Practical No. - 5

Aim: To study cloud security management..

Apparatus: Ubuntu operating system, Virtual machine, WAMP/ZAMP server, Any tool or technology thatcan be used for implementation of web application e.g., JAVA, PHP, etc.

Theory: Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use. Because of the cloud's very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider.

Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also likely include a business continuity and databackup plan in the case of a cloud security breach.

Physical security

Cloud service providers physically secure the IT hardware (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from 'world-class' (i.e. professionally specified, designed, constructed, managed, monitored and maintained) data centers. contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

Procedure:

SECURITY USING MFA (MULTI FACTOR AUTHENTICATION) DEVICE CODE:

1) GO TO AWS.AMAZON.COM

2) CLICK ON "MY ACCOUNT"

3) SELECT "AWS MANAGEMENT CONSOLE" AND CLICK ON IT

4) Give Email id in the required field

if you are registering first time then select "I am a new user" radio button

5) click on "sign in using our secure server" button

6) follow the instruction and complete the formalities

(Note: do not provide any credit card details

or bank details)sign out from

7) Again go to "My Account"

select "AWS management console" and click on it

Permissions in user account:

After creating the user by following above mentioned steps; you can give certain permissions to specific user

1) click on created user

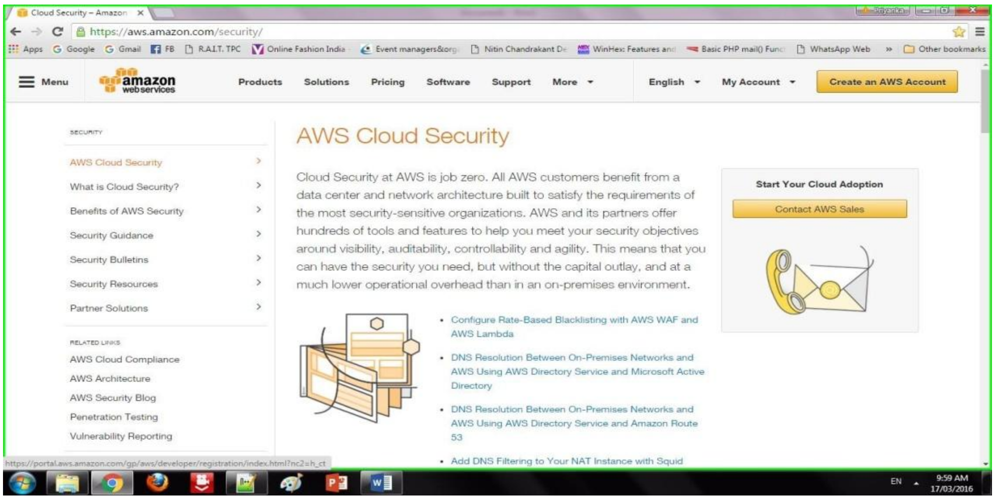
2) goto "Permissions" tab

3) click on "Attach Policy" button

4) select the needed policy from given list and click on apply.

RESULT:

