Technical Guide

클라우드 환경에서 재해복구

May 2021

SAMSUNG SDS

Contents

1. 개요

이 문서는 SDS 클라우드 환경에서 비즈니스 연속성과 회복탄력성(Resilience)를 보장하고, 비즈니스 니즈에 따른 DR(Diaster Recovery) 설계를 위한 재해 복구 계획 수립 방안에 대하여 다루고 있습니다.
서비스 중단은 언제든 발생할 수 있습니다. 네트워크 장애, 애플리케이션에 심각한 버그가 발생하거나, 어느 순간에는 자연 재해를 직접 겪는 경우도 있습니다. 사고가 발생하면 견고하고 철저한 테스트를 거친 재해 복구 계획의 중요성이 드러납니다.
잘 설계되고 테스트된 재해 복구 체계는 재해 발생 시 비즈니스의 영향을 최소화할 수 있습니다. SDS Cloud 는 고객이 구축한 시스템 사용 연속성을 위한 빌드 또는 확장하는 데 사용할 수 있는 강력하고 유연하며 경제적인 재해 복구 체계 구성을 위한 재료를 제공합니다.

재해(Disaster)의 정의는 정보기술 외부로부터 기인하여 예방 및 통제가 불가능한 사건으로 인해 정보기술서비스가 중단되거나, 정보시스템의 장애로부터의 예상 복구소요시간 이 허용 가능한 범위를 초과하여, 정상적인 업무 수행에 지장을 초래하는 피해를 의미합니다.
재해 복구(Disaster Recovery) 는 재해로 인하여 중단된 정보기술 서비스를 재개하는 것으로 재해복구를 위해서는 사전에 재해복구를 위한 계획 및 이를 지원하는 시스템이 준비되어야 하는데, 이를 각각 업무 연속성계획 (BCP, Business Continuity Plan) 및 재해복구시스템(Disaster Recovery System)이라 합니다.
업무 연속성계획은 두 가지 주요 측정항목을 정의하는 비즈니스 영향 분석으로 시작됩니다. 복구목표시간(RTO, Recovery Time Objective)는 재해로 인하여 서비스가 중단되었을 때, 서비스를 복구하는데까지 걸리는 최대 허용시간 말합니다. 복구목표시점(RPO, Recovery Point Objective)은 재해로 인하여 중단된 서비스를 복구하였을 때, 유실을 감내할 수 있는 데이터의 손실 허용시점을 말합니다.

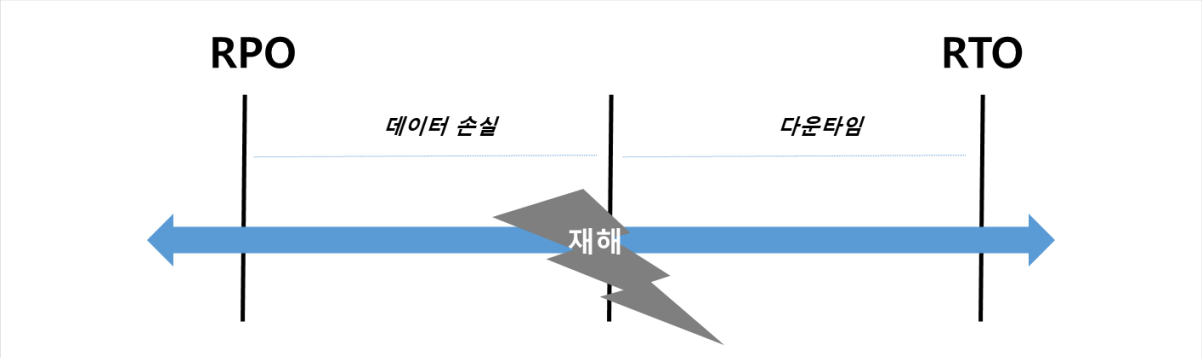

Figure 1. 재해 발생 시점을 기준으로 본 RPO와 RTO

일반적으로 RTO 및 RPO 값이 작을수록, 다시 말해 애플리케이션 중단으로부터 더 빠르게 복구되어야 할수록 애플리케이션의 실행 비용이 증가합니다.

