

Create the reviewer service account

First of we need to create service accounts and rolebinding so that infisical can sync and update into our k8s.

1. Obtaining the token reviewer JWT for Infisical (infisical-reviewer-service-account.yaml)

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: infisical-token-reviewer
  namespace: default
```

```
kubectl apply -f infisical-reviewer-service-account.yaml
```

1.2 Bind the reviewer service account (infisical-reviewer-cluster-role-binding.yaml)

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: infisical-token-reviewer-role-binding
  namespace: default
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: system:auth-delegator
subjects:
  - kind: ServiceAccount
    name: infisical-token-reviewer
    namespace: default
```

```
kubectl apply -f infisical-reviewer-cluster-role-binding.yaml
```

1.3 Next, create a long-lived service account JWT token (service-account-reviewer-token.yaml)

```
apiVersion: v1
kind: Secret
type: kubernetes.io/service-account-token
metadata:
  name: infisical-token-reviewer-token
  annotations:
    kubernetes.io/service-account.name: "infisical-token-reviewer"
```

```
kubectl apply -f service-account-reviewer-token.yaml
```

1.4 Link the secret in step 1.3 to the service account in step 1.1

```
kubectl patch serviceaccount infisical-token-reviewer -p '{"secrets": [{"name": "infisical-token-reviewer-token"}]}' -n default
```

1.5 Finally, retrieve the token reviewer JWT token from the secret.

```
kubectl get secret infisical-token-reviewer-token -n default -o=jsonpath='{.data.token}' |
base64 --decode
```

<https://infisical.com/docs/integrations/platforms/kubernetes/infisical-secret-crd#manual-long-lived-service-account-tokens>

And then expand authentication.kubernetesAuth.

Revision #7

Created 1 November 2025 14:35:39 by Admin

Updated 12 November 2025 13:03:34 by Admin