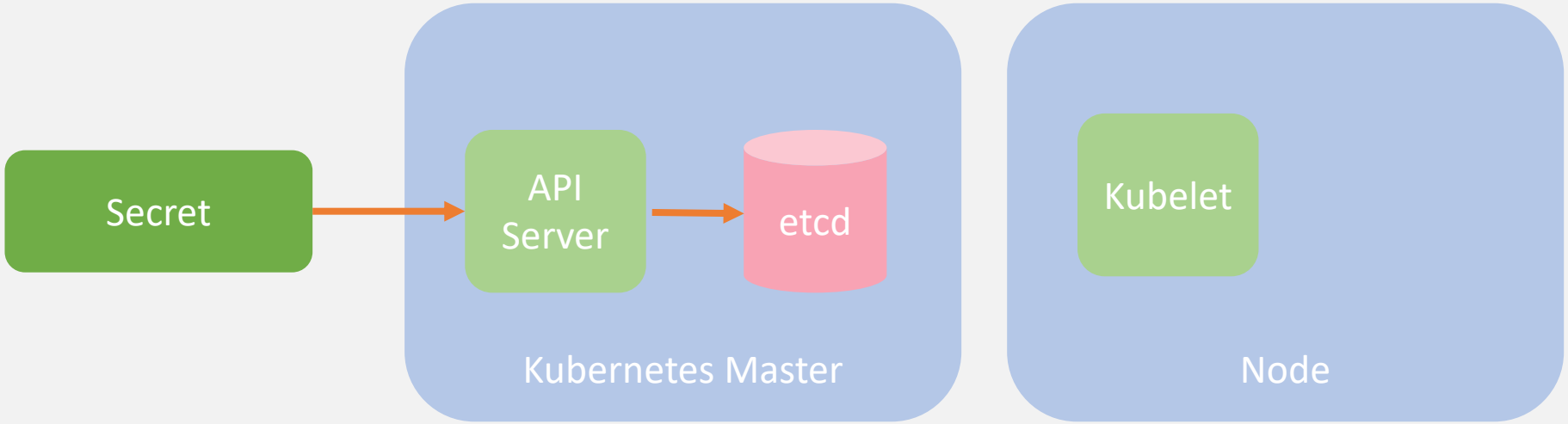
https://kubernetes.io/docs/concepts/overview/components/#etcd

An attacker who can successfully access your cluster database can compromise your entire cluster and have access to your application secrets and cloud resources.


THIS IS FINE.