RTO 및 RPO 값이 작을수록 복잡성이 커지기 때문에 이에 대한 관리 오버헤드 또한 증가합니다. 고가용성 애플리케이션을 사용하려면 물리적으로 분리된 두 데이터 센터 간의 배포를 관리하고 복제 등을 관리해야 합니다.

2. DR 계획 기초

2.1 재해복구시스템 복구수준별 유형

재해복구시스템은 복구수준별 유형에 따라 일반적으로 미러사이트, 핫사이트, 웜사이트, 콜드사이트로 구분됩니다.

□ 미러사이트(mirror site)
- 주센터와 동일한 수준의 정보기술자원을 원격지에 구축하여 두고 주센터와 재해복구센터 모두 액티브 상태(Active-Active)로 실시간 동시 서비스를 하는 방식
- 재해발생시 복구까지의 소요시간은 즉시(이론적으로는 0)
- 초기 투자와 유지보수에 높은 비용이 소요됨
- 웹 어플리케이션 서비스 등 데이터의 업데이트 빈도가 높지 않은 시스템 적용 가능
- 데이터베이스 어플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우 양쪽의 사이트에서 동시에 서비스를 제공하게 하는 것은 시스템의 높은 부하를 초래하여 실용적이지 않으므로, 핫사이트 구축이 일반적임

□ 핫사이트(hot site)
- 주 센터와 동일한 수준의 정보기술자원을 대기상태(Standby)로 원격지 사이트에 보유하면서(Active-Standby), 동기(Synchronous) 또는 비동기(Asynchronous) 방식의 실시간 미러링(Mirroring)을 통하여 데이터를 최신의 상태로 유지하고 있다가, 주 센터 재해시 재해복구센터의 정보시스템을 액티브로 전환하여 서비스하는 방식으로 RPO≒0을 지향함
- 재해발생시 복구까지의 소요시간(RTO)은 수시간(약 4시간이내)
- 초기 투자와 유지보수에 높은 비용이 소요됨
- 데이터베이스 어플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우, 재해복구센터는 대기상태(Standby)로 유지하다가 재해시 액티브(Active)로 전환하는 방식이 일반적임

□ 웜사이트(warm site)
- 핫사이트와 유사하나, 재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신, 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하거나, 전체적으로 규모를 축소하여 구성하는 방식.
- 실시간 미러링을 수행하지 않으며 데이터의 백업 주기가 수시간~1일 정도로

핫사이트에 비해 다소 긴 편으로, 일반적으로 RPO가 약 수시간~1일 수준임.
- 재해발생시 복구까지의 소요시간(RTO)은 수일~수주 수준임
- 구축 및 유지비용이 미러사이트 및 핫사이트에 비해 저렴하나, 초기의 복구수준이 완전하지 않으며, 완전한 복구까지는 다소의 시일이 소요됨

□ 콜드사이트(cold site)
- 데이터만 원격지에 보관하고, 이의 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고 있다가, 재해시에 데이터를 근간으로 하여 필요한 정보자원을 조달하여 정보시스템의 복구를 개시하는 방식.
- 주 센터의 데이터는 주기적(수일~수주)으로 원격지에 백업되며, 일반적으로 RPO가 수일~수주 수준임
- 재해발생시 복구까지의 소요시간(RTO)은 수주~수개월임
- 구축 및 유지비용이 가장 저렴하나, 복구소요시간이 매우 길고, 복구의 신뢰성이 낮음

2.2 재해복구시스템 구현 기술

재해복구시스템의 방식 중, 콜드사이트 방식은 시스템 운영 중에 주기적으로 백업한 데이터를 네트워크를 이용한 원격지 복제 기술을 활용하여 원격지에 소산 보관하는 방식입니다.

