	Bansilal Ramnath Agarwal Charitable Trust's Vishwakarma Institute of Information Technology **Department of Artificial Intelligence and Data Science**	
Name: Netal Prakash Daga		
Class: TY	Division: A	Roll No: 371016
Semester: V	Academic Year:2022-2023	
Subject Name & Code: Cloud Computing and Analytics		
Title of Assignment: Study and implementation of Identity Management.		
Date of Performance: 28/08/2022	Date of Submission: 01/12/2022	

Aim: Study and implementation of Identity Management.

Problem Statement: Study and implementation of Identity Management.

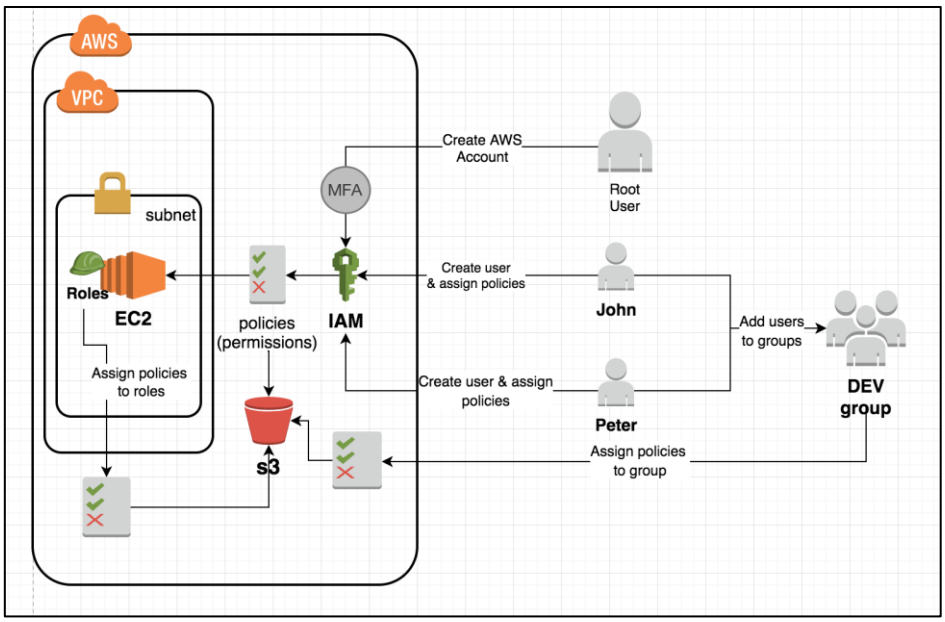
Background Information:

- **Identity and Access Management (IAM)** manages Amazon Web Services (AWS) users and their access to AWS accounts and services.
- It controls the level of access a user can have over an AWS account & set user, grant permission and allows a user to use different features of AWS account. Identity and access management is mostly used to manage users, groups, roles and Access polices
- The account we created to sign in Amazon web services is knows as root account and it holds all the administrative rights and has access to all parts of the account. The new user created in AWS account, by default they have no access to any services in the account & it is done with the help of IAM that the root account holder can implement access polices and grant permission to the user to access certain services.

Features of IAM:

- **Shared Access to your Account:** A team of people who are working for a project together can easily share resources with the help of the shared access feature.
- **Free of cost:** IAM feature of Aws account is free to use & charges are added only when you access other Amazon web services using IAM user.
- **Have Centralized control over your Aws account:** Any new creation of user, groups or any form of cancellation that takes places in Aws account is controlled by you and have the control over what & how data can be accessed by the user.

- **Grant permission to the user:** As root account holds of the administrative rights, user will be granted permission to Access certain services by IAM.
- **Multifactor Authentication:** Additional layer of security implemented on your account by third party, a six-digit number which you have to put along with your password when you log into your accounts.

