클라우드 네이티브 환경의 A-A센터와 재해복구 구축전략

(주) 맨텍솔루션 이진현
jhlee@mantech.co.kr

manTech
better solution

CONTENTS

1. 재해복구의 불편한 진실
2. 복구 성공율을 높이기 위한 방안들
3. K8S의 재해복구 환경과 구성
4. 국내 사례

이번 세션을 통해 알게 될 사실

- ✓ 국내 IT재해복구의 현황과 왜 실패하는가?
- ✓ 복구 성공률을 높이기 위해서는?
- ✓ K8S의 재해복구는 어떤 방법이 있는가?
- ✓ K8S가 재해복구 관점에서 기존 레거시 대비 유리한 점은?
- ✓ 재해복구의 구체적인 국내사례

1

“ 재해복구의 불편한 진실

재해로 인한 IT 중단은 늘 반복

- ✓ 2011년 농협, 2014년 SDS
  과천센터, 2018년 KT
  아현지사, 2022년 카카오사태
- ✓ 과거로 부터 무엇을 배웠는가?

2023년부터 강화되는 재해복구 관련 법안들

과학기술정보통신부 보도자료 당시 대한민국! 새로운 국민의 나라

보도시점 배포시점 배포 2023. 6. 27.(화)

디지털 재난관리 강화를 위한 「디지털 안전 3법*」 시행령 개정안 국무회의 의결

* 「방송통신발전 기본법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「전기통신사업법」

- 재난관리 대상 부가통신사업자 및 데이터센터 사업자 선정 기준 확정
- 보호조치 대상 데이터센터 시설 기준 설정, 재난 시 보고 방법 마련 등

과학기술정보통신부(장관 이종호, 이하 '과기정통부')는 디지털 재난관리 강화를 위한 「방송통신발전 기본법(이하 '방송통신발전법') 시행령」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법') 시행령」 및 「전기통신사업법 시행령」 개정안이 6월 27일(화) 국무회의를 통과하여 7월 4일(화)부터 시행될 예정이라고 밝혔다.

이번 시행령 개정은 판교 데이터센터 화재 및 서비스 장애 사고('22.10.15.)의 재발 방지를 위하여 지난 1월 3일 개정된 「방송통신발전법」, 「정보통신망법」 및 「전기통신사업법」에서 하위 법령에 위임한 사항을 규정하고, 「디지털서비스 안정성 강화 방안(3.30.)」의 후속조치로서 필요한 제도개선 사항을 반영하기 위해 이루어지는 것으로,

이미지 제공: 뉴시스

정부가 재해복구센터 구축을 의무화 해야 할 금융회사의 범위를 확대할 방침이다. 또한 전자금융사고 발생 시 피해보상이 원활히 이뤄질 수 있도록 책임보험 최저 보상한도도 상향한다.

금융감독원은 13일 서울 여의도 본원에서 이명순 수석부원장 주재로 9개 유관기관 담당자 및 22개 금융사 최고정보관리책임자(CIO)와 간담회를 열고 이같이 밝혔다.

앞서 금감원은 카카오 전산센터 화재를 계기로 금융IT 비상대책 점검에 나선 바 있다.

점검 결과 전자금융서비스를 제공하는 금융회사 중 118개 중소형사는 재해복구센터를 별도로 구축하지 않은 것으로 나타났다. 다만 이들은 관련 법규상 재해복구센터를 의무적으로 구축해야 하는 회사는 아닌 것으로 확인됐다. 재해복구센터가 구축돼 있는 회사들의 경우도 서버 용량이 주전산센터에 크게 미달하거나 대외기관 전용선이 누락돼 재해 발생시 정상적인 서비스 제공이 가능할지 의문인 곳도 있었다.

2023년 7월 13일 안전저널 기사

IT업계는 왜 그동안 재해복구에 인색했을까?