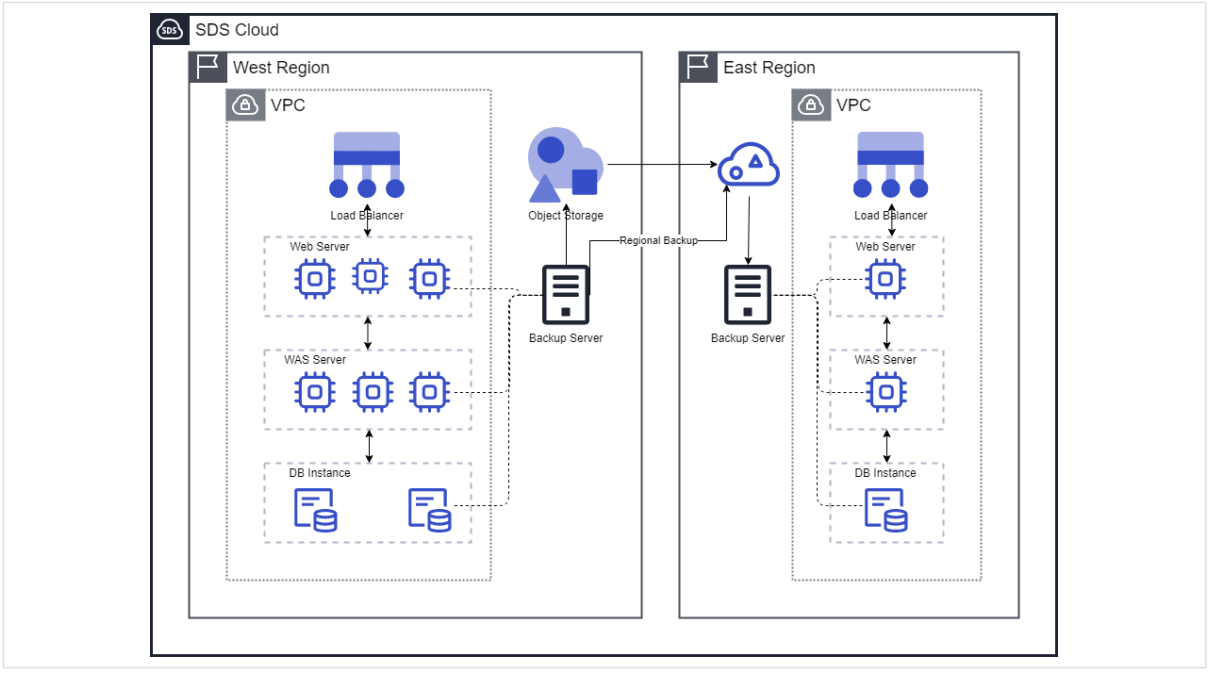

Figure 2. 백업 기반 복제 기술

핫사이트 이상 수준의 재해복구시스템을 구성하는 방법은 다음과 같이 분류할 수 있습니다.

