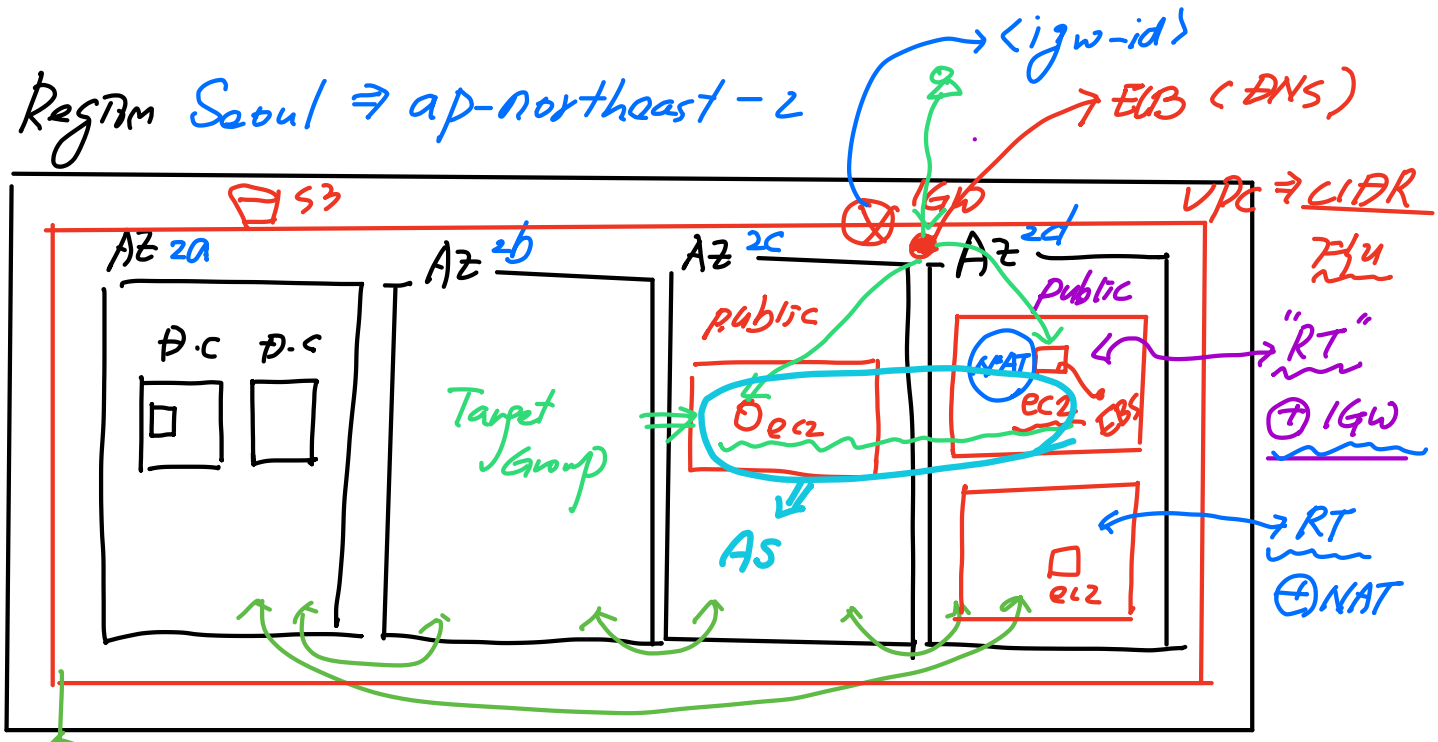
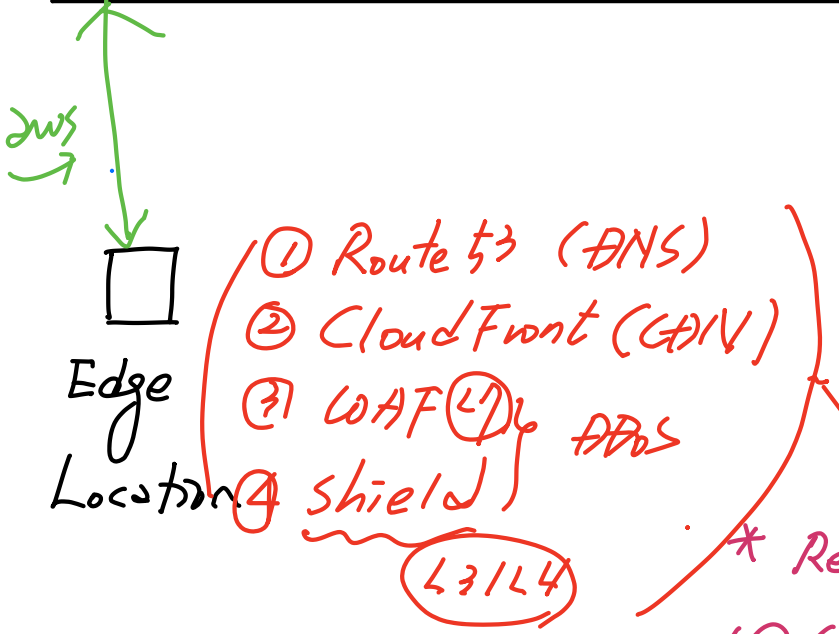
Global Infra + AWS Service





