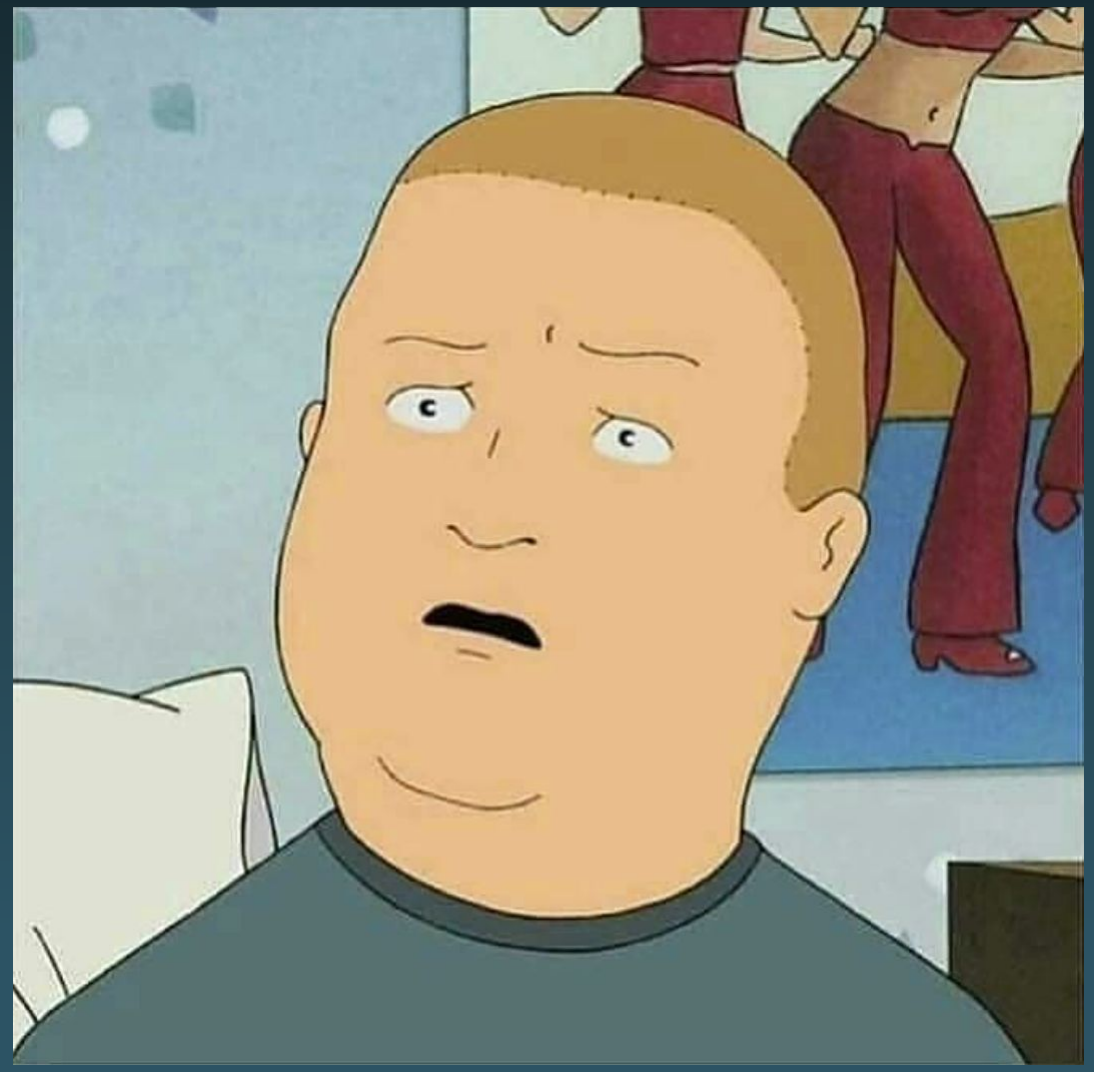
네?

openstack.

점검하라구요?



금융보안원
김용규

발표자 소개

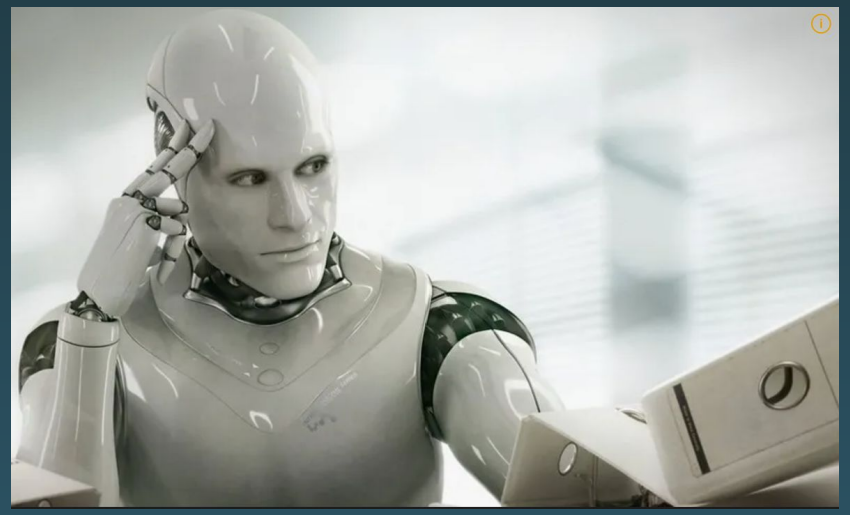
김용규 (ygkim@fsec.or.kr)

- 금융보안원 (2015.04. ~ 현재)
  - (現) CSP 안전성 평가
  - (前) 보안관제, 클라우드시스템 운영 등

- OpenStack, k8s, Ceph 등 다양한 오픈소스 아키텍처를 보안 관점에서 해석하고 설계 구조를 이해하는 데 관심이 많음

발표에 앞서..