□ 데이터 복제 방식

- H/W 적 복제방식: 스토리지 복제

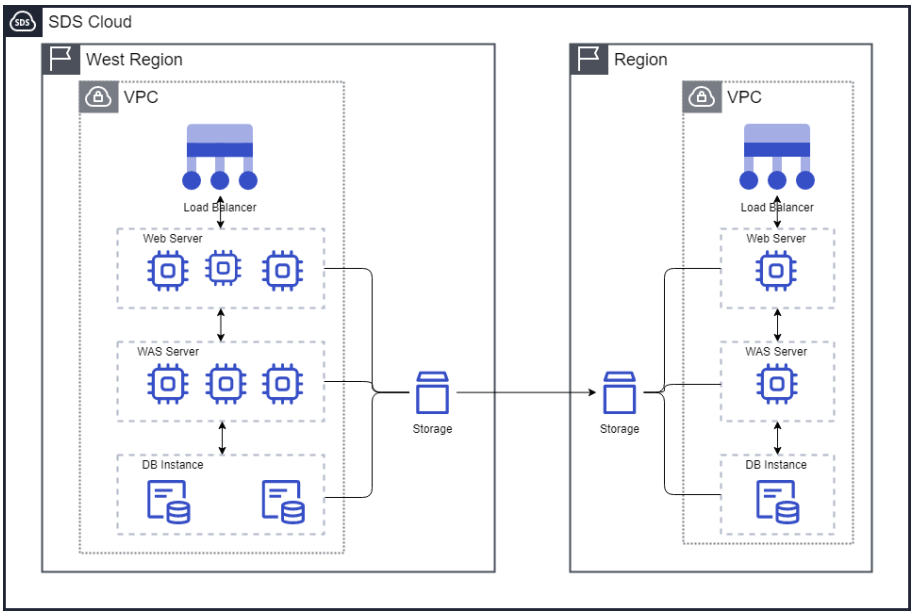

Figure 3. 스토리지 기반 복제 기술

- 물리 저장장치 수준: 디스크 장치를 이용한 복제
- Region 간 스토리지는 마이크로코드 수준에서 호환성을 제공
- 대용량 고성능 디스크를 사용하는 운영환경, 또는 File Server 실시간 복제 시에 주로 사용

- S/W 적 복제방식 : 전용 솔루션(S/W)의 데이터 복제기술 활용

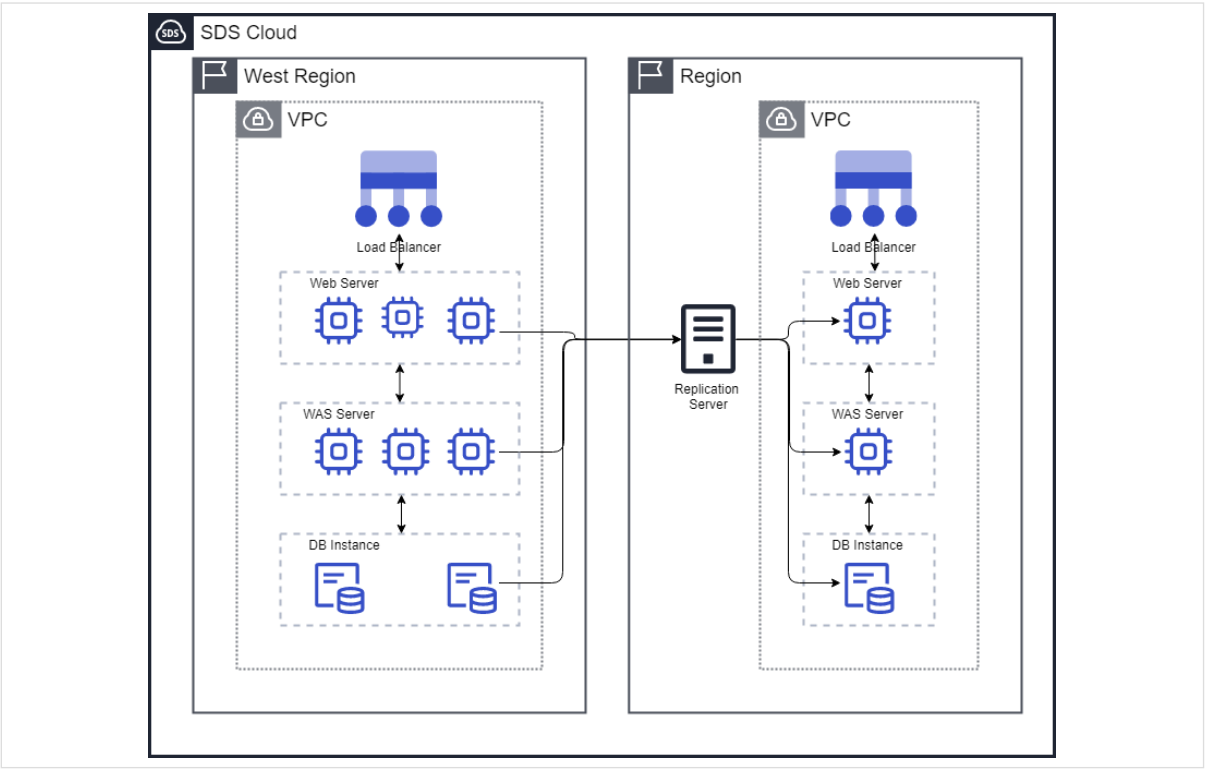

Figure 4. SW 기반 복제 기술

- 운영체제 수준: 데이터 복제 전용 솔루션을 이용한 복제
- DBMS 수준: DBMS에서 제공하는 기능 혹은 전용 솔루션 활용
- Region 간 스토리지는 이기종이어도 가능
- 복제 솔루션은 해당 서버 자체에서 수행되거나, 별도의 복제 전용 서버 자원을 사용하여 수행 되므로, 운영 환경의 용량과 부하를 감안하여 복제 서버 자원의 적정성을 검토해야 함