Service → Resource

① Resource-id : EC2

② ARN: arn: aws: service: →

EC2 → EC2 Instance <i-id>

AMI <ami-id>

S3 → S3 Bucket

관리형

① Instance : EC2 — EBS (Instance / volume) ⇒ DB Instance

S/W ⇐ Oracle

RDS, ElastiCache

VPC / Subnet / S.G

② Serverless : OS? S/W? (aws)

S3, DynamoDB

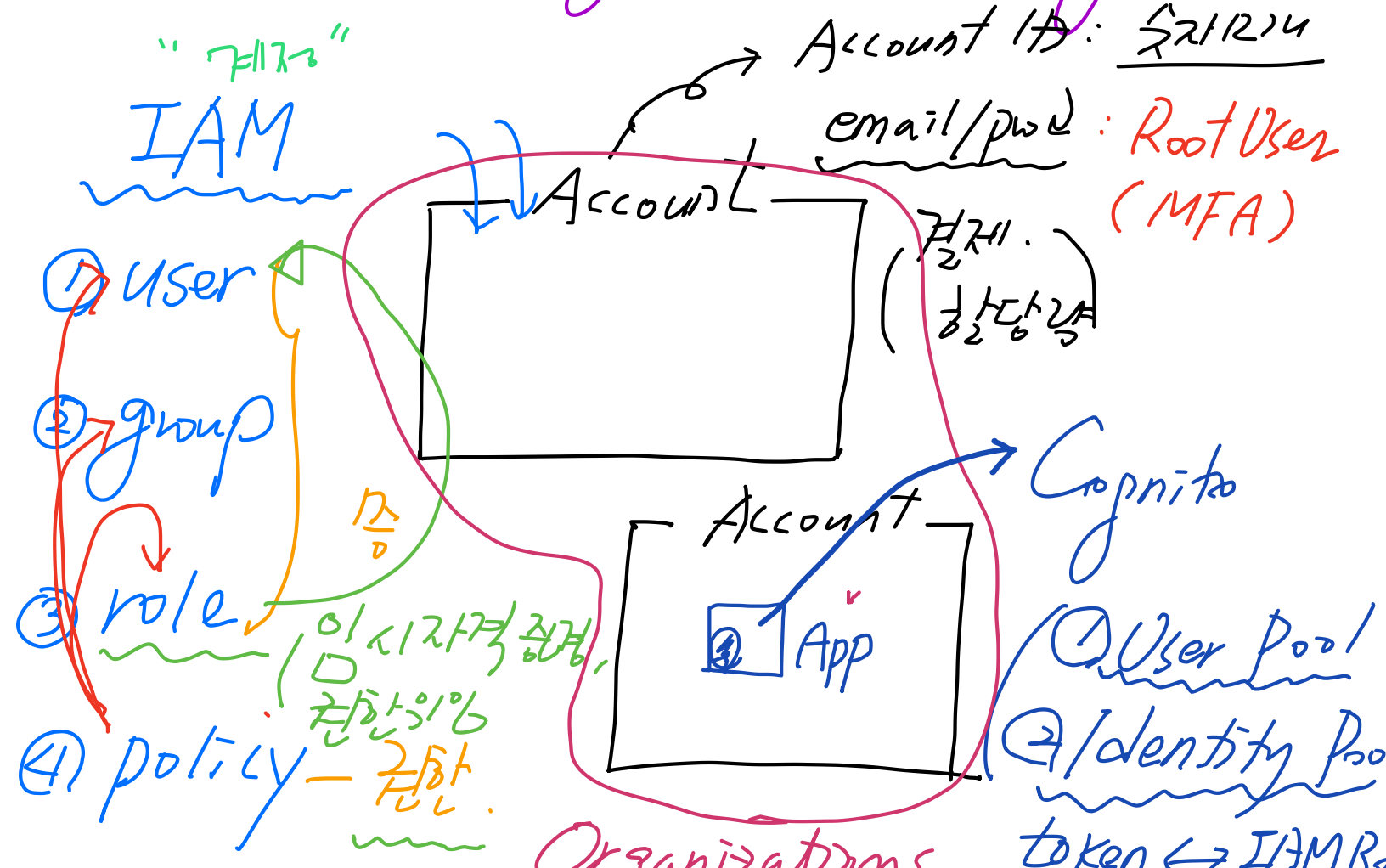
Lambda

API

기능

Authentication & Authorization

① IAM ② Organizations ③ Cognito.



Organizations

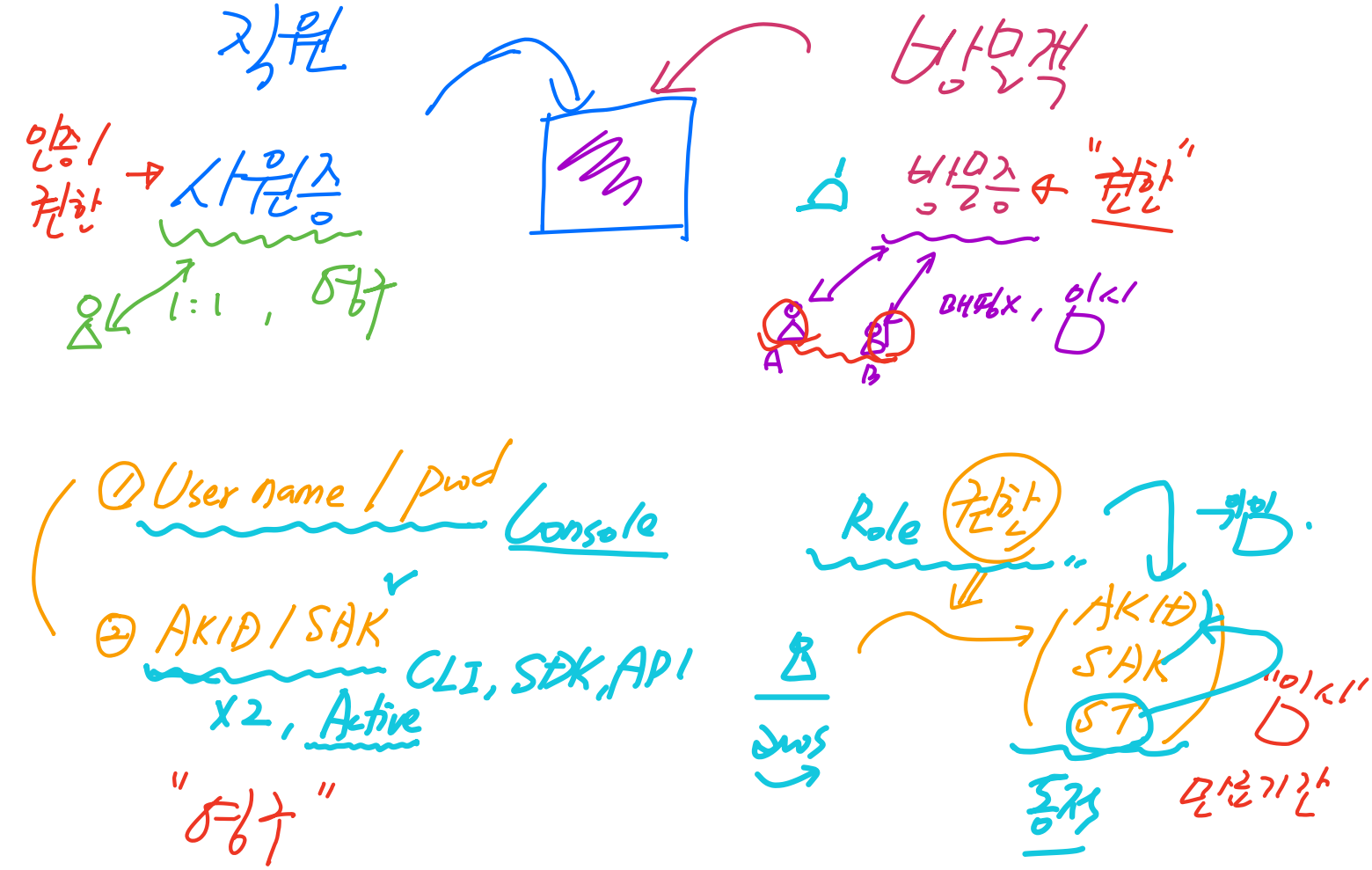
⇒ Organize (tree)

