International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I5P104

Volume 69 Issue 5, 22-25, May 2021
© 2021 Seventh Sense Research Group®

Original Article

Amazon Web Services Security Best Practices

Vandana Premkumar[1], Vinil Bhandari[2]

[1]*Technology Architect, New York Stock Exchange, New York City, NY, United States of America.*
[2]*Director of Technology, New York Stock Exchange, New York City, NY, United States of America.*

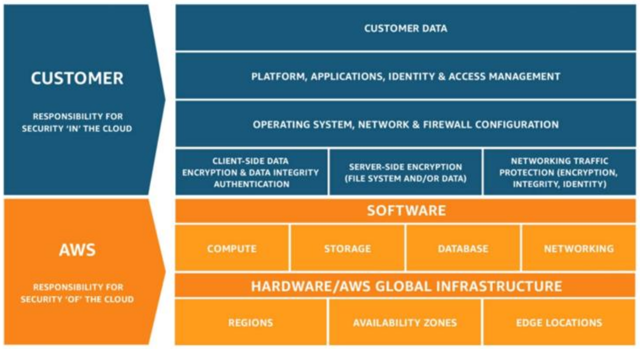
Received Date: 01 April 2021
Revised Date: 17 April 2021
Accepted Date: 08 May 2021

Abstract - *This paper is intended to share best practices that can be incorporated into existing and potential amazon web services infrastructures. These practices will ensure protect your organization's data and assets. In some companies, it is important to track the usage of resources for governance, and this paper will talk about how we can achieve that. Security also includes the topic of compliance which many corporates need to maintain to comply with government regulations.*

Keywords - *Security Best Practices, Authentication and Authorization, Cloud Compliance and Regulation, Identity Access Management, Secure Infrastructure.*

I. INTRODUCTION

AWS functions in a shared responsibility model, which requires AWS and customers to work together towards security objectives. AWS is responsible for protecting the infrastructure that all the services run on. The infrastructure consists of hardware, software, networking, and physical facilities the servers run on. Customer’s responsibility is determined by the service they are opting to use. This includes configurations and settings that will help them keep their assets secure[1].


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

This paper will focus on ten best practices that customers can adopt. These best practices are the latest and greatest and have been spoken in AWS re: Invent 2020 conference[2]. The AWS concepts that will help us cover all the ten best practices are

1. Amazon Simple Storage Service (S3)
2. Federation
3. CloudTrail
4. AWS Athena
5. Virtual Private Cloud (VPC) Subnets
6. AWS Prefix list and Firewall Manager
7. Identity Access Manager (IAM) Publicity
8. VPC endpoint policies
9. Connecting Securely to EC2 Instances
10. Route 53 – DNS Logging

II. AWS S3

Amazon Simple Storage Service is an object storage service with good performance that is scalable and secure. Preventive measures can be taken to mitigate some risks and monitor any data breaches.[3]

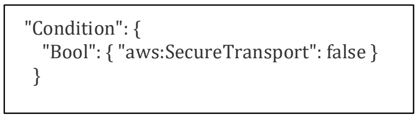
A. Securing Buckets

S3 buckets are created privately by default; we may need some objects to be public. It is best to keep all the objects private and grant access based on usage. Sometimes, you make want to make the bucket public. An object can be made public by combining bucket policies, ACL, and IAM policies. With time, when the application grows, these policies can become convoluted, and it is best to separate the objects into private and public buckets. A single bucket can be created for publicly accessed objects.

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"PublicRead",
      "Effect":"Allow",
      "Principal": "*",
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":["arn:aws:s3:::ijctt-public-s3-bucket/*"]
    }
  ]
}
```

B. Encrypting Data at Rest and Transit

We can encrypt data before storing it in S3 using AWS managed S3 keys or keys created in Key Management System (KMS). We can add in-transit encryption by adding the following condition to the policy



