https://drcode-devblog.tistory.com/21

[AWS] 재해복구(disaster recovery)

재해 : 비즈니스 연속성 또는 재무 상태에 부정적인 영향을 미치는 모든 이벤트
ex) 하드웨어/소프트웨어 장애, 네트워크 중단, 정전, 화재나 수해 등 거눔ㄹ의 물리적인 손상, 인간의 실수, 기타 일부 심각한 재해

재해 복구 : 사업 및 시스템이 발전함에 따라 지속적으로 수행해야 할 분석 및 개선 과정.
ex) 각 사업 서비스에 대해 수용 가능한 복구 시점과 시간을 결정

기존 재해 복구 방식
: 재해 시, 여분의 용량을 확보하기 위해 인프라를 복제
: 용량 확보, 설치 및 유지관리하여 예상되는 용량 요구 사항을 처리할 준비를 갖추어야 함
: 정상 운영 시 활용율이 낮거나 과다하게 프로비저닝되는 경우가 많음

AWS 재해 복구 방식
: 필요에 따라 인프라 확장 가능
: 확장성, 신뢰성, 보안성, 속도 보장
: 사용한 만큼만 비용 지불
: 최소 권한 설계가 가능하도록 역할 분리가 가능한 도구를 제공

재해 계획 두 가지 일반적인 업계 용어 - **복구 시간 목표 및 복구 시점 목표**
(1) 복구 시간 목표(RTO)
: 비즈니스 프로세스가 재해(또는 중단) 후 복구되어야 하는 시간 및 서비스 수준을 말하는 것으로, 비즈니스 연속성이 중단되어 발생하는 수용 불가능한 결과를 예방하기 위해 필요하다.
ex) 오후 12 시에 재해가 발생했고, RTO 가 8 시간이면, 재해 복구 절차는 수용 가능한 서비스 수준으로의 복구가 오후 8 시까지는 가능하도록 조처해야 하는 것

(2) 복구 시점 목표(RPO)
: 시간적으로 측정한, 수용 가능한 데이터 손실량을 말한다.
ex) RPO 가 1 시간이라면 재해가 정오에 발생했으므로 복구된 시스템에는 최소 오전 11 시까지의 모든 데이터가 포함되어야 한다

기존의 재해 복구 투자 관행
복제 환경을 지원하는 데 필요한 인프라에 포함되는 항목
: 전력 공급 및 냉각을 포함한 인프라 수용 시설
: 자산의 물리적 보호를 위한 보안 인프라

: 환경 확장을 위한 적합한 수용 능력
: 인프라를 수리, 교체 및 재생하기 위한 지원
: 최대 부하 환경에서의 대역폭 사용률을 견딜 수 있는 인터넷 연결을 제공하기 위한 인터넷 서비스 공급자(ISP)와의 계약
: 방화벽, 라우터, 스위치 및 로드 밸런서 같은 네트워크 인프라.
: 사용자 인증, DNS(도메인 네임 서비스), DHCP(동적 호스트 구성 프로토콜), 모니터링 및 경고 등의 애플리케이션 및 백앤드 서비스를 실행하는 서버 및 지원 데이터를 위한 스토리지 장치를 포함하는 모든 미션 크리티컬 서비스를 실행할 충분한 서버 용량.

서비스 중요도에 따라 복제 환경을 장애 내결함성 방식으로 구성 가능 -> 위에 나열된 전체 인프라를 복제하는 작업 수반

재해 복구에 필수적인 AWS 서비스 및 기능

- 지역(Region)
- 스토리지(S3, EBS, Import/Export, Storage Gateway)
- 컴퓨팅(EC2, AMI, 예약 인스턴스, 가용영역, VM Import)
- 네트워킹(Route 53, Elastic IP Address, ELB, VPC, Direct Connect)
- 데이터베이스(RDS, SimpleDB)
- 배포 오케스트레이션(CloudFormation)
- 보안

(1) 지역

: AWS 는 여러 지역에서 사용 가능하므로, 시스템을 완전히 배포할 장소뿐만 아니라 재해(버지니아 북부), 미국 서부(캘리포니아 북부), EU(아일랜드), 아시아 태평양(싱가포르), 아시아 태평양(도쿄)의 다섯 개 지역에서 사용 가능하다.

(2) 스토리지

1) Amazon Simple Storage Service(Amazon S3)

- 미션 크리티컬한 데이터 및 기본 데이터 저장을 위한 내구성이 뛰어난 스토리지 인프라를 제공
- 객체는 지역 내에서 여러 시설의 여러 장치에 중복 저장됨.
- Amazon S3 버전 관리, AWS MFA(Multi-Factor Authentication), 버킷 정책 및 Identity and Access Management(IAM)을 통해 데이터 보존 및 보관을 위한 추가 보호 수단을 제공한다.

2) Amazon Elastic Block Store(Amazon EBS)

- 데이터 볼륨의 PIT(Point In Time) 스냅샷을 생성하는 기능을 제공한다.
- 스냅샷은 새로운 Amazon EBS 볼륨을 시작하는 기점이 될 수 있으며 데이터를 장기간 보호할 수 있다

- 일단 볼륨을 생성하면 실행 중인 Amazon EC2 인스턴스에 연결 할 수 있다
- 인스턴스 수명과 관계없이 지속되는 오프 인스턴스 스토리지를 제공함

3) AWS Import/Export

- 전송용 이동식 스토리지 장치를 사용하여 대용량 데이터를 AWS 에서 더욱 빠르게 이동할 수 있도록 지원한다.
- AWS 는 Amazon 의 고속 내부 네트워크를 사용해 인터넷을 우회하여 스토리지 장치에서 직접 데이터를 송수신한다.
- 용량이 큰 데이터 세트의 경우 AWS Import/Export 가 대개 인터넷 전송보다 빠르며, 연결을 업데이트하는 것보다 비용 효율성이 높다.
- Amazon S3 버킷 안팎으로 또는 EBS 스냅샷으로 데이터를 마이그레이션 할 수 있다.

4) AWS Storage Gateway

- AWS 클라우드 스토리지와 온 프레미스 애플리케이션 사이에 데이터를 원활하게 마이그레이션할 수 있습니다.
- AWS Storage Gateway 는 볼륨 데이터를 사용자 인프라 및 AWS 에 로컬로 저장한다.
  -> 기존 온 프레미스 애플리케이션에서 데이터를 비용 효율적이고 안전하고 견고한 AWS 스토리지 인프라에 원활하게 저장하고 이 데이터에 액세스할 때의 지연 시간을 줄인다.

(3) 컴퓨팅

1) Amazon Elastic Compute Cloud(Amazon EC2)

- 클라우드에서 규모를 자유 자재로 변경할 수 있는 컴퓨팅 파워를 제공한다.
- 몇 분 이내에 EC2 인스턴스를 생성할 수 있는데, 이는 온전한 제어 권한이 귀하에게 있는 가상 머신이다.
- 재해 복구 측면에서는 이처럼 귀하가 제어할 수 있는 가상 머신을 신속하게 생성할 수 있는 기능이 필수적이다.

2) Amazon Machine Image(AMI)

- 운영체제에 맞춰 사전 구성되며, 일부 사전 구성된 AMI 에는 애플리케이션 스택이 포함될 수도 있다.
- 사용자만의 AMI 를 구성할 수도 있다.
- 재해 복구 측면에서는 사용자만의 AMI 를 구성하여 구별해 둔 후 복구 절차의 일부로 실행하는 것이 좋다.
- AMI 는 사용자가 선택한 운영체제 및 적절한 애플리케이션 스택과 사전 구성해야한다.

3) Amazon EC2 예약 인스턴스

- EC2 인스턴스의 운영 비용 절감을 위해 종종 사용되는데, 재해 복구와 특히 관련된 다른 장점이 있다.
- 예약 인스턴스는 필요한 용량을 실제로 필요할 때 사용할 수 있도록 해준다.

