AWS_210806

*Amazon CloudFront

Amazon CloudFront는 글로벌 CDN(Contents Delivery Network) 서비스로 저지연성과 고속 전송 속성을 지닌 콘텐츠 배포 기능을 제공. 콘텐츠 사용자 와 가까운 지역(엣지 로케이션)에 네트워크망을 구축하고 지역별 엣지 캐시를 통 해 사용자 경험 수준을 높여줌.

*Amazon CloudFront의 활용

정적 콘텐츠 캐싱, DDoS 공격 대응, 강화된 보안성, API 호출 가속화, 소프트웨어 배포, 비디오 스트리밍 등.

*AWS 웹 애플리케이션 방화벽(WAF)

-AWS가 제공하는 웹 애플리케이션 방화벽 서비스로, 웹 애플리케이션을 보호하는 역할. 커스터마이징 기능한 보안 규칙 정의를 통해 웹 애플리케이션에 대 한 접근을 허용 또는 거부할 수 있음.
-주요 용도 = 침해 시도로부터 보호(SQL 인젝션 공격, 크로스 사이트 스크립팅(XSS) 공격 등), 악성 요청 대응, DDoS 공격 방어 등.
-WAF는 CloudFront와 통합해 CDN의 배포 용량과 확장성을 높일수있음.
-WAF는 ALB(Application Load Balancer)와 통합해 ALB에 연결된 오리진 웹 서버를 보호할 수 있다.

*Amazon SQS(Simple Queue Service)

-클라우드 아키텍처 설계 시, 개발, 배포, 유지가 좀 더 쉽도록 애플리케이션을 분할해 작은 블록으로 구현하는 방식이 권장됨. 메시지 큐는 이와 같은 분 산 애플리케이션의 소통과 조정을 돕는다는 측면에서 의미가 큼.
-또한 분할된 애플리케이션의 코드는 좀 더 간소해지므로 성능, 신뢰성, 확장성이 높아지는 장점이 있음.
-매시지 큐는 클라우드 시스템의 여러 부분이 비동기적으로 서로 소통하고 업무 를 조정하도록 도우며, 임시로 메시지를 저장하는 버퍼buffer 메시지의 수신 및 발신을 위한 연결 부분인 엔드포인트(endpoints)를 제공.
-사용자는 큐에 메시지를 넣거나 큐에서 메시지를 꺼내 볼 수 있으며 보통의 메시 지는 작은 용량의 데이터로서 요청, 응답, 오류 메시지 또는 보통의 정보를 포함.

*Amazon SNS

-Amazon SNS(Simple Notification Server)는 클라우드 기반의 노티피케이션 서비스로 설정 및 관리 용이성은 물론 높은 수준의 확장성, 유연성, 비용효율성을 갖추고 있음. Amazon SNS는 서버리스 및 마이크로서비스 아키텍처에서 사용되는 비동기적인 서비스 대 서비스 커뮤니케이션을 제공하며, 특정 주제, 즉 토픽(topic)의 메시지를 배포하는 즉시 이 토픽에 구독 신청을 한 서비스가 해당 메시지를 받아볼 수 있음.

-Amazon SNS를 이용하려면 먼저 토픽을 생성해 구독 주제 또는 이벤트 타입을 지정필요.

-토픽에 구독 신청을 한 모든 컴포넌트가 전파 메시지를 수신할 수 있으며, 원치 않는 메시지는 구독자의 메시지 필터링 정책으로 걸러낼 수 있음.

*AWS Step Functions

-시각화된 워크플로를 통해 분산 애플리케이션 및 마이크 로 서비스 컴포넌트의 관리를 돕는 완전 관리형 서비스로서.

-기존의 Amazon 심플 워크플로, 즉 SWF를 대체하기 위해 만들어짐.

-Step Functions는 매우 작은 셀 스크립트 명령부터 수십억 개의 복잡한 임무에 이르기까지 매우 간단하게 스케일업 또는 스케일다운 가능.

-사용자는 AWS Step Functions를 이용해, 애플리케이션을 상태 저장 및 관리를 위한 스테이트 머신(state machine)으로 정의하고, 앱의 동작을 한 데 모아 일련의 스텝으로 관리할 수 있도록 도움.

-스테이트 머신에서 스테이트는 임무, 연속적 스텝, 병렬적 스텝, (선택) 의사결정 수, (대기) 타이머 등이 될 수 있음.

*AWS Elastic Beanstalk

-Elastic Beanstalk를 이용하면 AWS에 애플리케이션을 쉽고 간편하게 배포, 모니 터링, 확장가능. Elastic Beanstalk는 웹 애플리케이션을 배포할 수 있는 가장 간단하고 신속한 방 법이며, 사용자가 코드만 업로드하면 EC2, ECS, Auto Scaling, ELB 등 AWS 리소스에 대한 프로비전 업무를 대신 처리함.

-Elastic Beanstalk가 웹 애플리케이션 실행과 관련된 모든 인프라를 관리하므로, 사용자는 인프라 관리에 신경쓰지 않아도 되며, Elastic Beanstalk를 통해 관리 업무를 일원화할 수 있음.

-Elastic Beanstalk 애플리케이션은 실행 환경, 애플리케이션 버전, 저장 환경 설정 세 가지 핵심 요소로 구성.

1) 실행 환경(environment) = EC2, RDS, ELB, Auto Scaling 등 사용자는 하나의 애플리케이션을 위해 다수의 실행 환경을 생성할 수 있으며, 개 발 환경, 테스트 환경, 상용 환경 등으로 나눠서 애플리케이션 서비스를 제공가능.

2)애플리케이션 버전(application version) = S3에 저장된 애플리 케이션 실행 코드.
3)저장 환경 설정(saved configuration) = 환경 설정 및 리소스 동작을 정의.

*AWS OpsWorks

-AWS OpsWorks는 모든 유형과 규모의 애플리케이션 배포 및 운영을 돕는 환경 설정 관리 서비스, 애플리케이션의 신속한 환경 설정, 업데이트를 지원하고 , 자동화된 스케일링 및 헬스 모니터링 도구를 제공하는 서비스.
-사용자는 OpsWorks를 이용해 애플리케이션 및 아키텍처 구현은 물론, 패키지 설치, 소프트웨어 환경 설정, 스토리지 또는 로드 밸런서와 같은 리소스를 좀 더 유연하게 정의가능.
-OpsWorks가 제공하는 관리형 인스턴스인 Chef와 Puppet은 서버의 환경 설정 업무를 자동화하는 코드를 사용할 수 있는 자동화 플랫폼.
-EC2 인스턴스는 물론, 온프레미스 환경에 있는 서버의 환경 설정, 배포, 관리 업무를 자동화가능.
-OpsWorks는 Chef Automate, Puppet Enterprise, OpsWorks Stacks 세 가지 도구를 제공함.

1)Chef Automate :완전 관리형 Chef 서버이자 지속적 배포와 준 수 규정 및 보안 사항에 대한 테스트를 위한 종합적인 지동화 도구로 노드와 노 드별 상태 정보를 시각화한 사용자 인터페이스를 제공.
2)Puppet Enterpris : 관리형 Puppet Enterprise 서버이자 오케 스트레이션, 자동화 프로비저닝, 추적 데이터 시각화 등 종합적인 워크플로 지동 화 도구로 소프트웨어 및 운영체제 환경 설정, 패키지 설치, 데이터베이스 설정 등 제반 운영 업무에 대한 풀 스택 자동화 기능을 제공.
3)OpsWorks Stacks은 AWS와 온프레미스 환경의 애플리케이션 및 서버 관리를 도우며, 사용자는 OpsWorks Stacks을 이용해 전체 애플리케이션을 다수의 레이어를 지닌 스택 형식으로 모델링가능.

*Amazon Cognito

-Amazon Cognito는 다수의 모바일 디바이스에서 사용자를 좀 더 편리하게 관리 할 수 있도록 도와주는 사용자 신원 증명(user identity) 및 데이터 동기화 (data synchronization) 서비스.
-비 인증 신원 증명(unauthenticated identifies) 방식 지원.
-Amazon Cognito의 유저 풀(user pool)은 안전한 유저 디렉터리로서 수천만 명 의 사용자로 확장가능.
-표준 기반 신원 증명 제공자로서 OAuth 2.0, SAML 2.0, OpenID Connect 등 IAM 표준을 지원한.

-앱 사용 설정, 게임 플레이 상태 정보 등 모든 종류의 유저 데이터 및 키 밸류 페어를 동기화하는 데 사용가능.
-Amazon Cognito는 모바일 앱에서 AWS 리소스에 대한 접근 관리를 도우며, 리 소스 사용 권한을 롤(role) 형태로 정의하고, 유저에게 롤을 할당해 유저별로 접근이 가능한 리소스에만 선별적으로 접근가능.

*Amazon Elastic MapReduce

-Amazon EMR(Elastic MapReduce)은 위와 같은 문제를 해결하기 위한 서비스로서 EC2 및 S3 와 같은 탄력적인 인프라를 활용해 다수의 EC2 인스턴스를 분산 컴퓨팅 환경으로 구성한 관리형 Hadoop 프레임워크 서비스를 제공.
-Amazon EMR을 사용하려면, 먼저 S3에 데이터를 업로드하고, EMR 클러스터를 론칭, 클러스터가 론칭되면, 즉시 데이터를 분석가능.
-Amazon EMR은 관리형 서비스이므로 사용자는 클러스터에 몇 개의 노드를 추가할 것인지, 어떤 인스턴스 타입을 사용할 것인지, 클러스터에 어떤 애플리케이 션을 설치할 것인지만 고려하면 됨.

*AWS CloudFormation

-CloudFormation은 VPC 서브넷과 같은 간단한 업무부터 OpsWorks, Elastic Beanstalk 둥의 복잡한 업무까지 정의 가능
-CloudFormation을 사용할 때는 먼저 탬플릿을 생성. 템플릿은 JSON 포맷의 파일로서 인프라와 애플리케이션을 구성하는 AWS 리소 스의 환경 설정을 위한 설계도라 할 수 있으며, EC2는 RDS 등을 포함한 LAMP 스택과 같이 사용자를 위해 미리 정의해 둔 탬플릿도 사용가능.
-다음으로 탬플릿을 CloudFormation에 업로드함. 필요에 따라 인스턴스의 수, 인스턴스의 타입 등 파라미터를 선택하고 나면 CloudFormation이 AWS 리소스 스택을 프로비전 및 환경 설정.
-사용자는 AWS 관리 콘솔, CLI 또는 SDK 등을 이용해 템플릿을 수정해 업로드함 으로써 CloudFormation 을 갱신할 수 있음.
-CloudFormation 에서 인프라는 마치 코드처럼 다뤄짐.
-AWS CloudFormation을 이용하려면 탬플릿과 스택이 필요한데 사용자는 템플릿을 이용해서 AWS 리소스와 프로퍼티를 정의할 수 있고, 스택 생 성 시 CloudFormation은 탬플릿별로 리소스를 프로비저닝함.
-템플릿은 JSON 또는 YAML 포맷의 텍스트 파일로 AWS 관리 콘솔의 에디터 또는 텍스트 에디터로 작성 및 편집가능.

AWS CloudWatch 모니터링 서비스

-Amazon CloudWatch는 AWS 클라우드에 배포된 모든 리소스를 모니터링하기 위한 서비스로 헬스 체크, 활성화 수준 검토, 성능 확인 등 주요 지표를 모니터링

하며, AWS 클라우드 리소스는 물론, 클라우드 기반 애플리케이션을 모니터 링해 주요 성능지표를 시각화 및 분석함. 또 특정 지표 범위를 벗어나면 경고를 하도록 설정하거나 리소스 활성화 수준, 애플리케이션 성능, 운영 측면의 헬스 체크 등을 시각화해 제공함.

-Amazon CloudWatch의 주요 기능

1)성능 지표 수집 및 추적

2)실시간 모니터링 : AWS 리소스에 생긴 사소한 변화도 모두 감지가능. CloudWatch Events가 변화를 감지하면, 근실시간으로 지정된 타깃에 알림을 전송. 이 때의 타깃은 Lambda 함수, SNS 큐, Amazon SNS 토픽, Kinesis Stream 또는 기타 이벤트와 연결 된 타깃으로 설정가능.

3)모니터링 및 Logs 저장 : CloudWatch Logs는 기존 시스템, 애플리케이션, 커스텀 로그 파일을 이용해 사용자의 시스템, 애플 리케이션을 모니터링하거나 문제점을 해소할 수 있도록 도와줌.

*Amazon CloudTrail

-콘솔 CLI 등 도구를 통해 전달된 모든 API 호출 로그를 관리 하는 서비스.

-관리자는 CloudTrail을 이용해 (VPC 시큐리티 그룹 및 NACL과 같은) AWS 리소 스의 변경 추적, (AWS API 호출 기록을 통한) 규정 준수 여부 파악, (최신의 환경 설정 변경 내역을 통한) 운영상의 문제 발견 등, 다양한 업무를 처리가능.

-다른 계정 사용자는 CloudTrail 로그를 중앙 계정에 전송할 수 있으며, 중앙 계정은 이들 데이터를 가지고 분석 업무를 한 뒤, 다시 결과 데이터를 다른 계정 사 용자를 위해 배포가능.

-AWS CloudTrail의 이벤트 히스토리는 해당 리전에서 90일간 보존. 하나의 리전당 다섯 개의 트레일 생성가능.

*AWS Config

-사용자 계정에 포함된 AWS 리소스와 현재의 환경 설정에 대한 세부적인 목록을 제공하는 완전관리형 서비스.

-AWS Config를 이용해 다음과 같은 작업가능.

1)지속적 모니터링 : AWS Config는 AWS 리소스에 대한 지속적인 모니터링을 지원하며, 환경 설정 변경과 관련된 모든 사항 저장가능

2)지속적 평가 : AWS Config를 이용해 AWS 리소스에 대한 프로비전 및 환경 설정 규칙을 정의할 수 있으며, 변경 된 AWS 리소스 환경 설정 내역이 기업의 정책 및 규정에 부합하는 지를 감사 및 평가가능.

3)변화 관리 : AWS Config는 변화 관리 업무를 지원하며, 변경 내역, 발생 시간, 다른 AWS 리소스에 미치는 영향 등을 추적할 수 있음.(갑작스러운 시스템 다운, 규정 위반 감사, 보안 침해 가능성 평가 등에 활용.)

4)운영상의 문제해결 : AWS Config는 모든 변경 사항을 추적하고 지속적으로 리소스를 모니터링 하므로 운영상의 문제해 결에 활용가능

5)규정 준수 모니터링 : AWS Config를 기업의 전체 계정, 또는 다수 계정의 규정 준수 모니터링에 사용할 수 있고 리전의 규정 준수 상태 또는 리전 내 모든 계정의 규정 준수 상태를 확인할 수 있음.

*Amazon VPC Flow Logs

-VPC 네트워크 인터페이스의 IP 트래픽 정보를 수집 한 뒤 Amazon CloudWatch Logs를 이용해 로그 데이터를 저장하며, Elasticsearch 또는 Kibana 등의 서비스와 통합해 로그 데이터를 시각화하거나 인스턴스에 특정 트래픽이 도달하지 못하는 문제를 해결가능.

-VPC Flow Logs은 다음과 같은 네트워크 레벨에 따라 활성화가능.

-VPC 내의 모든 네트워크 인터페이스 추적.

-Subnet 서브넷 내의 모든 네트워크 인터페이스를 추적.

-Network interface 특정 네트워크 인터페이스의 트래픽을 추적.

-VPC Flow Logs는 네트워크 인터페이스에서의 실시간 로그 스트림을 수집하는 목적, 보안 모니터링 및 애플리케이션 문제 해결에도 활용, CloudWatch 성능 지표로 사용됨.

*AWS Trusted Advisor

-AWS Trusted Advisor의 다섯 가지 주요 기능.

1) 비용 최적화 : AWS에서 사용되지 않고 낭비되는 리소스 제거 또는 예약 용량으로의 전환을 통해 비용을 절약.

2)보안성 : AWS 리소스 간의 커뮤니케이션 상태 확인, 다양한 보안 기능 활성화, 리소스 성능 점검 등을 통해 애플리케이션의 보안성을 증대.

3)장애 대응성 : Auto Scaling, 헬스 체크, 다중 AZ, 백업 기능 등을 통해 애플리케이션의 가용성 및 중복구현성을 증대도모.

4)성능 서비스 용량 : 제한 확인, 프로비저닝된 처리 성능 요소의 활용, 활성화된 인스턴스 모니터링 등을 통해 애플리케 이션의 성능향상가능.

5)서비스 용량 제한 관리 : 서비스 용량 제한선의 80% 초과 여부를 확인. (스냅샷기준 판단)

*AWS Organizations

-계정 관리 업무를 일원화, 간소화하며, 다수의 AWS 계정 에 정책 기반 관리 기법을 적용할 수 있음.

-AWS Organizations의 서비스 통제 정책, 즉 SCP를 이용해 조직 내 다수의 계정 에서 AWS 서비스에 대한 이용을 중앙화된 방식으로 통제할 수 있고, 모든 계정 의 서비스 사용 비용을 단일 계정으로 통합해 지불할 수 있음

-AWS Organizations는 모든 계정 이용자에게 무료로 제공.

수고하셨습니다-!