C-

e-

e-

c-

e_

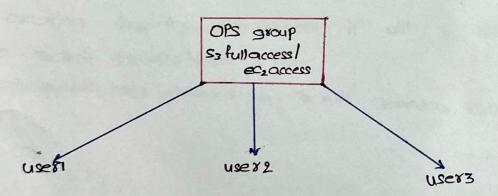
e-

IAM: Identity and Access Management

- -> we will be using the floot user most of the time.
- > Poot uses has the complete access (to coeate, delete, modify...etc)
- Ly IAM is used to execute individual user access to each and every resource.
- >IAM uses is an individual identity with specific Permissions to access besources with in a system.

IAM identity: Identity can be usex, group, toles.

- 1) GUI occess
- 2) CLI access / programmetic access.
- Instead of giving permission/specific acess to each and every of the user. I can add the users to a group, and what all the permissions were required, I can attach to the group.



To create a group:

User groups

create group

Name the group

Add users to the group

Attach permissions policies

create group

(900) 2011/109 loaned schools policy: Policy defines the permissions of the IAM Identity. specify the manimum level of permissions to organischion standard steele policies are like * Types of policies: 1) Identity Based Policies: a) In-line policy - An inline policy is a policy executed for a single IAM identity (a user, group, or role). Inline policies maintain a strict one-to-one relationship between a policy and an identity, They one deleted when you delete the identity. IAM ->users -> Add permissions -> create inline policy -> image -> service (choose a service) -> Actions (manual actions) -> Resources (all resources) neckie yexson. > beview policy -> Name -> create policy b) Managed policies: (i) AWS managed policies: that are created and managed by AWS. A service Role is on IAM (ii) customer managed policies: Managed policies that you create and manage in your AWS account customer managed policies Provide more precise control over your policies than AWS ranaged policies. zide ni znovoo molasa de emodes 2) Resource based policies:

attached directly to resources and specify fermissions specifications actions on the resource by some principals.

3) IAM permissions boundaries:

Define the maximum permissions for an IAM entity and are used as safe guards. e serve disco box sobol a year aculting

Access control lists (ACLs)

ai enoise medicag or passasile attached to resources and control cross-account permissions tor principals from other accounts.

5) Organizations service control policies (seps):

throtal MALL set to enviseinness with envise policy Specify the maximum level of permissions for an organization's accounts. These policies are used to limit the permissions that can be assigned within member accounts.

6

9

9

2

C-

2

C

C

cl

C

are advanced policies used during temporary secsions for roles or lederated users.

retirects a policy and an identity

time 2 sources of tentrality

a dimension washes much elegionist and emissioning

12 Sibilar bacount

Role:

IAM sole is an identity within your Aws account that has specific permissions. It suite stores a encissioned that a sessue MAI

It is similar to an IAM user, but is not associated with a specific person. soviers policy a none a mode policy

Types of Roles:

1) AMS : Sezvice Role: Los belooms so roll: 25/6/10/ become 2/1/A (i) A service Role is an IAM role that, a service assumes to perform actions on your behalf. were sometime transport 2000 were at sometime born

2) AWS account:

Allows entities in other AWS accounts belonging to you or a 3rd pasty to pestosm actions in this account. Resource boased poli

3) Web identity:

someon of phospits barbarile some usexs federated by the specific external web identity provides to assume this sole to pestorm actions in this account.

4) SAML 20 federation (security Assertion markup language); Allows users federated with SAML 2.0 from a corporate directory to perform actions in this account.

AND SO THERE 5) custom trust policy! create a custom trust policy to enable others to perform actions in this account. which pro it hastings son to mixed the (2300 months of the Property of March 1996), 2 early show the state of the second of t on a sale of the brodge our homory of the second toward on them the me work to write one of math the Stoppeds show ENS A horizont block .872 of u to special posed to see al. the broad aligned that can be willowed in a single for is said. alledde sucinu ad bloods and parall of legards sent sents 200 The state of the s 20 design of 1933 addition teamers mas sur, 203 mil % 293 Stall of 83 Addition house that we to soll most all a 200 statement and to be some one of all the solling afficient solves and in 100 thought seems born at ask in a 27) " estedado estad gitama popular en nejerar puesa suntes hande cardan to the state of th

Cur mor

C -

C-

Cam

C-

-

C-

C-

C-

C-

C

C-

C

C

C

C

C

C

C

C

6

C

C

C

C

0

6

6

6

C

* Simple storage service the

4 23 is a global service.

4 23 service is not restricted to any region.

L> 53 Bucket is a region specific.

Fixed means, the moment we upload it to the S3 we can't edit them. If we wan't to make any changes, we should download it and make changes.

-> S3 bucket has a storage of upto 5TB.

The largest object that can be uploaded in a single PUT is 5GB.

→ S3 Bucket name should be unique globally,

In AWS we have 3 different storages:

1) EBS (Elastic Block storage).

2) S3 (Simple Storage service)

3) EFS (Elastic File Systems).

* In EBS, we can connect multiple EBS to single EC2. we can't connect multiple EC2 to single EBS.

