# TTP Detail – T1578.001

## TTP Information

Name: Create Snapshot

Description: An adversary may create a snapshot or data backup within a cloud account to evade defenses. A snapshot is a point-in-time copy of an existing cloud compute component such as a virtual machine (VM), virtual hard drive, or volume. An adversary may leverage permissions to create a snapshot in order to bypass restrictions that prevent access to existing compute service infrastructure, unlike in [Revert Cloud Instance](https://attack.mitre.org/techniques/T1578/004) where an adversary may revert to a snapshot to evade detection and remove evidence of their presence.

An adversary may [Create Cloud Instance](https://attack.mitre.org/techniques/T1578/002), mount one or more created snapshots to that instance, and then apply a policy that allows the adversary access to the created instance, such as a firewall policy that allows them inbound and outbound SSH access.(Citation: Mandiant M-Trends 2020)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Tools

* Pacu