① Account
(Management ⇒ Member ⇒ Resource)

② OU

③ Policy (SCP, Tag Policy)

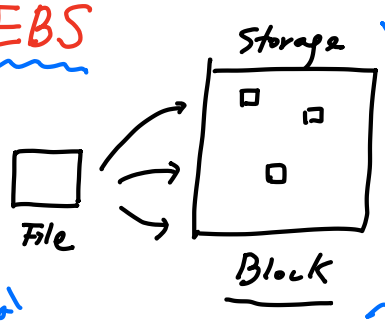
IAM User vs IAM Role

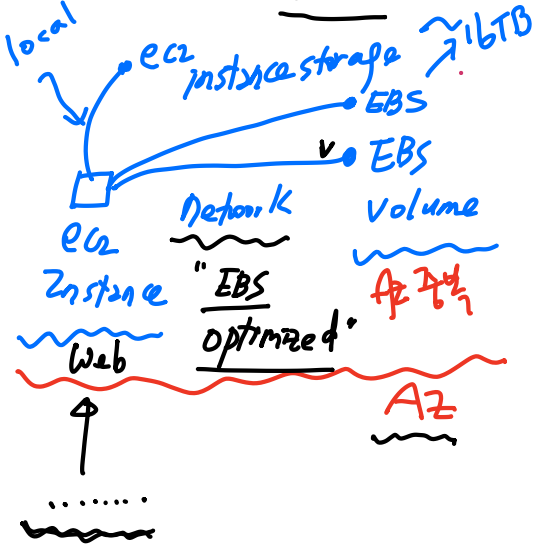


AWS Storage

Block

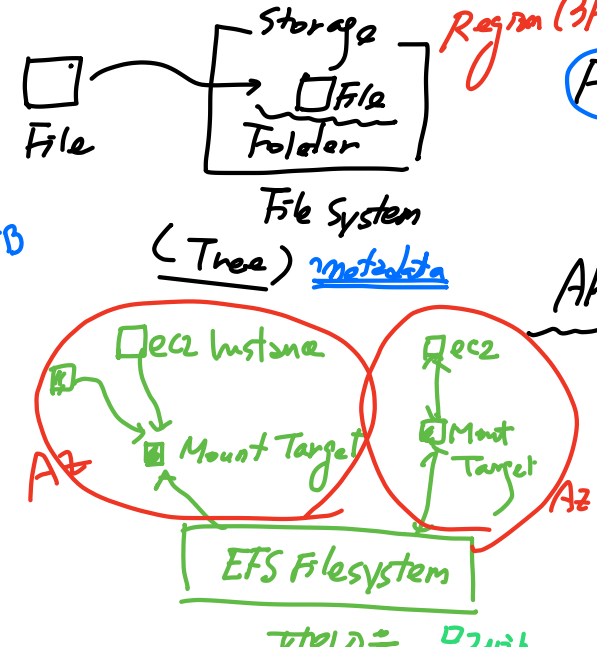
(Instance Storage
EBS





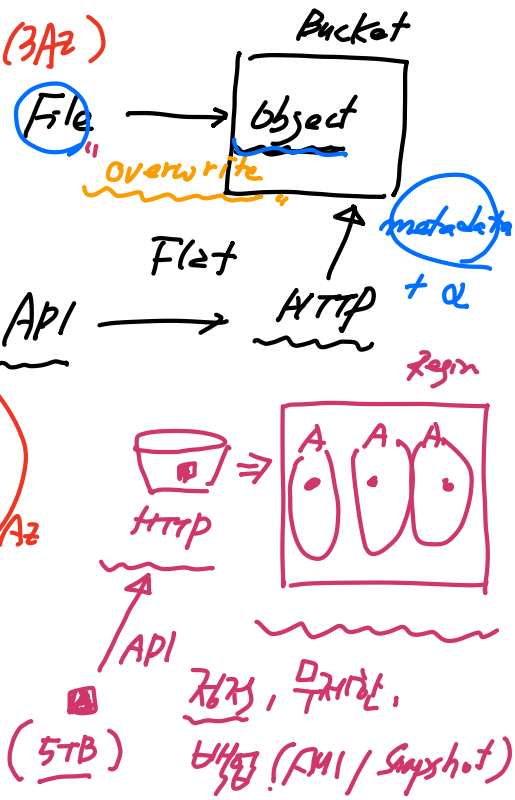
File

(EFS (NFSv4)
FSx (NTFS)



Object

(S3
S3 Glacier



Review Day01

Global Infra

① Region ② AZ ⇒ AWS Service
③ Edge Location : 지연시간 ★

VPC

Region

① CIDR (IP대역) : private IP 10.0.0.0/16 ⇒ 2^{16}
② subnet : AZ. private / public (Internet Gateway)
③ Route Table : 경로 (Dest. / Target)

기본 (X)

"10.0.0.0/16 local" ← 삭제X
(+) 0.0.0.0/0 IGW
(+) 0.0.0.0/0 nat

④ Gateway
① Internet Gateway : in/out (Internet)
② NAT Gateway : out (Internet)