□ 데이터 전송 방식

- Sync. (동기 복제)

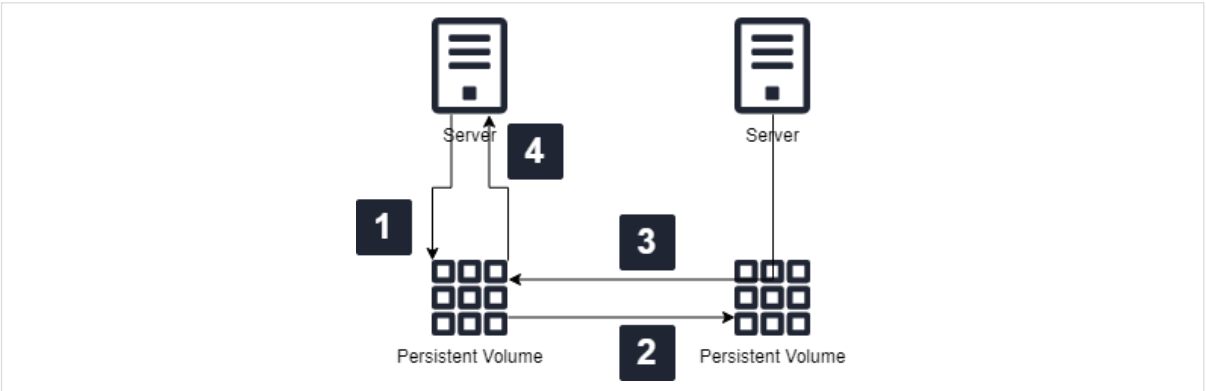

Figure 5. 실시간 동기 방식 복제

- 원격 스토리지에 데이터가 Write 되기 전까지는 메인 스토리지 I/O는 완료되지 않음.
- 원격 복제본의 데이터복제는 언제나 메인 스토리지 원본과의 거리에 비례하며, 복제작업에 따른 스토리지 서비스 응답시간은 다소 증가할 수 있음.
- RPO 손실없이 데이터 복구 및 신속한 서비스 재개가 가능함
- 전송 거리 및 I/O 패턴에 따라 시스템 서비스 영향도가 민감함.

- Async. (비동기 복제)

