Mohammadamin Sheikhtaheri March 29, 2020
0930853

Cloud IAM Comparison Report

All of the major platforms such as AWS, Azure, and Google Cloud, have the same core IAM platform directory, which provides the users accessing the cloud means of authentication. In terms of applying the permissions to access resources, each major cloud platform has its own way of accomplishing this. AWS is the most flexible when it comes to the method of granting or revoking access compared to Azure and Google Cloud, this is due to the fact that AWS is the oldest and most mature cloud platform.

Using AWS, you can create various policies, which have the ability to access which may be highly specific (ex. Reading from a single topic in SNS), or general such as giving full access to all resource types (ex. Such as predefined “AdministratorAccess” policy). AWS provides its users with predefined policies, as well as the option for them to create their own custom policies. These policies can be directly assigned to individuals, groups, or to roles. Roles are basically objects that act as abstraction layers between policies and accounts.

GCP’s concept revolves around projects. Each project has its own IAM configuration, which is very similar to the way GCP handles billing. All IAM permissions apply to all the resources that are within the specific project that they are assigned to. Due to this, an organization will typically make a GCP project for every application or initiative, so that resources are all related. Similar to AWS, GCP also provides its users with the ability to create and define custom roles that can be assigned to users and groups.

Azure’s IAM also has a unique way of assigning permissions that fall somewhere between GCP and AWS in terms of how flexible it is. Azure provides quite a few “standard roles” which essentially assign permissions to various resources, the most common roles being contributor and owner. Contributor allows anything to be done to the resources within your scope, and owner lets you change the permissions to those resources. In Azure, the levels are: the entire subscription which allows access to all resource groups; to an individual resource group, or to individual resources. The resource groups are unique to Azure and personally, the resource groups are difficult to understand, but they are quite useful once you wrap your head around them.

Although I do not have much experience with Google's cloud services, I do have experience with AWS and Azure. Personally, I prefer AWS's IAM configuration and model to be much easier to understand and to actually put to use. Setting up permissions for the various parts of my projects, both AWS and Azure were decently easy to configure IAMs. However, I believe Azure in general is more difficult to understand than AWS, but where Azure loses in simplicity, it shines in efficiency and speed.

In conclusion, all of the IAM solutions that are provided by the major cloud services AWS, Azure, and GCP have slightly different approaches. However, they all address the needs of organizing any workloads by any organization, no matter how big or how small the group is.

REFERENCES:

- https://www.twistlock.com/2018/09/25/iam-roundup-aws-vs-azure-vs-gcp/
- https://medium.com/@jaychapel/cloud-user-management-comparison-aws-vs-azure-vs-gcp-vs-alibaba-cloud-1035fb1ab6ef
- https://www.computerworld.com/article/3429365/aws-vs-azure-vs-google-whats-the-best-cloud-platform-for-enterprise.html