# TTP Detail – T1651

## TTP Information

Name: Cloud Administration Command

Description: Adversaries may abuse cloud management services to execute commands within virtual machines. Resources such as AWS Systems Manager, Azure RunCommand, and Runbooks allow users to remotely run scripts in virtual machines by leveraging installed virtual machine agents. (Citation: AWS Systems Manager Run Command)(Citation: Microsoft Run Command)

If an adversary gains administrative access to a cloud environment, they may be able to abuse cloud management services to execute commands in the environment’s virtual machines. Additionally, an adversary that compromises a service provider or delegated administrator account may similarly be able to leverage a [Trusted Relationship](https://attack.mitre.org/techniques/T1199) to execute commands in connected virtual machines.(Citation: MSTIC Nobelium Oct 2021)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Tools

* AADInternals
* Pacu

## APTs (Intrusion Sets)

* APT29