시스템을 바라보는 관점

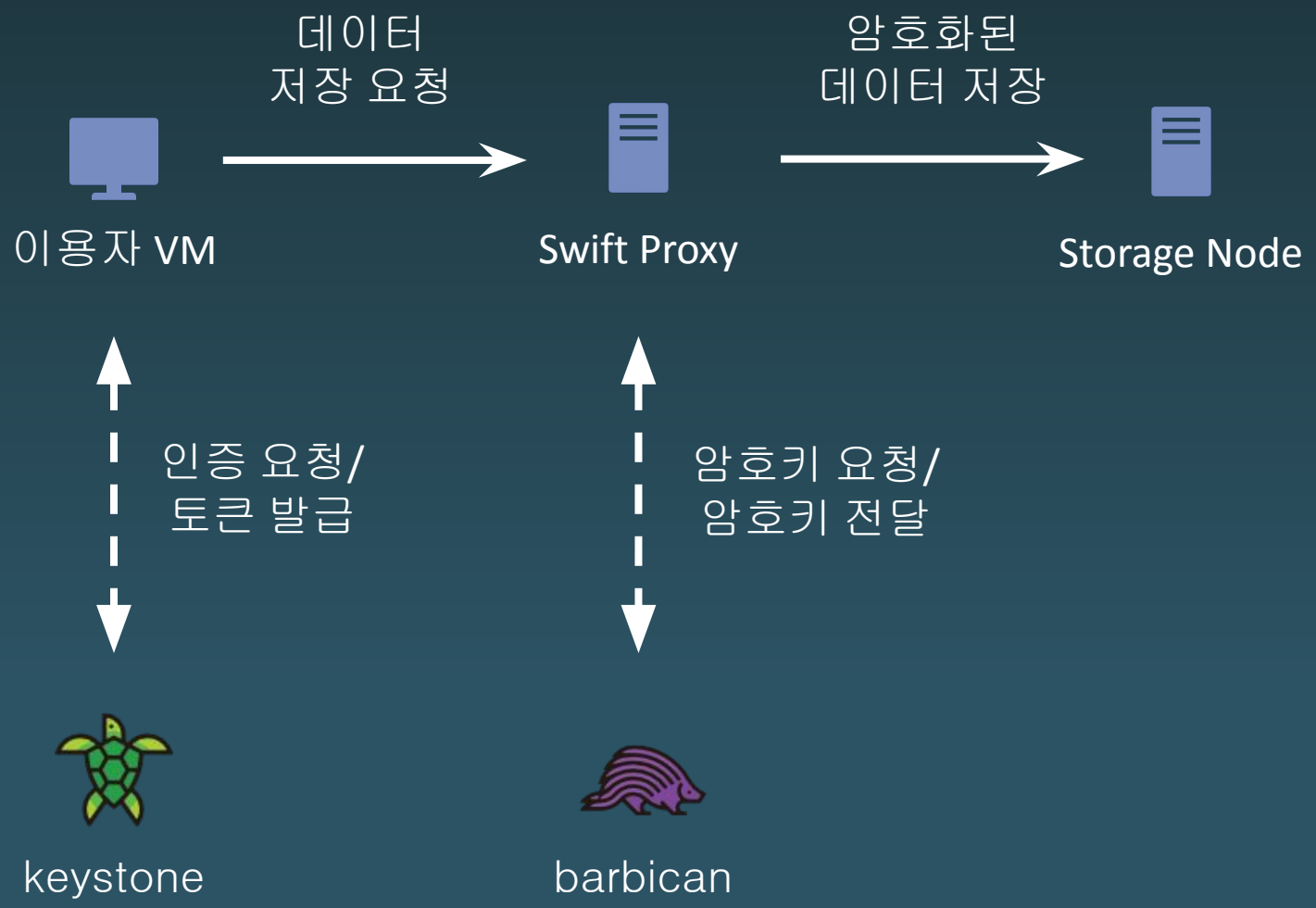


- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)
- 책임 영역(Responsibility Scope)
- 컴플라이언스 준수 여부(Compliance Adherence)