4) 가용 영역

- 다른 가용 영역에 장애가 발생할 경우 분리되도록 설계된 별개의 위치로, 동일 지역의 다른 가용영역에 저렴하고, 지연 시간이 짧은 네트워크 연결을 제공한다.

- 별도의 가용 영역에서 인스턴스를 시작함으로써 단일 위치에서 장애가 발생할 경우 애플리케이션을 보호할 수 있다.

- 지역은 하나 이상의 가용 영역으로 구성된다.

5) Amazon EC2 VM Import

- 머신 이미지를 기존 환경에서 Amazon EC2 인스턴스로 손쉽게 가져올 수 있다.

(4) 네트워킹 - 재해 처리시 다른 장소에서 장애 조치할 때 네트워크 설정을 수정해야할 가능성이 크다.

1) Amazon Route 53

- 가용성과 확장성이 높은 DNS(도메인 이름 시스템) 웹 서비스이다.

- 개발자와 기업이 매우 신뢰할 수 있고 비용 효율적인 방식으로 최종 사용자를 인터넷 애플리케이션에 라우팅

2) Elastic IP Address

- 동적 클라우드 컴퓨팅에 적합하게 설계된 고정 IP 주소이다.

- 그러나 기존의 고정 IP 주소와 달리 엘라스틱 IP 주소를 사용해 공인 IP 주소를 특정 지역 내에 있는 계정의 인스턴스에 프로그래밍 방식으로 다시 매핑하여 인스턴스 또는 가용영역 장애를 마스킹할 수 있다.

- 재해 복구를 위해 대부분의 필수 시스템에 대한 IP 주소를 사전 할당하여 재해가 발생하기 전에 IP 주소를 미리 알 수 있다.

-> 이로써 재해 복구 계획을 간단히 실행할 수 있다.

3) Elastic Load Balancing

- 수신되는 애플리케이션 트래픽을 여러 Amazon EC2 인스턴스에 자동으로 분산한다.

- 애플리케이션의 내결함성을 크게 높이고, 수신되는 애플리케이션 트래픽에 응답하는 데 필요한 로드 밸런싱 용량을 원활하게 제공할 수 있음.

- 엘라스틱 IP 주소를 사전 할당하는 것과 마찬가지로, Elastic Load Balancer 를 사전 할당하여 DNS 이름을 미리 알 수 있어 재해 복구 계획을 간단히 실행할 수 있다.

4) Amazon Virtual Private Cloud(Amazon VPC)

- AWS 클라우드에서 개인적이고 격리된 공간을 프로비저닝하고, 가상 네트워크를 정의해 AWS 리소스를 시작할 수 있다.

- 또한, IP 주소 범위, 서브넷 생성, 라우팅 테이블과 네트워크 게이트웨이의 구성을 선택하는 등 가상 네트워킹 환경을 완벽히 제어할 수 있다.

- 이렇게 하면 기업 데이터 센터와 VPC 를 VPN 으로 연결하여 AWS 클라우드를 기업 데이터 센터의 연장선으로 활용할 수 있다.

- 재해 복구 측면에서는 Amazon VPC 를 사용하여 기존 네트워크 토폴로지를 클라우드까지 확장할 수 있다.
- 이는 특히 일반적으로 내부 네트워크에 있는 기업 애플리케이션을 복구할 때 적합하다.

5) Amazon Direct Connect

- 귀하의 프레미스에서 AWS 로 전용 네트워크를 간편하게 연결할 수 있다.
- 많은 경우, 이 서비스는 네트워크 비용을 줄이고, 대역폭 처리량을 높이며, 인터넷 기반 연결보다 더 일관된 네트워크 환경을 제공한다.

(5) 데이터베이스

1) Amazon Relational Database Service(Amazon RDS)

- 클라우드에서 관계형 데이터베이스를 더욱 간편하게 설정, 관리 및 확장할 수 있다.
- Amazon RDS 를 재해 복구 준비 단계에서 사용하여 이미 실행 중인 데이터베이스에 있는 중요 데이터를 보존하거나 복구 단계에서 사용하여 생산 데이터베이스를 실행할 수도 있다.

2) Amazon SimpleDB

- 데이터베이스 관리 작업 부담을 덜어주는 고가용성의 유연한 비관계형 데이터 스토리지이다.
- 이 스토리지는 재해 복구 준비 및 복구 단계에서도 사용할 수 있다.

(6) 배포 오케스트레이션 - 자동화 방식으로 필요한 리소스를 생성할 수 잇으므로 복구단계에서 매우 유용

1) AWS CloudFormation

- 개발자와 시스템 관리자가 관련 AWS 리소스 집합을 쉽게 생성하고, 예측 가능하게 순서대로 프로비저닝하도록 지원
- 사용자의 환경에 맞는 템플릿을 생성하고 필요한 만큼 관련 리소스(스택) 집합을 배포할 수 있다.

(7) 보안

AWS 를 사용한 재해 복구 시나리오

- 백업 및 복구

- AWS 로의 간단한 복구를 위한 파일럿 라이트

- 웜 대기 솔루션

- 다중 사이트 솔루션

(1) 백업 및 복구

- Amazon S3 가 백업 데이터에 이상적인 솔루션인 이유는 99.9%의 객체 내구성을 제공하도록 설계됐기 때문

- 어떤 위치에서든 액세스 가능

- S3 에 백업할 수 있는 다양한 상용 및 오픈 소스 백업 솔루션이 있다.

- AWS Import/Export 서비스는 스토리지 장치를 직접 AWS 에 연결함으로써 대규모의 데이터 세트 전송이 가능함

- AWS Storage Gateway 서비스를 사용하면 온 프레미스 데이터 볼륨의 스냅샷이 백업을 위해 Amazon S3 에 자동 복사되므로 나중에 이 스냅샷에서 로컬 볼륨이나 AWS EBS 볼륨을 생성할 수 있다.

- AWS 에서 실행되는 시스템의 경우, 고객은 Amazon S3 에도 백업을 할 수 있다. Amazon RDS 의 Elastic Block Store(EBS) 볼륨 및 백업의 스냅샷은 Amazon S3 에 저장된다. 또는 Amazon S3 로 파일을 직접 복사하거나 백업 파일을 생성하여 Amazon S3 에 복사할 수도 있다. Amazon S3 에 백업 데이터를 저장하는 다양한 백업 솔루션이 있으며, Amazon EC2 시스템에서도 이러한 솔루션을 사용할 수 있다.

