# TTP Detail – T1069.003

## TTP Information

Name: Cloud Groups

Description: Adversaries may attempt to find cloud groups and permission settings. The knowledge of cloud permission groups can help adversaries determine the particular roles of users and groups within an environment, as well as which users are associated with a particular group.

With authenticated access there are several tools that can be used to find permissions groups. The <code>Get-MsolRole</code> PowerShell cmdlet can be used to obtain roles and permissions groups for Exchange and Office 365 accounts (Citation: Microsoft Msolrole)(Citation: GitHub Raindance).

Azure CLI (AZ CLI) and the Google Cloud Identity Provider API also provide interfaces to obtain permissions groups. The command <code>az ad user get-member-groups</code> will list groups associated to a user account for Azure while the API endpoint <code>GET https://cloudidentity.googleapis.com/v1/groups</code> lists group resources available to a user for Google.(Citation: Microsoft AZ CLI)(Citation: Black Hills Red Teaming MS AD Azure, 2018)(Citation: Google Cloud Identity API Documentation) In AWS, the commands `ListRolePolicies` and `ListAttachedRolePolicies` allow users to enumerate the policies attached to a role.(Citation: Palo Alto Unit 42 Compromised Cloud Compute Credentials 2022)

Adversaries may attempt to list ACLs for objects to determine the owner and other accounts with access to the object, for example, via the AWS <code>GetBucketAcl</code> API (Citation: AWS Get Bucket ACL). Using this information an adversary can target accounts with permissions to a given object or leverage accounts they have already compromised to access the object.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Tools

* AADInternals
* Pacu
* ROADTools