Permission Groups Discovery: Cloud Groups, Sub-technique T1069.003 - Enterprise

Archived: 2026-04-05 14:10:04 UTC

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 `Get-MsolRole` PowerShell cmdlet can be used to obtain roles and permissions groups for Exchange and Office 365 accounts [1] [2].

Azure CLI (AZ CLI) and the Google Cloud Identity Provider API also provide interfaces to obtain permissions groups. The command `az ad user get-member-groups` will list groups associated to a user account for Azure while the API endpoint `GET https://cloudidentity.googleapis.com/v1/groups` lists group resources available to a user for Google.[3][4][5] In AWS, the commands `ListRolePolicies` and `ListAttachedRolePolicies` allow users to enumerate the policies attached to a role.[6]

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 `GetBucketAcl` API [7]. 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.

Source: https://attack.mitre.org/techniques/T1069/003