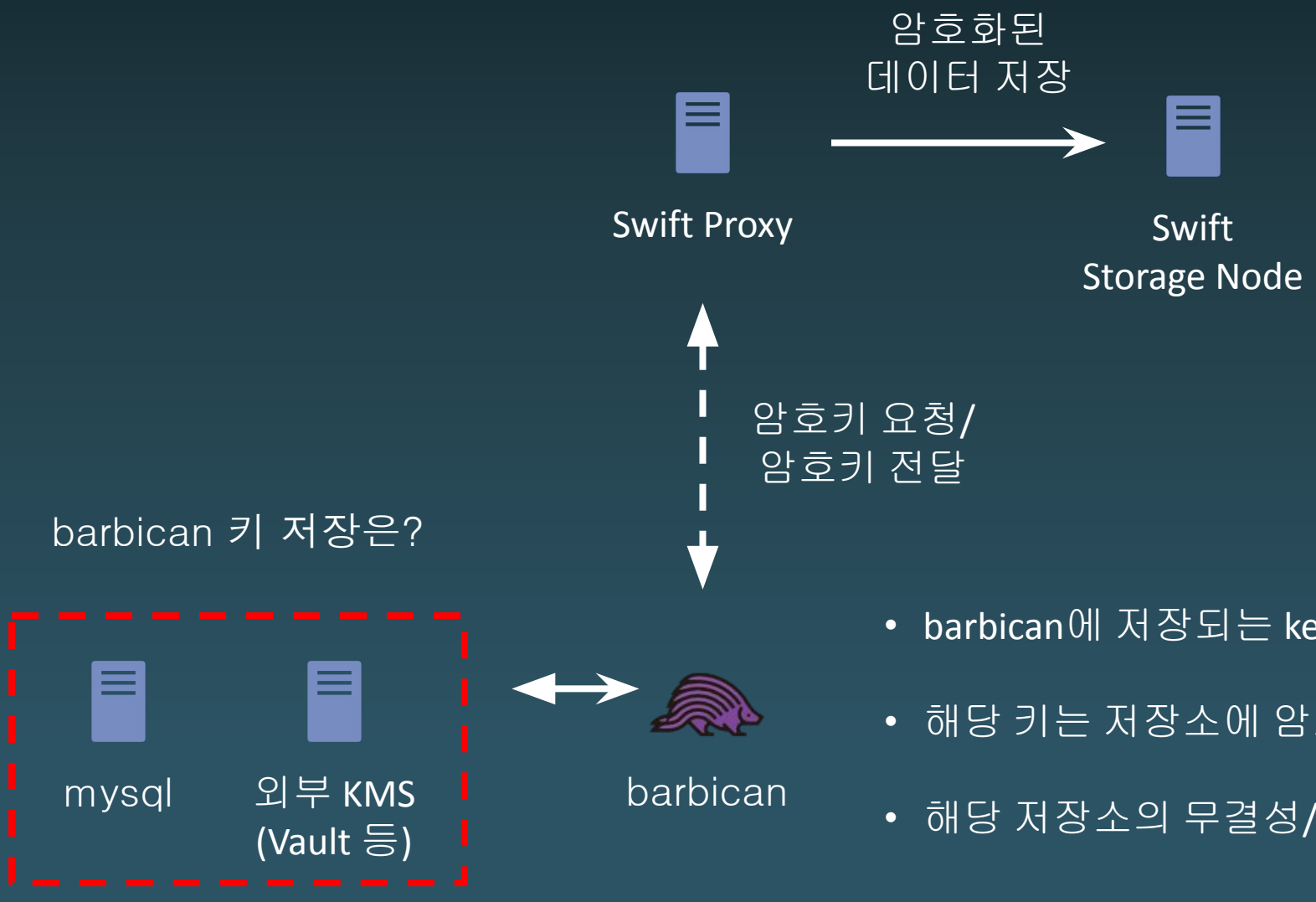
기밀성(Confidentiality)

- 암호화 대상을 식별하고 있는가?
- 암호화에 사용된 알고리즘은 적정한가?
- 암호화에 사용된 키는 안전하게 관리 되고 있는가?

(예시) Swift 기반 Object Storage 아키텍처

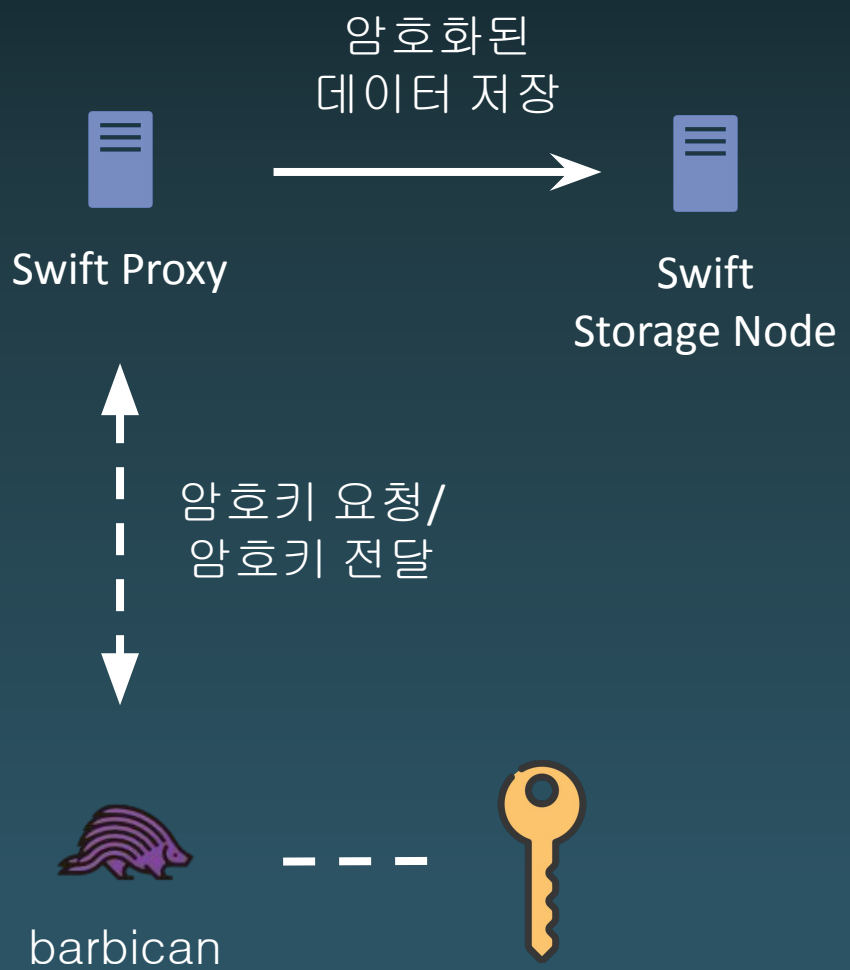


기밀성(Confidentiality)



- barbican에 저장되는 key는 어느 저장소에 저장되는가?
- 해당 키는 저장소에 암호화되서 저장되는가?
- 해당 저장소의 무결성/가용성은 어떻게 보장되는가?