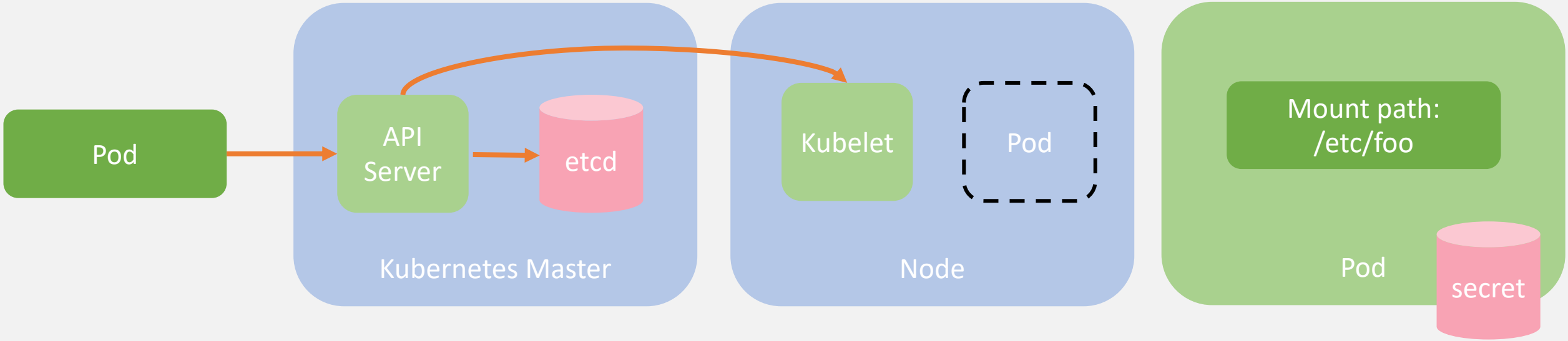
Secrets

kubectl create secret generic secret1



Pod using Secret

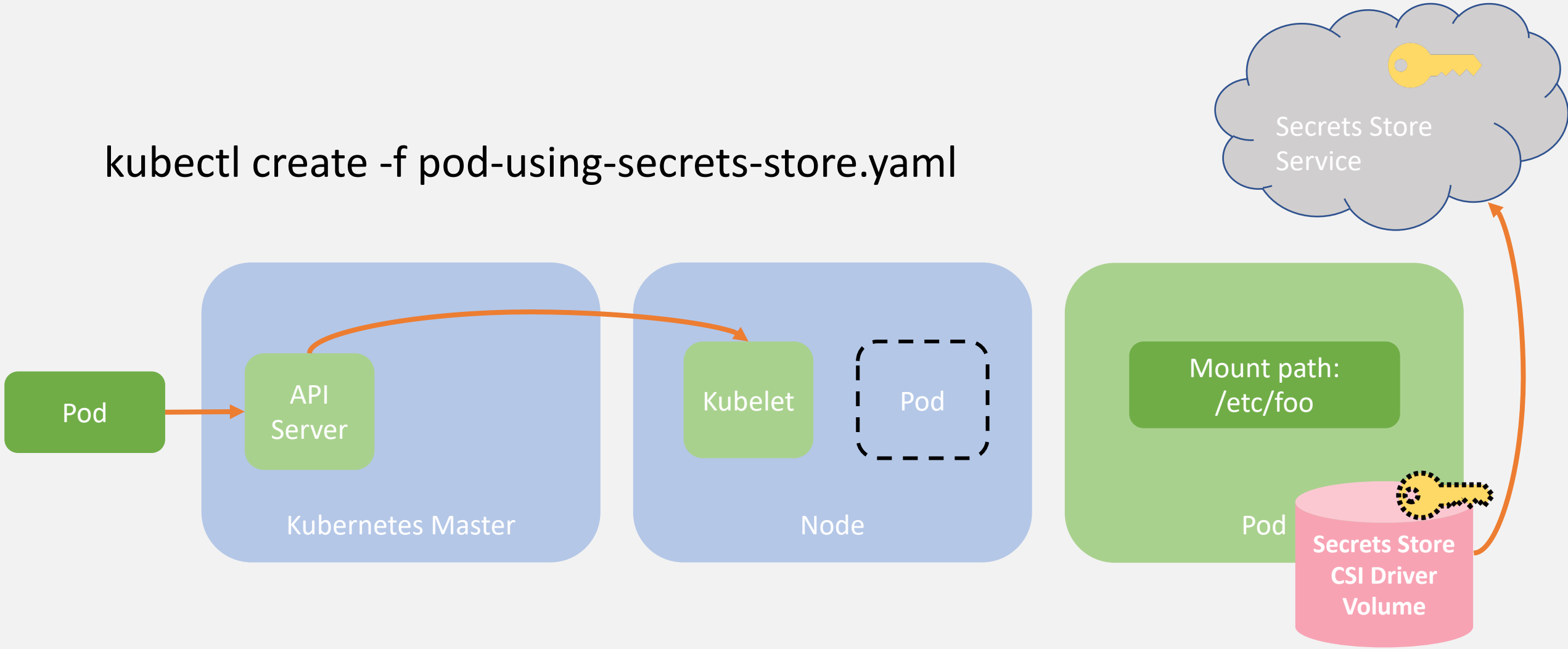
kubectl create -f pod-using-secret.yaml



What if instead of storing my secrets in etcd, I want to store and manage access outside of Kubernetes?

