International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

A Study on Cloud Computing Security: Amazon Web Service

Ragi Rajesh & Konka Kishan
[1]Assistant Professor, CSE Department, ST.Martins Engineering College, JNTUH
[2]Assistant Professor, CSE Department, ST.Martins Engineering College, JNTUH

***Abstract**: Cloud computing is an emerging technology is distributing environments. Cloud computing which is becoming popular among all distributed technologies. Cloud computing provides lot of benefits and it is a cost effective model. The security is the major concern in the cloud environments. Amazon web service is the trusted provider in the cloud computing for security reasons. The Amazon web service is a web service provides the services in the cloud. This paper describes the study on the security in the cloud computing with Amazon web service. .*

Keywords:

Cloud Computing, Amazon Web Service

1. Introduction

. Cloud computing is most used by the user to access the data remotely. The users prefer the remote cloud to move their applications and data easily and simple to access it. The cloud computing provides the different services for the users in the IT organizations. The cloud computing services are infrastructure as a service, platform as a service, and software as a service. Cloud computing can handle the different types of services through types of clouds. The public cloud is especially used in the sharing computing with some companies. The private cloud is allocated to particular organization and maintained it for the security reasons. The hybrid cloud is used to combine the public and private clouds together to minimize the change.

Amazon web services cloud web hosting it provide reliable and cost effective solutions. The Amazon web service uses the virtual machines of different configuration as per the requirement. It allows the mapping of independent servers and provides the configure options.

AWS Management Console is a web application for managing Amazon Web Services. AWS Management Console consists of list of various services to choose from. It also provides all information related to our account like billing.

This console provides an inbuilt user interface to perform AWS tasks like working with Amazon S3 buckets, launching and connecting to Amazon EC2 instances, setting Amazon Cloud Watch alarms, etc.

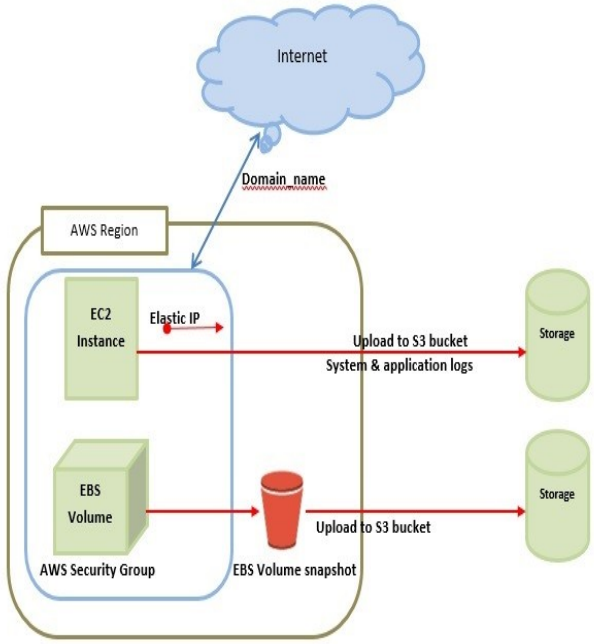


Figure 1: Amazon basic web service architecture

Virtual private cloud allows the users and uses the Amazon web service resources in a virtual network. The customers customizes the virtual address by selecting own Internet protocol address range, configuring the routing tables and network gateways. The Amazon web services that can be used by the virtual private clouds are Amazon EC2, Amazon Route 53, Amazon Work spaces, Auto Scaling, Elastic Load Balancing,

How to Use Amazon VPC?

Following are the steps to create VPC.

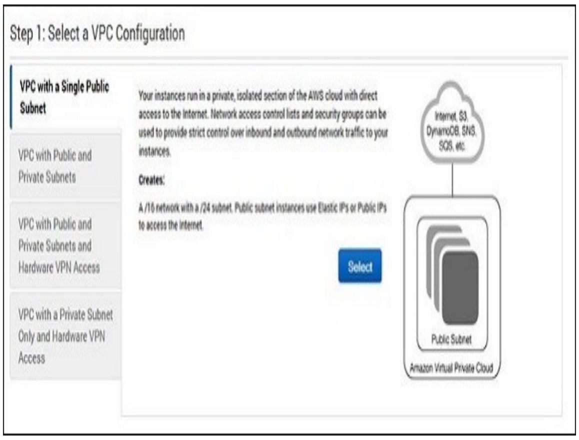
Create VPC

Step 1 – Open the Amazon VPC console

Step 2 – Select creating the VPC option on the right side of the navigation bar. Make sure that the same region is selected as for other services.