* In S3, we can transfer data from multiple EC2 to Sz. from different C

* E'FS con also be used across different Ecz. in Same region.

create Bucket -> Name -> AWS region -> Object ownership (ACLS disabled) ->

-> Block all public access -> Bucket versioning -> perfault encryption -> create (disable)

Bucket

Acress control list (Acis) grants permissions at object exlevel. a busket decret. senior believed and not still when the > Bucket policy applies only to buckets. Another 22 is the less in select the backet is permissions as storic and site hosting >> By default so storage class is standard. > when we upload any object, that will be moved to the Standard storage class. \rightarrow we have different classes in S3. >) Standard IA These are called as lifecycle rules for Sz objects. Links 23/12/24 ~ 2) S3 glader 3) Deep archieve Glacier of 1811 popular and print and and the 4) Standard strate of 20 22 yet 22000 of its restord been >> S3 Standard - High durability, low-latency, and used for Arequently accessed data. Sz standard-1A - lower cost than standard but with retrieval fees; best for less trequently accessed data. 3-353 - one zone -1A - cheaper than standard -1A but stored in a single Az, making it less resilient. 3-33- Glacies Deep archive- cheapest storage for long-term setention, but setseival takes 12-48 hours. >> 53- Glaciex Instant Retrieval - low cost, instant access by archive data that is takely accessed. -> sz- Gloclex flexible petrieval - Lower cost than Instant Retrieval but re-trieval times range from minutes to hours.

we can also use our so bucket to host a website. Static websites can be hosted using s3. continue of the state of the content

1

Amozon S3 -> Buckets -> Select the bucket -> permissions -> Stortic website hosting -> edit -> Enable -> chapter tosting type (Host a static website) -> index document (file name which was created) -> - Error document (file which was created). -> save changes. CONTRACTOR OF PARTIES

6

-

6

6

6

0

Amazons > Buckets > Select the Bucket > adoct a objects > upload > Add files -> upload.

Littl now we are using the object URL to open the file.

we need bucket URL to access my Sz as a static website.

Buckets -> select the bucket -> properties -> static website hosting -> URL the same of the same of

estate per entre de la companya della companya della companya de la companya della companya dell

A . a & E & sa are a sing

in the second of the second of

-

9

6

6

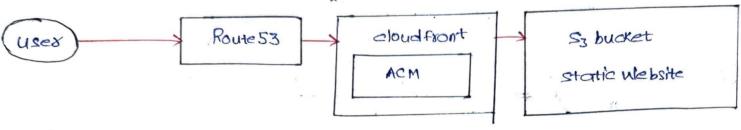
C

C

C

what have you stored in SI during your project?

We have used S3 to store UPC flow logs, images related to our application and to deploy one static website.



Revouly,

-> whenever a user wants to access the static website, we were just copying the bucket URL and boowing it.

- -> cloud front will help us to improve the perforance and also reduce the latency.
- Routess is used to configure the Domain and servers.
- -> AWS ACM (Amazon certificate Manager) is a service that helps you manage SSL/TSL certificates for securing network communications and websites.

SSL - secure socket byes

TSL - Transport Layer security.

- 4) with the help of ACM, I can purchase SSL certificante to my domain.
- HACM will add security to my URL with the help of SIL.
- Ly By adding SSL certificate to my URL, we can ensure that the data is encrypted:
- 4 SSL is used to establish an encrypted connection between a webserver and a client. SSL ensures a secure data transmission.

I Alo one can stool the dotta if SSL is configured. > If 222 is not configured users will not trust our website. Have always need to make sure that not secured our application is sel configured. >> As it is hard to remember each and every URL. 1 we will be buying a domain. So, whenever we try to access that domain , that will redirect the access to the URL attached to that domain automatically. R53 -> 53 is the post number for the DNS service. → DNS → Domain name system. et of toponos of 25/6t 8520 saft maker, smit totil and soft - Route 53 -> Begister domain -> Hosted zones -> execute Hosted zone -> →Domain name → public Hosted zone → Create Hosted zone amos sit sot enjust si dent most kosu who was it a > It will receive four different records by NS (Name server). = > A Name server (NS) record is a type of DNS record that specifies which authoritative name genvers are responsible for a domain. These name servers handle DNS queries and direct traffic to the correct locations. 100 91741 2- alcouch alpho a adjudistallo oposes a 200/tudioseio a mostipula) - we have our domain in Godddy q we are trying to host in the Route 53, so, we need to map them, while the color was s with the help of Nome servers: we need to configure the Name servers in Goddddy domain name.

-> create S3 Bucket with some Domain name!

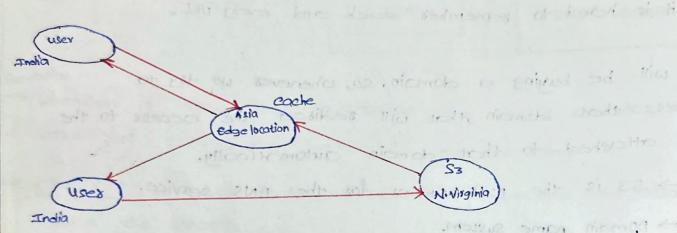
cloud foont, cloud front will help us to improve the performance of websites and also it will secure our application.

L) Edge locations are used in abud front.

cl

c

cl



No virginia, while responding back, Edge location will store some of cooke and respond back to the user.

is it any other user from India is trying for the same request, instead of connecting to the Sz in Nivirginia. It will connect to the cache location (Paper location). Then the Edge location will respond back to the user.

1> so, the time taken to travel the packets has been reduced.

La so, the performance and speed of the website will be improved.

cloud Front -> Distributions -> execute distribution -> origin domain -> HTTP only >> viewer protocol policy (HTTP and HTTPs) -> price class (use NiAmerica, Asia, Middle Foot

and Atrica) - create distribution.

copy the distribution comain name (run in browser).