Container service account

> **Info**
>
> ID: MS-TA9016
> Tactic: Credential Access, Lateral Movement, Persistence
> MITRE technique: T1528

Service account (SA) represents an application identity in Kubernetes. By default, a Service Account access token is mounted to every created pod in the cluster and containers in the pod can send requests to the Kubernetes API server using the Service Account credentials. Attackers who get access to a pod can access the Service Account token (located in `/var/run/secrets/kubernetes.io/serviceaccount/token`) and perform actions in the cluster, according to the Service Account permissions. If RBAC is not enabled, the Service Account has unlimited permissions in the cluster. If RBAC is enabled, its permissions are determined by the RoleBindings \ ClusterRoleBindings that are associated with it.

An attacker which get access to the Service Account token can also authenticate and access the Kubernetes API server from outside the cluster and maintain access to the cluster.

Mitigations

ID	Mitigation	Description
MS-M9025	Disable Service Account Auto Mount	Disable service account auto mount.
MS-M9003	Adhere to least-privilege principle	Configure the Kubernetes RBAC such that each service account will have the minimal necessary permissions for the application's functionality.