③ Virtual private Gateway : on-premise

기본 (in/out) Allow

⑤ Virtual Firewall
① NACL → subnet, 상태비저장 (in/out)
② Security Group → Resource (Instance), 상태저장 (in)
⇒ EC2 Instance, RDS DB Instance, ALB

Allow

"웹 → ALB → EC2 → RDS"

EC2

① metadata* → public IP, host name, role, ...
v1, v2
/169.254.169.254/

② EC2 Instance Connect ⇒ S.G ⇒ SSH(22)*

CloudWatch

① metric → ② Alarm ★ (임계치)

+α

③ Log

④ event ⇒ EventBridge

⑤ Dashboard

Monitoring → Observability ★

(① metric
② log
③ Trace — X-Ray) CloudWatch

CloudTrail

① API 호출 (누가. 언제. 어떤장비. 무엇) ⇒ JSON
90일 default , 비API → Console Login/Logout

② S3 , CloudWatch Logs ⇒ Audit.

IAM Role

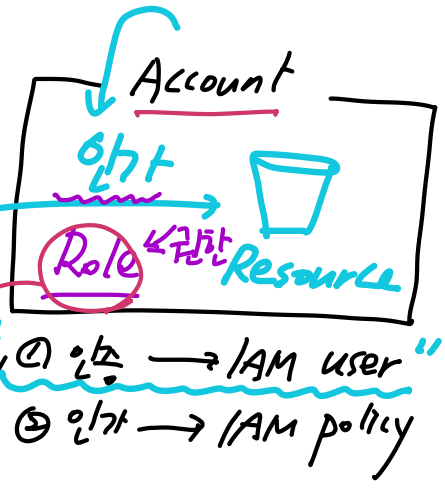
① user ② group ③ role ④ policy

Account

① 외부인증

① 다른 Account
② SAML, OIDC
③ Web (OIDC)