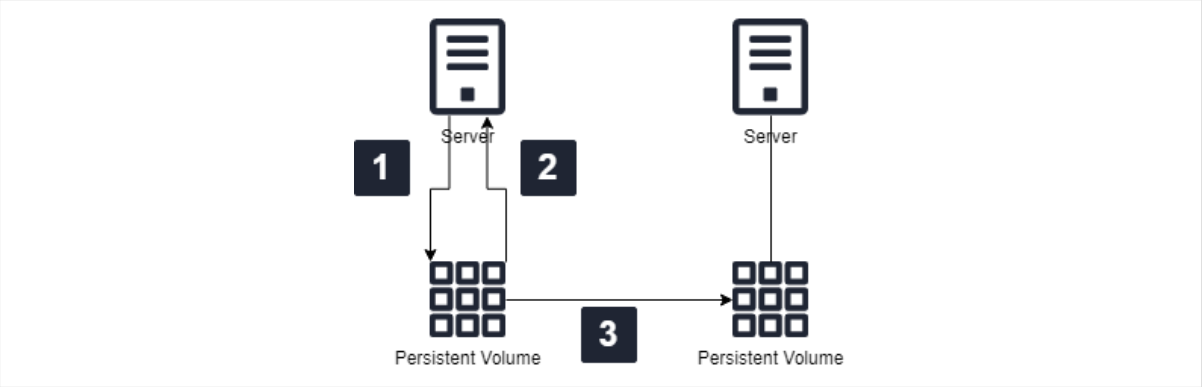

Figure 6. Near 0 비동기 방식 복제

- 수 ms 이하 데이터까지 실시간으로 데이터를 비동기 방식으로 데이터 복제 가능
- DR Site의 데이터는 Time Stamp와 Sequence Number를 이용하여 정합성 보장 가능
- RPO/RTO는 데이터 손실이 거의 없이(Near 0) 데이터 복구 및 신속한 서비스 재개 가능
- 시스템 서비스 영향은 데이터 복제 구성으로 인한 운영 서비스에는 영향이 거의 없으므로 장거리 데이터 전송에 적합하거나, I/O 패턴이 민감하지 않음
- 스케줄 기반으로 주기적으로 복제될 수 있으며, RPO 와 RTO 는 복제 주기에 영향을 받음

3. SDS 클라우드가 제공하는 DR 구성 옵션

SDS 클라우드에서는 복잡성이 낮고 비용이 저렴한 백업을 활용한 복제 방식과 Region 간 전체 자원에 대한 실시간 복제 방식까지 재해 복구 전략에 맞는 3 가지 방식을 제공하고 있습니다.

예를 들어 과거의 규정 준수 중심의 데이터의 경우 데이터에 빠르게 액세스할 필요가 없으므로 RTO 값이 크큰 백업/복구 DR 패턴이 적합했습니다. 그러나 온라인 서비스에서 중단이 발생하는 경우 가능한 한 빨리 고객 관련 애플리케이션과 데이터 부분을 모두

복구할 수 있어야 합니다. 그런 경우에는 핫 standby 패턴이 적절합니다. 일반적으로 업무상 중요하지 않은 이메일 알림 시스템은 웜 standby 패턴의 대상일 수 있습니다

3.1 Backup and Restore

백업/복구는 데이터 손실과 corruption 을 막기위한 가장 손쉬운 접근 방법입니다.
SDS 백업을 통해 self 백업 정책을 설정하고, 스케줄 기반으로 VM 이미지 백업과 DB 백업, 파일 스토리지 snapshot 을 수행하며, 같은 Region 내에 Object Storage 에 안전하게 저장합니다. 백업 시 다른 Region 에 있는 Object Storage 에 직접 백업할 수 있습니다.
Object Storage 는 async/scheduled 방식으로 버킷에 있는 object 를 다른 Region 으로 복제합니다.
DR 상황이 발생할 경우 다른 Region 에 복제되어 있던 백업 데이터를 가지고 복구할 수 있습니다.