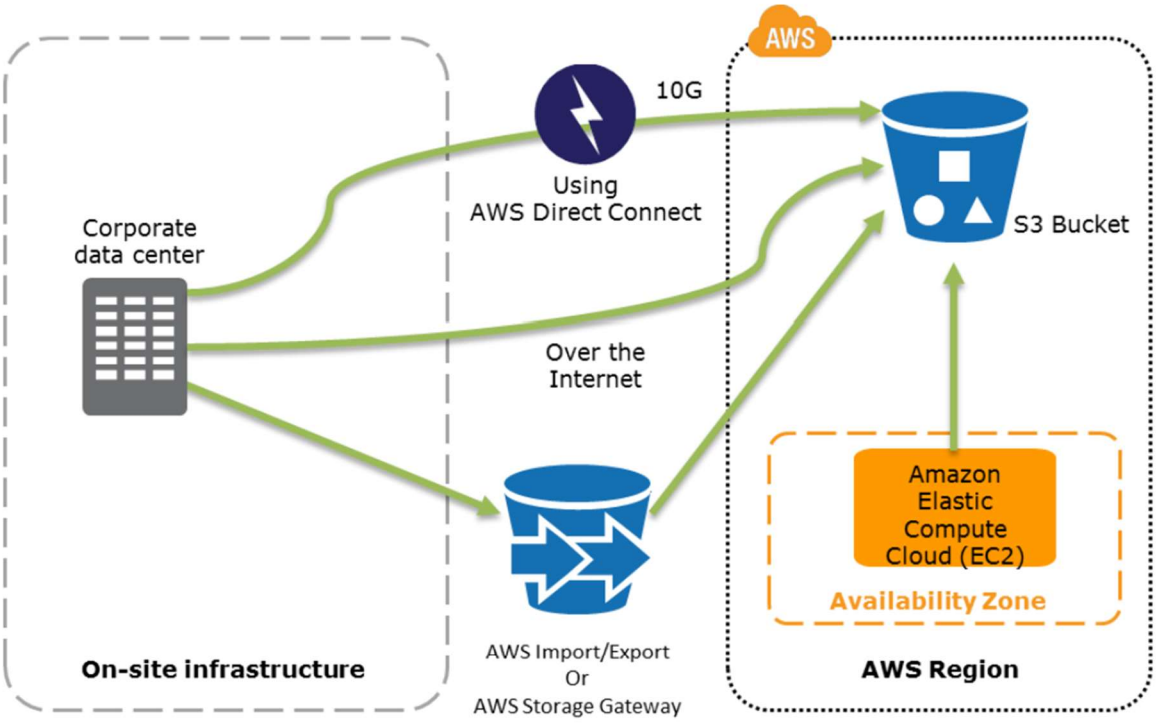

그림 1: 현장 인프라 또는 AWS 로부터 S3 에 데이터를 백업하는 옵션

데이터 백업은 시작에 불과하다. 재해 시나리오에서는 데이터 복구를 테스트할 수 있어야 하고, 데이터 복구가 신속하고 신뢰할 만한 방식으로 이루어져야 한다. 고객은 자신의 시스템이 데이터를 적절히 보존하고, 데이터 보안을 유지하도록 구성되었는지, 데이터 복구 절차를 이미 테스트했는지 확인해야 한다.

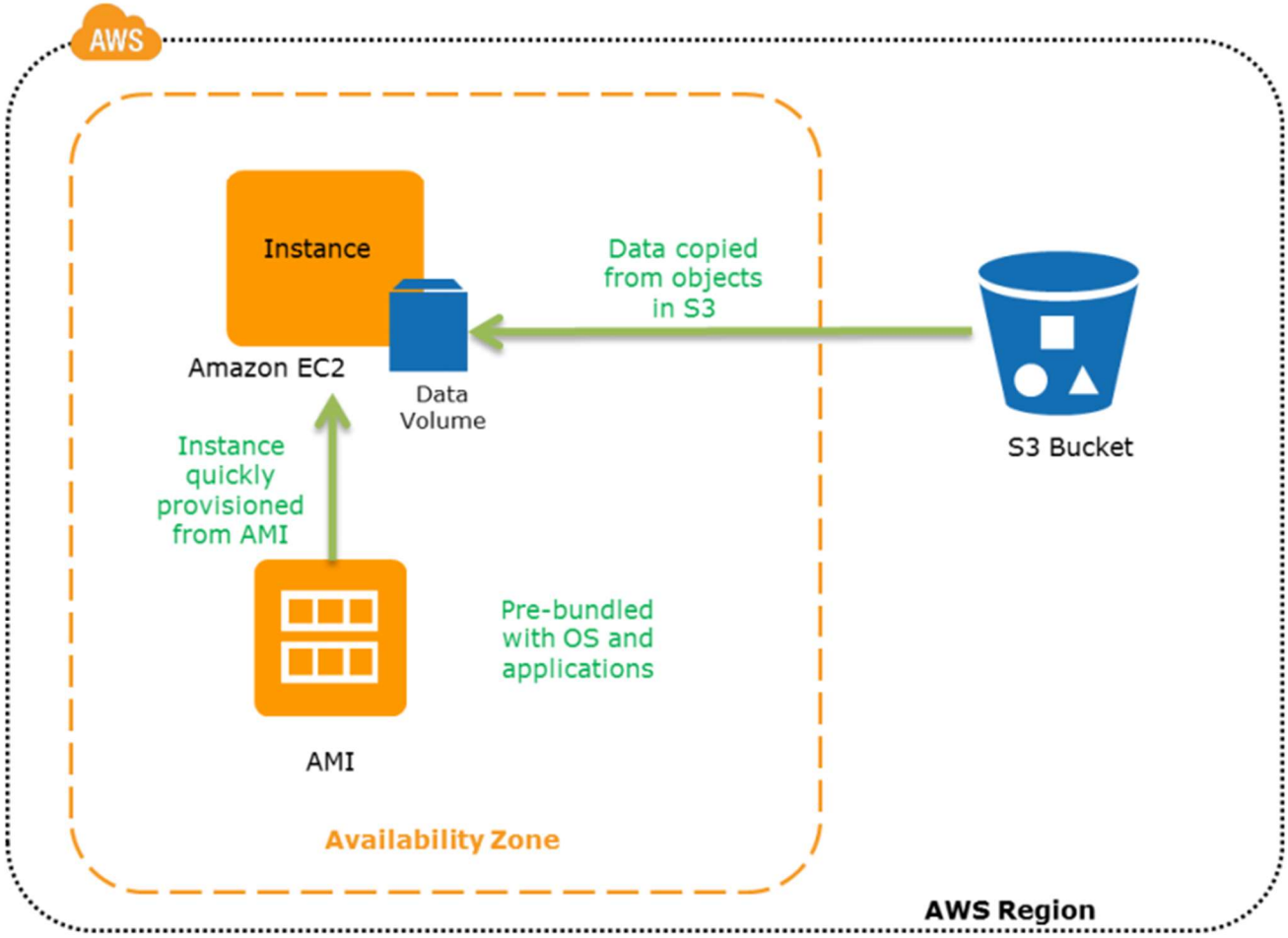

그림 2: S3 백업에서 AWS EC2 로 시스템 복구

백업 및 복구를 위한 핵심 단계 :

- 사용자의 데이터를 AWS 에 백업할 적절한 도구 또는 방법을 선택한다.
- 이 데이터에 대한 적절한 보존 정책이 있는지 확인한다.
- 이 데이터에 대한 적절한 보안 방법(암호화 및 액세스 정책 등)이 마련되어 있는지 확인한다.
- 이 데이터의 복구 및 시스템 복구를 정기적으로 테스트한다.

AWS 로의 신속한 복구를 위한 파일럿 라이트

파일럿 라이트의 개념은 가스 히터에서 비롯되었다. 가스 히터는 항시 켜지는 작은 불꽃으로 전체 난로를 점화하여 필요할 때 집을 따뜻하게 할 수 있다.

이 시나리오는 백업 및 복구 시나리오와 비슷하지만, 시스템의 가장 중요한 핵심요소가 이미 구성되어 AWS(파일럿 라이트)에서 실행되고 있는지를 확인해야 한다. 복구 시점이 되면 중요한 코어 주변으로 전체 생산 환경을 신속하게 프로비저닝해야 한다.

파일럿 라이트를 위한 인프라 요소에는 기본적으로 데이터베이스서버가 포함되는데, 이 서버의 데이터는 Amazon EC2 에 복제된다. 시스템에 따라 AWS 에 복제해야 하는 중요 데이터가 데이터베이스 외부에 있을 수도 있다. 이것이 시스템의 중요한 코어(파일럿 라이트)이다. 코어 주변으로 AWS 의 모든 다른 인프라 요소(난로의 나머지 부분처럼)가 신속하게 프로비저닝되어 전체 시스템을 복구하는 것이다.

비즈니스 크리티컬한 서비스를 복구하기 위해 인프라의 나머지 부분을 프로비저닝하려면 일반적으로 Amazon 머신 이미지(AMI)로 번들링된 사전 구성된 서버가 있어야 한다. 이 서버는 복구 시점 통지를 받는 즉시 시작된다.

복구를 시작할 때, 이 AMI 의 인스턴스가 신속하게 준비되어 파일럿 라이트 주변의 배포 범위에서 각자의 역할을 찾는다.

네트워킹 관점에서 보면 엘라스틱 IP 주소(재해 복구 준비 단계에서 미리 할당할 수 있음)를 사용하여 인스턴스와 연결하거나 Elastic Load Balancing 을 사용하여 트래픽을 여러 인스턴스에 분배할 수도 있다. 다음으로 CNAME 을 사용하여 Amazon EC2 인스턴스 시점이나 Elastic Load Balancing 시점으로 DNS 레코드를 업데이트한다.