Step 1: go to aws.amazon.com

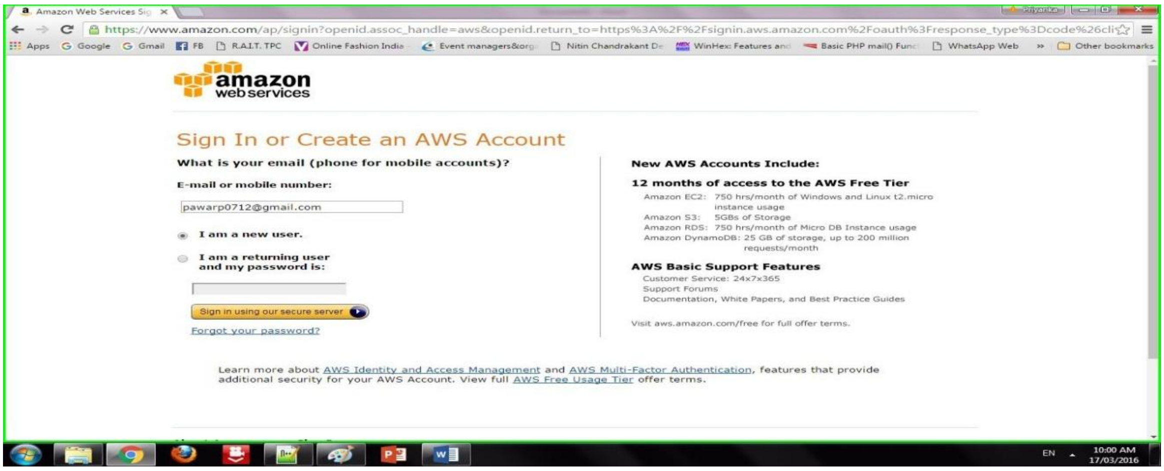


AWS Cloud Security

Cloud Security at AWS is job zero. All AWS customers benefit from a data center and network architecture built to satisfy the requirements of the most security-sensitive organizations. AWS and its partners offer hundreds of tools and features to help you meet your security objectives around visibility, auditability, controllability and agility. This means that you can have the security you need, but without the capital outlay, and at a much lower operational overhead than in an on-premises environment.

- Configure Rate-Based Blacklisting with AWS WAF and AWS Lambda
- DNS Resolution Between On-Premises Networks and AWS Using AWS Directory Service and Microsoft Active Directory
- DNS Resolution Between On-Premises Networks and AWS Using AWS Directory Service and Amazon Route 53
- Add DNS Filtering to Your NAT Instance with Squid

Step 2: Click on "My Account". Select "AWS management console" and click on it. Give Email id in therequired field



https://www.amazon.com/ap/signin?openid.assoc_handle=aws&openid.return_to=https%3A%2F%2Fsignin.aws.amazon.com%2Foauth%3Fresponse_type%3Dcode%26cli

amazon web services

Sign In or Create an AWS Account

What is your email (phone for mobile accounts)?

E-mail or mobile number: pawarp0712@gmail.com

● I am a new user.

○ I am a returning user and my password is:

Sign in using our secure server

Forgot your password?

New AWS Accounts Include:

12 months of access to the AWS Free Tier

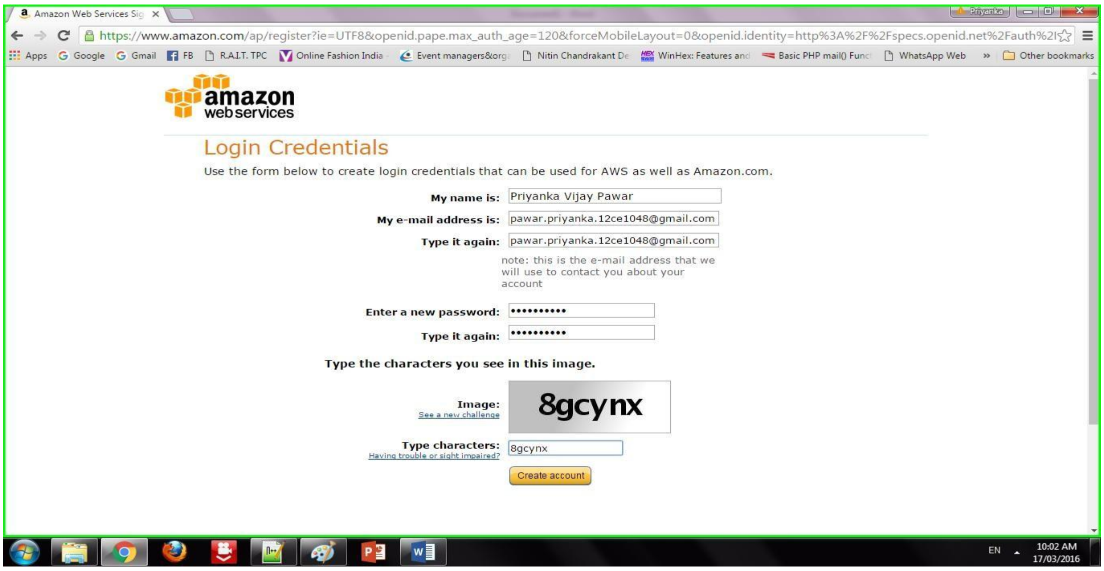
Amazon EC2: 750 hrs/month of Windows and Linux t2.micro instance usage
Amazon S3: 5GBs of Storage
Amazon RDS: 750 hrs/month of Micro DB Instance usage
Amazon DynamoDB: 25 GB of storage, up to 200 million requests/month

AWS Basic Support Features

Customer Service: 24x7x365
Support Forums
Documentation, White Papers, and Best Practice Guides

Visit aws.amazon.com/free for full offer terms.