인증



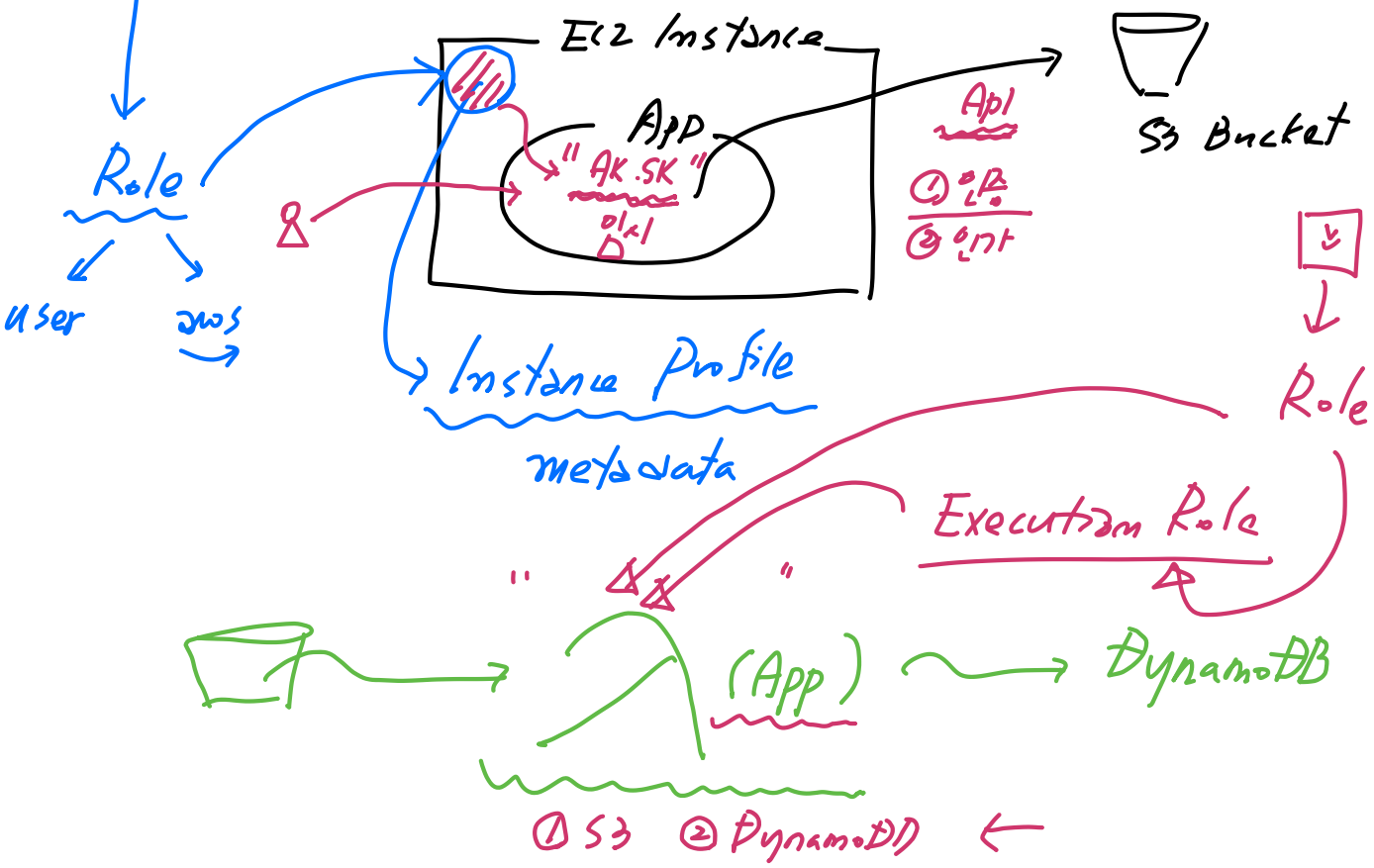
임시자격증명

STS (Security Token Service)