기밀성(Confidentiality)

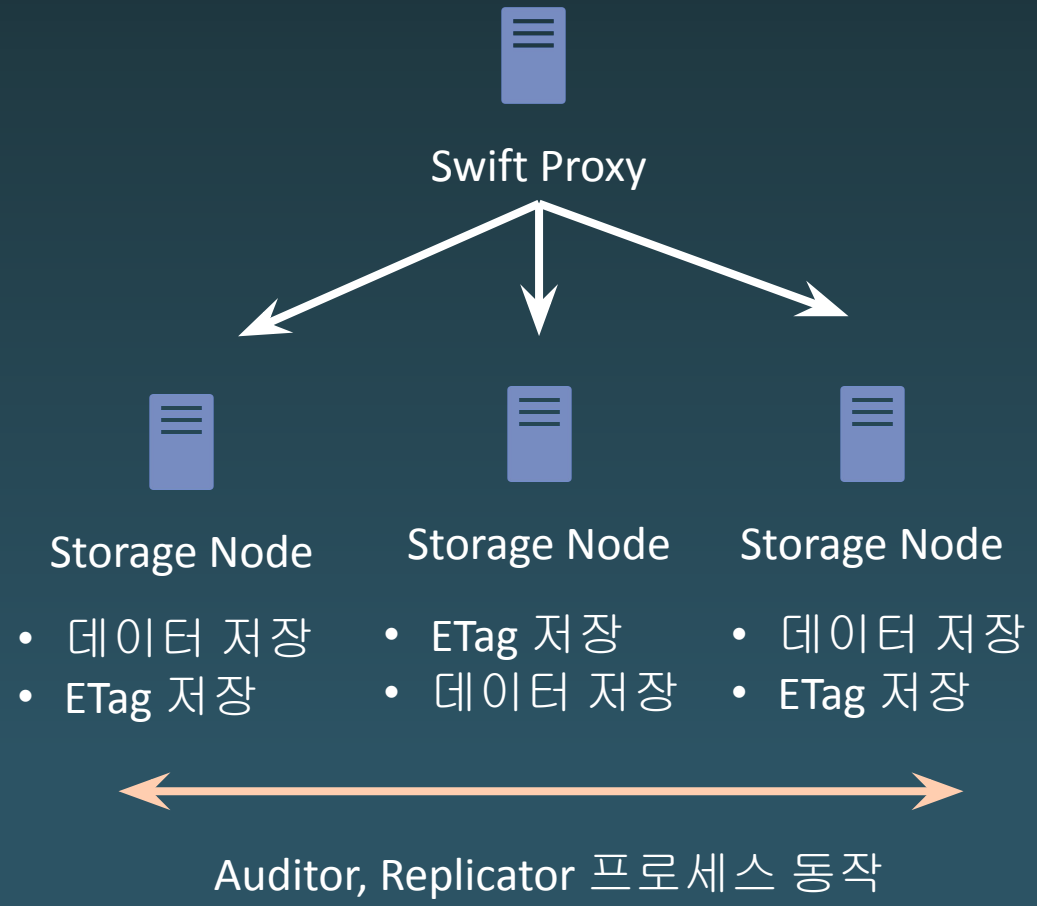


- (생성) 누가 키를 생성하는가?
- (사용) 암호키 접근 가능한 사람은 누구인가?
- (회전) 암호키 회전주기는 어떻게 되어 있는가?
- (백업) 암호키를 별도 백업 수행하는가?
- (삭제/폐기) 암호키 삭제는 언제 이뤄지는가?

무결성(Integrity)

- 저장 시 / 읽을 때/ 저장 중 무결성 검증을 수행하는가?
- 무결성이 깨질 경우 운영자 인지·확인을 수행하는가?

무결성(Integrity)