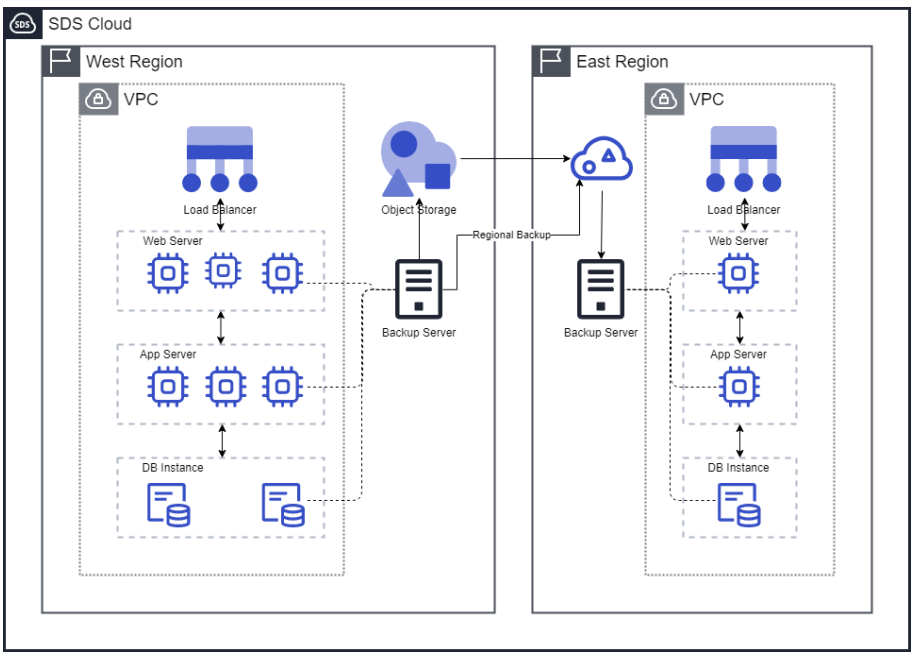

Figure 7. 백업 및 복구 방식을 이용한 재해 복구

1. 백업이 필요한 서버에 Agent를 설치하고 각 서버에 백업 정책(스케줄 백업)을 설정함.
2. Region 사이의 복제 회선을 통해 Object Storage 데이터를 동기화함
3. 재난 상황이 발생하면 Virtual Server 자원을 신청하고 Object Storage에 백업된 OS 이미지를 활용해 해당 서버를 복구해 서비스를 재개함

3.2 Warm Standby

비즈니스의 핵심 시스템인 DB 데이터는 복구에 오랜 시간이 소요되므로 백업 및 복구 방식으로는 더 높은 수준의 RPO 와 RTO 를 맞출 수 없습니다.
SDS 클라우드는 DB 시스템에 대하여 동일 Region 에 실시간 복제를 통하여 안전하게 보호하고 있으며, 고가용성의 HA 솔루션으로 서비스의 연속성을 보장할 수 있습니다. 또한 다른 Region 에 async 기반의 실시간 복제를 수행하여 RPO near 0 수준의 복제를 제공합니다. Web/WAS Application 은 SDS 백업 솔루션을 통하여 백업 데이터량에 따라 수분~수시간으로 백업 주기를 단축하고, DR 발생 시 DR 사이트에서 복구 합니다.

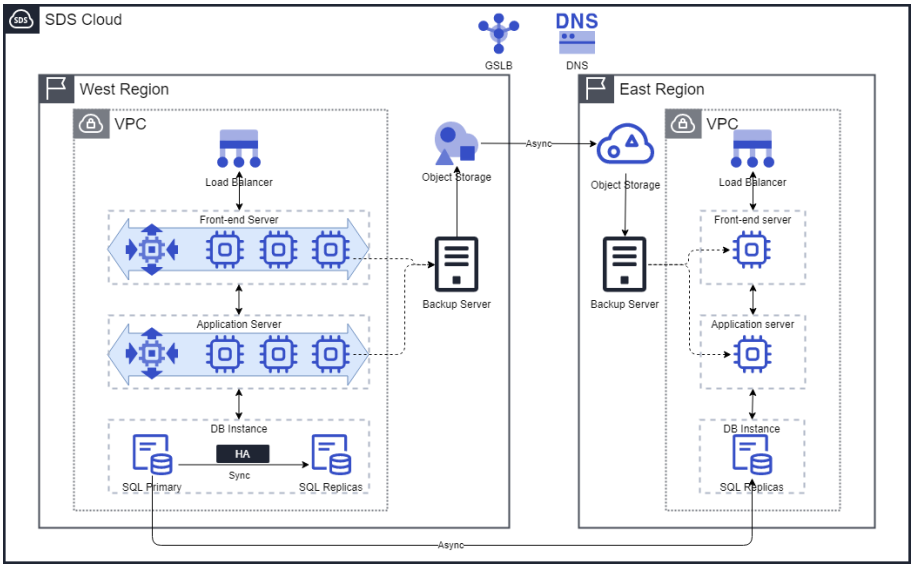

Figure 8. 백업/복구 및 SW 기반 복제 솔루션을 이용한 재해 복구

1. 백업이 필요한 서버에 Agent를 설치하고 각 서버에 백업 정책(스케줄 백업)을 설정한다 Region 사이의 복제 회선을 통해 서버를 동기화함
2. Region 사이의 복제 회선을 통해 Object Storage 데이터를 동기화함
3. DB Service는 S/W복제방식 중 비동기 복제 솔루션을 이용해 데이터를 동기화함
4. 재난 상황이 발생하면 Web/WAS는 Object Storage에 백업된 OS 이미지를 준비된 Virtual Server에 복구하고, DB 서비스는 비동기 복제한 데이터로 복구

3.3 Hot Standby

전체 비즈니스에 대하여 실시간 복제를 통하여 가장 높은 수준의 데이터 보호와 복구를 제공합니다. VM OS 뿐만 아니라 Block 스토리지에 저장된 DB, 파일 데이터에 대하여 SW 기반 실시간 복제를 수행합니다. File 스토리지, object 스토리지는 물리 스토리지 기반 실시간 복제를 수행합니다. Region 내 전체 자원에 대하여 실시간 복제를 제공하므로서, RPO near 0 수준의 데이터 보호를 제공하며, 4hr 이내 빠른 복구가 가능합니다.