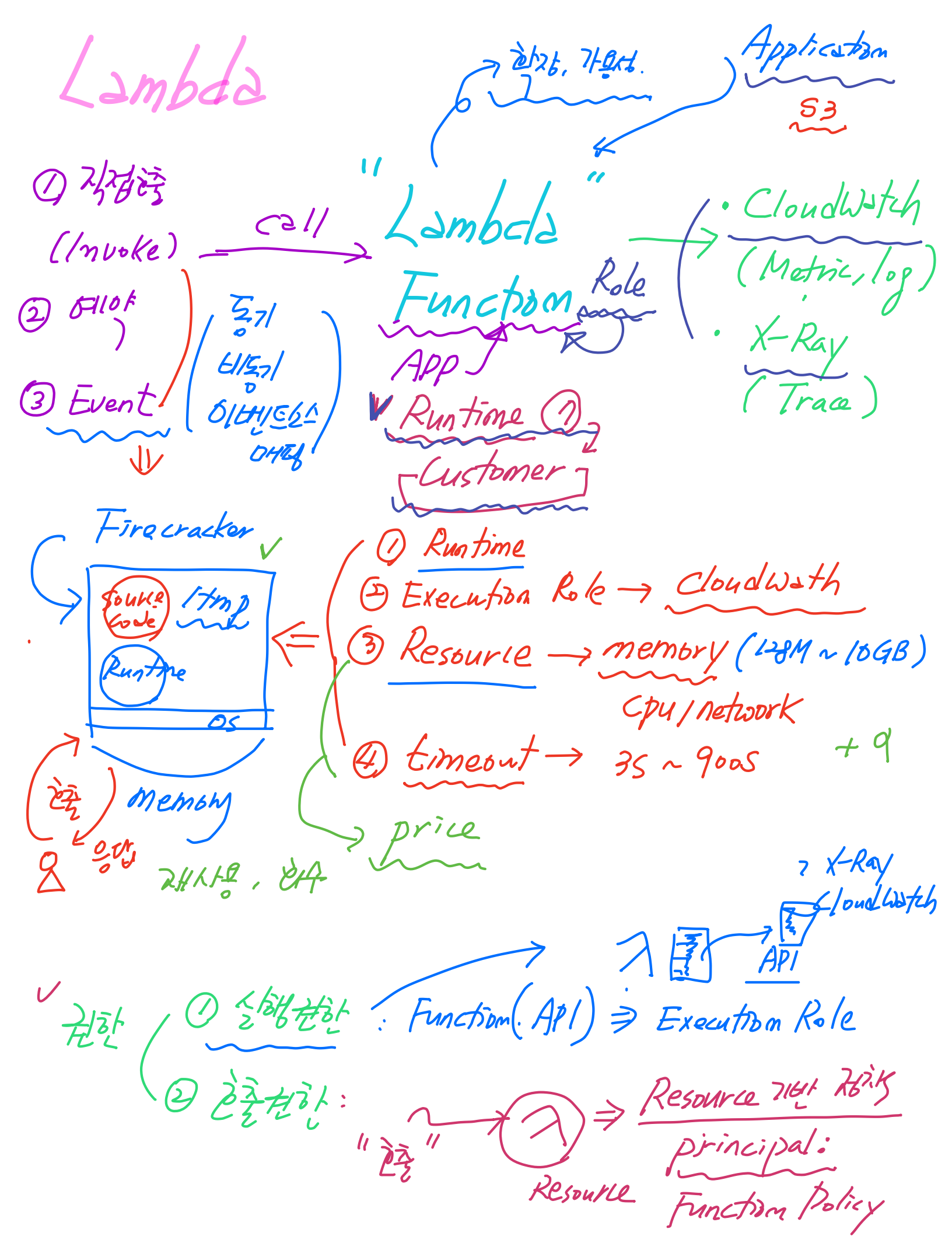
AKID, SAK, Session Token

Policy

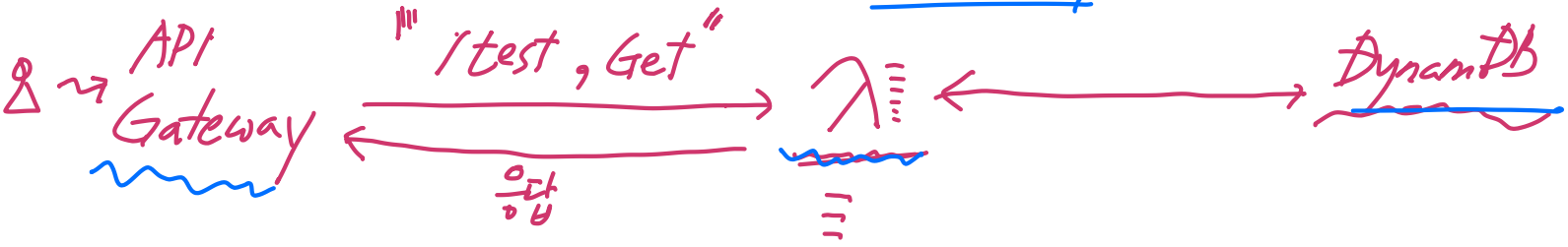
② Aws Service



Lambda

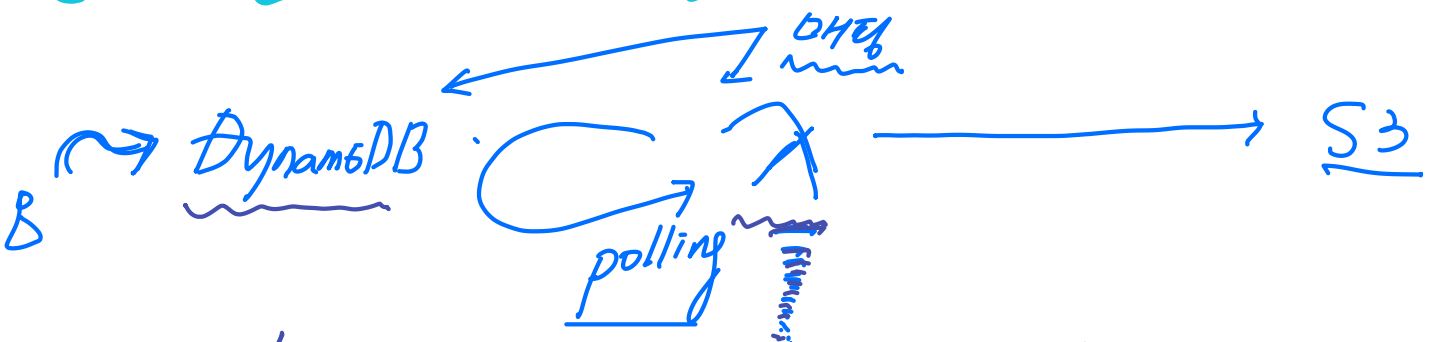

환경, 가용성.
Application
S3
① 직접호출
(Invoke)
call
"Lambda Function"
Role
② 에러
③ Event
동기
비동기
이벤트소스
매핑
App
Runtime ①
Customer
· CloudWatch
(Metric, log)
· X-Ray
(Trace)
Firecracker
source code
Html
Runtime
OS
① Runtime
② Execution Role → CloudWath
③ Resource → memory (128M ~ 10GB)
CPU / network
④ timeout → 3s ~ 900s
+ 9
price
연결
응답
memory
재사용, 보안
? X-Ray
CloudWatch
API
권한
① 실행권한 : Function(API) ⇒ Execution Role
② 호출권한 :
"호출"
Resource
⇒ Resource 기반 정책
principal:
Function Policy

① 동기식 → (① 실행권한 : DynamoDB, CloudWatch ……
② 호출권한 : API Gateway



② 비동기식 → (① 실행 : DynamoDB, S3, CloudWatch ……
② 호출 : S3

③ 이벤트 소스 매핑 : Kinesis, DynamoDB, SQS, MQ



(① 실행 : S3, DynamoDB, CloudWatch …
② 호출 : X