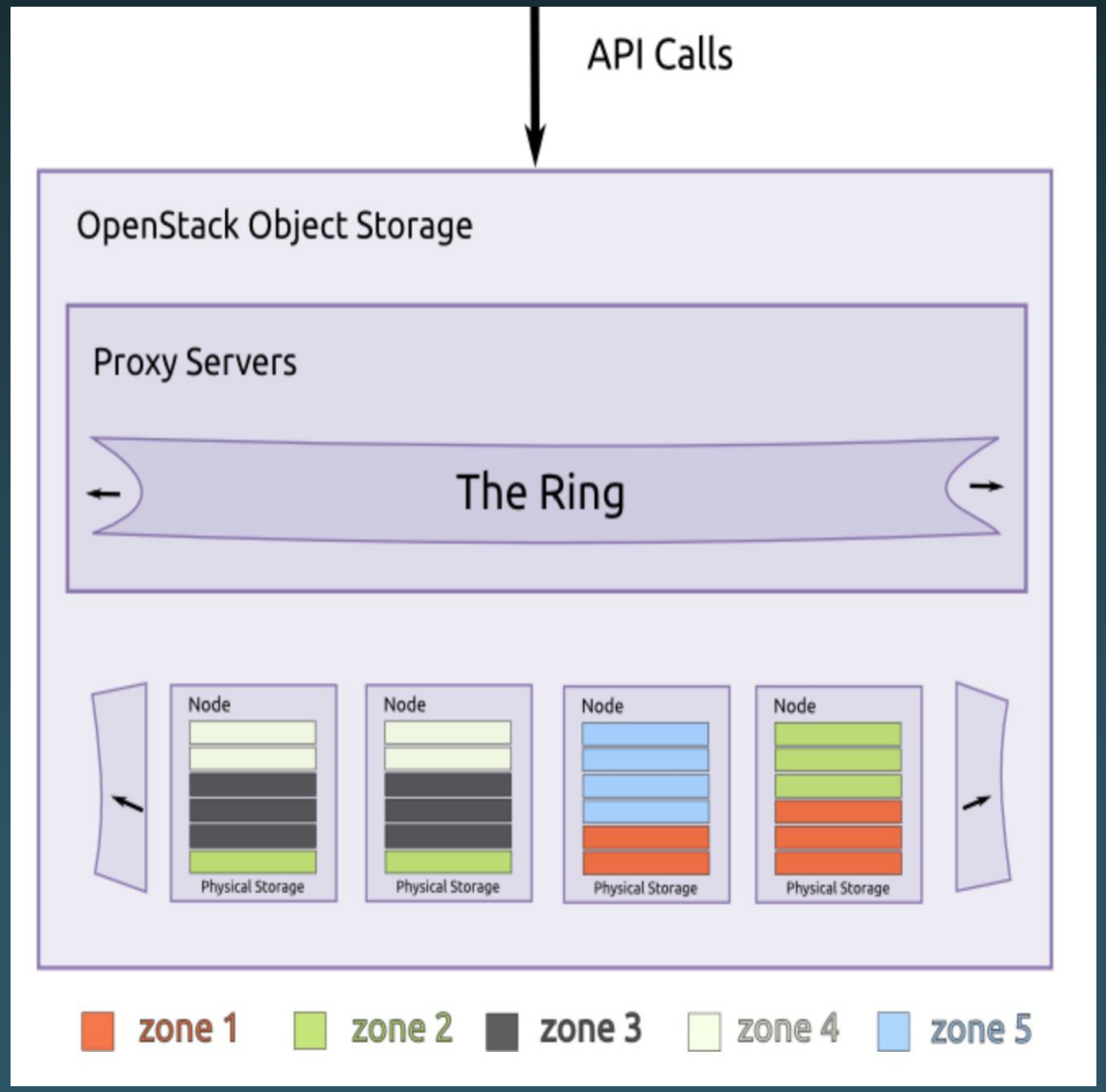


- Auditor 프로세스가 정상 동작중인가?
- 운영자가 Auditor 프로세스 종료 시 인지할 수 있는가?
- Auditor, Replicator가 정상적으로 동작할 경우, 운영자가 확인하는 절차가 존재하는가?

가용성(Availability)

- 서비스에 사용되는 서버 등이 이중화 구성으로 되어 있는가?
- RPO, RTO, Failover 등 복구 목표와 절차가 수립되어 있는가? 해당 복구 목표가 이용자의 컴플라이언스를 준수할 수 있는가?
- 장애 발생에 대비 훈련을 주기적으로 수행하고 있는가?

가용성(Availability)



- Zone 간 복제가 물리적으로 분리되어 있는가?
- 장애 발생 또는 FailOver 시 운영자가 인지할 수 있는가?
- Zone 장애를 가정한 훈련을 수행하고 있는가?

책임 영역 & 컴플라이언스 준수 여부

- 책임 영역

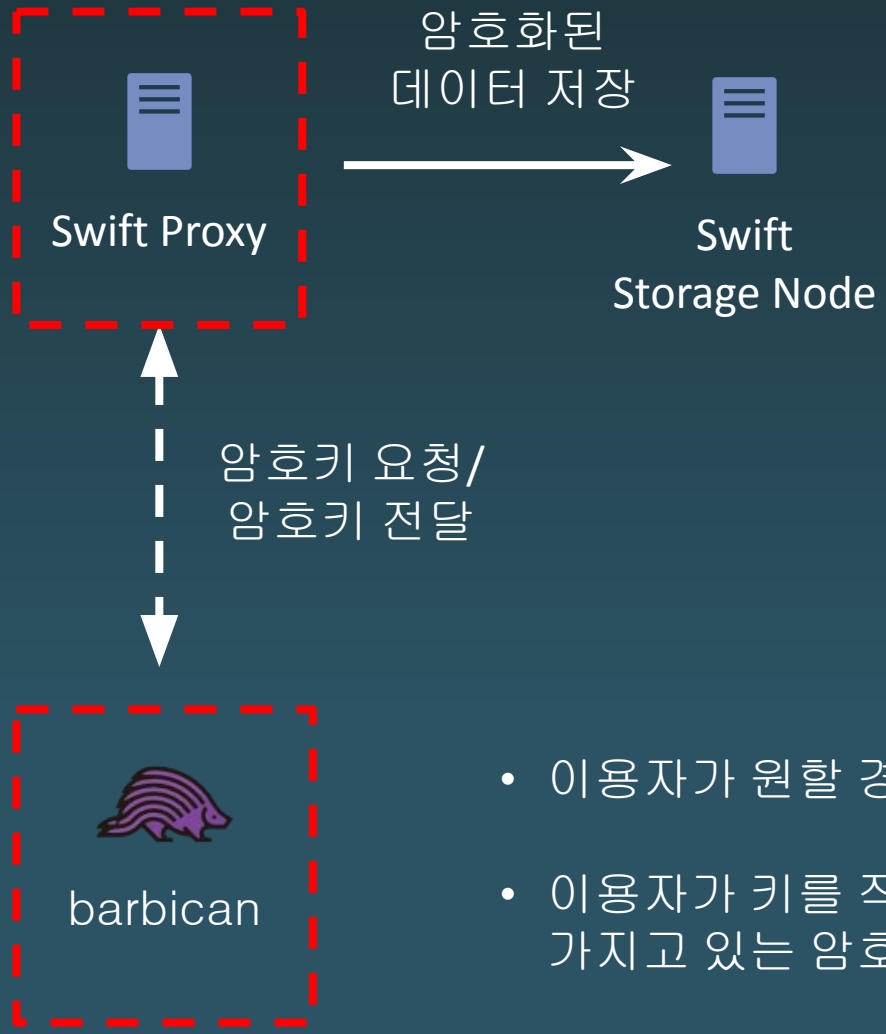
- 서비스 책임영역은 어떻게 구분되어 있는가?
- 이용자 책임영역에 대해 명확히 알리고 있는가?
- 이용자 책임영역에 접근 할 수 있는 경우, 이에 대한 통제방안은 어떻게 수립하고 이행하고 있는가?

- 컴플라이언스 준수 여부

- 관련 산업에 해당하는 관계 법령 및 법규를 준수하고 있는가? (개보법, 정통망법, 클라우드법, 전자금융감독규정 등등..)
- 관계 법령 및 법규가 변경되었는지 주기적으로 살피고, 이를 정책 및 운영에 반영하고 있는가?

