IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

Organize and Supervise Resources in Multi-account of AWS

Israrul Haque[1*], Ashif Ali [2]

[1,2]Dept of Computer Science, Al-Falah University, Faridabad, India

[*]*Corresponding Author: hisrarul@gmail.com, Tel.: +91-9711011556*

DOI: https://doi.org/10.26438/ijcse/v7i8.260262 | Available online at: www.ijcseonline.org

Accepted: 10/Aug/2019, Published: 31/Aug/2019

***Abstract*—** Cloud computing is an emerging technology. It allows the customer to run the application by provisioning on-demand resources. There are cloud providers like AWS who allows their customer to provision resources. Customer may provide access to the multiple users to enable them to run their workloads using different services like EC2, S3, RDS, etc. With the help of different services provided by AWS, we can reserve computer power, storage, etc. Amazon Web Services (AWS) allows the customer to assign tags on their resources. The tags also known as metadata can be used to organize and manage resources in cloud computing. Tagging the resources in multiple accounts of AWS cloud computing is subject to errors and additional efforts. Our goal is to design a solution to automatically assign the tag on the resources so that we can easily organize and supervise resources in multi-account of AWS.

***Keywords*—**Cloud Computing, AWS, Resource Tagging

I. INTRODUCTION

Cloud computing [1] offers on-demand compute power, storage, and other IT resources to the customer via the internet. Amazon Web Services (AWS) [2], a leader in cloud computing is widely adopted by global customers. They offer several types of services like compute, storage, analytics, machine learning, etc. AWS lambda [3] is a service which allows you to invoke code and run complex environment without provisioning servers in the backend. The lambda functions can be triggered by a response service when it comes to saving costs in the production environment. We can optimize our solution of tagging [5] multiple resources by using lambda function on a response of an event trigger. Tagging is a set of key and value pair and it acts as metadata. The metadata allows us to manage resources like ec2 instance.

The purpose of this discussion is to allow the customers to tag their resources, automatically created in multiple accounts so that the resources in the cloud can organize properly for different users. With the help of tags on the resources, the cost allocation can be done and according to the usage of the resources, permissions will be granted or revoked. When an IAM user [6] will be creating an ec2 instance in the account, CloudTrail [7] service will be keeping track of API calls. An event rule [8] will be created in the CloudWatch [9] service which will be sending the data from one account to another using event bus [10]. Proper tagging of the resources can be used to anticipate cost allocations and billing report in the automated environment. There are different tagging categories [11] available such as technical tags, tags for automation, security tags and business tags. Some business tags like owner or creator tags can be labeled on the resources such as an ec2 instance to identify who is accountable to answer. When customers wanted to have multiple accounts for maximum billing isolation so it is mandatory to use Multiple Account Strategies [12] and managing them using AWS Organization [13] service. Each resource in all the accounts should be tagged with Owner/Creator in order to do the cost allocation in a well-defined manner.

II. RELATED WORK

Organizing the resources in the AWS account is always a hectic task. It becomes extremely complex when users want to manage resources in multiple accounts. It becomes even more difficult when customer infrastructure starts to grow and they need to create more resources. The metadata needs to add to the resources which can use to filter and find the resources. The metadata is also known as customer-defined key and values which can be added manually. It will be a time-consuming process and prone to errors. When multiple users have access to create resources then it will be a difficult task to add tags for each resource correctly. The process of adding tags can be delayed if the system administrator tries to organize resources manually [14]. It can lead to several problems such as unorganized resources in multiple accounts and wrong prediction of cost allocations etc. The customers

are using either manual ways or a custom script in the individual accounts to manage tags on the resources. We will be working on automated version to manage resources on multiple accounts of AWS.

III. METHODOLOGY

We have to try to build a design a solution which is helping us to tag resources available in the multiple accounts of AWS from a central account automatically.