덜 중요한 시스템의 경우에는 EBS 스냅샷의 형태와 같이 AWS 에서 이용 가능한 설치 패키지 및 구성 정보가 덜 있는지 확인할 수 있다. 이는 애플리케이션 서버 설정 속도를 높여주는데, 여러 가용 영역에서 다수의 볼륨을 신속하게 생성하여 EC2 인스턴스에 연결할 수 있기 때문이다. 그런 다음 적당하게 설치 및 구성할 수 있다.

파일럿 라이트 방법은 상기 "백업 및 복구" 시나리오 보다 복구 시간을 더 단축할 수 있는데, 시스템의 핵심 요소가 이미 실행되고 있고 지속적으로 업데이트되기 때문이다.
애플리케이션을 완전히 복구하기 위한 설치 및 구성 작업이 남아있다. AWS 를 사용해 인프라 자원의 프로비저닝 및 구성을 자동화해 상당한 시간을 절약하고 절약하고 인간의 실수로부터 보호할 수 있다.

준비 단계 :

다음 그림은 준비 단계를 보여준다. 이 단계에서는 복구 단계 시, 전체 환경이 시작되는 작은 코어인 파일럿 라이트에 정기적으로 변경되는 데이터를 복제해야 한다. 운영체제 및 애플리케이션과 같이 업데이트 빈도가 비교적 적은 데이터는 Amazon 머신 이미지(AMI)로 정기적으로 업데이트 및 저장할 수 있다.

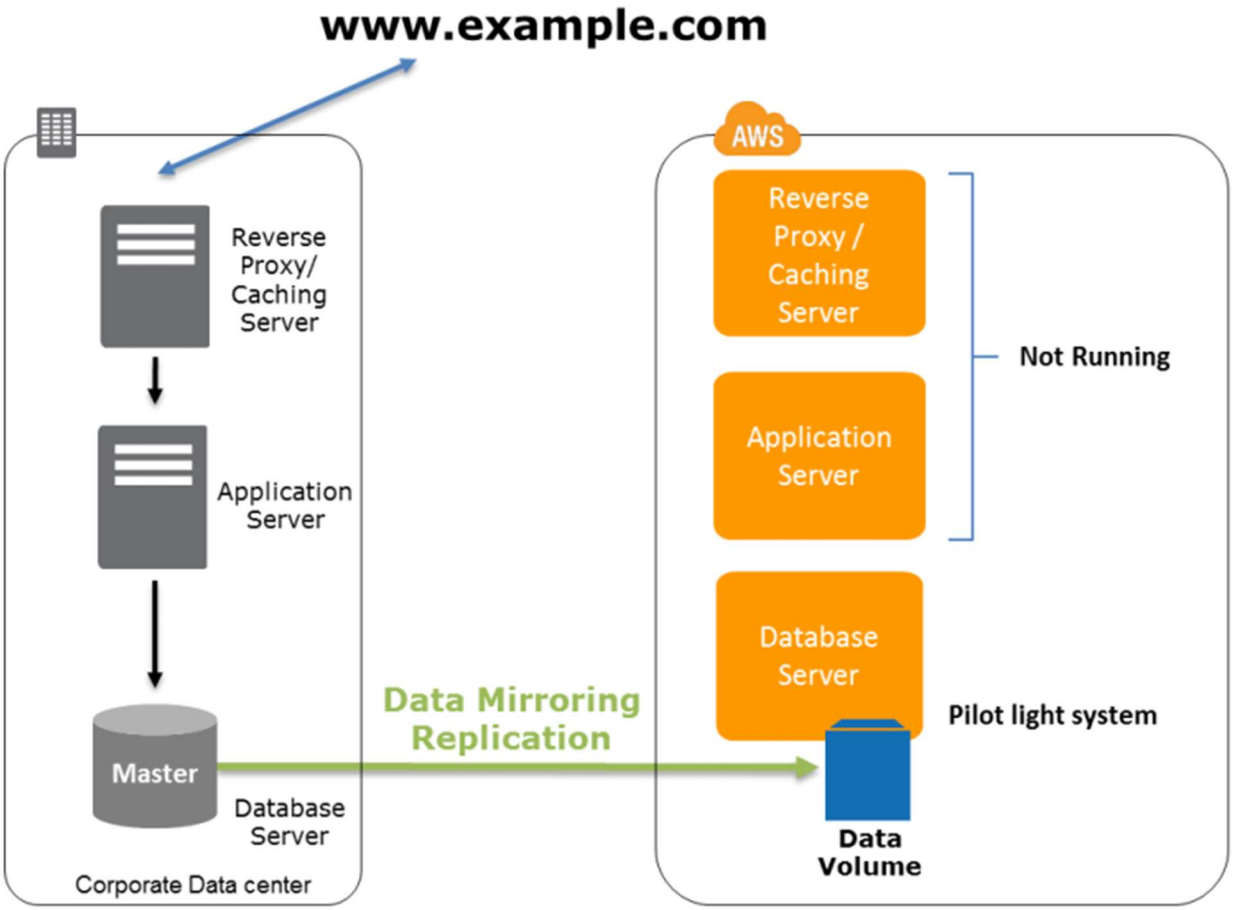

그림 3: 파일럿 라이트 시나리오의 준비 단계

준비 핵심 사항 :

- 데이터를 복제 또는 미러링하도록 EC2 인스턴스를 설정한다.
- AWS 에 모든 사용자 정의 지원 스프트웨어 패키지가 있는지 확인한다.
- 빠른 복구가 필요한 핵심 서버의 Amazon 머신 이미지(AMI)를 생성 및 관리한다.
- 이 서버를 정기적으로 실행하고, 테스트하고, 소프트웨어 업데이트 및 구성 변경 사항을 적용한다.
- AWS 리소스의 프로비저닝을 자동화할 것인지 고려한다.

복구 단계 :

파일럿 라이트 주변 환경의 나머지 부분을 복구하기 위해, 적절한 인스턴스 형태로 몇 분 내에 Amazon 머신 이미지(AMI) 에서 시스템을 시작할 수 있다. 동적 데이터 서버의 경우, 크기를 조정하여 필요에 따라 생산 불륨을 처리하거나 적당히 용량을 추가한다. 대개의 경우 수평적 확장(가능한 경우)은 가장 비용 효율적인 방법이며, 시스템에 용량을 추가하는 확장성 있는 방법이다. 그러나 더 큰 EC2 인스턴스 유형을 선택하여 수직으로 확장하는 것도 가능하다. 네트워킹 관점에서 보면 필요한 DNS 업데이트는 무엇이든 병렬로 처리할 수 있다.

일단 복구한 후에는 중복을 최대한 빨리 복구해야 한다. 생산 환경에 장애가 발생한 직후에 재해 복구 환경에 장애가 발생할 확률은 적지만, 이 위험성 역시 염두에 두어야 한다. 시스템을 정기적으로 백업하고 데이터 계층에 추가 중복을 고려해 볼 수 있다.