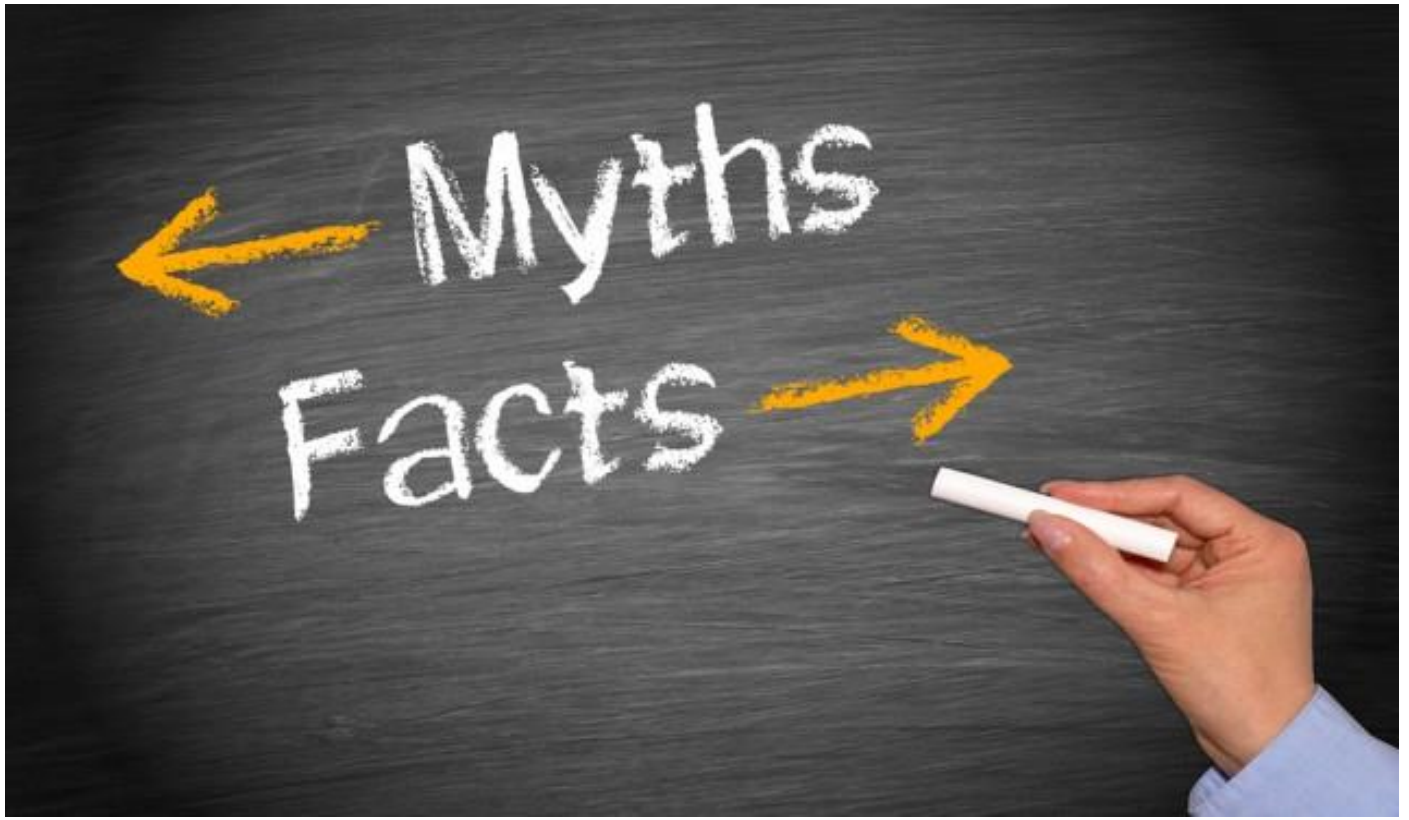
< 비용 >

< 복잡 >

< 의구심 >

백업과 복구의 불편한 진실

- ✓ 백업 데이터의 복구 실패율은 약 40%
- ✓ 이로인한 비지니스 복구 실패율은 무려 70%에 육박
- ✓ 백업본과 복제본을 활용한 복구 훈련을 대부분 수행하지 않음
- ✓ 긴급할 때 ACE는 다른 곳에서 일하고 있다.



