CIS 4030 - A3 Part #2

Comparing IAM systems on AWS, Azure, and Google Cloud

By: Loui Zibdawi

Overview

Identity and access management systems are a framework for the managing of digital identities, or people. Basic functions of an identity and access management system include:

- Allowing administrators to create roles with specific actions disabled and enabled
- Provide a centralized directory service with oversight as well as visibility into the company user base
- Identifying individuals in a system and giving them roles
- Creating groups of individuals or users that have shared roles
- Managing the addition, updating or removal of users and their roles in the system
- Protecting sensitive data in the system by only allowing it to be available users with the proper security clearance

I will be comparing the identity and access management systems of AWS, Azure and Google Cloud.

AWS

Amazon Web Services - IAM

The main functionality that AWS identity and access management allows for include:

- Shared access
    - With IAM you are able to give multiple people access to your AWS account
- Customized roles
    - IAM allows administrators to create custom roles with the ability to perform specific actions across AWS resources (Ex. The ability to upload to S3)
- Distributed permissions

    - IAM allows for unique permissions to be set for different people for different resources. This allows one user to have varying roles across key resources such as S3, EC2 and dynamoDB.
- Multi-factor authentication (MFA)
    - Can require 2FA for all users

Amazon Web Services - Directory Service

This AWS resource allows for integration with Microsoft Directory Service. The main advantages of this include:

- Centralized user/role management
- Integration of microsoft products (E.g. My SQL apps, sharepoint, etc) with AWS EC2 products.
- Single sign-on across products

Amazon Web Services - Organizations

AWS organizations allow for the functionality of IAM to be shared across multiple AWS organizations. This allows for large organizations to manage their user base across their many applications and products.

Azure

Azure - Role-based access control

Azure RBAC allows administration to control who has access to Azure resources as well as the actions they are permitted to do within those resources. RBAC is a simplified version of AWS IAM with only roles being considered.

Azure - Active Directory

Azure Active Directory is their solution to control a directory of users across your application with functionality to allow for things such as single log in, multi factor authentication, etc.

Azure - Active Directory B2C

Azure business-to-consumer (B2C) allows for the managing roles in customer-facing applications. This allows creators of applications to create user groups and customize their individual or group roles. Differing from Azure RBAC, this solution allows for the managing of customer roles and also allows for integration with Azure Active Directory.

Azure - Active Directory Connect

Azure Directory Connect is azure's integration solution for Microsoft Directory Service. Similar to AWS Directory Service it allows for centralized user/role management, integration of microsoft products (E.g. My SQL apps, sharepoint, etc) and single sign-on across products

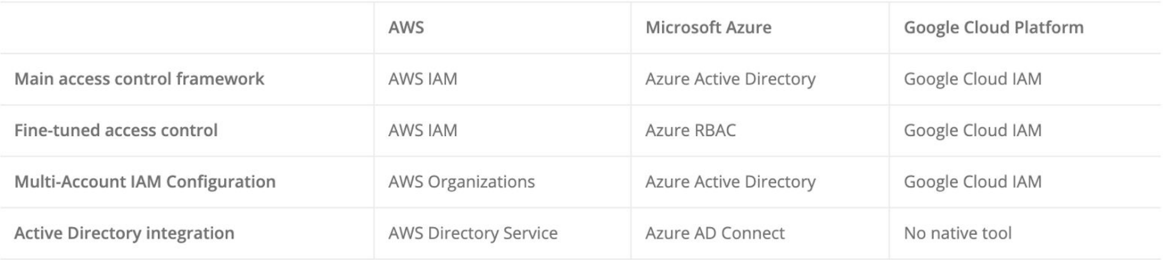
Google Cloud

Google Cloud - IAM

Google Cloud IAM provides one central resource that allows a majority of the functionality of Azure and AWS, and the main difference is that they discourage integration with Microsoft Active Directory and even do not support it. Another difference is the use of a single resource, unlike its counterparts (AWS having IAM and Directory Service and Azure having RBAC, AD, AD-B2C and AD Connect).

Comparison

A summary of the resources of AWS, Azure and Google Cloud for functionality related to IAM are outlined in the table below.



	AWS	Microsoft Azure	Google Cloud Platform
Main access control framework	AWS IAM	Azure Active Directory	Google Cloud IAM
Fine-tuned access control	AWS IAM	Azure RBAC	Google Cloud IAM
Multi-Account IAM Configuration	AWS Organizations	Azure Active Directory	Google Cloud IAM
Active Directory integration	AWS Directory Service	Azure AD Connect	No native tool

In 2018, the cloud computing market was led by Amazon Web Services, occupying 32.3% of the market share worth $7.3 billion, Microsoft Azure behind with 16.5% of the market share worth $3.7 billion and Google Cloud in 3rd with 9.5% market share worth $2.2 billion.

Conclusion

In my personal opinion it seems that AWS is the best IAM provider as it focuses heavily on integration across its many, extremely popular resources. It provides abilities comparable to each of its counterparts and it is growing at the fastest rate as a company. Azure would be my 2nd selection as it has the Microsoft Active Directory asset within the company and would provide the fastest integration with it's many existing users. The last IAM service I would go with is Google Cloud seeing as it is just not as popular and refuses to integrate with Microsoft Active Directory to expand its usability.