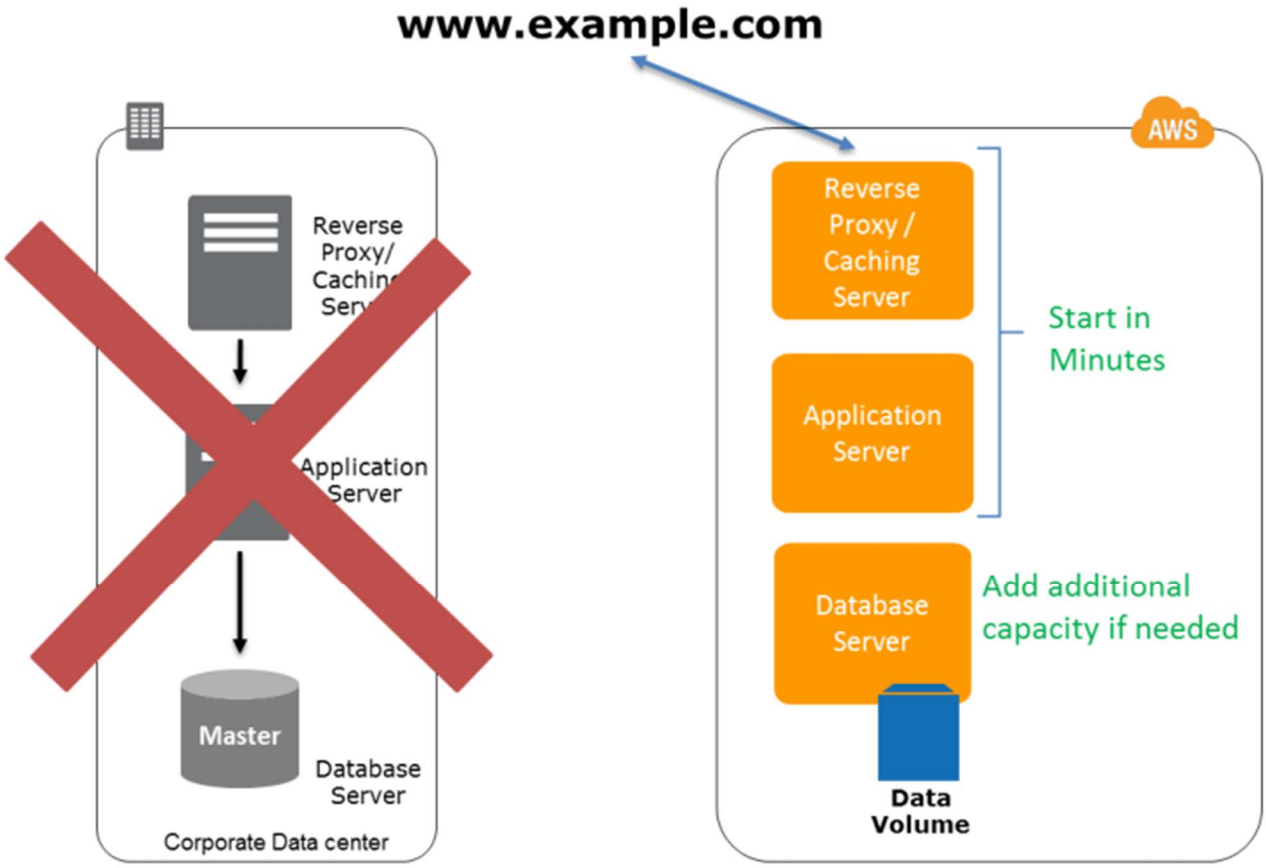

그림 4: 파일럿 라이트 시나리오의 복구 단계

복구 핵심 사항 :

- 사용자 정의 AMI 에서 애플리케이션 EC2 인스턴스를 시작한다.
- 필요 시, 데이터베이스 / 데이터 저장 인스턴스의 크기를 조정 및 / 또는 확장한다.

- EC2 서버 지점으로 DNS 를 변경한다.
- AMI 에 기반하지 않는 시스템을 설치 및 구성한다. 이때, 자동화 방식으로 수행하는 것이 이상적이다.

AWS 의 웜 대기 솔루션

웜 대기 솔루션은 파일럿 라이트 요소와 준비 과정을 제공한다. 이 솔루션을 사용할 경우 일부 서비스는 항상 실행되므로 복구 시간을 더욱 단축할 수 있다. 비즈니스 크리티컬한 시스템을 확인한 후 AWS 에 완전히 복제하여 항상 실행할 수 있다.

이러한 서버는 규모가 제일 작은 EC2 인스턴스에서 실행할 수 있다. 이 솔루션은 최대 생산 부하를 처리할 정도로 규모가 확장되지는 않지만 기능은 온전하게 작동한다. 이 솔루션은 테스트, 품질 보증 및 내부 사용 목적 등 비생산 작업에 사용할 수 있다.

재해 시, 이 시스템은 생산 부하를 처리할 수 있도록 신속하게 규모를 확장한다. AWS 에서는 로드밸런서에 더 많은 인스턴스를 추가하거나 작은 용량의 서버가 더 큰 EC2 인스턴스 유형에서 실행되도록 크기를 조정함으로써 규모를 확장할 수 있다. 위에서 설명한 바와 같이 대개의 경우 수평적 확장(가능한 경우) 이 수직적 확장보다 더 많이 이용된다

준비 단계 :

다음 다이어그램은 웜 대기 솔루션의 준비 단계를 보여주며, 이때 현장 AWS 솔루션이 나란히 실행된다.

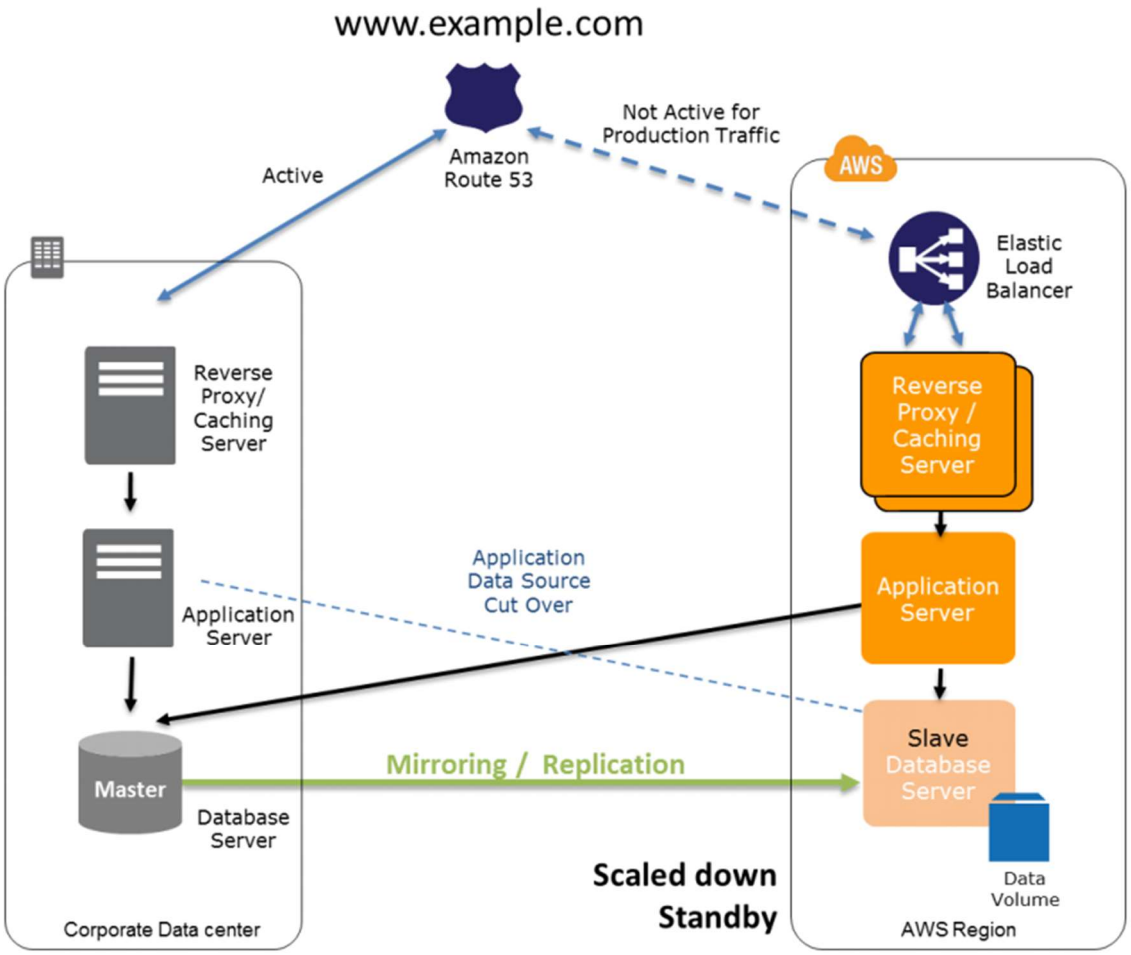

그림 5: "웜 대기" 시나리오의 준비 단계

준비 핵심 사항 :

- 데이터를 복제 또는 미러링하도록 EC2 인스턴스를 설정한다.
- Amazon 머신 이미지(AMI)를 생성 및 관리한다.
- EC2 인스턴스 또는 AWS 인프라의 최소 풋프린트를 사용하여 애플리케이션을 실행한다.
- 실제 환경에 맞게 소프트웨어 및 구성 파일을 패치하거나 업데이트 한다.