```
"Condition": {
  "Bool": { "aws:SecureTransport": false }
 }
```

C. Setup Lifecycle Policies

In order to ensure unwanted data can no longer be accessed by hackers, we can set up a lifecycle policy on buckets to move old data to the private bucket and delete it if it's no longer needed.

D. S3 Block Public Access

In order to avoid developers from accidentally marking a bucket as public, security admins can block public access.

E. AWS Trusted Advisers

This is a built-in feature that analyzes AWS resources in all your accounts and recommends best practices. Security is one of the aspects they provide recommendations on.

III. AWS FEDERATION

This tip is important for the team that is in charge of the security of the organization. It's a good practice to keep the credentials temporary. This can be possible by using federations. If there is an existing corporate directory, we can synch identities to AWS SSO service in order to map people to different environments. If you do not have an active directory, you could use AWS IAM users and groups to create a pool of users. [4]

IV. CLOUDTRAIL

There are a detective and preventative security best practices in cloud trail.

A. Detective Best Practices

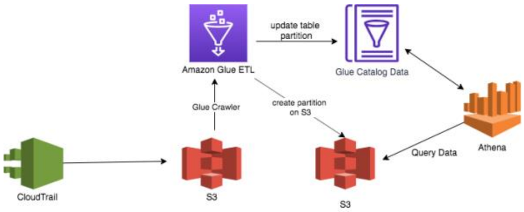
In order to detect any threat, you must create a trail for your AWS account. By default, cloud trial provides 90 days of event history for management events. However, it is not permanent and may not be tracking events that you are interested in. You can create one trail that logs all the management events in all regions and following trails on logs specific to AWS resources like Code Pipeline. A validated log trail is also essential for asserting the log files have not been changed. CloudTrail log integrity uses industry-standard: SHA-256 for hashing and SHA-256 with RSA for digital signing[5]. We can also integrate CloudTrail with CloudWatch logs to monitor and receive alerts. For example, we can track invalid logins to the AWS console using key security and network-related management events.

B. Preventative Best Practices

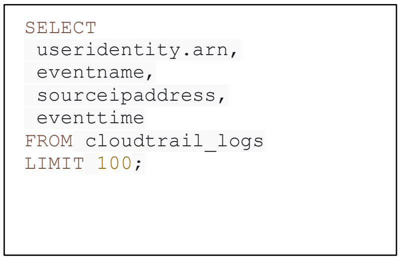
Log CloudTrail logs to a dedicated S3 bucket. This will ensure the integrity, completeness, and availability of these logs during an audit. If you use AWS Organizations, it is best to create a trail to track at the organization level. Logs delivered to S3 are encrypted by AWS using SSE-S3 keys. If you want to manage the security layer, you can use SSE-KMS so that you can create and manage your Keys, also called Customer Master Key (CMK). The buckets that store the logs need to have the least privileged access. This will make sure the logs maintain its integrity for auditing and forensic purposes. We can also enable Multi-Factor Authentication (MFA) Delete to prevent accidental deletes.

V. AWS ATHENA

AWS Athena gives you a fast and cost-effective interactive query service that makes it easy to query petabytes of data in S3 . There are no data warehouses or clusters that need to be managed. We can use this service to query our cloud trail logs. This service uses AWS Glue which is a fully managed ETL tool to extract, transform and load the data into a more readable catalog.



Sample query that can be used as a template[6]



