Trouble shooting
시나리오 기반 문제

logging & monitoring

cloudwatch

ⓐ IAM Usr can't see cloudwatch Dashboard
- IAM User has permission?
  redirect to EC2AutoScale,
- cloudwatch metrics, Log, SNS, etc

ⓑ EC2 Logs into CloudWatch.
- cloudwatch (agent) installed or not?
- cloudwatch agent enabled?/running?
- EC2 instance role have permission to write cloudwatch Log?

ⓒ Unauthorized EC2 instance terminated by Lambda
- cloudwatch events has permission to invoke Lambda
- Lambda has permission to terminate EC2 (excution role)

Cloud Trail

ⓐ cloudtrail Logs not in S3?
- cloudtrail is enabled?
- provided correct bucketname?
- S3 bucket policy?
- S3 & Lambda data event 대량 Volume
  ∴ disabled by default

ⓑ Auditors can't see cloudtrail logs
- Auditor IAM usr & group has read access?
  IAM policy [AWSCloudTrailReadOnlyAccess]

VPC troubleshooting

route table & Security Group & Access control check

ⓐ internet access issue?
- check NAT Gateway / Internet Gateway
- check VPC Flow logs for troubleshooting

Security group (stateful); inbound & outbound needed
NACL (stateless); explicit deny & block specific IpAddr

Eg. VPC peering
- configure a routing table in both VPCs
- non transitive 방식으로 연결

Authentication & Authorization

- Explicit DENY
  overrules everything
- no explicit Deny & at least 1 explicit allow = allow
- Least Privilege
  DENY by default

- AWS organization ★
  Check "permission boundary"

cross account

ⓐ S3 bucket; DEV acct → accessing S3 S(PROD
- DEV accnt permission to call
  PROD IAM role; STS: AssumeRole
- Prod accnt allow dev account to assume role
  & add dev account in trust relationship

ⓑ KMS & CMK
external account accessing other's CMK
- external account has IAM policy to run KMS API calls
  (kms: Encrypt, kms: decrypt, .etc)
- Internal accnt's key policy allows
  external account as trust account in key policy

Lambda

- Function policy : which AWS resource allowed to invoke
  (내가 피리를 불면)
- excution role : excuting 한 뒤 (불면)
  아이들이 따라온

ⓐ Lambda writes CloudWatch Logs
- Lambda excution roles define; writing cloudwatch logs
- & Lambda has permission to write cloudwatch Logs

ⓑ Lambda integrate with RDS that has creds in secret manager.
- Lambda require permission to access secretmanager.
  defined by excution role

ⓒ Does Function policy allows cloudwatch to invoke Lambda?

KMS & CMK

ⓐ specific user/group can't access CMK.
- key policy : resource based, attached to CMK.
  define key users, admin, & trusted external accounts
- IAM policy : assign user, group, role
  define the allowed actions (kms: ListKeys, kms: Encrypt, Decry

identity Federation.

correct API calls
- STS: AssumeRole with WebIdentity : authenticated by ID provider (FB)
- STS: AssumeRole with SAML : 〃 by SAML compliant ID 〃 (AD)
- STS: AssumeRole : 〃 by AWS