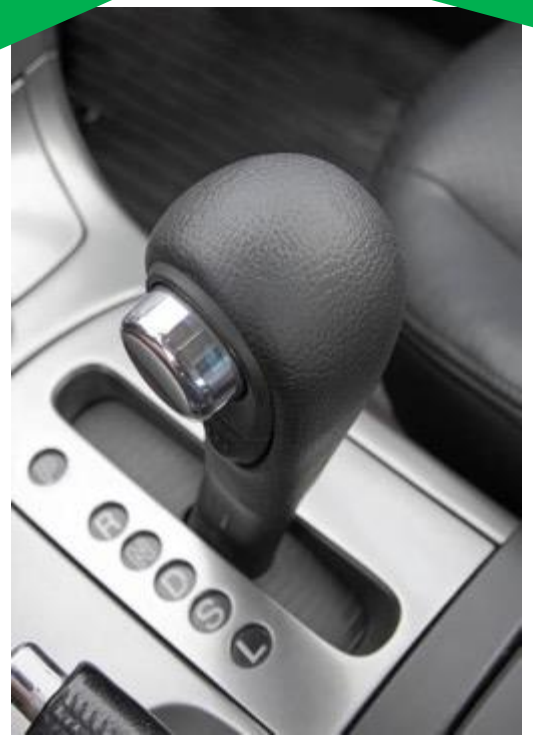
* 출처 : 2015년 12월 9일 베타뉴스

https://betanews.com/2015/12/09/myths-and-facts-about-backup-restore-and-disaster-recovery/

