AWS Notes:

Create :

Root user(dev & prod)

IAM user with MFA(dev & prod)

IAM Admin with MFA (dev & prod)

IAM Access keys for CLI

Flash cards:

AWS Basics

1. EC2 – to launch instances in VPC for cloud computing
2. S3 – Data storage bucktes. 1 default /region, others in AZ. Bucket name golablly unique (naming convention – 3 to 63 chrs, lower case. No. of buckets per acc. 100 to 1000)
3. CloudFormation – Launching services through template. Fill template and feed to CF to convert to Logical Stack and then to Physical services/instances
4. Cloud watch – TO monitor the services metrics like CPU utilization for EC2 etc.
5. Shared model compatibility – Customer & Aws responsibilities of the services
6. HA, FT & DR (HA – minimise outage,FT – work through tolerance, DR – restore from back up in different Data centre)
7. Route 53 – Domain register & Hosted zones. Register domain, will create 4 Named space.
8. DNS – Root zone,Named space, Zone file.
9. Record sets – A (IPv4), AAAA(IPv6) MX query,CNAME

IAM :

IAM Policies – DENY(Explicit),ALLOW(Explicit),DENY(Implicit)

A screenshot of a phone

Description automatically generated with low confidence

Arn – Amazon resource name : uniquely identify the resource with any AWS accounts.

2.IAM groups – Just containers for IAM groups with attached policies. Can’t login to IAM groups or can’t be referenced by resource policies. 300 groups per account. No nesting(not groups within groups)

3. create IAM user in IAM group and assign group policies – demo.

4.IAM roles – Different from IAM user. IAM roles are assumed to access AWS services/products for multi users,external accounts, external application. It is temporary and can be discarded. It uses trust policy & permission policy to assign the role to the user to access AWS services. It can be referenced by the service policy. It will create temp. security credentials based on trust & permission policy to access the AWS services. IAM role can be assigned for unlimited users/application.It is assigned by ID federation.

5.Service linked role is different from IAM role.

6. AWS Organisation – Master/management/payer account to hold other AWS accounts in an organisation. Gen. account is master account and other accounts(prod – member accounts) are added into it. Also we can create new account within master account. It is like a container not physical identity.It is a nested one.Heriarchy : Organisation(Master) –> organisation unit - > Member accounts.

7. SCP – Service control policy. Powerful. Limits the usage of services for IAM user within an account. It can even limit the root user to access services. Deny Allow Deny priorities.

8.Cloud trials: It is a product to log Api calls & Account events. It could be regional or for all regions. No data events captured unless enabled.

9.Implementing Cloud trial in Management account and logging in Cloud watch by assuming role to interact with Cloud trial. Logs uploaded in S3 bucket. Management events only. Data events comes with price.

A screenshot of a computer

Description automatically generated with low confidence

1. AWS control Tower. Easy to setup & govern Multi accounts in a region. Poweful than AWS organisation as it has additional features like Guard trials (security governance),account factory, IAM identity centre(single sign on),Resources are created and managed in an hour.

A screen shot of a computer

Description automatically generated with low confidence

S3 :

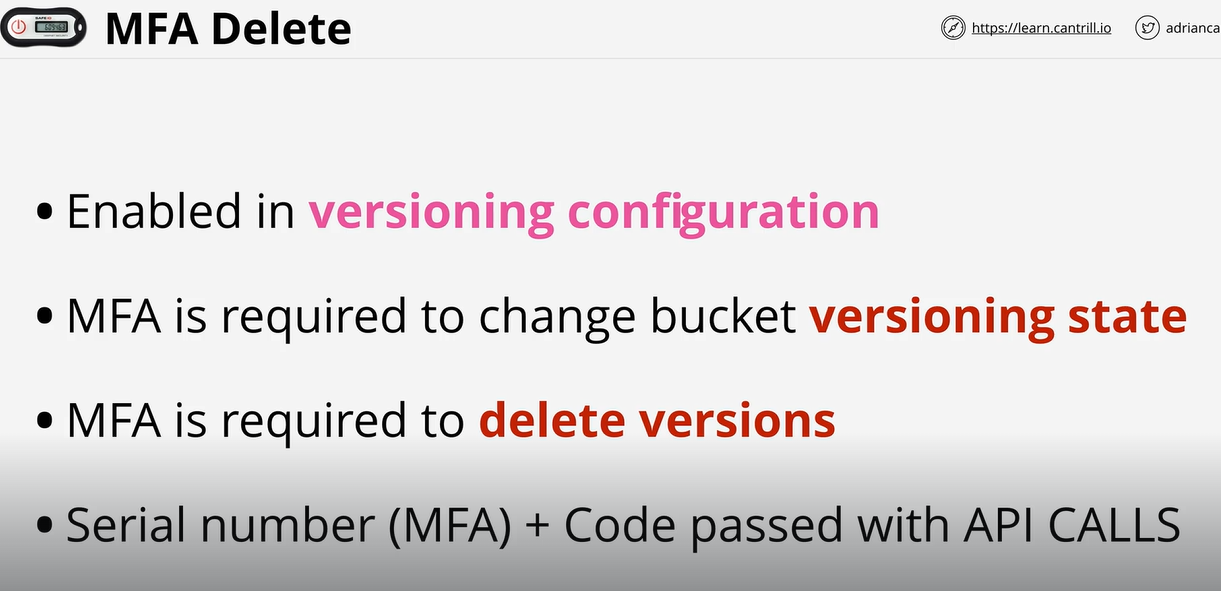
1. S3 security – resource policies.

A screenshot of a computer

Description automatically generated with low confidence

1. Creating static website using S3(not clear.May re visit)
2. Bucket versioning & MFA delete. Bucket with disabled status can be enabled but NEVER set to disabled again. Enabled bucket can be suspended and can set back to enable again.

MFA Delete:



1. Demo Bucket versioning for static hosting website upload images in S3.
2. S3 performance optimization – One data stream(5GB) to bucket cause delay and if it fails, then data lost and service need to be restarted. So data is broken into multipart 5GB to 10,000 parts is transferred parallely to bucket. Only the failed part needs to be re started. S3 accelerator transfer - S3 transfer allocation is through edge point to bucket rather than directly through public routes
3. Create bucket & enable Transfer accelerator for better performance.
4. KMS (Key management service)

A screenshot of a computer

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated with low confidence