Step 3 – Click the start VPC wizard option.

Step 4- click VPC with single public subnet option on the left side.



Step 1: Select a VPC Configuration

- VPC with a Single Public Subnet
- VPC with Public and Private Subnets
- VPC with Public and Private Subnets and Hardware VPN Access
- VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

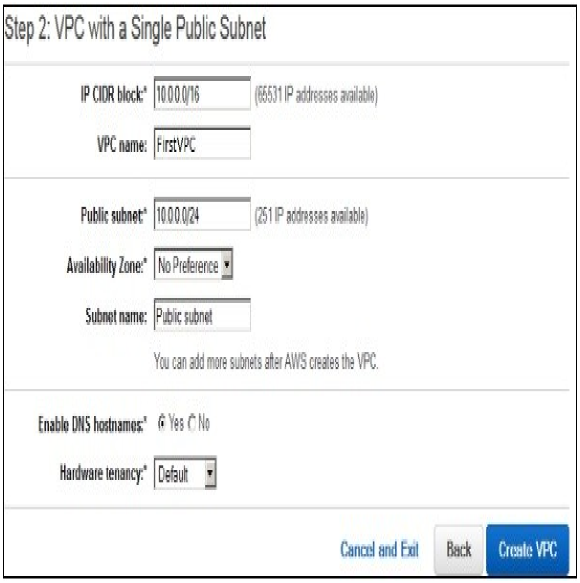
Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Public Subnet
Amazon Virtual Private Cloud

Step 5 – A configuration page will open.

Step 6-Fill in the details like VPC name, subnet name and leave the other fields as default. Click the Create VPC button.



Step 2: VPC with a Single Public Subnet

IP CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

VPC name: FirstVPC

Public subnet:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Subnet name: Public subnet

You can add more subnets after AWS creates the VPC.

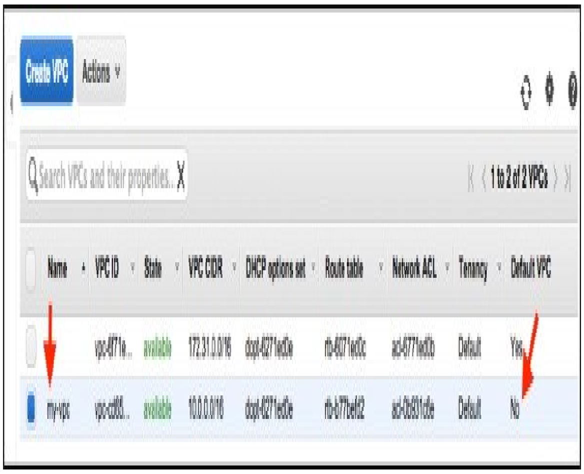
Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

Step 6 – A dialog box will open, showing the work in progress.

Step 7-When it is completed, select the OK button.

The Your VPCs page opens which shows a list of available VPCs. The setting of VPC can be changed here.



Name	VPC ID	State	VPC CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
	vpc-4f71e...	available	172.31.0.0/16	dopt-4271ed0e	rtb-4071ed0c	acl-4771ed0b	Default	Yes
my-vpc	vpc-cd65...	available	10.0.0.0/16	dopt-4271ed0e	rtb-b77bef42	acl-0b931dfe	Default	No

2. Literature Review

The literature identifies three different broad service models for cloud computing: a) Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality for example Google Docs, Gmail and MySAP. b)Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine. c) Infrastructure as a Service (IaaS), where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services. Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) and Simple DB. The literature also differentiates cloud computing offerings by scope. In private clouds; services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organization's data centre delivers cloud computing services to clients who may or may not be in the premises [2]. Public clouds are the opposite: services are offered to individuals and organizations who want to retain elasticity and accountability without absorbing the full costs of in-house infrastructures [2]. Public cloud users Author Name(s) and Affiliation(s) are by default treated as untrustworthy. There are also hybrid clouds combining both private and public cloud service offerings [3].

This section includes survey conducted by international data corporation (IDC). It shows the strength of cloud computing to be implemented in IT industry and gives the potential inspiration to CSP. The section contains the survey related to the growth of cloud, security aspect, cloud is the first priority to the vendors, revenue report, future and current usage, state of cloud to the IT users and popularity survey of cloud computing.

3. Proposed Work

In the cloud computing security is the fundamental aspect and requires some research models like trusted computing and Data centric security.