관심의 초점을 Shifting 해야함

Backup

Replication



복구에
초점을

Application recovery

Business recovery

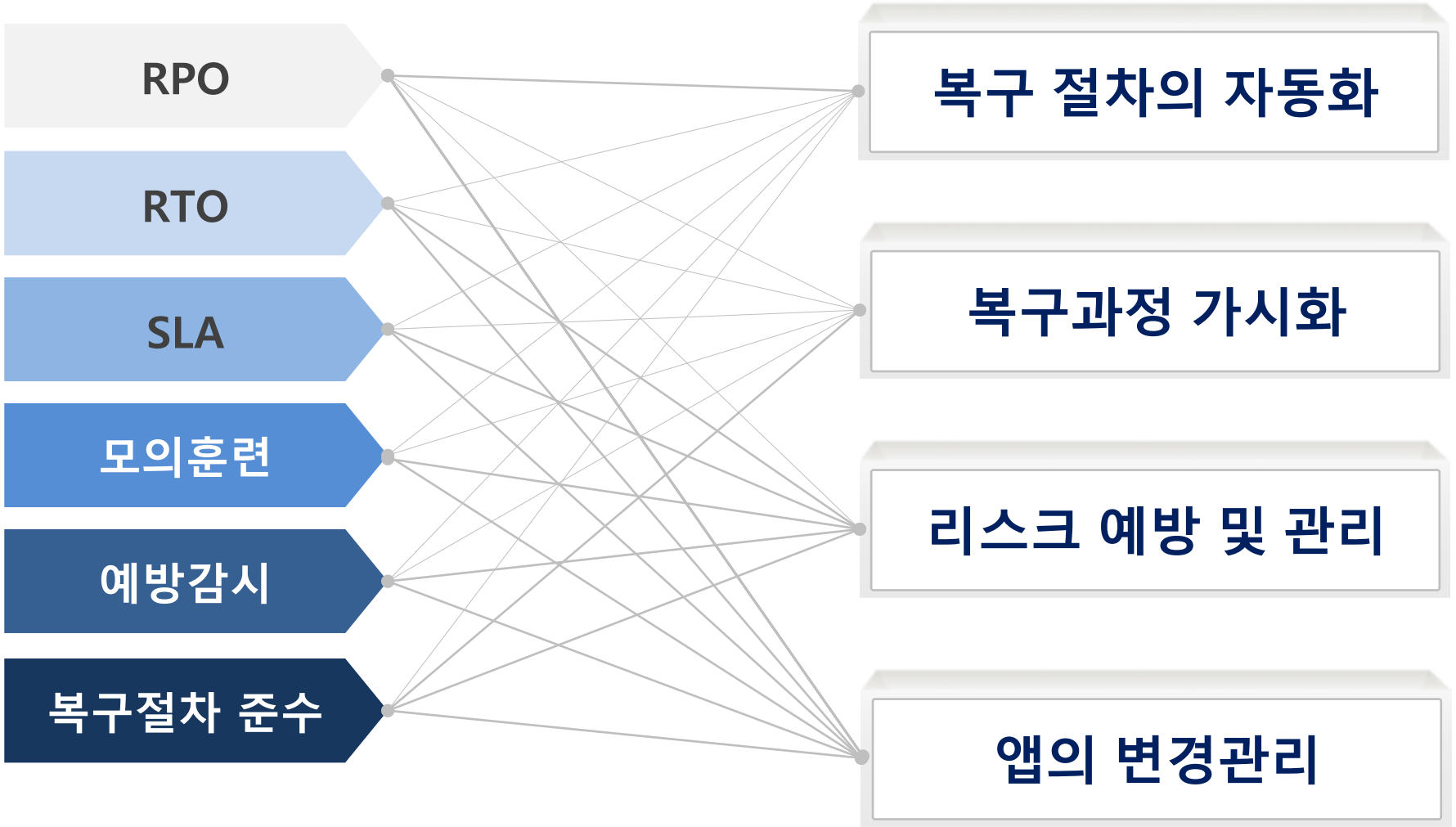
Restore

모의훈련

2

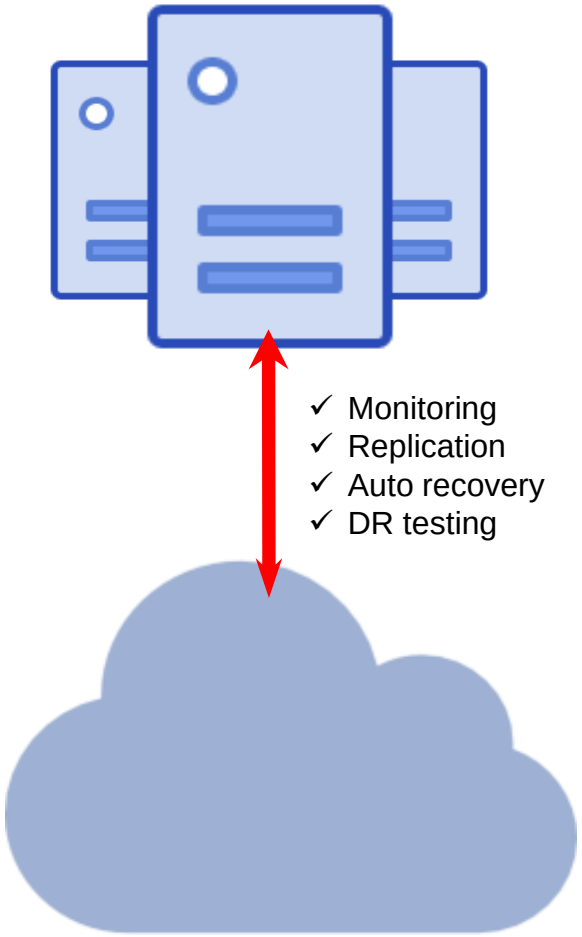
“복구 성공율을 높이기 위하 방안들

재해복구의 복잡성과 의구심을 해결할 과제



재해복구의 비용 이슈의 해결은?