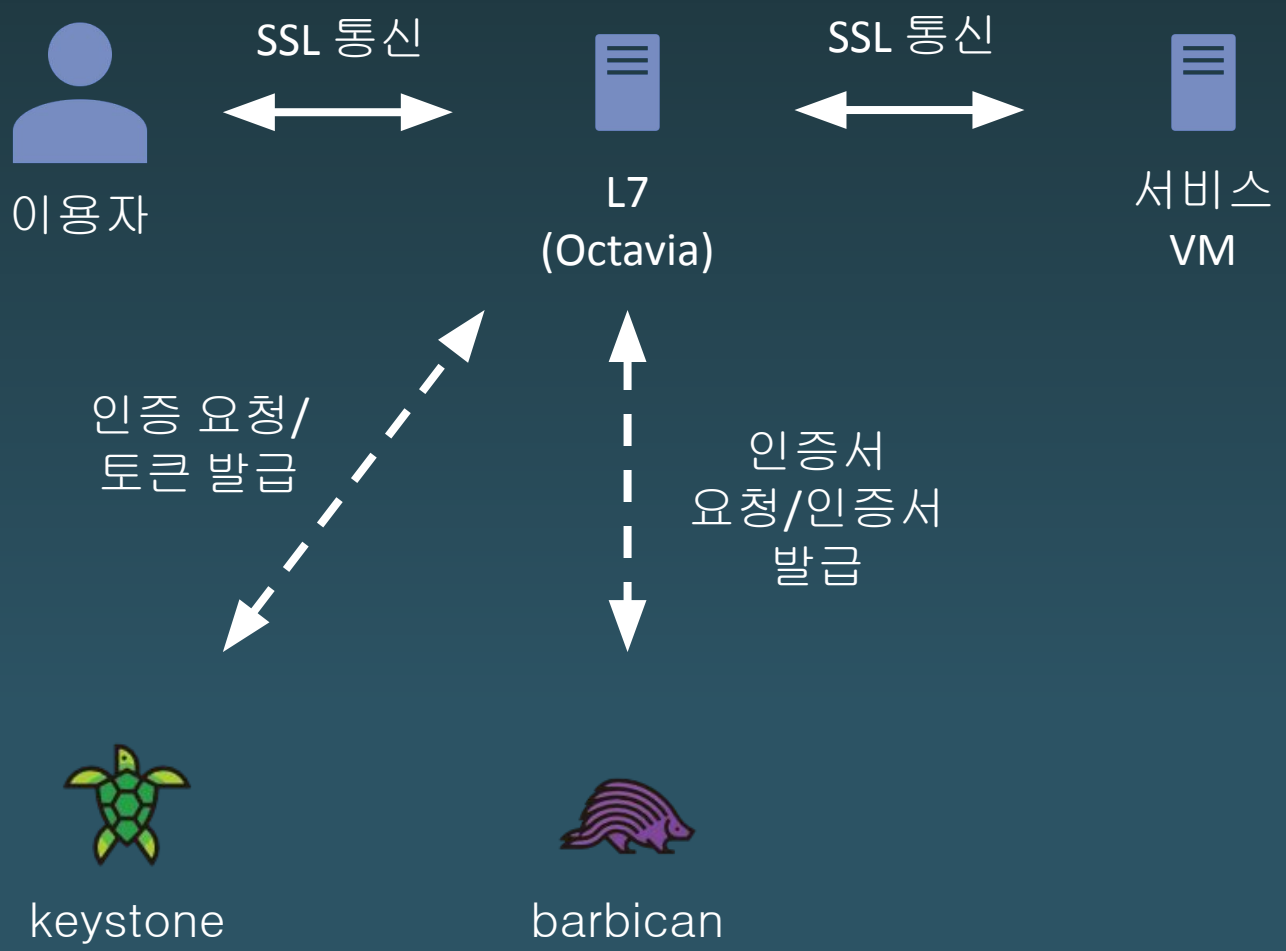
책임 영역 & 컴플라이언스 준수 여부

- 운영자가 이용자 데이터 영역에 접근할 수 없는가?
- 이용자 요청 시 audit 로그 제출이 가능한가?