복구 단계 :

생산 시스템에 장애가 발생할 경우, 대기 환경은 생산 부하를 처리하도록 확장되며, DNS 레코드는 모든 트래픽을 AWS 로 라우팅하도록 변경된다.

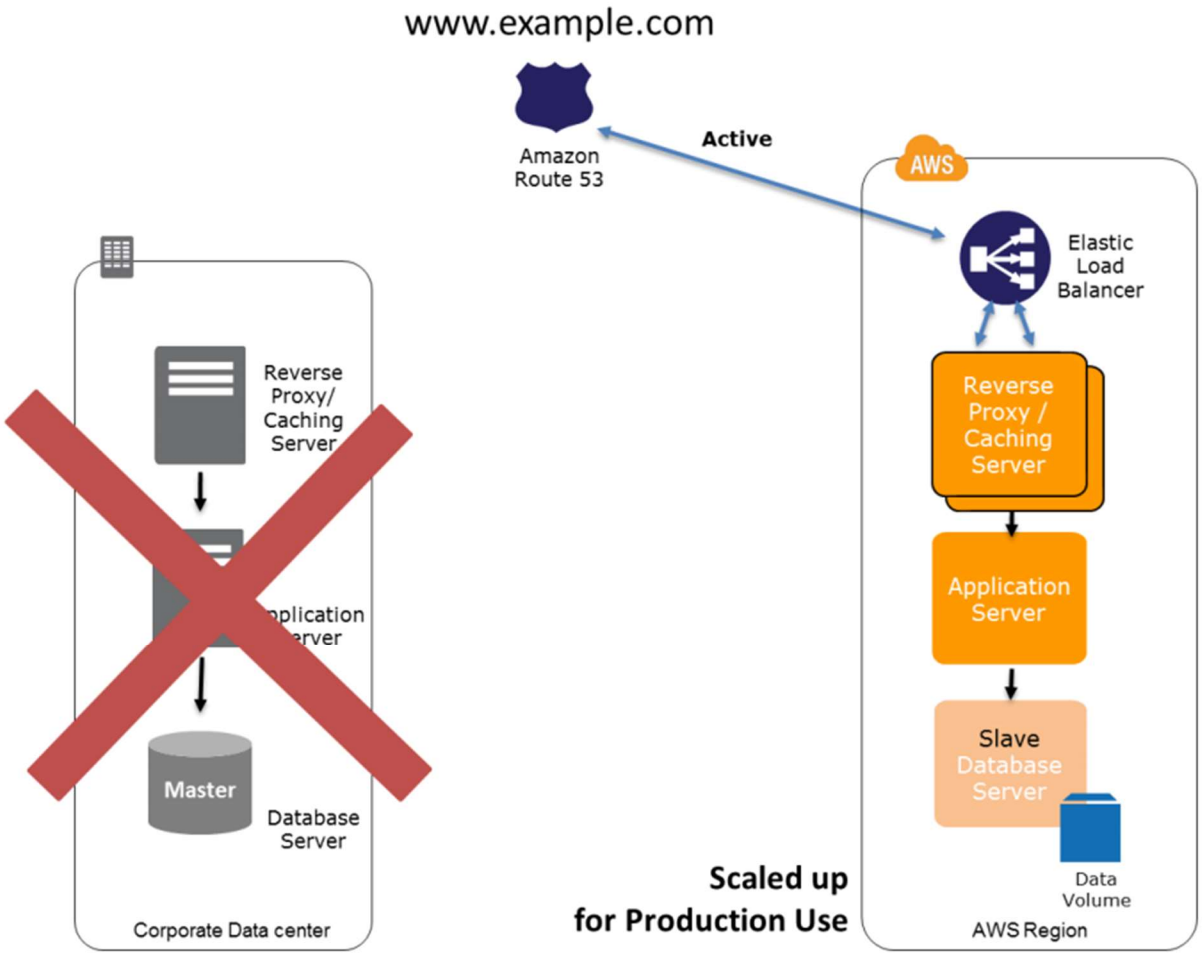

그림 6: "웜 대기" 시나리오의 복구 단계.

복구 핵심 사항 :

- 필요하다면 더 큰 EC2 인스턴스 유형에서 애플리케이션을 시작한다.(수직적 확장)
- Load Balancer 로 서비스 내에서 EC2 의 크기를 증가시킨다.(수평적 확장)
- DNS 레코드를 변경하여 모든 트래픽이 AWS 환경으로 라우팅되게 한다.
- AWS 의 규모를 적정하게 조정하거나 증가된 부하를 수용할 수 있도록 Auto Scaling 사용을 고려한다.

AWS 및 현장에 배포된 다중 사이트 솔루션

다중 사이트 솔루션은 액티브-액티브 구성으로 기존의 현장 인프라뿐 아니라 AWS 에서도 실행된다.

사용하는 데이터 복제 방법은 선택한 복구 시점에 의해 결정된다.

Amazon Route 53 와 같은 가중 DNS 서비스는 서로 다른 사이트로 생산 트래픽을 라우팅하는 데 사용된다.

일정량의 트래픽은 AWS 의 인프라로 전송되며, 나머지는 현장 인프라로 전송된다.

현장 재해 시, DNS 가중치를 조정하여 모든 트래픽을 AWS 서버로 보낼 수도 있다. 최대 생산 부하량을 처리할 수 있도록 AWS 서비스 용량을 신속하게 증가시킬 수 있다. EC2 Auto Scaling 을 이용해 이 과정을 자동화할 수 있다.

기본 데이터베이스 서비스의 장애를 감지하고 AWS 에서 실행되는 병렬 데이터베이스 서비스로 이관되기 위해 몇 가지 애플리케이션 로직이 필요할 수 있다.

이 시나리오의 비용은 정상 운영 중 AWS 가 처리하는 생산 트래픽의 양에 따라 결정된다. 복구 단계에서는 트래픽을 사용한 만큼, 그리고 전체 재해 복구 환경을 사용한 기간에 대해서만 비용을 지불하면 된다.

"항시 작동하는" AWS 서버에 대해 예약 인스턴스를 구입하여 비용을 더욱 줄일 수 있다.

준비 단계 :

아래 그림에서 DNS 를 사용하여 트래픽의 일부를 AWS 사이트로 라우팅하는 것을 볼 수 있다. AWS 의 애플리케이션은 현장 생산 시스템의 데이터 원본에 액세스할 수 있다. 데이터는 AWS 인프라에 복제되거나 미러링된다.