Pod using Secrets Store CSI driver

kubectl create -f pod-using-secrets-store.yaml



https://github.com/deislabs/secrets-store-csi-driver

CSI Inline Volume Implementation #74086

Merged **k8s-ci-robot** merged 3 commits into `kubernetes:master` from `vladimirvivien:csi-inline-volume-api` o

Conversation 179 Commits 3 Checks 0 Files changed 42

vladimirvivien commented on Feb 14 • edited ▾ Member

/kind api-change
/kind feature

What this PR does / why we need it:
This PR only implements the API and Kubelet/Driver changes for CSI inline volume.

See also

- KEP - CSI Inline Volume
- Feature - kubernetes/enhancements#596

Old PRs (for historical context)
#67452, #68232

Release note:

```
Alpha support for ephemeral CSI inline volumes that are embedded in pod specs.
```

/SIG storage

secrets-store.csi.k8s.com Driver Parameters

EDITOR

```yaml
kind: Pod
apiVersion: v1
metadata:
  name: nginx-secrets-store-inline
spec:
  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.com
        readOnly: true
        volumeAttributes:
          providerName: "azure"
          usePodIdentity: "false"         # [OPTIONAL] if not provided, will default to "false"
          keyvaultName: ""                # the name of the KeyVault
          objects:  |
            array:
              - |
                objectName: secret1
                objectType: secret        # object types: secret, key or cert
                objectVersion: ""         # [OPTIONAL] object versions, default to latest if empty
              - |
                objectName: key1
                objectType: key
                objectVersion: ""
          resourceGroup: ""               # the resource group of the KeyVault
          subscriptionId: ""              # the subscription ID of the KeyVault
          tenantId: ""                    # the tenant ID of the KeyVault
        nodePublishSecretRef:
          name: secrets-store-creds
```

Prerequisites for Secrets Store CSI Driver

- Minimum system requirements
  - Kubernetes v1.13.0+
  - CSI interface 1.0.0-rc2
- Inline ephemeral volume
  - Kubernetes v1.15.0-alpha.2+
  - Feature-gates
    - CSIInlineVolume=true

Demo: Secrets Store CSI driver

https://github.com/deislabs/secrets-store-csi-driver

With the Kubernetes Secrets Store CSI driver, we can store and retrieve secrets from a Secrets store and mount the data as a volume to containers.

Provider interface

- Backend plumbing to access objects from the external secrets store
- Conforms to the current API
- Callback mechanism to mount objects to a target path

EDITOR

```
// Provider contains the methods required to implement a Secrets Store CSI Driver provider.
type Provider interface {
    // MountSecretsStoreObjectContent mounts content of the secrets store object to target path
    MountSecretsStoreObjectContent(
        ctx context.Context,
        attrib map[string]string,
        secrets map[string]string,
        targetPath string,
        permission os.FileMode
        ) error
}
```