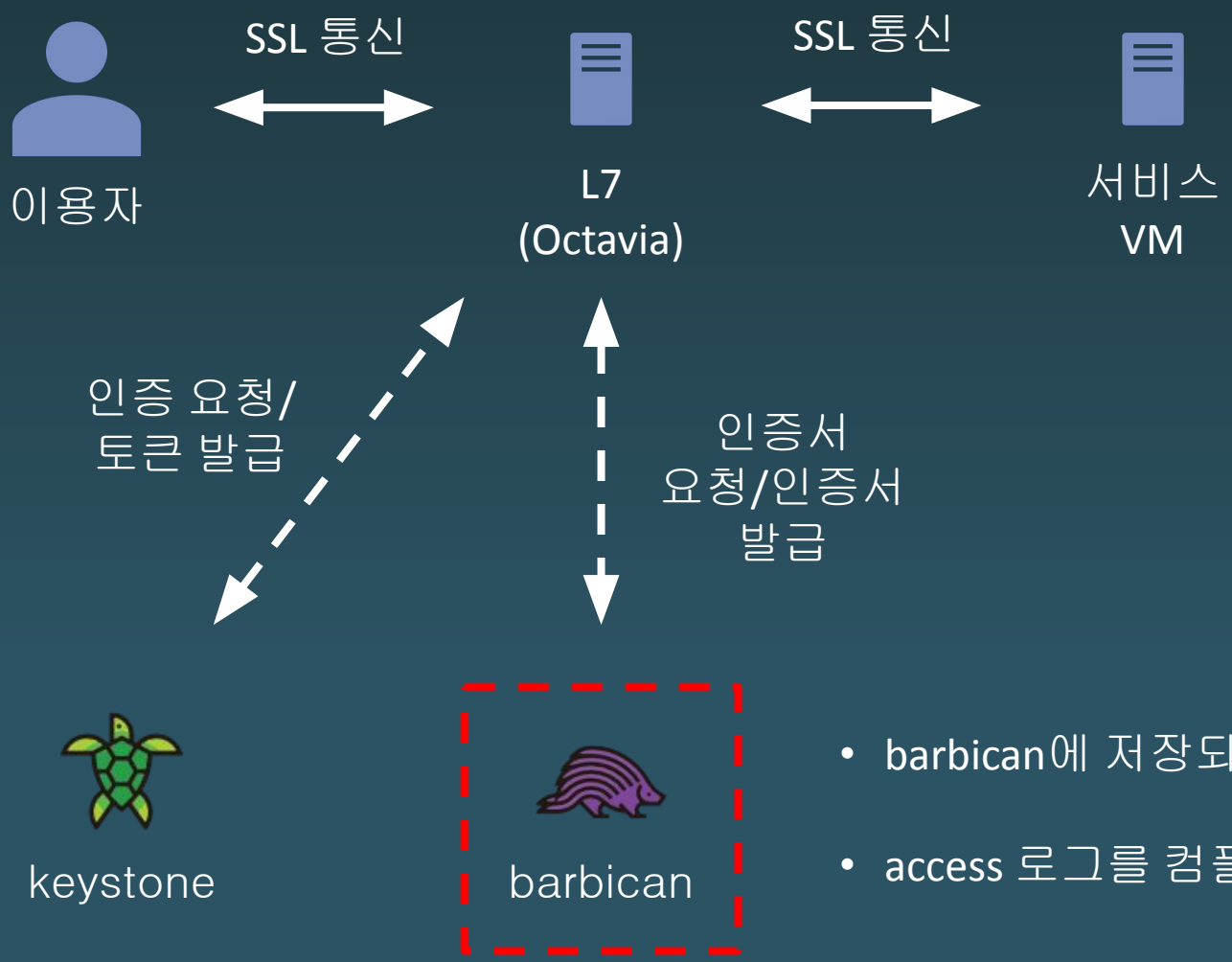


- 이용자가 원할 경우 이용자 키로 암호화가 가능한가?
- 이용자가 키를 직접 핸들링하지 못할 경우, 이용자가 가지고 있는 암호키 생명주기 정책 지원이 가능한가?