```
SELECT
 useridentity.arn,
 eventname,
 sourceipaddress,
 eventtime
FROM cloudtrail_logs
LIMIT 100;
```

VI. VPC SUBNETS

Companies have Virtual Private Cloud with private and public subnets. Public subnets have access to the internet through an internet gateway. Private subnets have no access to the internet. The public subnet is where you would provision your application load balancer, which the public can access. The database is installed in a private subnet, so it's more secure. These subnets come with id's which are unique. However, these id's are not user-friendly and can get cumbersome to manage in larger organizations. It is a good practice to tag these. IAM policies can be written based on the tags. These tags will also be very handy when VPC is provisioned using infrastructure as code. The number one security tool in VPC is the EC2 security group. VPC is a member of one or more security groups, and these security groups have rules. These include inbound and outbound traffic rules for protocols.

VII. AWS PREFIX-LIST AND FIREWALL MANAGER

In a large organization, there are tools to manage security groups on a scale. One of the relatively new tools is the prefix-list, which was announced in June 2020. A prefix list is a group of CIDR blocks that can be used to configure security groups. VPC allows you to create a prefix list that can be audited and applied across all your accounts. This allows the organization to consistent security posture and routing behavior. [3][7]

AWS Firewall Manager is a higher-level AWS service that is integrated into the organization. It does not require access to a management account to set it up. You can designate an account in an organization called the delegated administrator. This account will manage the firewall manager across the organization. AWS Firewall manager helps [8]

- Protect resources of all resource types like CloudFront distributions, API Gateway REST API, application load balancer, AppSynch GraphQL API. AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests.
- Protect resources with specific tags.
- Allows you to apply security group rules to all members or specific subnets in the AWS organization.
- Subscribe member accounts to AWS Shield Advanced.
- Provide centralized monitoring for DDOS attacks across your organization.

VIII. IAM POLICIES

An intersection of network-based security and authorization-based security is a very powerful combo. IAM Policies help to enforce rules on who can do what and from where. AWS resources can either be accessed by an application or an employee who works for the organization. When an application is accessing the resource, we know exactly which EC2 instance the application is installed in. The EC2 instance belongs to a VPC and subnet. You could lock the resource to have asserted the usage only from this network origin. The employee who is accessing the resource will belong to a corporate VPN. You can also add the rule to have the specific VPN from which the resource is accessible.

IX. VPC ENDPOINT POLICIES

VPC Endpoint policies govern the rules to access AWS services the application connects to. The default access to an endpoint is to allow full access to the service. An endpoint policy does not override or replace IAM policy. For endpoint policies that are applied to gateway endpoints, if you specify Principal in the format "AWS": "AWS-account-ID" or "AWS": "arn:aws:iam::AWS-account-ID: root," access is granted to the account root user only and not all IAM users and roles for the account. [9]

X. CONNECTING TO EC2

Typically we use SSH keys to access EC2 instances. If EC2 is in a public subnet, we can ssh to it using public IP. If it's in a private subnet, we will need a bastian host through which we can ssh to the box. The fact is that private key is outside the world of AWS and not guaranteed to be secure. That's where AWS Systems Manager (SSM) comes into the picture. It makes it easier to connect to EC2 instances easier and more secure. SSM uses API's to connect to EC2 Instances. It no longer needs SSH private keys to connect. The use SSM API, which gets authenticated and authorized against IAM policies.API calls are loged in cloudtrail. The sessions are logged in cloudwatch logs. From a network perspective, the user need not need a direct connection to the EC2 instance, and the EC2 instance runs an SSM agent that has an open tunnel to SSM messages and SSM services. [3]

XI. ROUTE 53 – DNS LOGGING

We can now configure Route 53 to log information of DNS resolving queries. The information that can be logged are domain and subdomain that is requested, DNS records(AAA or A), Endge location that responded to the DNS query, DNS response codes such as NoError or ServFail. These DNS logs are sent to CloudWatch logs. If you don't need detailed DNS logs, we can use CloudWatch metrics to see the total number of DNS queries that Route 53 responded to. Query log example

```
1.0 2020-12-13T08:16:02.130Z Z123412341234 example.com A
NOERROR UDP FRA6 192.168.1.1 -
1.0 2020-12-13T08:15:50.235Z Z123412341234 example.com AAAA
NOERROR TCP IAD12 192.168.3.1 192.168.222.0/24
1.0 2020-12-13T08:16:03.983Z Z123412341234 example.com ANY
NOERROR UDP FRA6 2001:db8::1234 2001:db8:abcd::/48
1.0 2020-12-13T08:15:50.342Z Z123412341234 bad.example.com A
NXDOMAIN UDP IAD12 192.168.3.1 192.168.111.0/24
1.0 2020-12-13T08:16:05.744Z Z123412341234 txt.example.com TXT
NOERROR UDP JFK5 192.168.1.2 -
```

VI. CONCLUSION

AWS provides several tools and configurations to have control and confidence in securing your infrastructure in the cloud. AWS allows you to automate security rules and policies so that you can focus on innovating your business. When you follow AWS core security best practices, you can rest assured that you are maintaining the company requirements of security and compliance, such as data protection, loyalty, and confidentiality.

APPENDIX A

Third-party AWS Security Tools that help secure your assets:[3]

- Security Monkey was developed by Netflix to monitor any changes in AWS policies. It provides an audit on S3 to make sure it is secure.
- Cloud Custodian helps to make sure the best practices are being followed.
- Cloud Mapper was created by Duo Security. This provides a visual representation of AWS infrastructure to enhance the identification of further security issues.

REFERENCES

[1] AWS Shared Responsibility Model, Amazon Web Services, Jan 2021, http://www.amazon.com.

[2] Ten easy and effective ways to secure your AWS environment, Becky Weiss, 2020 AWS re: Invent,https://youtu.be/MCp2wB63UQI

[3] 7 best practices to Secure AWS S3 storage, Anand Yadav, Feb 2020 retrieved from geekflare

[4] Identity federation in AWS, Amazon Web Services, April 2021

[5] Security Best Practices in AWS CloudTrail, Amazon Web Services, April 2021

[6] Querying AWS CloudTrail Logs , Amazon Web Services, April 2021

[7] Amazon Virtual Private Cloud (VPC) customers can now use their own Prefix Lists to simplify the configuration of security groups and route tables, Amazon Web Services, June 2020

[8] AWS Firewall Manager," Amazon Web Services, April 2021

[9] Control access to services with VPC endpoints, Amazon Web Services, April 2021

[10] Public DNS query logging, Amazon Web Services, April 2021