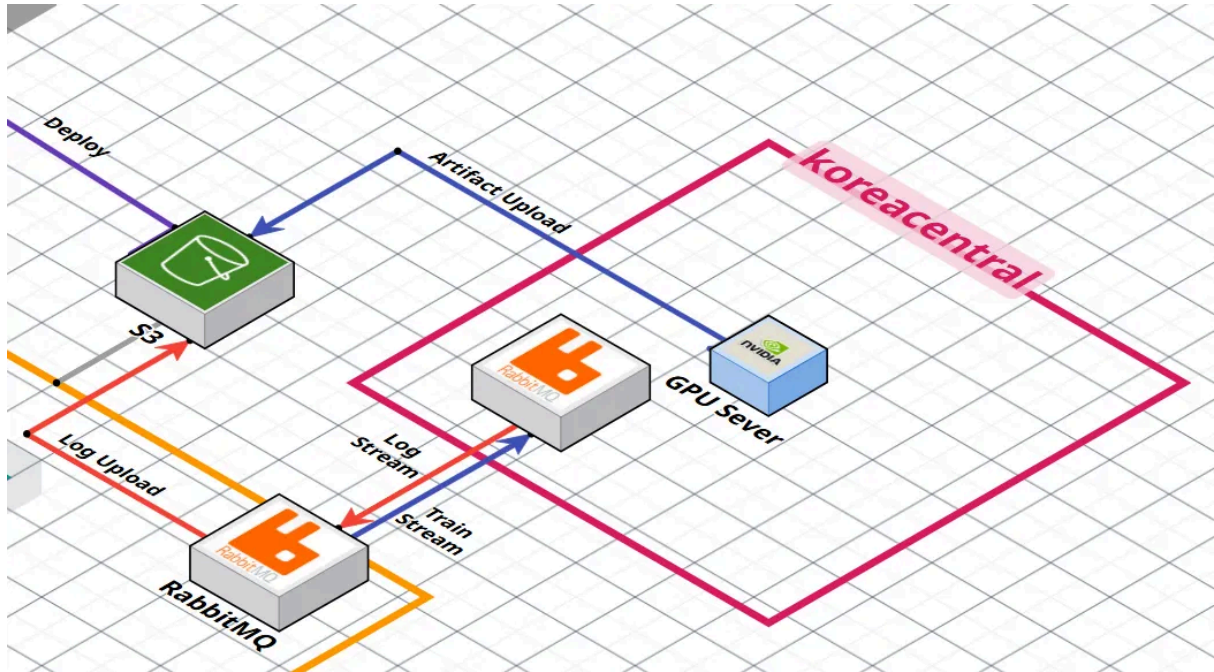


모델 학습 아키텍처



모델 학습 워크플로우

AWS 계정 (내 계정)

— S3 Bucket

— datasets/

— models/

— results/

※ 퍼블릭 차단, ACL 비활성, SSE-S3 암호화 적용

— EC2 (SSAFY 계정)

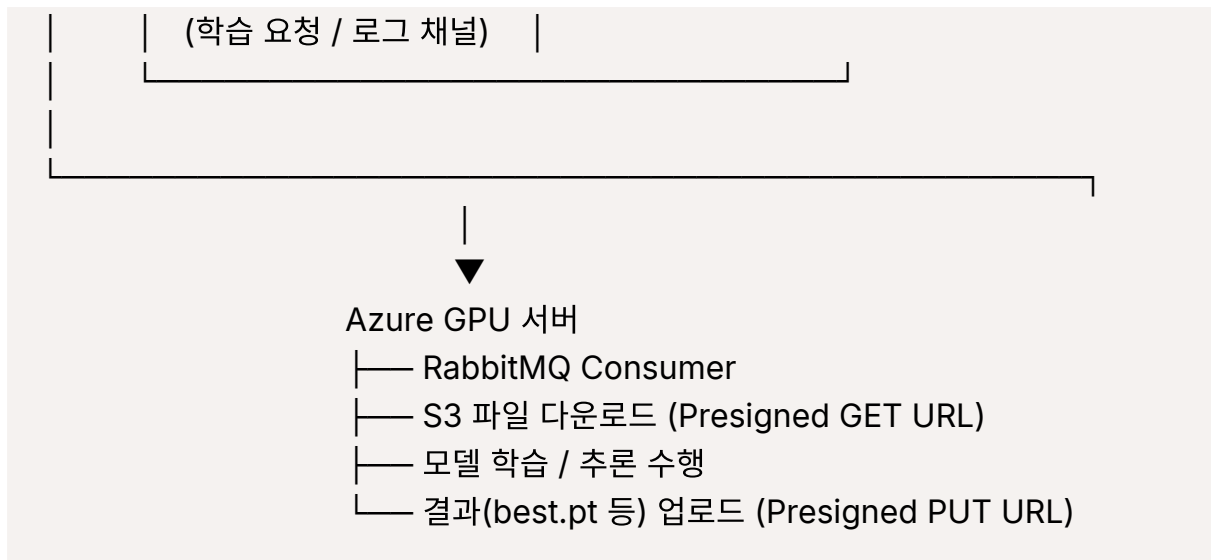
— FastAPI 서버

— RabbitMQ Producer

— boto3 (내 AWS Access Key / Secret Key 환경변수로 등록)

— Presigned URL 생성 (S3 다운로드/업로드용)

RabbitMQ Stream Broker



데이터 플로우

1. EC2(FastAPI) → boto3로 S3 Presigned URL 생성
2. EC2 → RabbitMQ로 학습 요청 메시지 전송

```
{  
  "event": "TRAIN",  
  "dataset_uri": "<presigned GET url>",  
  "model_uri": "<presigned GET url>"  
}
```
3. Azure GPU 서버 → RabbitMQ 메시지 수신
→ S3에서 dataset/model 다운로드 후 학습 수행
4. 학습 완료 후 GPU 서버 → EC2에 결과 업로드 요청 메시지 전송
5. EC2 → Presigned PUT URL 생성 후 RabbitMQ로 전달
6. GPU 서버 → PUT 요청으로 S3에 결과 업로드
7. EC2 → 업로드 확인 및 메타데이터 저장

보안 구조

- S3 : 퍼블릭 액세스 차단 + ACL 비활성 + SSE-S3 암호화 유지
- EC2 : 내 AWS AccessKey/SecretKey로 presigned URL만 생성

- GPU 서버 : AWS 자격증명 없음, presigned URL로만 접근
- RabbitMQ : TLS + 인증 토큰으로 교차 클라우드 메시지 보안