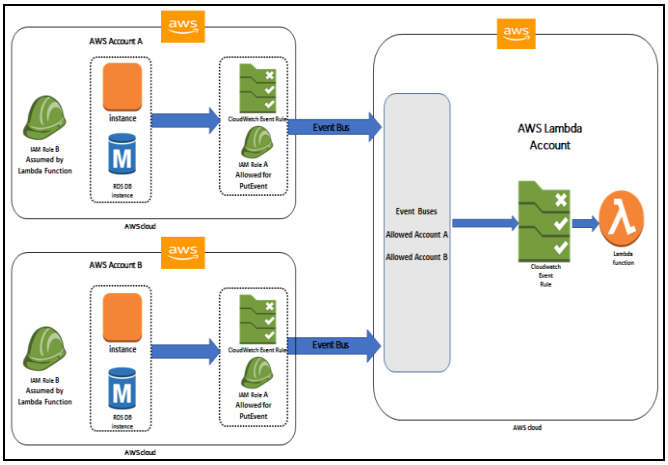

Figure 1. Architecture Diagram of Resource Tagging in Multi-Account Strategy

IV. RESULTS AND DISCUSSION

Figure 1 demonstrates the solution for tagging resources upon their creation in multiple accounts. As shown in the figure, we have implemented three accounts in AWS. On account A and B, the users will be having permission to create resources. We have a 3rd account in AWS is being referred to as Lambda account. In Lambda account, we have deployed our lambda function. Tagging of resources can also be done by provisioning different lambda functions in each account, but it will be difficult to manage each lambda function. If we required to update the functionality of the lambda function, then system administrator may take significant amounts of time which can lead to delays. It will also reduce the productivity of sysops team. These days, we follow the multi-account strategy where a customer may use more than 500 accounts. In such cases, it is important to supervise each resource in every account automatically. Let's discuss what all resources are required to build between the cross accounts [15].

As shown in figure 1, the first task is to allow the cross +accounts to send the event data to the Lambda account using an event bus. We need to create an event rule in the Lambda account that should trigger the lambda function. It is important to make sure that event rule trigger the lambda function only on a few occasions only, for example, when users create an ec2 instance in the cross accounts A and B. As we want to restrict the event rules to specific API calls, it is necessary to define the detail-type as "AWS API Call via CloudTrail" [16] in the event rule. To enable the mentioned detail-type, we must enable CloudTrail in all accounts. As soon as, the user creates resources the event rule triggers the target [16]. The targets can be used to process the events, there will be two distinct targets of event rule in the Lambda and A/B accounts. In account A/B, the target will be an event bus whereas lambda function will be targeted in the Lambda account.

Another step towards the accomplishment of this solution is to create an IAM role [18]. In Lambda account, we need to create an IAM role, which will be having permissions write logs in the CloudWatch and also permissions to assume a role available in account A and B. Here, we need to provide the permission to IAM role in account A and B to tag the resources.

As shown in Figure 1, the last step is to create a lambda function in the Lambda account. The lambda function will be invoked in every response of events, send by the CloudWatch event rule. In this lambda function, we have to define a role which can be assumed. For troubleshooting purposes, we can use CloudWatch Log groups [19] and stores the log events.

.

V. CONCLUSION AND FUTURE SCOPE

After deployment of this architect design on a multi-account approach, we can automatically tag the resource with customer-defined metadata. These metadata will allow us to manage resources. There is a limitation with respect to the time when we try to send event data from one to another account so it takes the time of 60-120 seconds. Future scopes to provide the event data instantly so that run time solution can be provided and set the budget amount for the users.

REFERENCES

[1]. https://docs.aws.amazon.com/whitepapers/latest/aws-verview/what-is-cloud-computing.html
[2]. https://docs.aws.amazon.com/whitepapers/latest/aws-overview/introduction.html
[3]. https://aws.amazon.com/lambda/
[4]. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html
[5]. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html
[6]. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html
[7]. https://aws.amazon.com/cloudtrail/
[8]. https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CWE_GettingStarted.html
[9]. https://aws.amazon.com/cloudwatch/

[10]. https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatchEvents-CrossAccountEventDelivery.html
[11]. https://aws.amazon.com/answers/account-management/aws-tagging-strategies/
[12]. https://aws.amazon.com/answers/account-management/aws-multi-account-billing-strategy/
[13]. https://aws.amazon.com/organizations/
[14]. https://d1.awsstatic.com/whitepapers/aws-tagging-best-practices.pdf
[15]. https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html
[16]. https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/Create-CloudWatch-Events-CloudTrail-Rule.html
[17]. https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html
[18]. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
[19]. https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CloudWatchLogsConcepts.html

Authors Profile

Israrul Haque pursued Bachelor of Computer from Indian Institute of Engineer (IEI) in 2017 and pursing MTech in Computer Science from Al-Falah University. He has expertise in Cloud Computing and overall industry experience is 5 years in AWS, Azure, Google Cloud Computing. Also having experience in latest technologies such as orchestration of containerization.

Ashif Ali pursued B.Tech from Computer Science & engineering in 2008 and M.Tech from Computer Science in 2012 from M.D.U University, Rohtak. He is currently pursuing Ph.D. And currently working as Assistant Professor at Al-Falah University, department of computer science. He is a member of the Indian Science Congress Association and Indian Association of Engineers. He is the editorial board member of IJAIR and IJIRST He has published more than 20 research papers in reputed international journals and conferences His main research work focuses on Big Data Hadoop, Artificial Intelligence and Data Structure. He has an overall 8 years of teaching experience with good exposure to the research field.