Learn more about AWS Identity and Access Management and AWS Multi-Factor Authentication, features that provide additional security for your AWS Account. View full AWS Free Usage Tier offer terms.



https://www.amazon.com/ap/register?ie=UTF8&openid.pape.max_auth_age=120&forceMobileLayout=0&openid.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F

amazon web services

Login Credentials

Use the form below to create login credentials that can be used for AWS as well as Amazon.com.

My name is: Priyanka Vijay Pawar

My e-mail address is: pawar.priyanka.12ce1048@gmail.com

Type it again: pawar.priyanka.12ce1048@gmail.com

note: this is the e-mail address that we will use to contact you about your account

Enter a new password: ••••••••••

Type it again: ••••••••••

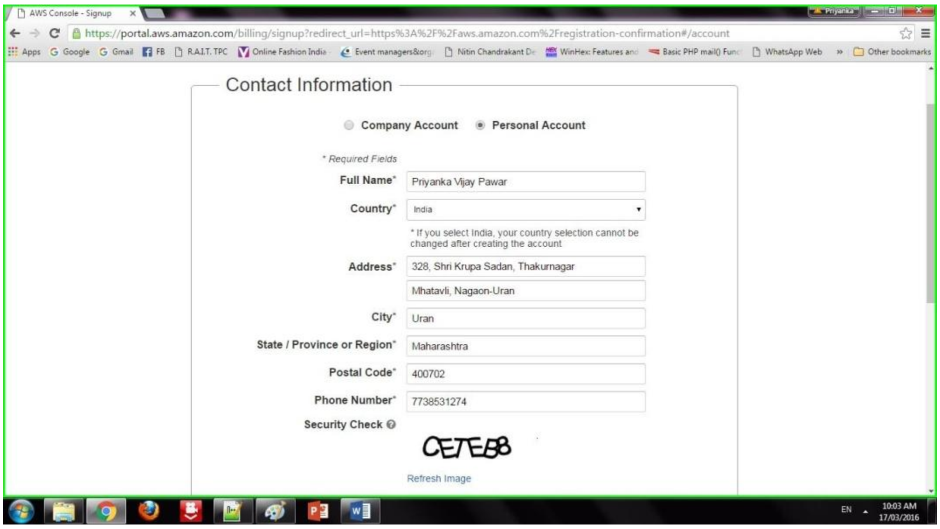
Type the characters you see in this image.

Image: 8gcynx
See a new challenge

Type characters: 8gcynx
Having trouble or sight impaired?

Create account

Step 4: Sign in to an AWS account



https://portal.aws.amazon.com/billing/signup?redirect_url=https%3A%2F%2Faws.amazon.com%2Fregistration-confirmation#/account

Contact Information

○ Company Account ● Personal Account

* Required Fields

Full Name* Priyanka Vijay Pawar

Country* India

* If you select India, your country selection cannot be changed after creating the account