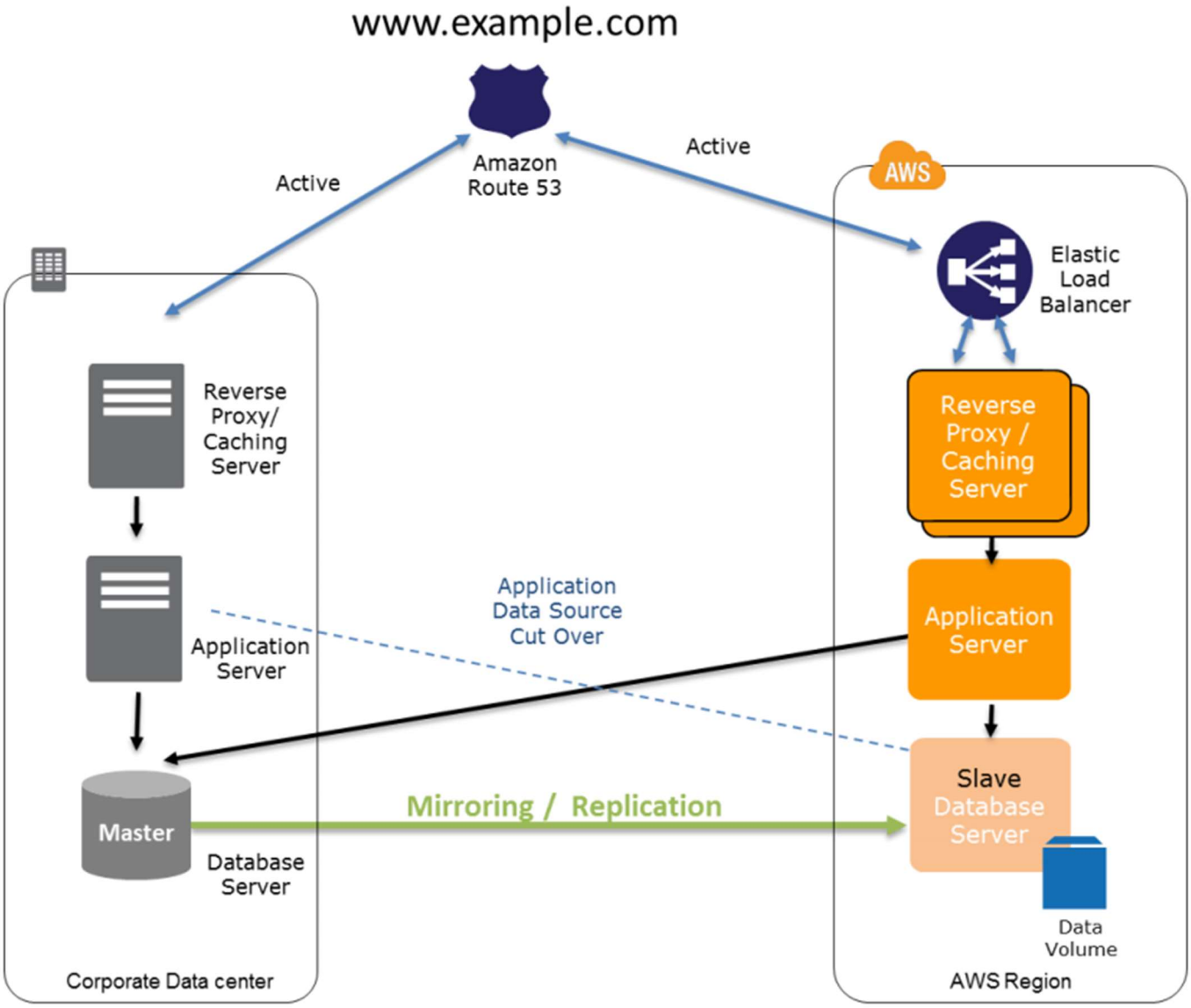

그림 7: "다중 사이트" 시나리오의 준비 단계.

준비 핵심 사항 :

- 생산 환경을 복제하도록 AWS 환경을 설정한다.
- DNS 가중치 또는 이와 유사한 기술을 설정하여 두 사이트에 전송되는 요청량을 분배한다.

복구 단계 :

아래 그림은 재해가 현장에 발생했을 때의 상황을 보여준다. 트래픽은 DNS 업데이트를 통해 AWS 인프라로 이관된다.

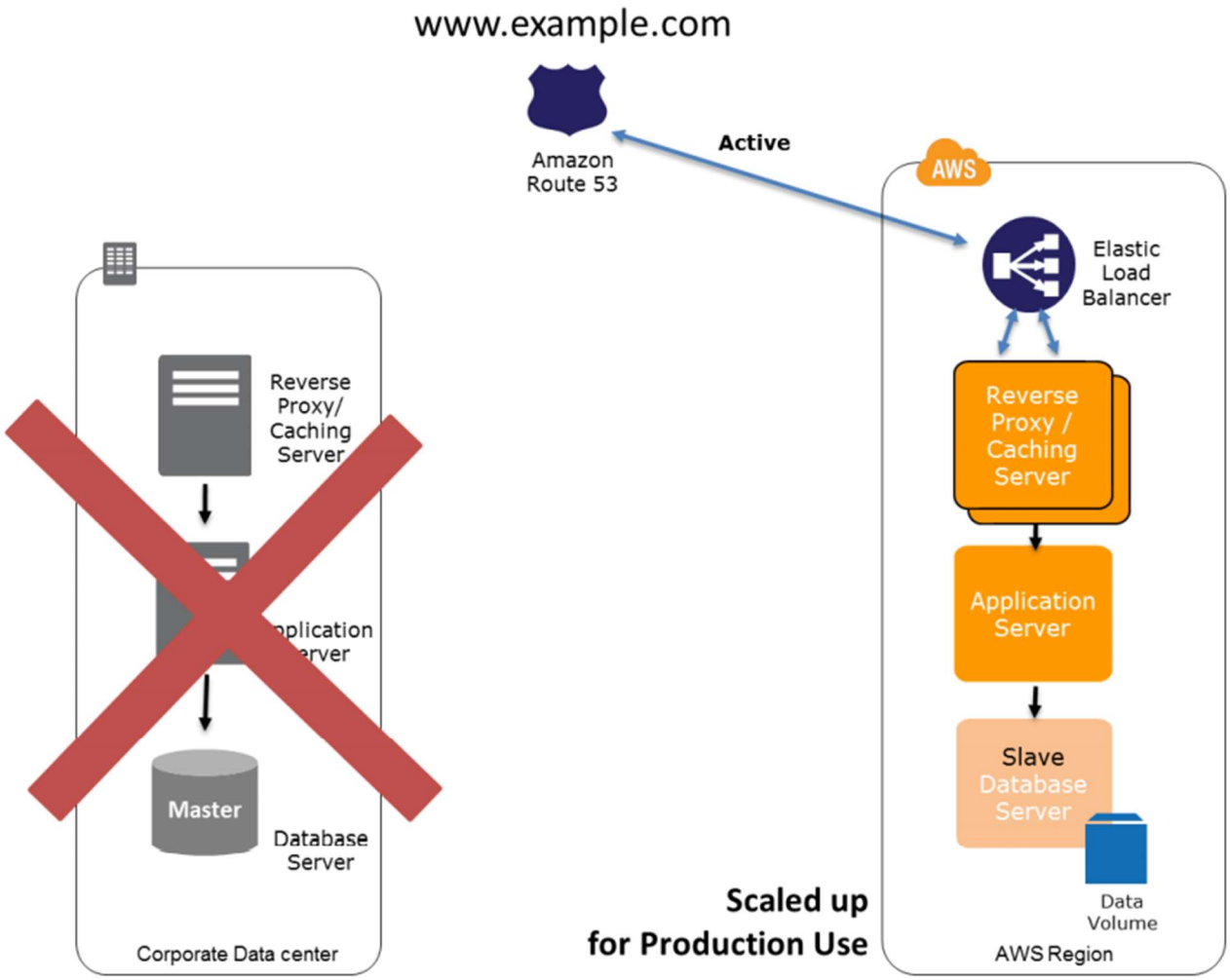

그림 8: 현장 및 AWS 인프라를 이용한 "다중 사이트" 시나리오의 복구 단계.

복구 핵심사항 :

- DNS 가중치를 변경하여 모든 요청이 AWS 사이트로 전송되도록 한다
- 로컬 AWS 데이터베이스 서버를 사용하도록 장애 조치에 대한 애플리케이션 로직을 구성한다.
- AWS 의 규모를 적정하게 자동으로 조정하도록 Auto Scaling 사용을 고려한다.

다중 AZ 아키텍처를 설계하여 다중 사이트 솔루션의 가용성을 더 증가시킬 수 있다.

데이터 복제

원격지에 데이터를 복제할 때, 고려해야 할 몇 가지 요인이 있다.