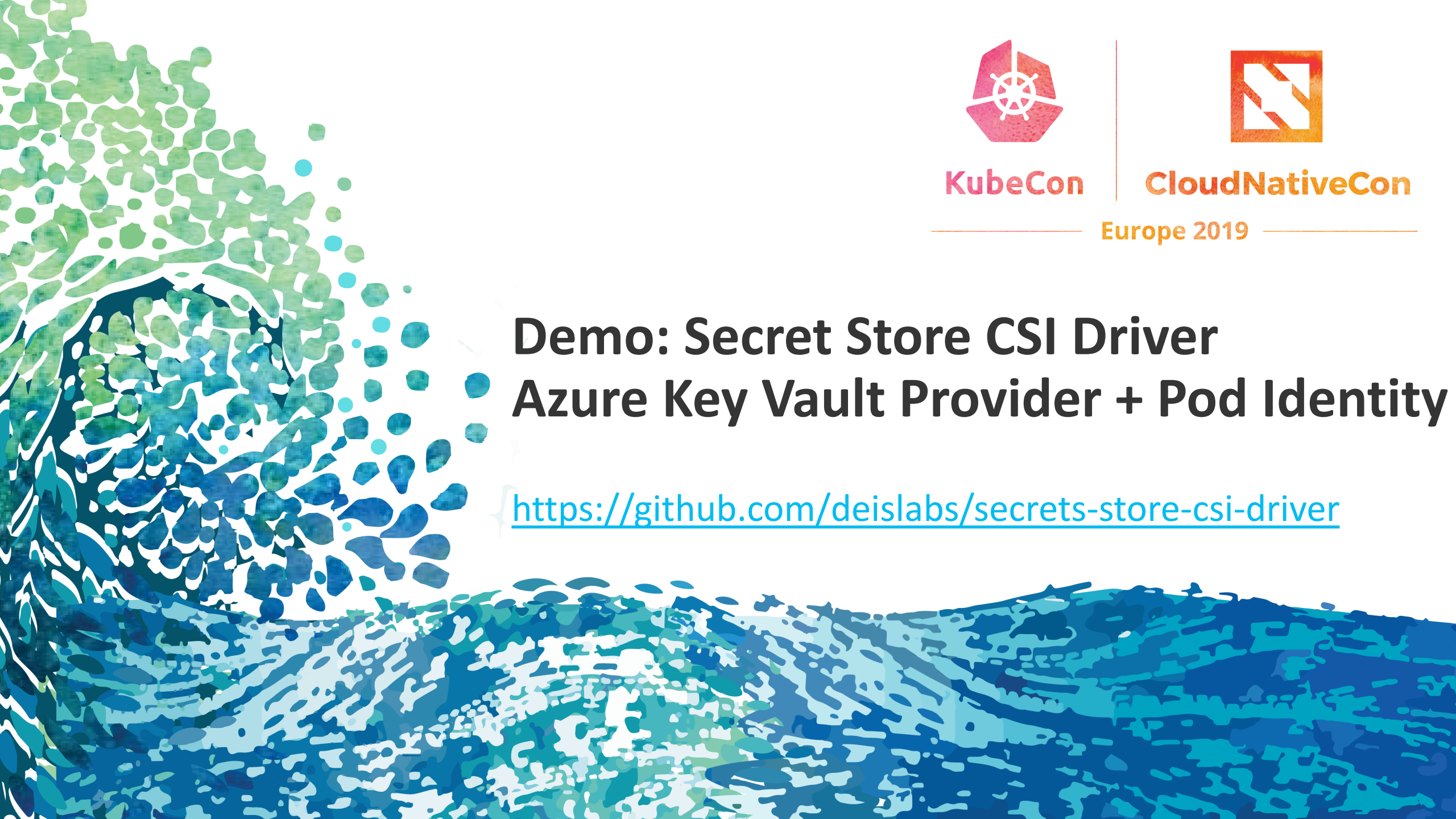
KubeCon | CloudNativeCon Europe 2019

Vault

Demo: Secret Store CSI Driver HashiCorp Vault Provider

https://github.com/deislabs/secrets-store-csi-driver

What if I want to restrict specific pods access to my secrets store?



Demo: Secret Store CSI Driver
Azure Key Vault Provider + Pod Identity

https://github.com/deislabs/secrets-store-csi-driver

With Azure Active Directory Pod Identity, we can restrict and enable specific pods access to Azure Key Vault instance based on the pod’s identity.

Project Status

- Provider Status
  - Azure Key Vault - alpha
  - HashiCorp Vault - alpha
- Come help!
    - Issues
    - Feedback
    - User stories
    - Development