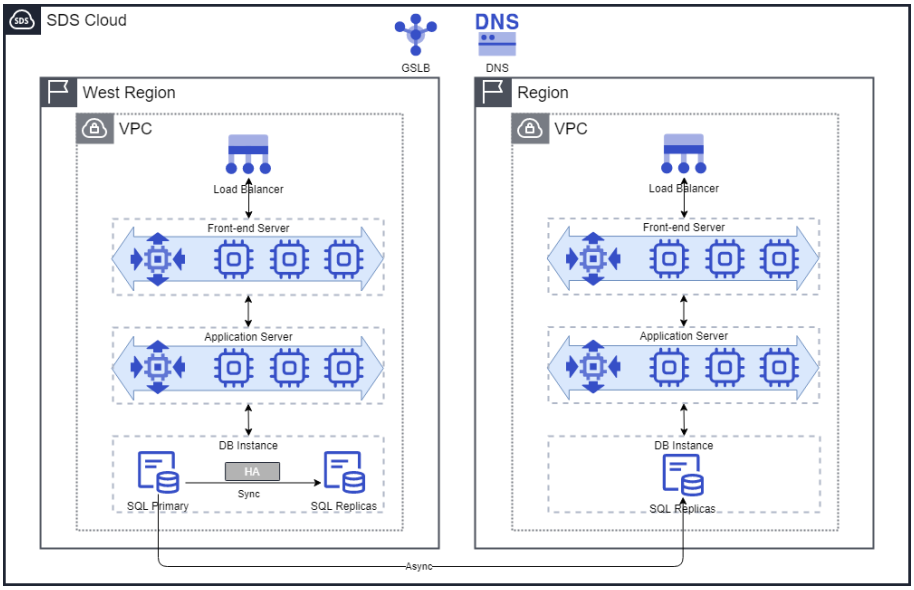

Figure9. S/W 기반 비동기 복제를 이용한 재해복구

1. DB, Web Server, Application Server에 대해서 S/W 기반의 동기화 솔루션을 통해 정책을 설정. 고객이 주/DR Site에 Virtual Server/Bare Metal Server 상품 신청 후 직접 설치/구성함
2. 파일 스토리지/오브젝트 스토리지는 물리 스토리지의 동기화 솔루션을 통해 정책을 설정함. 최초 스토리지 상품을 신청할 때, 혹은 이후 추가 변경하여 복제 서비스 신청함
3. Region 사이의 복제 회선을 통해 서버를 동기화. 고객이 주/DR Site 간 복제 전용 네트워크 상품 신청하여 직접 구성함
4. 재난 상황이 발생하면 다른 Region 에서 이미 복제되어 있는 자원을 가지고 서비스를 복구

SDS 클라우드는 검증된 솔루션 파트너를 통해 기업의 비즈니스 및 서비스 연속성을 위한 최적화된 고가용성, 재해 복구 솔루션을 제공하고 있습니다.

3.4 고려사항

Region 간 복제를 통해 DR 을 구성한 경우 복제 회선의 트래픽 사용량을 추산해 전체 DR 비용에 대해 예측을 해야 합니다. 또한 RPO 목표에 부합하도록 백업 정책(백업 주기 설정)과 복제 주기를 구성해야 합니다.

특히 퍼블릭 클라우드 서비스에 대해서 SDS Cloud 자원을 통한 DR 구성은 퍼블릭 클라우드 서비스 사업자의 Outbound 복제 트래픽 량과 그에 따른 네트워크 비용을 분석하고 의사결정을 해야 합니다.

이상으로 SDS 클라우드 자원을 활용한 DR 구성방안에 대하여 살펴봤습니다.