- 사이트 간의 거리 : 거리가 멀수록 일반적으로 지연 시간 및 / 또는 지터가 더 발생하기 쉽다.
- 이용 가능한 대역폭 : 연결 범위와 다양성
- 애플리케이션에 필요한 데이터 전송 속도 : 데이터 전송 속도는 이용 가능한 대역폭보다 낮아야 한다.
- 복제 기술은 네트워크를 효과적으로 사용할 수 있도록 병행해서 사용 가능해야 한다.

데이터 복제 시 두가지 주요 방법이 있다.

동기 복제

데이터가 여러 위치에서 개별적으로 업데이트된다. 이 작업은 네트워크 성능과 가용성에 의존한다.

비동기 복제

데이터가 여러 위치에서 개별적으로 업데이트되지 않는다. 데이터는 네트워크 성능과 가용성이 허용하는 범위에서 전송되며, 애플리케이션은 데이터를 계속 작성한다. 이러한 데이터는 아직 완전히 복제되지 않을 수 있다.

많은 데이터베이스 시스템이 비동기 데이터 복제를 지원한다. 데이터베이스 복제본은 원격에 배치 가능하며, 복제본은 기본 데이터베이스 서버와 완전히 동기화될 필요는 없다. 이 점은 많은 시나리오에서 허용되는데, 이를테면 백업 소스 또는 보고/읽기 전용 사용 사례가 이에 해당한다.

AWS 에서는 지역 내 가용 영역이 잘 연결되어 있으나, 물리적으로는 분리되어 있다. 예를 들어, "다중 AZ" 모드를 사용하는 경우 Amazon Relational Database Service 는 동기 복제를 통해 2 차 가용 영역에 데이터를 복제한다. 이렇게 함으로써 기본 가용 영역을 사용할 수 없게 될 경우에도 데이터 손실을 방지할 수 있다.

AWS 지역은 서로 완전히 독립되어 있으나, 액세스하고 사용하는 방식은 모두 같다. 고객은 서로 다른 대륙 간처럼 멀리 떨어진 위치의 재해를 해결하는 복구 프로세스를 만들 수 있다. 장거리 재해 복구 시 흔한 문제나 비용이 발생하지 않는다. 고객은 데이터와 시스템을 두 곳 이상의 AWS 지역에 백업하여 대규모 재해가 발생하더라도 서비스를 복구할 수 있다. 고객은 AWS 지역을 사용하여 작업 프로세스의 복잡성을 상대적으로 줄이고 전 세계 최종 사용자에게 서비스를 제공할 수 있다.

재해복구 계획의 개선

탄탄한 재해 복구 계획을 수립하기 위해서는 몇 가지 중요한 단계를 따라야 한다.

테스트

재해 복구 솔루션을 배치한 다음에는 테스트를 해야 한다. "게임 데이"는 재해 복구 환경에 장애 조치를 수행하는 날이다. 충분한 설명서를 준비하여 실제 상황이 발생했을 때 프로세스를 최대한 간소화하도록 한다.

AWS 에서는 게임 데이 시나리오를 테스트하기 위한 복제 환경을 신속하고 비용 효율적으로 구성할 수 있으며, 일반적으로 기존의 생산 환경을 변경할 필요가 없다. AWS CloudFormation 을 사용하여 AWS 에 완벽한 환경을 배포할 수 있다.

이 서비스는 템플릿을 사용하여 AWS 리소스에 대해 설명하며, 전체 환경을 생성하기 위해 필요한 관련 종속성 또는 런타임 매개 변수에 대해서도 설명한다.

차별화된 테스트는 다양한 종류의 재해를 대비하고 있는지 확인하기 위한 중요한 요소이다. 다음은 "게임 데이" 시나리오 예이다.

- 특정 사이트와 컴퓨터 세트에 전력 손실 발생
- 단일 사이트의 ISP 연결 손실
- 핵심 비즈니스 서비스에 영향을 미치는 바이러스가 다중 사이트에 작용함
- 사용자의 실수가 데이터 손실을 야기하여 PIT(Point in Time) 복구가 필요하다

모니터링 및 경보

정기적인 점검과 충분한 모니터링을 실시하여 재해 복구 환경이 서버 장애나 연결 문제, 애플리케이션 문제 등으로 영향을 받았을 때 경고해 주어야 한다. Amazon CloudWatch 를 통해 AWS 리소스의 메트릭에 액세스할 수 있다. 경보는 어떤 메트릭에서든 정의된 임계값에

따라 설정할 수 있으며, 필요한 Amazon Simple Notification Service 메시지를 전송하여 예기치 않은 동작 발생에 대해 경고할 수 있다. AWS 에서 어떠한 모니터링 솔루션이든 사용할 수 있다.

사용자의 회사가 인스턴스 메트릭뿐만 아니라 게스트 OS 통계 및 애플리케이션 상태를 모니터링하기 위해 사용하는 기존의 모니터링 및 경고 도구를 계속 사용할 수도 있다.

백업

재해 복구 환경으로 전환한 경우, 지속적으로 정기적인 백업을 해야 한다. 백업 및 복구를 정기적으로 테스트하는 것은 폴백 솔루션에 필수적이다.

AWS 를 사용하면 재해 복구 인프라를 "항시 작동"할 필요 없이 저렴한 비용으로 자주 재해 복구 테스트를 수행할 수 있다.

사용자 액세스

AWS Identity and Access Management(IAM)을 사용하여 재해 복구 환경의 리소스에 안전하게 액세스할 수 있다.

이 방식으로 재해 복구 환경에서 작업하는 동안 사용자의 책임을 분리하는 역할/사용자 기반 보안 정책을 만들 수 있다.

자동화

구성 관리 또는 오케스트레이션 소프트웨어를 사용하여 AWS 기반 서버와 온 프레미스 서버에 애플리케이션 배포를 자동화할 수 있다. 자동화를 통해 두 환경 모두에서 애플리케이션 및 구성 변경 관리를 손쉽게 처리할 수 있다.

몇 가지 인기 있는 오케스트레이션 소프트웨어 옵션이 제공된다.

AWS CloudFormation 은 몇 가지 도구와 함께 작동하여 인프라 서비스를 자동으로 프로비저닝한다. 처음 부팅 시 사용자 데이터를 인스턴스로 전달하고, 인스턴스 유형 또는 역할을 결정하기 위해 구성 관리 도구로 이동시킬 수 있다.

이를 통해 정확한 소프트웨어 및 구성이 배포되었는지 확인한다. 자동화의 전반적인 목표는 인스턴스 상태가 변경되지 않도록 자동으로 유지하는 것이다.

Auto Scaling 을 사용하여 인스턴스 풀의 규모가 CloudWatch 에서 지정한 메트릭에 따른 수요량을 충족하기에 적합한지 확인할 수 있다. 재해 복구 측면에서 다시 말하면 사용자가 환경을 더 많이 사용하면 이러한 증가된 수요를 충족하도록 솔루션을 자동으로 확장할 수 있다는 것이다. 이벤트가 종료되고 사용량이 잠재적으로 감소하면 솔루션을 최소 수준의 서버로 다시 축소할 수 있다.

소프트웨어 라이선스와 재해 복구

AWS 환경에 대한 라이선스를 제대로 받았는지 확인하는 것은 다른 어떤 환경에 대한 라이선스를 받는 것 못지 않게 중요하다.

Amazon 은 라이선스 관리를 용이하게 해주는 다양한 모델을 제공한다.

예를 들어, "Bring Your Own License"를 몇몇 소프트웨어 구성 요소 또는 운영 체제에서 사용할 수 있다.

또는 라이선스 비용이 시간당 요금에 포함되어 있는 소프트웨어군도 있다. 이를 "License included"라고 한다.

"Bring Your Own License"는 재해 시, 기존의 소프트웨어 투자 요소를 활용할 수 있다. "License included"는 재해 복구 테스트 기간과 같이 매일 사용하지 않는 재해 복구 사이트에 대한 사전 라이선스 비용을 최소화한다.