DHCP

Ensure instance in VPC does not use AWS DNS, by create a new DHCP options set and replace the existing one

Lose encryption keys

If customer key which used to encyprt EBS is deleted, the data inside EBS volume can be still accessed from EC2

Secret Manager

Secret manager rotate secrets of RDS database. Application experience intermittetnt sign-in failures.

- Implement Exponential backoff in app
- Use multi-user rotation

KMS

Bash script encrypt file size 2kb.

Use “aws kms encrypt” to encrypt the file. No envelope encryption si required in this case because the file size is smaller than 4kb.

If is larger than 4kb, use “aws kms generate-data-key” then use plain text data key to encrypt file

For Redshift cluster service, master key encrypt cluster key encrypt database key encrypt data encryption key

CMK key ID needed for kms encryption.

CMK key ID NOT REQUIRED for decryption.

Cloudtrail

Cloudtrail logs are ENCRYPTED by default.

Aws Config

Can be triggered when:

- Changes happen
- Every 1,3,6,12,24 hours

To use, ensure trust policy in place for AWS Config service whitn role

Mobile Auth

Mobile app need these to configure social IDP:

- App Client ID
- App Client Secret

- List of scopes (authorize your app to access)

S3

What to do to allow company A users to access object?

- A give cross-account permission to B to upload to A's bucket
- B must grant object's ACL to A, giving full permission

Can use aws:Referer key in condition of bucket policy. This allow read access to objects, and make sure request must originate from specific webpages

Use aws:PrincipalOrgID to ensure only users in AWS Organization have access to bucket

Can also configure for same-region replication

What is required to have cross-region replication?
1. Bucket policy on the dest bucket must allow the source bucket owner to replicate objects

2. S3 source object owner must grant source bucket owner full access permissions to the objects in the bucket

Cognito

To provide limited samples for free:

- Enable Unauthenticated identities in Amazon Cognito Identity Pools
- Assign IAM role with appropriate S3 access permissions to this Unauthenticated identities in Amazon Cognito Identity Pools

To integrate congnito with gateway:

- Create cognito_user_pools authorizer
- Configure single-space separated list of Oauth scopes on the API method

To have captcha as part of sign-in process, create an Auth Challenge Lamda trigger

IPSEC

Data encryption across internet

Protection of data in transit over internet

Peer identity authN between VPN gateway and customer gateway

Data integrity protection across internet

VPC Interface Endpoint / Gateway endpoint

S3 and DynamoDB use VPC Gateway

IAM

Enable “aws-portal:ViewUsage, aws-portal:ViewBilling” to allow user to AWS usage report

Can upgrade support plan to use AWS Trusted Advisor and use exposed key access check

Can create lambda and get last accessed details using IAM access advisor APIs.

Incident Response

For investigation and forensic, Use NACL to block → detach from ASG → snapshot EBS → Tag EC2 for investigation

If account is compromised, delete it and change all iam user password

EBS

AWS wipes data of EBS volumes before volume available for reuse

ELB

Use HTTPS listener to encrypt in transit

To support Perfect forward secrecy (PFS), need to use ECDHE-

U can add 2 different certificates to ALB listener as it supports multiple TLS certificates using SNI

API Gateway

Use API gateway access logs to contain details about user and Ips accessing the API

CloudFront

Use signed URL and signed cookies to restrict access for selected users

RTMP Distrubution can only be used with CloudFront signed URL

OIA is used when content from S3 can only be served through CloudFront

ACM

To get certificates, you can create an audit report to list all certificates that private CA issued or revoked. Its JSON format report in S3 bucket

If use cloudfront, cert must be in us-east-1 (N. virginia)

If need HA on multiple region, create multiple root Cas in different regions

Lambda

Use execution role to determine permitted actions of the lambda

Use lambda function policy to permit WHAT can call the function