03. Kafka 거버넌스

작성자 : 알 수 없는 사용자 (pj.youngsukkim24@kalmate.net), 최근 변경 : 김원일 - 5월 10, 2024

클라우드기반 메시징 플랫폼 거버넌스 정책

메시징 플랫폼의 효율성 향상, 안정성 및 확장성을 강화할 수 있으며, 실시간 데이터 처리/통합과 분석, 비즈니스 운영을 현대화 하여 경쟁 우위를 확보 할 수 있는 클라우드기반 메시징 플랫폼을 구축하기 위한 거버넌스를 수립 함.

- 실시간 데이터 처리
- 확장성 및 내결함성
- 데이터 통합 및 관리
- 스트림 처리 및 분석
- Event Driven Architecture
- 데이터 파이프라인 현대화
- 오픈소스 생태계 적용
- 다양한 레퍼런스 활용

1. 원칙

원칙

- **환경 구성 원칙**
  - Confluent Kafka 환경은 Confluent Cloud에 Dedicate 자원으로 PRD(운영), STG/DEV(개발/스테이지)로 2개의 환경으로 구분하여 운영
  - 명명 규칙은 STG/DEV 공동 사용 자원의 경우 "TEST"로 정의
  - Confluent Cloud의 Dedicate VPC와 대한항공 AWS 환경의 VPC는 PrivateLink를 통하여 연계 운영
  - PrivateLink 구성은 Shared VPC의 3개 AZ에 구성
  - Confluent Cloud Console의 Dedicate VPC 자원 접근을 위해 AWS Route53 Private Hosted Zone으로 각 Kafka 클러스터에 대한 도메인 존을 구성
  - PrivateLink에 대한 접근 제어는 Shared VPC이 Private Endpoint의 SecurityGroup으로 구성
  - 오피스 망에서의 접근을 위해 상암 Private DNS(keseldc101, keseldc102)에 Kafka 클러스터에 대한 도메인 존을 AWS Route53 Inbound Resolver로 Forwarding 구성
  - Connect는 통합 운영(PRD), 통합 Stage(STG), 통합 개발(DEV) 환경의 각 EKS 클러스터에 설치하여 구성
  - Confluent Kafka 제품 중 Schema Registry는 Public SaaS 제품으로 구성하여 Confluent Cloud의 Dedicate 환경 외부에 구성
- **Confluent Kafka 적용 범위**
  - Confluent Kafka 는 내부 시스템 간 연계에 활용
  - 외부 시스템과의 연계 시에는 MQ를 연계 채널로 구성하고 MQ와 Confluent Kafka간에 IBM MQ Connect로 연계
- **User와 Service Account**
  - User의 권한은 Confluent Cloud Console의 접근 및 사용 권한으로 국한 함.
  - Application의 권한은 반드시 Service Account를 할당 받아 사용하는 것을 원칙으로 함.
- **Topic 권한 부여 원칙**
  - Topic은 송신자 소유를 원칙으로 함.
  - Topic의 업무 구분 및 시스템 명은 송신자 기준으로 부여 함.
  - 소유 Topic의 권한은 Read, Write 부여
  - 수신 Topic의 권한은 Read 부여

레이블 없음