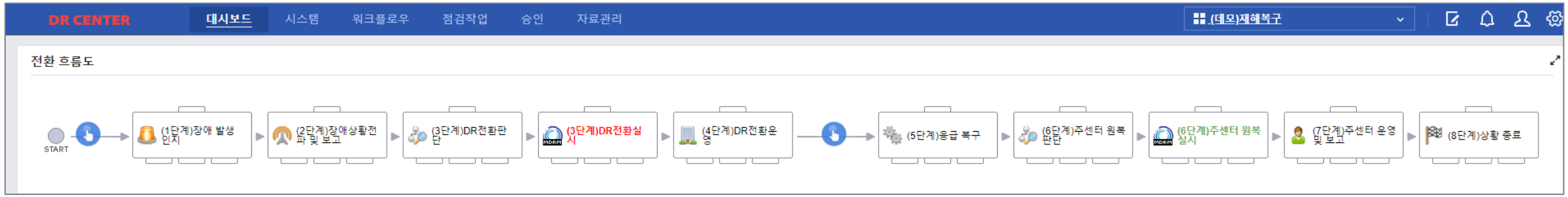
- ✓ 퍼블릭 클라우드와 연계한 A-S 혹은 A-A 하이브리드 구성
- ✓ DR센터 건립 비용 불필요
- ✓ 서버, 스토리지 등 자원 구매 불필요
- ✓ Active Active 구성 시 대기 자원에 대한 비용 낭비가 없음
- ✓ Pay as you Go 방식의 주기적 모의 훈련과 복구



