A STUDY ON THE SECURITY ISSUES IN AMAZON WEB SERVICES

***J. Ramyabharathi*[1], *Dr.G.Anitha*[2]**

ABSTRACT

Amazon Web Services (AWS) provides a variety of cloud computing platforms with high accessibility and loyalty, provided several tools that facilitate customers to run an extensive range of applications. It is highly important for AWS to offer clients services to guard the secrecy, reliability and accessibility of their systems and data for in order to obtain the clients' trust. The intention of this paper is to answer questions such us, "How AWS does does help to protect the data?" Specifically, AWS physical and operational security processes are described for the network and server infrastructure under AWS's management, as well as service-specific security implementations.

Keywords : Amazon Web Services (AWS), Platform, Security, Gateway.

I. INTRODUCTION

The organizers of AWS and CAF concentrate on six areas. In general business people and those in Governance concentrate on business capabilities, and therefore the Platform, security, and Operations have their focus on technical capabilities.

AWS Storage Entry Security :

The AWS Storage security entry services connects the environment code that can be applied with the cloud-based storage to construct faultless and secured incorporation between Information Technology environment and the infrastructure of AWS' storage. This process allows the transfer of information to AWS for maintaining reliability and consistency. It also helps with the ways to protect the Amazon S3 storage service recuperation.

AWS Storage Gateway provides three different choices :

⏩ Gateway-stored Volumes

This is the place where the cloud is the backup. In this option, your volume data is stored locally and then pushed to Amazon S3, where it is stored in redundant, encrypted form, and made available in the form of Elastic Block Storage (EBS) snapshots.. When using this model, the environment storage is most important for supplying low-latency access to the complete dataset, thus the cloud storage is considered as backup.

⏩ This is the place where the cloud is considered as primary. With this choice the volume information is stored in Amazon S3 in encrypted form, which is visible in the enterprise's network through the associate iSCSI interface. Any recently accessed information is cached in the local storage for low-latency native

[1] Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore.

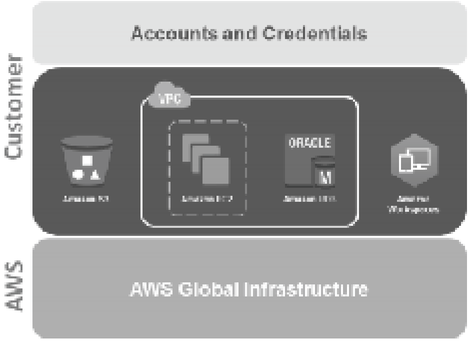
[2] Assistant Professor, Department of CS, CA & IT, Karpagam Academy of Higher Education, Coimbatore.

access. When using this model, the cloud storage is considered as primary; however, the low- latency access is gained by the active operating set.

Gateway-Virtual Tape Library (VTL)

This kind of AWS Storage Gateway is able to set up the Gateway Virtual Tape Library. This VTL consists of up to ten virtual tape drives for one entry, one media changer and 1500 virtual tape cartridges. Every virtual transport replies to the interface. Thus, the obtainable backup system in the disk to tape or disk to disk cannot be modified. No matter what choice is made, the information is serially transferred from the local storage hardware to AWS over SSL. The information is kept encrypted in Amazon S3.

The data is stored encrypted in Amazon S3 using Advanced Encryption Standard (AES) 256, a symmetric- key encryption standard using 256-bit encryption keys. The AWS Storage Gateway only uploads data that has changed, minimizing the amount of data sent over the Internet.



AWS Security Responsibilities

Amazon Internet Services is liable to protect the world-wide infrastructure, which tracks all of the services offered within the AWS cloud. The AWS architecture that is composed of software, hardware and networking to process the AWS services. Protecting this AWS architecture, no one can visit our information centers or offices to examine this protection primary. AWS security offers many reports, which are verified by auditors.

AWS protects the configuration of its products. Some AWS services give measurability and elasticity of resources with the extra good thing being handled. AWS can manage tasks like information fixture, firewall configuration and disaster recovery for these services. However, this service performs the overall protection configuration work.

Customer Security Responsibilities

The virtual servers, storage, databases and desktops can be provisioned in minutes rather than weeks with the AWS cloud. The cloud-based analytics and advancement tools are used to store the information in the knowledge centers or within the cloud. AWS services can verify how much amount of configuration work is to be performed as a portion of the security tasks.

For example, for EC2 instances, you're responsible for management of

the guest OS any application software or utilities you install on the instances,

and the configuration of the AWS-provided firewall (called a security group) on each instance. These are basically the

same security tasks that you're used to performing no matter where your servers are located.

Network Security

The AWS network has been designed for the purpose of giving permission to pick the degree of security and flexibility which is suitable for the capacity. To construct organically discrete, fault-tolerant web infrastructure with cloud resources, AWS can be developed as a superlative network infrastructure that is suspiciously supervise and accomplished.

Secure Network Architecture

The AWS network has been designed for the purpose of giving permission to pick the degree of security and flexibility which is suitable for the capacity. To construct organically discrete, fault-tolerant web infrastructure with cloud resources, AWS can be developed as a superlative network infrastructure that is suspiciously supervise and accomplished.ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic.

ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACLManage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

Secure Access Points

To monitor the inbound and outbound communications and the traffic between the networks, AWS places a small amount of access points in the cloud. The access points are called as API endpoints or customer access points. The secure HTTP access is allowed by these API endpoints. It also allows the launch of a secure communication session with the local storage or computing the instances within AWS.