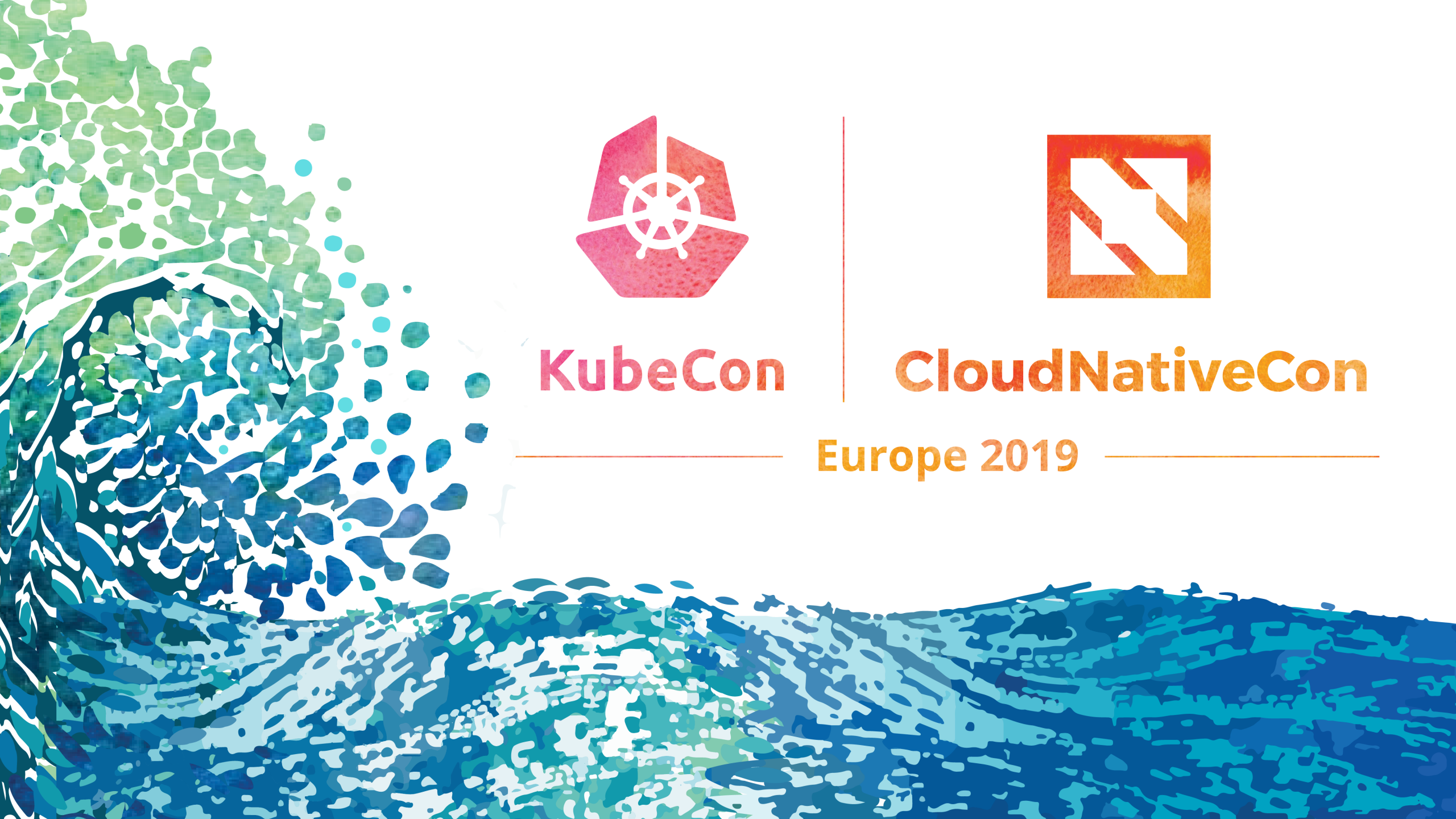
More features!

- More providers
- Pod identity for more providers
- Option to sync to k8s secrets?

Resources

- Secrets-Store-CSI driver: https://github.com/deislabs/secrets-store-csi-driver
  - Azure key vault provider: https://github.com/deislabs/secrets-store-csi-driver/tree/master/pkg/providers/azure
  - HashiCorp Vault Provider: https://github.com/deislabs/secrets-store-csi-driver/tree/master/pkg/providers/vault
- AAD Pod Identity: https://github.com/Azure/aad-pod-identity
- Kubernetes Key Vault FlexVolume: https://github.com/Azure/kubernetes-keyvault-flexvol


KubeCon
CloudNativeCon
Europe 2019
Thanks!
Questions?
@anubhavm @ritazzhang


KubeCon
CloudNativeCon
Europe 2019