Address* 328, Shri Krupa Sadan, Thakurnagar
Mhatavli, Nagaon-Uran

City* Uran

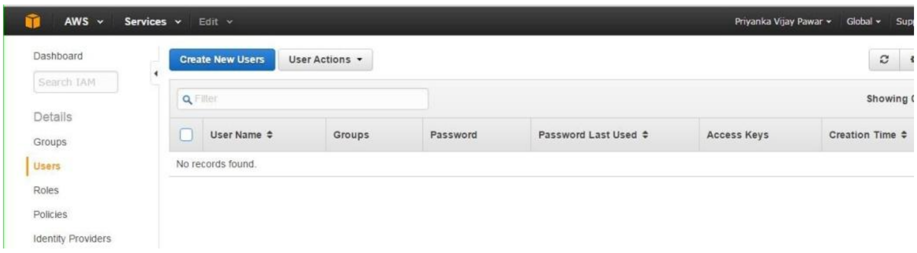
State / Province or Region* Maharashtra

Postal Code* 400702

Phone Number* 7738531274

Security Check CETEB8

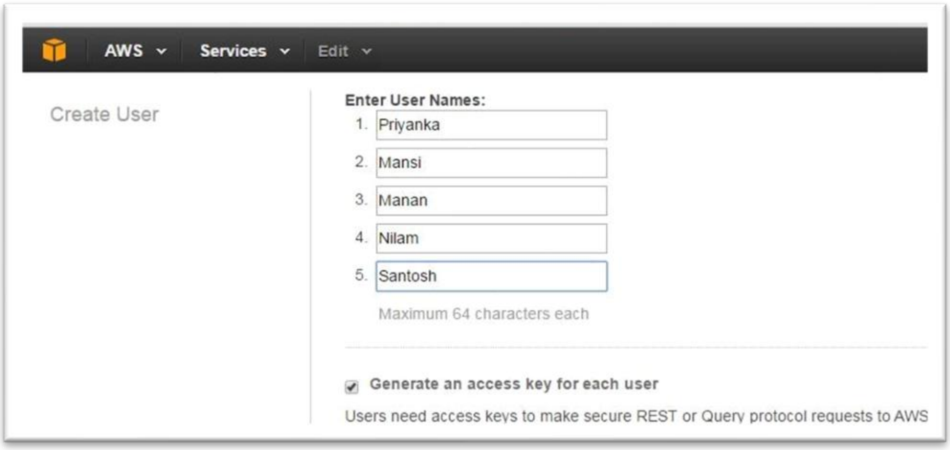
Refresh Image



☐	User Name	Groups	Password	Password Last Used	Access Keys	Creation Time

No records found.

Step 5 : Creation of users



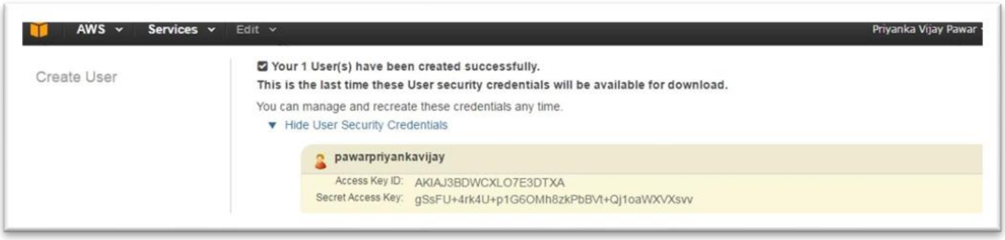
Enter User Names:

1. Priyanka
2. Mansi
3. Manan
4. Nilam
5. Santosh

Maximum 64 characters each

☑ Generate an access key for each user

Users need access keys to make secure REST or Query protocol requests to AWS



☑ Your 1 User(s) have been created successfully.
This is the last time these User security credentials will be available for download.

You can manage and recreate these credentials any time.

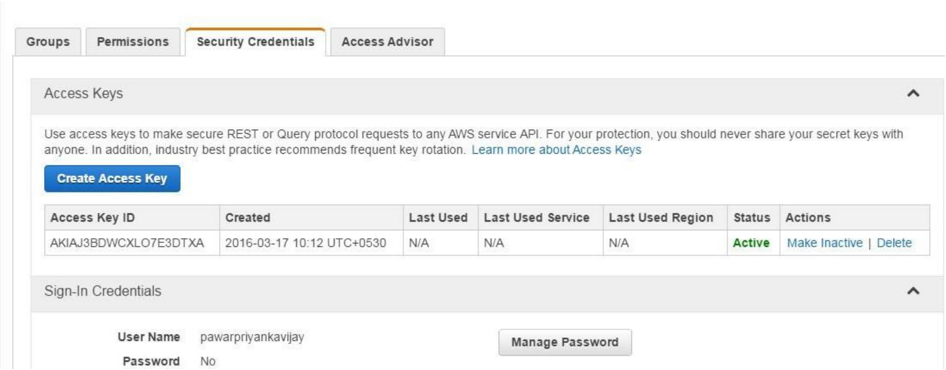
▼ Hide User Security Credentials

pawarpriyankavijay

Access Key ID: AKIAJ3BDWCXLO7E3DTXA
Secret Access Key: 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