(예시) Octavia 기반 L7 아키텍처

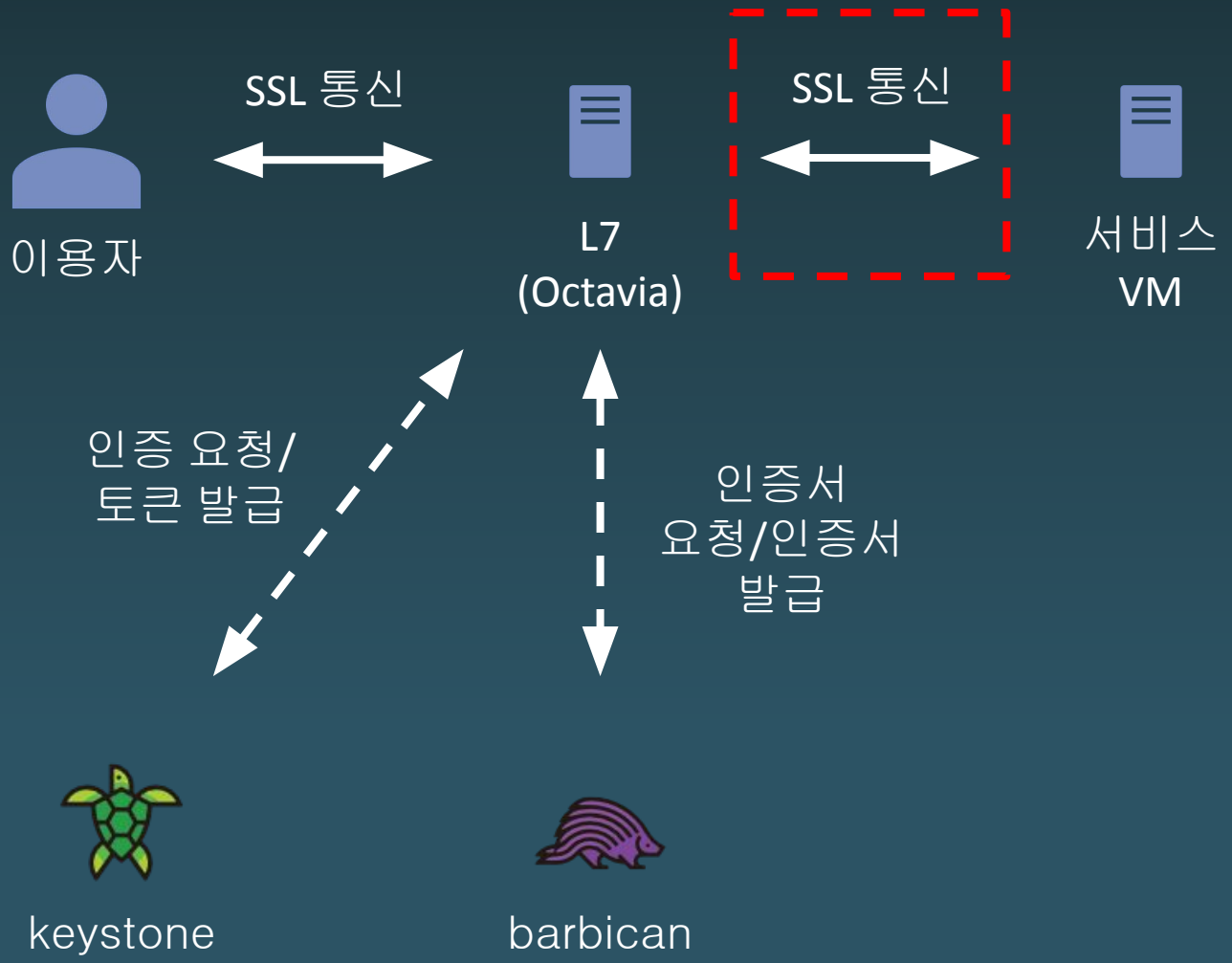


(예시) Octavia 기반 L7 아키텍처



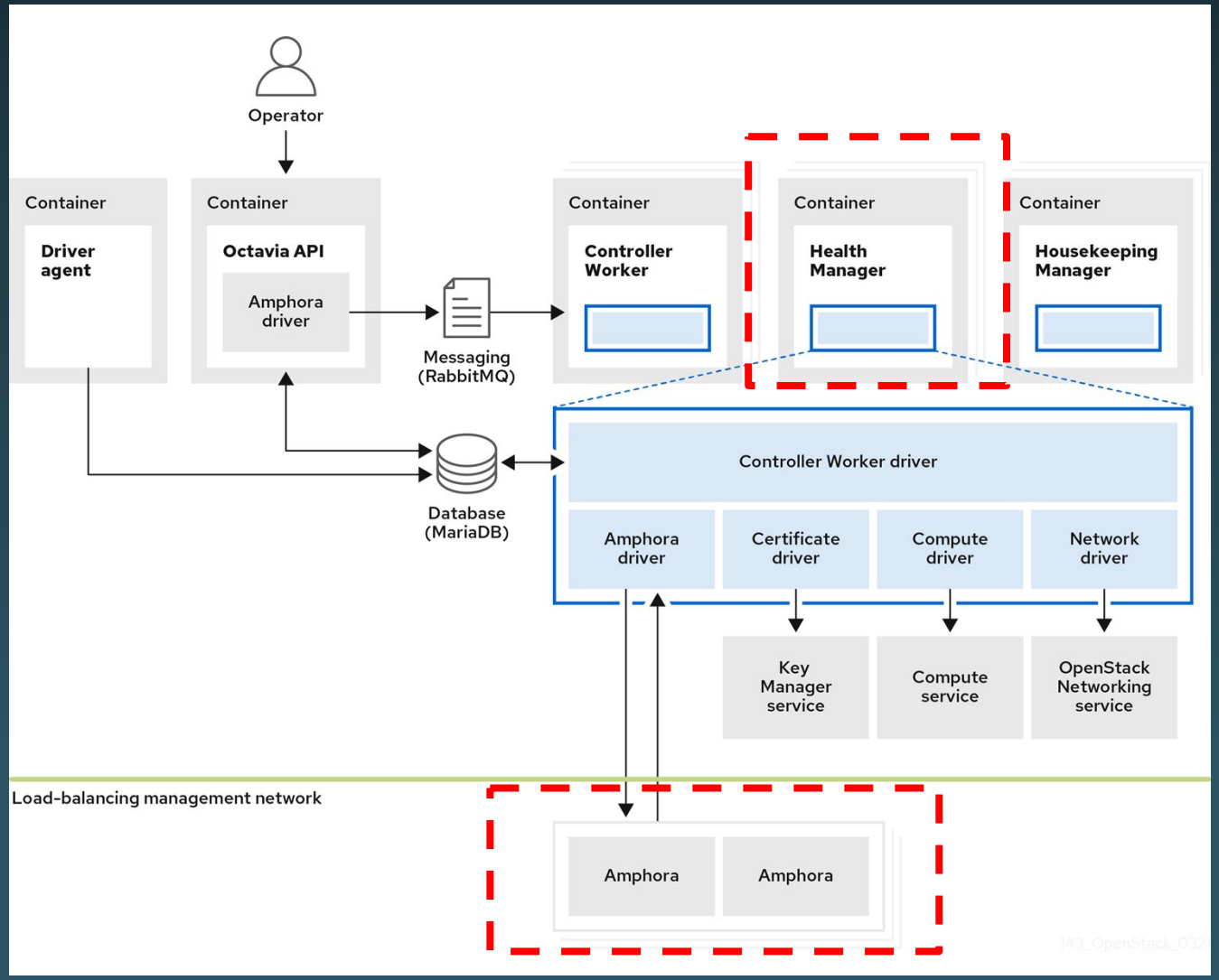
- barbican에 저장되는 인증서 관리 책임영역은?
- access 로그를 컴플라이언스에 맞게 관리하고 있는가?

(예시) Octavia 기반 L7 아키텍처



- barbican에 저장된 인증서로 L7까지 TLS 연결이 끝났는데, L7과 서비스 VM간 SSL 통신은 어떻게 구현되었는가?

(예시) Octavia 기반 L7 아키텍처

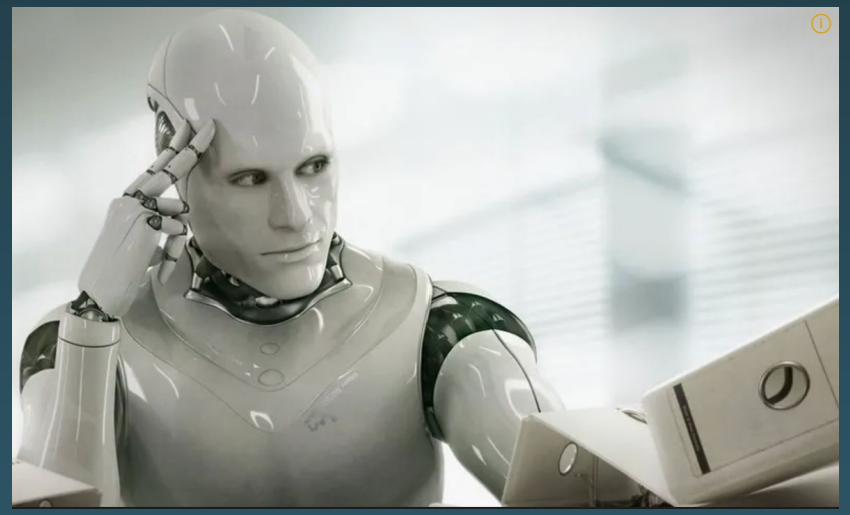


- Amphora 이중화가 되어 있는가
- Health Manager 장애 시 운영자가 인지 가능한가?

마무리 정리

운영자 관점

audit 관점



Q&A

감사합니다