

## Bansilal Ramnath Agarwal Charitable Trust's Vishwakarma Institute of Information Technology

# Department of Artificial Intelligence and Data Science

Student Name: Vidhyapati Umesh Shelke

Class: TY Division: A Roll No: 371069

Semester: 5<sup>th</sup> Academic Year: 2022-23

Subject Name & Code: Cloud Computing

Title of Assignment: Assignment 4: Study and implementation of Identity

Management.

Date of Performance: 5/12/2022 Date of Submission: 6/12/2022

Aim: Study of Cloud Computing & Architecture.

Problem Statement: Study of Cloud Computing & Architecture.

Software Requirements: AWS Console

#### **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.

#### 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.





Evaluate what IAM approach is right for you

3 Define a strategy for implementing your IAM plan

- Take inventory of your current approved Cloud versus On-Premise applications
- Estimate extent of non-sanctioned application deployed, i.e. "Shadow IT"
- Take inventory of your End-user access preferences- e.g. what is the role of Mobile
- What drives your strategy:
  - Consider Security, Productivity, Compliance concerns
  - Cloud versus on-premise deployments
  - Out-of-Box ready versus custom development
  - Open standards versus proprietary interfaces, e.g. SAML, SCIM, NAPPS
- Assemble key stakeholders
- Define a cloud vendor onboarding certification policy (CVOC)
- Define deployment plan
  - Requirements
  - Dependencies
  - Milestones
  - Timelines
  - Metrics
- Implement IAM solution
- Gain end user acceptance

**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.

Integrate to existing Directory

Establish Application Catalog Rollout Key Productivity Apps

Implement SSO & MFA Implement User Provisioning

Expand App Rollout Analyze and provide/solicit Feedback

For Example:

Active Directory

Connectors to 1,000's of Cloud Apps Office 365 Google Apps Desktop SSO (IWA)

Onboard e.g. Application entitlements Offboard Salesforce Social apps Travel Expense reporting

User experience Platform Access Usage

```
Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\HP> aws configure --profile dssant85

AWS Access Key ID [None]:

AWS Secret Access Key [None]:

Default region name [None]:

PS C:\Users\HP> aws configure --profile dssant85

AWS Access Key ID [None]: ropefile dssant85

AWS Access Key ID [None]: 4256655555

AWS Secret Access Key [None]: ropefile dssant85

AWS Secret Access Key [None]: ropefile dssant85

Default region name [None]: us-east-1

Default output format [None]: json

PS C:\Users\HP> aws configure --profile dssant85
```

### Github Repo Link:

https://github.com/Vidhyapati/CCA-Assignments

#### 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.