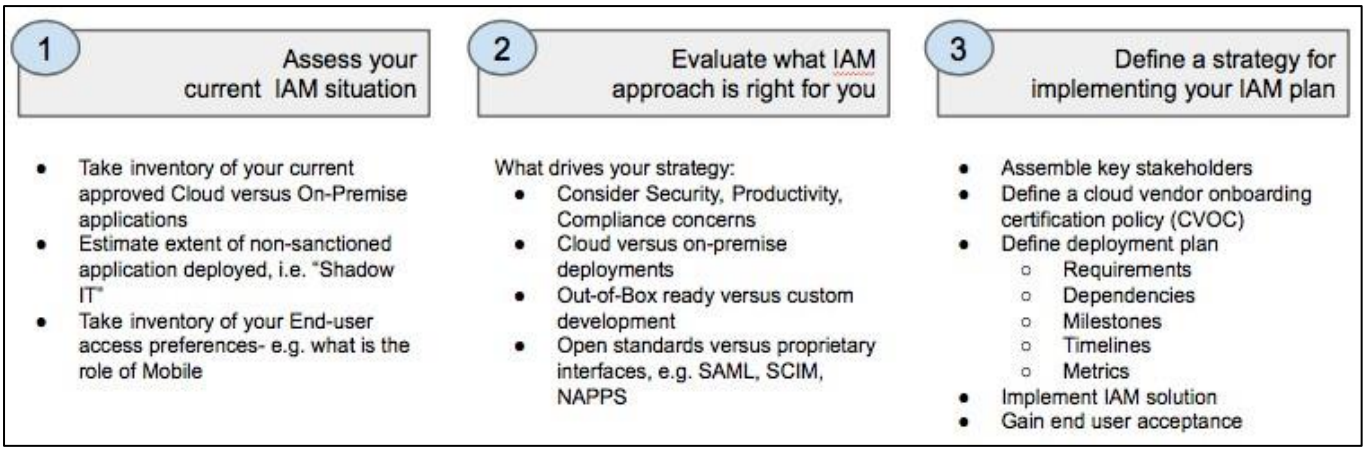


Cloud Resource Requirements: AWS Console

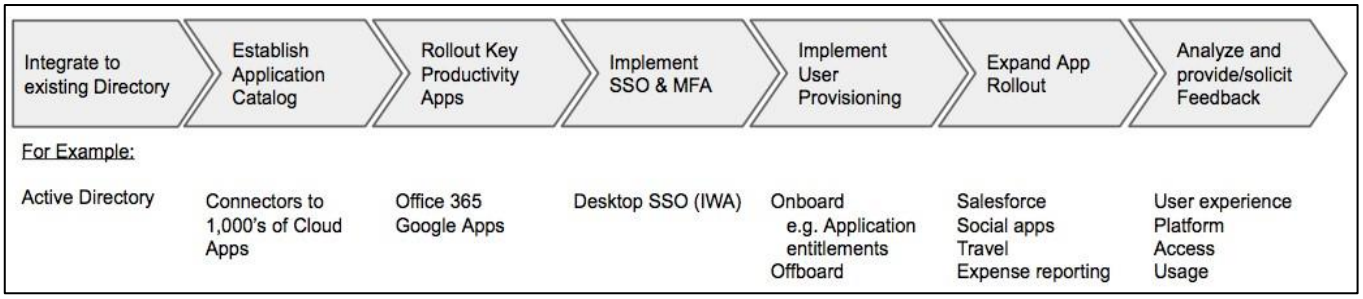
Steps:

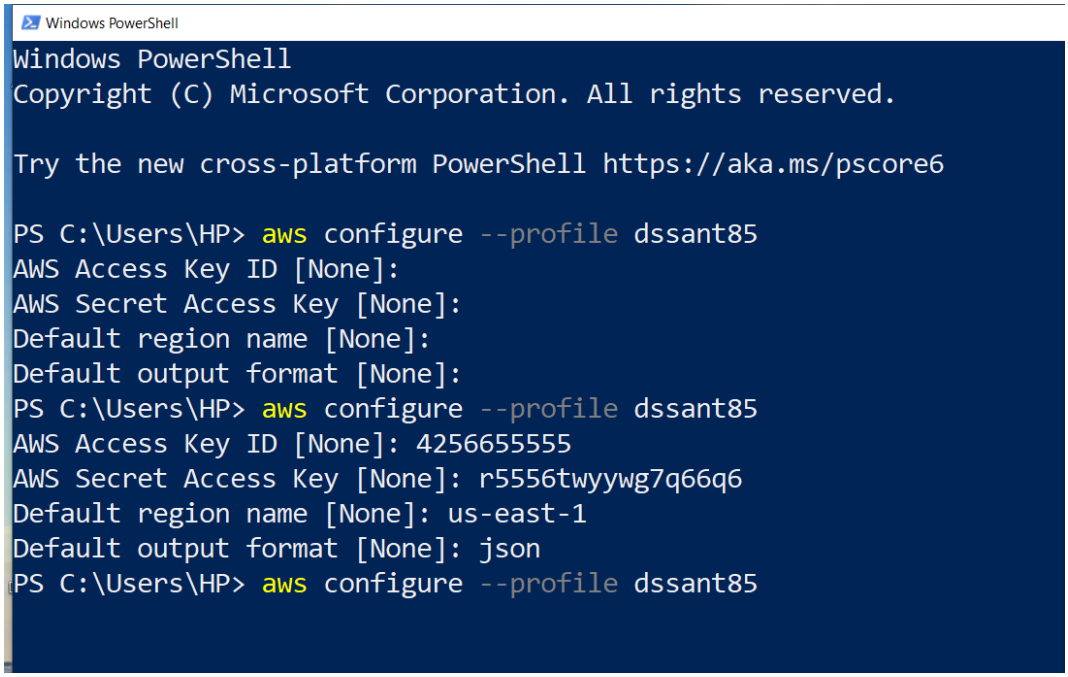
Step 1] Assess your current IAM situation.

Step 2] Evaluate what IAM approach is right for you: Factors need to considered are direct integration, vendor practices, cost factors.



Step 3] Define a strategy for implementing your IAM plan: The key to a successful implementation includes engaging the right stakeholders early, driving toward achievable milestones supporting early successes, and then expanding the reach and scope of your solution. Stakeholders might include representatives from your IAM, Network, Compliance and Human Resource teams.





Conclusion:

Identity and Access management authenticates the user by verifying the user that they are who they say they are. IAM cloud identity tools are more secured and flexible, it gives permission only to the appropriate level of access, instead of accessing through the username and password.