Step 6: Adding users to group

Step 7: Creating Access key

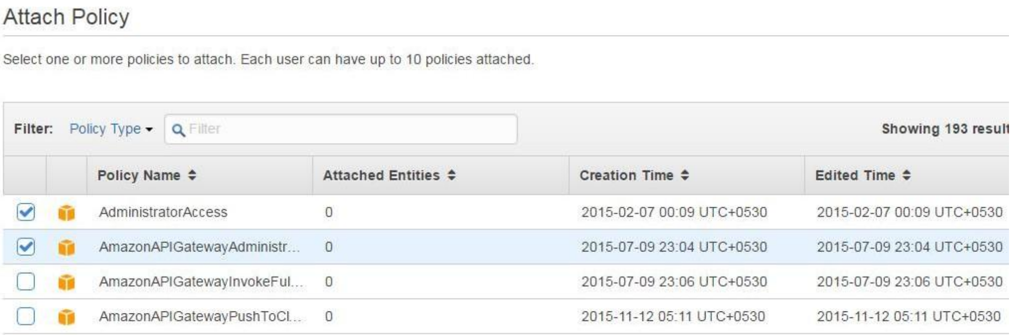


Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation. Learn more about Access Keys

Access Key ID	Created	Last Used	Last Used Service	Last Used Region	Status	Actions
AKIAJ3BDWCXLO7E3DTXA	2016-03-17 10:12 UTC+0530	N/A	N/A	N/A	Active	Make Inactive | Delete

User Name pawarpriyankavijay
Password No

Step 8: Setting permission to user.

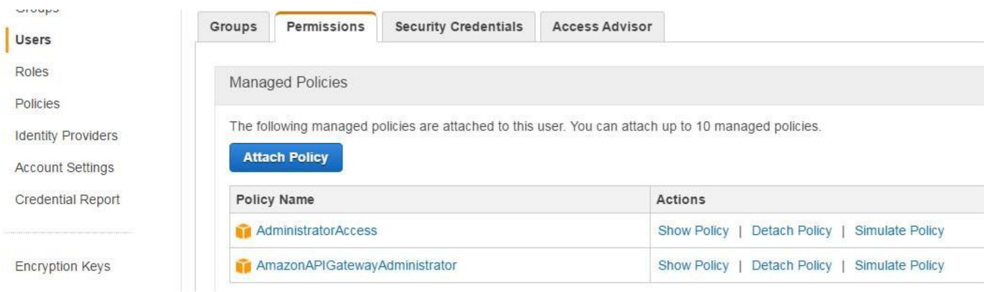


Attach Policy

Select one or more policies to attach. Each user can have up to 10 policies attached.

Filter: Policy Type ▾ Filter Showing 193 result

		Policy Name ⇕	Attached Entities ⇕	Creation Time ⇕	Edited Time ⇕
☑		AdministratorAccess	0	2015-02-07 00:09 UTC+0530	2015-02-07 00:09 UTC+0530
☑		AmazonAPIGatewayAdministr...	0	2015-07-09 23:04 UTC+0530	2015-07-09 23:04 UTC+0530
□		AmazonAPIGatewayInvokeFul...	0	2015-07-09 23:06 UTC+0530	2015-07-09 23:06 UTC+0530
□		AmazonAPIGatewayPushToCl...	0	2015-11-12 05:11 UTC+0530	2015-11-12 05:11 UTC+0530

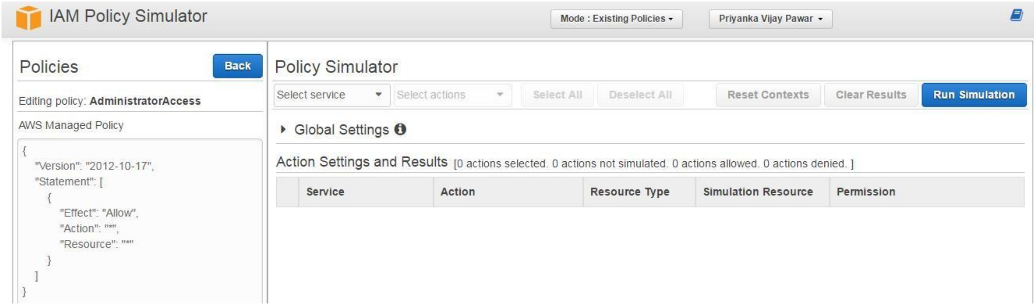


Managed Policies

The following managed policies are attached to this user. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
AdministratorAccess	Show Policy | Detach Policy | Simulate Policy
AmazonAPIGatewayAdministrator	Show Policy | Detach Policy | Simulate Policy



Editing policy: **AdministratorAccess**

AWS Managed Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission

Conclusion:

We have studied how to secure the cloud and its data. Amazon EWS provides the best security withits extended facilities and services like MFA device. It also gives you the ability to add your own permissions and policies for securing data more encrypted.