infrastructure security

KMS

Key is regional, your svc also should be in same region 동일 리전이어야함함

[Scenario] (But 5 bucket admin can't see)
encrypt /w KMS - AWS admin & key admin can see the contents
// w SSE AES - 동가능함함

[Nuance]
EC2 SSH key pair - authentication, putty 로는 key gen

→ EBS /S3 encryption, using KMS key pair
EBS 암호화 snapshot 옮겨 update encryption 안변경됨됨
because KMS, you can't export keys

RDS, Redshift, S3, EBS
Elastic transcoder, Workmail 등과 integrated

customer-master-keys
KM: 데이터암호화화

CMK

AWS marketplace
(But S3 bucket admin can't see)

KMS Grants
in CLI

temporary, granular permission
only for allow Cnot Deny)

create-grant /list-grant /revoke-grant
grant-token

→ key policy condition

ViaService
eg. kms: ViaService
"EC2.us-west-2.amazonaws.com"

Cross Accounts - KMS
① allow the AWS account in keypolicy [Enable Access 입력key in the key policy who accounts CMK]
② attach IAM policy 'll KMS 를 사용하려는 EC2 Enable access to KMS
keypolicy에 등록해야함함 in the IAM policy on external 등록
kms: Encrypt, kms: Decrypt 등록필요없음음

EC2-keypair
http://169.254.169.254/...
/home/user/.ssh/authorized_keys
EC2 instance metadata

App public key - attached to
Can add roles on an existing EC2
Deleting 해도 pair on console 에서 delete key 가능
if you lose key pair, then re-snapshot 배포하면 된다it

AWS Hypervisor
EC2는 Xen Hypervisor 기반으로함함

PV (paravirtualization) only Linux
Ring 0: host OS — Jr. elevate access to
Ring 1: guest OS — host OS
Ring 3: application
HVM (HW VM) performance ↑ → Windows or Linux

Access
AWS can access to Hypervisor (hosts)
(administrator - mgmt plane
MFA must
log lawuate)

Memory Scrubbing
More visibility & contro IP charged by host
physically dedicated

AWS WAF
AWS 외부에서 오는 요청 방어어
cloudfront - globally
(App) Loadbalancer - Regionally

ALLOW everything / DENY everything / count request, etc
{ IP주소, country, request length, }Condition 으로로
{ SQL, script, request header, string }

cf. AWS Shield - DDoS
(advanced) $3000 /real-time response team

Dedicated instance
전용호스트 HW 를 dedicated instance
on demand/ reserved (no 기본값) /spot (90가지)
charged by instance

Dedicated host
place visibility & contro IP charged by host
physically dedicated
Server-bound Software license 등등 ⊕
affinity b/twn host & instance
targeted instance placement
off capacity 로 allocation request.