# TTP Detail – T1098.006

## TTP Information

Name: Additional Container Cluster Roles

Description: An adversary may add additional roles or permissions to an adversary-controlled user or service account to maintain persistent access to a container orchestration system. For example, an adversary with sufficient permissions may create a RoleBinding or a ClusterRoleBinding to bind a Role or ClusterRole to a Kubernetes account.(Citation: Kubernetes RBAC)(Citation: Aquasec Kubernetes Attack 2023) Where attribute-based access control (ABAC) is in use, an adversary with sufficient permissions may modify a Kubernetes ABAC policy to give the target account additional permissions.(Citation: Kuberentes ABAC)

This account modification may immediately follow [Create Account](https://attack.mitre.org/techniques/T1136) or other malicious account activity. Adversaries may also modify existing [Valid Accounts](https://attack.mitre.org/techniques/T1078) that they have compromised.

Note that where container orchestration systems are deployed in cloud environments, as with Google Kubernetes Engine, Amazon Elastic Kubernetes Service, and Azure Kubernetes Service, cloud-based role-based access control (RBAC) assignments or ABAC policies can often be used in place of or in addition to local permission assignments.(Citation: Google Cloud Kubernetes IAM)(Citation: AWS EKS IAM Roles for Service Accounts)(Citation: Microsoft Azure Kubernetes Service Service Accounts) In these cases, this technique may be used in conjunction with [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation