1. EC2 RI(예약 인스턴스), RDS는 예약인스턴스가 존재한다.

2. S3 Glacier는 데이터 보관을 위한 안전하고 내구력 있으며 저렴한 스토리지 클래스이다.

여러 가용 영역에 걸쳐 99.99999%의 객체 내구성을 제공하도록 설계

3. Amzone Connect는 사용하기 쉬운 옴니채널 클라우드 콜 센터로 기업이 저렴한 비용으로 우수한 고객 서비스를 제공할 수 있도록 한다.

Amazone Connect는 컨택 센터 운영을 단순화하고 상담원 효율성을 개선하며 비용을 절감하고 수백만 고객을 지원하도록 확장할 수 있다.

4. Amazone WorkSapaces는 완전관리형 Daas (Desktop) 솔루션이다. 몇 분만에 윈도우나 리눅스 데스크탑을 프로비저닝하고 신속하게 확장하여 전 세계 작업자에게 수천 개의 데스크톱을 제공할 수 있다.

5. Well – Architected는 앱 및 워크로드에 사용할 보안, 성능, 복원력 및 효율성이 뛰어난 인프라를 구축하는 클라우드 아키텍트를 돕기 위해 개발되었다.

운영 우수성 원칙

운영 우수성 원칙은 비즈니스 가치를 제공하고 지속적으로 프로세스와 절차를 개선하기 위해 시스템을 실행 및 모니터링하는 데 중점을 둡니다. 주로 변경 자동화, 이벤트 응답 및 일상적인 작업을 관리하기 위한 표준의 정의와 같은 내용을 주로 다룹니다.

보안 원칙

보안 원칙은 정보와 시스템을 보호하는 데 중점을 둡니다. 데이터의 기밀성 및 무결성, 권한 관리를 통한 사용자 작업 식별 및 관리, 시스템 보호와 보안 이벤트 탐지를 위한 제어 설정 같은 항목을 주로 다룹니다.

안정성 원칙

안정성 원칙은 워크로드가 의도하는 기능을 원하는 시점에 올바르고 일관적으로 수행하도록 하는 데 중점을 둡니다. 회복력 있는 워크로드는 장애에서 빠르게 회복되고 비즈니스와 고객의 요구 사항을 충족합니다. 분산 시스템 설계, 복구 계획, 변경 처리 방법 등의 항목을 주로 다룹니다.

성능 효율성 원칙

성능 효율성 원칙은 IT 및 컴퓨팅 리소스를 효율적으로 사용하는 데 중점을 둡니다. 워크로드 요구 사항에 적합한 리소스 유형 및 크기 선택, 성능 모니터링과 정보에 입각한 의사 결정을 통해 비즈니스 요구 사항의 변화에 맞춰 효율성을 유지하는 방법 같은 항목을 주로 다룹니다.

비용 최적화 원칙

비용 최적화 원칙은 불필요한 비용 발생을 피하는 데 중점을 둡니다. 지출 영역 파악 및 통제, 가장 적절하고 적합한 수의 리소스 유형 선택, 시간대별 지출 분석과 초과 지출 없이 비즈니스 요구 사항에 맞춘 조정 같은 항목을 주로 다룹니다.

6. AWS Personal Health Dashboard는 AWS에 고객에게 영향을 미칠 수 있는 이벤트가 발생할 때 알림 및 해결 지침을 제공한다. AWS 리소스의 기반이 되는 AWS 서비스의 성능 및 가용성에 대한 맟춤형 뷰를 제공한다.

7. AWS Step Function을 사용하면 시각적 워크플로를 사용해 분산 앱 및 마이크로서비스의 구성 요소를 손쉽게 조정할 수 있다. 오케스트레이션에 사용하며, 각각 기능을 수행하는 개별 구성 요소를 사용하여 앱을 구축하면 앱을 빠르게 확장하거나 변경할 수 있다.

Step Function은 앱의 기능을 통해 구성요소와 단계를 조정할 수 있는 안정적인 방법이다.

8. ALB는 경로 기반 라우팅, 호스트 기반 라우팅 및 양방향 통신채널을 지원한다.

NLB는 TCP 및 UDP 로드 밸런싱을 제공한다.

9. Amazon FSx for Windows File Server는 업계 표준 SMB(서버 메시지 블록) 프로토콜을 통해 액세스 가능한 고도로 안정적이고 확장 가능한 완전관리형 파일 스토리지 서비스를 제공합니다.

10. IAM, AWS Certificate Manager는 SSL인증서롤 사용한다.

11. AWS Budget (예산)을 사용하면 비용 또는 사용량이 예산 금액을 초과할 것으로 예상될 때 알림을 받도록 사용자 지정 예산을 설정할 수 있다.

12. AWS Service Health Dashboard는 AWS가 있는 모든 리전에 대해 표 형식으로 서비스의 상태 및 가용성에 대한 최신정보를 게시한다.

모든 리전에서 모든 AWS 서비스의 일반 상태 및 가용성에 대한 최신 정보를 게시한다.

13. APN 컨설팅 파트너는 모든 유형과 규모의 고객이 AWS에서 워크로드와 앱을 설계, 구축, 마이그레이션 및 관리하여 AWS 클라우드로의 마이그레이션을 가속화하는데 도움을 주는 전문 서비스이다.

APN 기술 파트너는 AWS 클라우드에서 호스팅 되거나 통합되는 하드웨어, 연결 서비스 또는 소프트웨어 솔루션을 제공한다.

14. Well Architected의 안정성 원칙을 제공하는 서비스는 IAM, VPC, TrustedAdvisor 등이 있다.

15. 앱의 성능 모니터링은 성능효율성 원칙의 예시이다.

16. 리소스의 구성 변경에 대한 추적은 AWS Config의 기능이며, Config는 AWS 리소스의 구성을 평가, 감사 및 평가할 수 있는 서비스이다. 리소스 구성을 모니터링하고 기록하며 원하는 구성에 대해 기록된 구성 평가를 자동화한다.

17. Inspector는 AWS에 배포된 앱의 보안 및 규정 준수를 개선하는데 도움이 되는 자동 보안 핑가 서비스이다.

18. Well – Archited 프레임워크에서 인프라를 코드로 유지하도록 권장하는 원칙은 운영우수성 원칙의 예시이다.

19.  VPC 엔드포인트를 사용하면 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이도 AWS PrivateLink에서 제공하는 지원되는 AWS 서비스 및 VPC 엔드포인트 서비스에 VPC를 비공개로 연결할 수 있습니다

20. CMK는 고객 마스터 키로 KMS의 리소스이다.

21. DynamoDB와 S3는 VPC 엔드포인트를 지원한다.

22. Amazone SageMaker는 모든 개발자 및 데이터 사이언스가 기계학습 모델을 빠르게 구축, 훈련 및 배포할 수 있도록 하는 완전관리형 서비스이다.

23. Amazone Comprehend는 기계학습을 사용하여 텍스트 안에 있는 통찰력과 관계를 찾아내는 자연어 처리 서비스이다.

24. AWS CodeDeploy와 같은 도구를 사용하여 소규모의 점진적인 변경 사항을 애플리케이션에 배포하면 애플리케이션에 전적으로 영향을 미칠 수 있는 과감한 업데이트를 도입할 필요 없어 안정적인 운영을 할 수 있습니다.

25. AWS Firewall Manager를 사용하여 DDOS 규칙을 추가하면 AWS WAF로 DDOS 보호가 가능하다.

26. AWS 침투테스트를 허용하는 서비스로는

EC2, NAT 게이트웨이, ELB, RDS, CloudFront, Aurora, API Gateway, Lambda, LightSail 등이 있다.

27. 액세스 키는 IAM 사용자 또는 AWS 계정 루트 사용자에 대한 장기 자격 증명입니다. 액세스 키를 사용하여 AWS CLI 또는 AWS API에 대한 프로그래밍 요청에 서명할 수 있습니다

28. Amazone CloudWatch Logs는 각 로그 그룹에 대한 보존 정책을 조정하며, EC2 인스턴스에서 앱 로그를 모니터링 할 수 있다.

29. AWS 비용 및 사용보고서를 사용하면 월 수준으로 집계하여 세부정보를 제공한다.

30. AWS 클라우드에서 비용을 모니터링하고 최적의 Saving Plan을 선택하기 위해서는

AWS Cost Explorer를 사용하면 좋다.

31. IAM 액세스 어드바이저는 데이터 분석을 사용하여 권한 보호 기능을 안전하게 설정하도록 지원한다. 사용자에게 부여된 권한을 검토하는데 도움을 준다

IAM 자격 증명 보고서 : 계정의 모든 사용자와 암호, 액세스 키 및 MFA 디바이스를 포함한 다양한 자격 증명의 상태를 나열하는 자격 증명 보고서를 생성하고 다운로드 할 수 있습니다. 사용자에게 부여된 권한을 검토하는 데 사용되지 않습니다.

32. Amazon Elastic Compute Cloud (Amazon EC2)는 초당 청구를 지원하여 클라우드에서 안전하고 크기 조정이 가능한 컴퓨팅 용량을 제공하는 웹 서비스입니다. AWS 클라우드에서 서버를 프로비저닝하고 기본 OS에 액세스하는 가장 쉬운 방법입니다.

Amazon EC2는 개발자에게 제공하는 유연성, 제어 및 상당한 비용 절감 측면에서 기존의 온프레미스 호스팅 시스템과 근본적으로 다릅니다. 따라서 Amazon EC2 인스턴스를 AWS 클라우드의 강력한 인프라가 지원하는 자체 사용자 지정 서버로 취급할 수 있습니다.

컴퓨팅 요구 사항이 예기치 않게 변경되면 Amazon EC2를 요구 사항에 맞게 확장 할 수 있습니다. 개발자는 특정 시점에서 사용 중인 EC2 인스턴스 수를 제어 할 수 있습니다.

개발자는 Amazon EC2를 사용하여 언제든지 인스턴스를 시작, 종료, 시작 또는 종료하도록 선택할 수 있을 뿐만 아니라 인스턴스 구성을 완전히 사용자 지정할 수도 있습니다.

33. AWS Fartget는 컨테이너에 적합한 서버리스 컴퓨팅 엔진으로 ECS에서 작동한다. Fargate에서는 앱을 빌드하는데 쉽게 초점을 맞출 수 있으며, 서버를 관리할 필요가 없어 비즈니스에 집중이 가능하다.

34. S3 Standard, Intelligent – Tiering으 데이터 검색 요금을 부과하지 않는다.

35. APN을 활용하여 인프라에 마이그레이션에 대한 맞춤형 솔루션을 제공받을 수 있다.

36. 보안 그룹은 인스턴스에서 인바운드 및 아웃 바운드 트래픽을 제어하기 위한 가상 방화벽 역할을 합니다. 보안 그룹은 서브넷 수준이 아닌 인스턴스 수준에서 작동합니다. 보안 그룹은 상태 저장입니다. 인스턴스에서 요청을 보내면 해당 요청에 대한 응답 트래픽이 인바운드 보안 그룹 규칙에 관계없이 유입 될 수 있습니다. 보안 그룹은 트래픽 허용 여부를 결정하기 전에 모든 규칙을 평가합니다.

네트워크 액세스 제어 목록 (NACL)은 하나 이상의 서브넷에서 들어오고 나가는 트래픽을 제어하기 위한 방화벽 역할을 하는 VPC의 선택적 보안 계층입니다 (즉, 서브넷 수준에서 작동 함). 네트워크 ACL에는 번호가 매겨진 규칙 목록이 포함됩니다. NACL은 가장 낮은 번호의 규칙부터 순서대로 규칙을 평가하여 트래픽이 네트워크 ACL과 연결된 서브넷 안팎으로 허용되는지 여부를 결정합니다. 규칙에 사용할 수 있는 가장 높은 수는 32766입니다. AWS는 나중에 필요한 곳에 새 규칙을 삽입 할 수 있도록 규칙을 증분 (예 : 10 또는 100 증분)으로 생성하여 시작하는 것이 좋습니다

37. S3 멀티 스레딩 요청은 병렬구성의 좋은 예시이다.

38. AWS Gloal Accelerator는 로컬 또는 글로벌 사용자를 대상으로 앱의 가용성과 성능을 개선하는 서비스이다.

39. EC2 Instance Connect는 SSH을 사용하여 인스턴스에 연결하는 간단하고 안전한 방법이다.

Instance Connect를 이용하면 브라우저 기반 클라이언트, Amazon EC2 Instance Connect CLI 또는 사용자가 선택한 SSH 클라이언트를 사용하는 Linux 인스턴스에 연결할 수 있습니다.

40. CloudFormation은 AWS 계정 및 리전에서 동일한 AWS 인프라를 프로비저닝하는데 사용한다.

41. Amazon CloudWatch Logs를 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS CloudTrail, Route 53 및 기타 소스에서 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다.

CloudWatch Logs는 확장성이 뛰어난 단일 서비스에서 사용하는 모든 시스템, 애플리케이션 및 AWS 서비스에서 로그를 중앙 집중화할 수 있습니다.

42. VPC의 요소는  Virtual Private Cloud(VPC) — 사용자의 AWS 계정 전용 가상 네트워크입니다.

\* 서브넷 — VPC의 IP 주소 범위입니다.

\* 라우팅 테이블 — 네트워크 트래픽을 전달할 위치를 결정하는 데 사용되는 라우팅이라는 규칙 집합입니다.

\* 인터넷 게이트웨이 — VPC의 리소스와 인터넷 간의 통신을 활성화하기 위해 VPC에 연결하는 게이트웨이입니다.

\* VPC 엔드포인트 — 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결을 필요로 하지 않고 PrivateLink 구동 지원 AWS 서비스 및 VPC 엔드포인트 서비스에 VPC를 비공개로 연결할 수 있습니다. VPC의 인스턴스는 서비스의 리소스와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 기타 서비스 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

43. EFS와 DynamoDB는 기본적으로 고가용성을 지원한다.

44. 서버 액세스 로깅은 버킷에 대해 이루어진 요청에 따른 상세 레코드를 제공합니다. 서버 액세스 로그는 많은 애플리케이션에 있어 유용합니다. 예를 들어 액세스 로그 정보는 보안 및 액세스 감사에 유용할 수 있습니다. 또한 고객층을 파악하고 Amazon S3 결제 요금을 확인할 수 있습니다.

S3 버킷에 대한 요청을 감사하는데도 사용한다.

45. 예약 인스턴스는 최대 75%, 스팟인스턴스는 최대 90%

46. Amazone Aurora는 고성능 사용 데이터베이스이다. MySQL, PostgreSQL 호환 관계형 데이터베이스 자가 복구 기능이 있고 처리량이 높은 데이터베이스에 사용이 된다.

47. 권한을 부여할 때 누구에게 권한을 부여할지, 어떤 Amazon S3 리소스에 대한 권한을 부여할지, 해당 리소스에 대해 허용 할 특정 작업을 결정합니다. 버킷과 객체는 Amazon S3 리소스입니다. 기본적으로 리소스 소유자만 이러한 리소스에 액세스 할 수 있습니다. 리소스 소유자는 리소스를 생성하는 AWS 계정을 나타냅니다.

버킷 정책과 사용자 정책은 Amazon S3 리소스에 대한 권한을 부여하는 데 사용할 수 있는 두 가지 액세스 정책 옵션입니다. 둘 다 JSON 기반 액세스 정책 언어를 사용합니다. 버킷에 버킷 정책을 추가하여 다른 AWS 계정 또는 IAM 사용자에게 버킷 및 버킷의 객체에 대한 액세스 권한을 부여합니다. 사용자 정책은 IAM 사용자가 버킷 중 하나에 액세스 할 수 있도록 허용하는 정책입니다.

48. Amazone GuardDuty는 악성활동을 모니터링하고 위협을 탐지하여 계정을 보호하는 서비스이다.

49. RDS의 다중 AZ사용은 장애를 위한 설계에 대비한 준수사항이다.

50. Amazone ElasticCache의 솔루션 방식 두 가지

Redis, Memcached용이 있다.

51. VPC에서는 서브넷, 인터넷 게이트웨이, NAT 게이트웨이, 탄력적 IP, NACL, 보안그룹 구성한다

52. AWS Storage Gateway는 사실상 무제한의 클라우드 스토리지에 대한 온프레미스 액세스 권한을 제공하는 하이브리드 클라우드 스토리지 서비스입니다. Storage Gateway를 사용하는 고객은 하이브리드 클라우드 스토리지의 주요 사용 사례에서 스토리지 관리 간소화 및 비용 절감 효과를 얻을 수 있습니다. 여기에는 백업을 클라우드로 이동하고, 클라우드 스토리지에서 지원되는 온프레미스 파일 공유를 사용하고, 온프레미스 애플리케이션에서 AWS의 데이터에 낮은 지연 시간으로 액세스하는 혜택도 포함됩니다.

53. AWS Trusted Advisor 모범 사례 점검 항목

AWS Trusted Advisor는 비용 최적화, 보안, 내결함성,성능 및 서비스 한도라는 5가지 카테고리에 대한 다양한 모범 사례 점검 항목 및 권장 사항을 제공합니다.

비용 최적화

사용되지 않는 유휴 리소스를 제거하거나 예약 용량을 약정하여 AWS에서 비용을 절약할 수 있는 방법을 확인합니다.

\* Amazon EC2 예약 인스턴스 최적화

\* 사용률이 낮은 Amazon EC2 인스턴스

\* 유휴 상태의 Load Balancer

\* 사용률이 낮은 Amazon EBS 볼륨

\* 연결되지 않은 탄력적 IP 주소

\* Amazon RDS 유휴 DB 인스턴스

\* Amazon Route 53 지연 시간 리소스 레코드 세트

\* Amazon EC2 예약 인스턴스 임대 만료

\* 사용률이 낮은 Amazon Redshift 클러스터

보안

결함을 없애고, 다양한 AWS 보안 기능을 사용하며, 권한을 점검하여 애플리케이션 보안을 개선합니다.

\* 보안 그룹 – 제한 없는 특정 포트(무료!)

\* 보안 그룹 – 제한 없는 액세스

\* IAM 사용(무료!)

\* Amazon S3 버킷 권한(무료!)

\* 루트 계정의 MFA(무료!)

\* Amazon RDS 보안 그룹 액세스 위험

\* AWS CloudTrail 로깅

\* Amazon Route 53 MX 및 SPF 리소스 레코드 세트

\* ELB 리스너 보안

\* ELB 보안 그룹

\* IAM 인증서 스토어의 CloudFront 사용자 지정 SSL 인증서

\* 오리진 서버의 CloudFront SSL 인증서

\* 노출된 액세스 키

\* Amazon EBS 퍼블릭 스냅샷(무료!)

\* Amazon RDS 퍼블릭 스냅샷(무료!)

\* IAM 암호 정책

\* IAM 액세스 키 교체

내결함성

Auto Scaling, 상태 확인, 다중 AZ 및 백업 기능을 활용하여 AWS 애플리케이션의 가용성과 중복성을 높입니다.

\* Amazon EBS 스냅샷

\* Amazon EC2 가용 영역 밸런싱

\* Load Balancer 최적화

\* VPN 터널 중복성

\* Auto Scaling 그룹 리소스

\* Amazon RDS 백업

\* Amazon RDS 다중 AZ

\* Auto Scaling 그룹 상태 확인

\* Amazon S3 버킷 로깅

\* Amazon Route 53 이름 서버 위임

\* Amazon Route 53 높은 TTL 리소스 레코트 세트

\* Amazon Route 53 장애 조치 리소스 레코드 세트

\* Amazon Route 53 삭제된 상태 확인

\* ELB 연결 드레이닝

\* ELB 교차 영역 로드 밸런싱

\* Amazon S3 버킷 버전 관리

\* AWS Direct Connect 연결 중복성

\* AWS Direct Connect 위치 중복성

\* AWS Direct Connect 가상 인터페이스 중복성

\* Amazon Aurora DB 인스턴스 접근성

\* EC2 Windows 인스턴스용 EC2Config 서비스

\* EC2 Windows 인스턴스용 PV 드라이버 버전

\* ENA 드라이버

\* NVMe 드라이버

성능

서비스 한도를 점검하고, 프로비저닝된 처리량을 활용하는지 확인하고, 과다 사용되는 인스턴스를 모니터링하여 서비스 성능을 개선합니다.

\* 높은 사용률의 Amazon EC2 인스턴스

\* Amazon EBS 프로비저닝된 IOPS(SSD) 볼륨 연결 구성

\* EC2 보안 그룹에 있는 많은 수의 규칙

\* 인스턴스에 적용된 많은 수의 EC2 보안 그룹 규칙

\* Amazon Route 53 별칭 리소스 레코드 세트

\* 과다 사용된 Amazon EBS 마그네틱 볼륨

\* Amazon CloudFront 콘텐츠 전송 최적화

\* CloudFront 헤더 전달 및 캐시 적중률

\* EBS에 대한 Amazon EC2 처리량 최적화

\* CloudFront 대체 도메인 이름

서비스 한도

서비스 한도의 80%가 넘는 서비스 사용량이 있는지 점검합니다. 값은 스냅샷을 기반으로 하므로 현재 사용량은 다를 수 있습니다. 한도 및 사용량에 변경 사항이 반영되는 데 최대 24시간이 걸릴 수 있습니다.

AWS Trusted Advisor는 Amazon Elastic Block Store (Amazon EBS) 볼륨 구성을 확인하고 볼륨이 과소 사용된 것으로 보일 때 경고할 수 있습니다. 볼륨이 생성되면 요금이 부과됩니다. 볼륨이 일정 기간 동안 연결되지 않았거나 쓰기 활동이 매우 적으면 (부트 볼륨 제외) 볼륨이 사용되지 않을 수 있습니다.

54. AWS Systems Manager는 AWS 인프라에 대한 가시성과 제어를 제공합니다. Systems Manager는 통합된 사용자 인터페이스를 제공하므로 여러 AWS 서비스의 운영 데이터를 보고 AWS 리소스 전체에서 운영 작업을 자동화할 수 있습니다. Systems Manager를 사용하면 Amazon EC2 인스턴스, Amazon S3 버킷 또는 Amazon RDS 인스턴스와 같은 리소스를 애플리케이션별로 그룹화하고, 모니터링과 문제 해결을 위해 운영 데이터를 보고, 리소스 그룹에 조치를 취할 수 있습니다. Systems Manager는 리소스 및 애플리케이션 관리를 간소화하고, 운영 문제를 탐지 및 해결하는 시간을 단축하며, 인프라를 대규모로 안전하게 운영 및 관리할 수 있게 해줍니다.

55. IAM 정책은 AWS환경에서 권한 및 액세스 제어를 시행하는 서비스이다.

56. AWS X-ray는 복잡한 마이크로서비스로 구성된 복잡한 마이크로 서비스 앱에 이르기까지 개발중인 앱과 프로덕션에 적용된 앱 모두 분석할 수 있다.

57. HTTP/S 트래픽의 부하 분산에 사용하는 로드밸런서는 ALB이다.

58. 온프레미스 환경에서 AWS로 마이그레이션 할 경우 기업과 고객들은 관리부담에 벗어나 비즈니스 활동에 집중 할 수 있다는 이점이 있다.