To retain clients with FIPS cryptographic necessities, the SSL-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant. In addition, AWS has organized network devices that are devoted to managing the communications with Internet service providers (ISPs). Every Internet-facing edge of the AWS network provides more than one communication service with the benefit of redundant connection. Each and every connection must have dedicated network devices.

Transmission Protection

To protect against eavesdropping, tampering, and message forgery for connecting to an AWS access point via HTTP or HTTPS using Secure Sockets Layer a cryptographic protocol is designed. .

Amazon Corporate Segregation

The AWS Production networks and the Amazon Corporate networks are differentiated by the way of a set of network security or the isolation mechanisms.

The developers and directors of AWS on the company network, who have to be compelled to access the AWS cloud parts so as to

keep up with them, should expressly ask for the process all the way. All request area units are verified and sanctioned by the service owner.

Fault-Tolerant Design

The infrastructure of AWS has the highest degree of accessibility and offers the ability to arrange a flexible Information Technology infrastructure. AWS has implemented its systems to endure system or hardware collapse with minimum impact on the customer.

Data centers are organized in various global regions. Every data center in all regions is giving service to the customers online. There is no data center that is "cold". When a data center failure occurs, these types of automated processes move customer data traffic away from the affected area into a safe place. For enabling enough facility for data traffic the core application may be implemented in an N+1 configuration.

AWS offers the facility along with the elasticity to position the occurrences and accumulates the data within relative areas as well as numerous accessibility regions. Every availability zone is considered as an autonomous failure region. This means that the availability regions are located in lower risk plains and that they are physically divided within a typical region. To make use of the uninterrupted supply of power and onsite backup generators, they are fed through dissimilar grids from the separate utilities to shrink the points of failure. Availability regions are associated with multiple tier-1 transit providers redundantly.

Network Protection and Monitoring

To provide prominent service and availability, AWS uses a huge range of automatic monitoring systems. These tools are used for monitoring the server and network usage, port scanning activities, application usage and unauthorized intrusion attempts. These tools also have the capability to place conventional performance metrics thresholds for abnormal activity.

Systems within AWS are broadly automated to monitor the operational metrics. The automatic alarms are configured to alert the operations and the administration personnel, when early warning thresholds are crossed on key operational metrics. An on-call schedule is also used. So, the personnel are always available to reply to operational issues. This includes a pager system alarms that are rapidly and consistently communicated to the operation personnel.

The purpose of maintaining the documentation is to inform the operation personnel in managing events or issues. The conferencing technique that supports communication and logging capabilities is used, when the resolution of an issue needs collaboration. Skilled call leaders assist the communication and development of progress, when managing the issues that need cooperation. Investigations are arranged after any considerable operational issue, despite the impact of peripherals. The contents are outlined so that the reason is found and preventive measures are to be applied in the future.

During weekly operation meetings the implementation of the pre-emptive actions is tracked. There are many considerable protections offered by AWS network against traditional network security issues, and can be employed for additional protection.

- Distributed Denial Of Service (DDoS) Attacks.

AWS API endpoints are hosted on large, Internet-scale, world class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi homed across a number of providers to achieve Internet access diversity.

Conclusion

The AWS is a well-designed Framework, which facilitates the analysis and development of cloud-based architectures, and it is good to understand the business impact of the design decisions. General design principles are addressed, and also the best practices and guidance in five conceptual areas are specified. Thus, the AWS is outlined as the pillar of a Well-Architected Framework.

References

1. "Amazon Web Services: Overview of Security Processes", White Papers, June 2014.

2. http://aws.amazon.com/what-is-aws/.

3. Andrei Dobrin, GrigoreStamatescu, Cristian Dragana, Valentin Sgarciu, "Cloud challenges for networked embedded systems: A review", System Theory Control and Computing (ICSTCC) 2016 20th International Conference on, pp. 866-871, 2016.

4. BehlAkhil, BehlKanika, An analysis of Cloud Computing Security Issues. 2012 IEEE.

5. Chen Deyan, Zhao Hong, Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering, 2012.

6. Mladen A. Vouk, "Cloud Computing - Issues Research and Implementations", Journal of Computing and Information Technology -CIT 16, vol. 4, pp. 235-246, 2008.

7. Nilesh R. Patil, Rajesh Dharmik, "Secured cloud architecture for cloud service provider", Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) World Conference on, pp. 1-4, 2016

8. PrasadPadhy Rabi, Patra ManasRanjan, ChandraSatyapathy Suresh, "Cloud Computing: Security Issues and Research Challenges", IJCSITS, vol. 1, no. 2, December 2011.

9. Robinson Glen, Narin Attila, Elleman Chris, "Amazon Web Services- Using AWS for Disaster Recovery", White Papers, October 2014.

10. Shukla Shipra, Kumar Singh Rakesh, Security of Cloud Computing System using Object Oriented Technique, IEEE, July 2012.

11. Zachariah PabiGariba, John Andrew Van Der Poll, "Security Failure Trends of Cloud Computing", Collaboration and Internet Computing (CIC) 2017 IEEE 3rd International Conference on, pp. 247-256, 2017.

12. Zhang Qi, Cheng Lu, BoutabaRaouf, "Cloud Computing: State-of-the-art and research challenges", J Internet ServAppl, 2010.