# TTP Detail – T1136.003

## TTP Information

Name: Cloud Account

Description: Adversaries may create a cloud account to maintain access to victim systems. With a sufficient level of access, such accounts may be used to establish secondary credentialed access that does not require persistent remote access tools to be deployed on the system.(Citation: Microsoft O365 Admin Roles)(Citation: Microsoft Support O365 Add Another Admin, October 2019)(Citation: AWS Create IAM User)(Citation: GCP Create Cloud Identity Users)(Citation: Microsoft Azure AD Users)  
  
In addition to user accounts, cloud accounts may be associated with services. Cloud providers handle the concept of service accounts in different ways. In Azure, service accounts include service principals and managed identities, which can be linked to various resources such as OAuth applications, serverless functions, and virtual machines in order to grant those resources permissions to perform various activities in the environment.(Citation: Microsoft Entra ID Service Principals) In GCP, service accounts can also be linked to specific resources, as well as be impersonated by other accounts for [Temporary Elevated Cloud Access](https://attack.mitre.org/techniques/T1548/005).(Citation: GCP Service Accounts) While AWS has no specific concept of service accounts, resources can be directly granted permission to assume roles.(Citation: AWS Instance Profiles)(Citation: AWS Lambda Execution Role)  
  
Adversaries may create accounts that only have access to specific cloud services, which can reduce the chance of detection.  
  
Once an adversary has created a cloud account, they can then manipulate that account to ensure persistence and allow access to additional resources - for example, by adding [Additional Cloud Credentials](https://attack.mitre.org/techniques/T1098/001) or assigning [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003).

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

## Tools

* AADInternals

## APTs (Intrusion Sets)

* APT29
* LAPSUS$