The trusted computing is to gain the trust service provide by providing security policies. The cloud computing environment third parties plays major role in between the client and IT organizations. The remote cloud can be handled by remote server. Trusted computing system is considered the data security and encrypts the data application and provides the decrypted keys to the information and trusted computing services adding new hardware to the systems. The trust computing platform uses two services provided by TCP are trusted boot and encryption. The TCP maintains two components trusted virtual machine monitors and trusted coordinators. Trusted virtual machine monitor especially for provides the virtual machines and provides the protection against inspection and modification of Customers virtual machines. The trusted coordinator is responsible for running virtual machines by some set of network nodes.

The Data centric security refers the security of data rather than security of applications. The first way to provide the data centric security is encrypting the information. The owner who has decrypting the key can only accesses the data and no one can read it and write the data. The strong encryption may not be useful due to in the cloud the data is processed in the encrypted form. Data centric security is made of different services those are useful to protect the data in the cloud.

The services are

1. Storage infrastructure services
2. Data services
3. Management services
4. Access services

The architecture of data centric security protects the data by observing and enforcing the rules of privacy. The individuals can share their documents securely. The documents contain the security rules with them like logs capture activities and security policies enforced. Data centric architecture is responsible for handing, observing over the confidential documents.

AWS (AMAZON WEB SERVICE)

AWS is the cloud computing provider. This service is a perfect example of true cloud computing

Which is not only provides excellent cloud services but also provides confidentiality; integrity and availability of the customer's data. AWS give the on demand services. The IT resources are available at cheap prices and no upfront investment is required for the resources. The customer just has to pay for the resources that he consumes on variable basis. AWS provide the flexibility in terms of amount of resources the customers need. If they need more than demanded then they can easily scale up and if they don't need the resources that they have then they can turn them off and stop paying. Another benefit of AWS is it makes the work easier and faster. With traditional architecture it was difficult to develop the application as it takes lot of time to get a server. AWS cloud computing one can deploy hundreds or thousands of servers without any delay. Hence AWS allows quick development and deployment of an application and hence it allows the team to experiment more frequently.

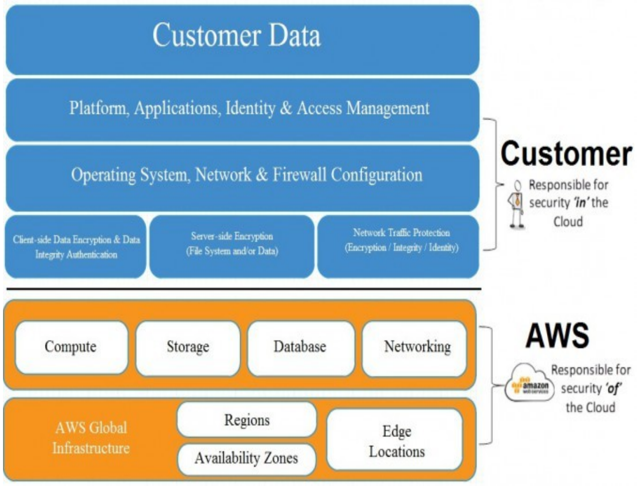

Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption / Integrity / Identity)
Customer
Responsible for security 'in' the Cloud
Compute
Storage
Database
Networking
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS
Responsible for security 'of' the Cloud

Figure 2: Amazon Web Services with Security

4. Conclusion

Cloud computing provides many services and advantages but security is the problem around the data access and privacy protection. Cloud computing should be secure, robust and mitigate the risks. The Amazon web services have good performance in the cloud computing environments. The Amazon web services provide the network security over the streaming data, securing data with encryption and backup and recovery approach. This paper describes the trust by providing security in the cloud computing environments.

5. References

[1]] Qi Zhang, Lu Cheng, RaoufBoutaba. Cloud Computing: State-of-the-art and research challenges.J Internet ServAppl (2010).

[2] Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satyapathy. Cloud Computing: Security Issues and Research Challenges. IJCSITS Vol. 1, No. 2, December 2011.

[3] Meiko Jensen, JorgSehwenk et al. “On Technical Security Issues in Cloud Computing”. IEEE International Conference on Cloud Computing, pp 109-116, October 2009.

[4] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma. Cloud Computing Security- Trends and Research Directions. 2011 IEEE World Congree on Services.

[5] Mariana Carroll, Alta van der Merwe, Paula Kotze. Secure Cloud Computing. Benefits, Risks and Controls. 2011 IEEE.