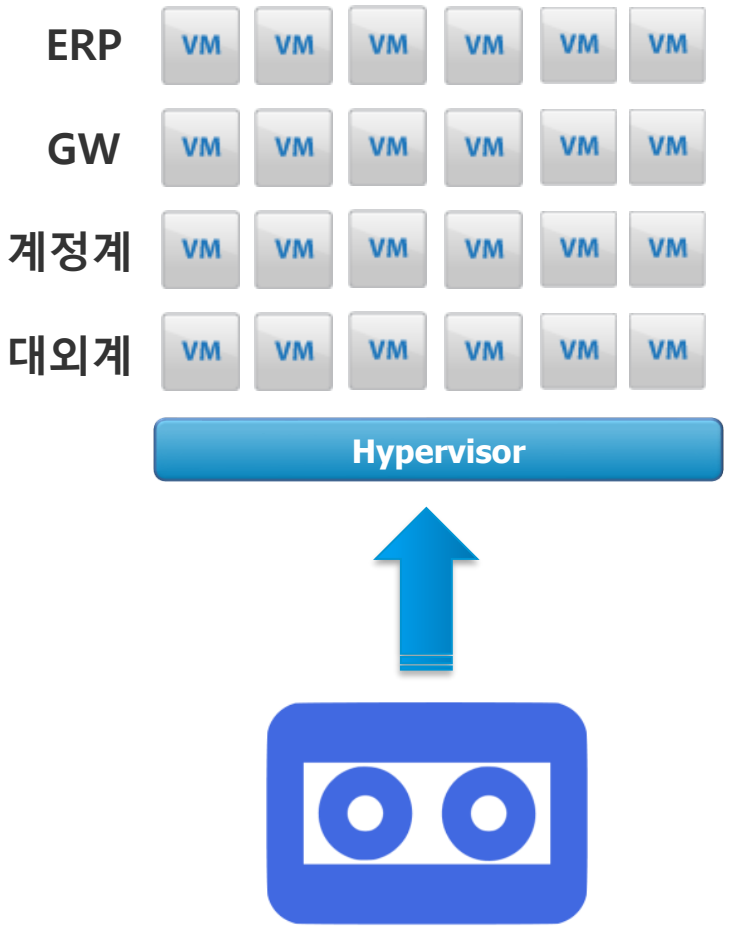
워크플로우 기반의 재해복구 자동화는 필수 요소

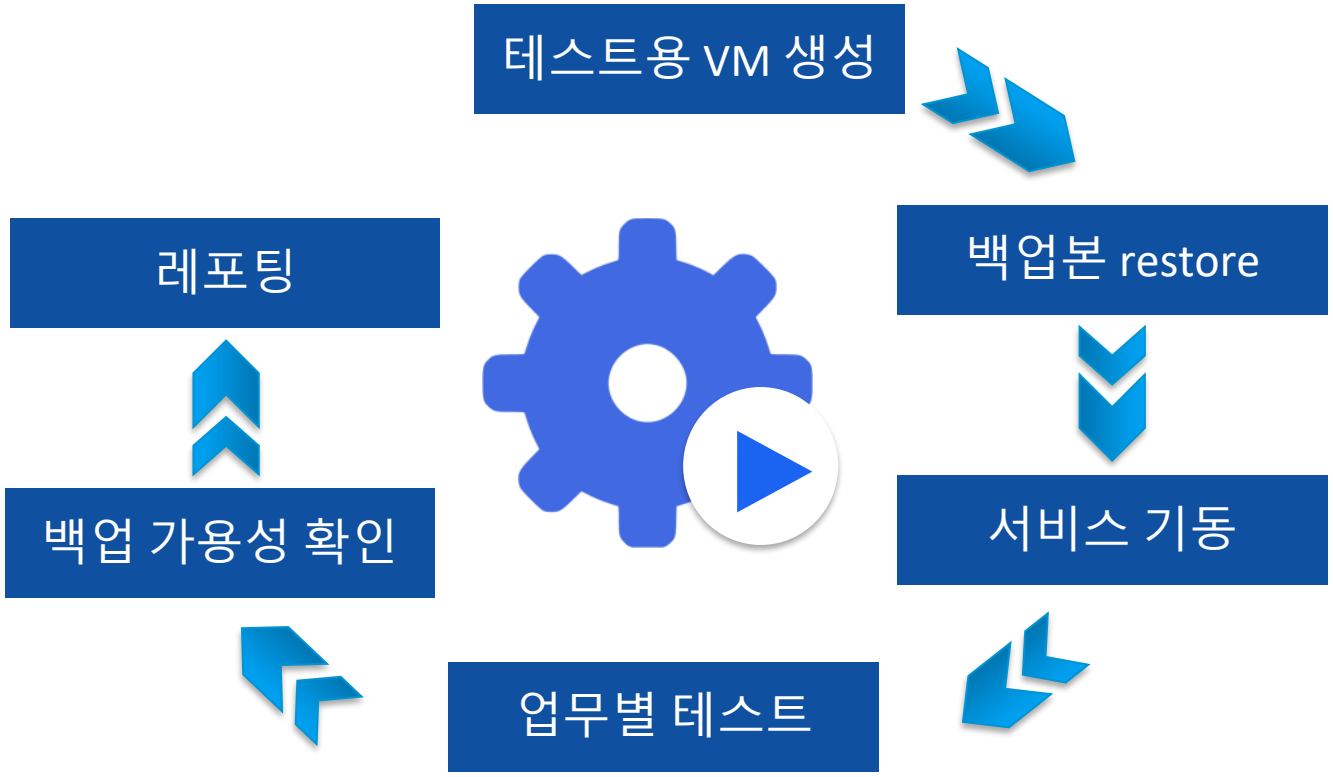
"시나리오 기반의 자동화 적용 – 절차 및 복구 자동화 "

복구 절차	수동 전환(매뉴얼)	자동화 전환	
(1단계) 재해 발생	매뉴얼	절차 자동화	
(2단계) 보고 및 통제	매뉴얼	절차 자동화	
(3단계) 협력사 및 담당자 비상 소집	매뉴얼(사전통보/2시간 소집)	절차 자동화	즉시 복구 가능 (재해복구 운영 인력)
(3단계) DR 전환 판단	매뉴얼	절차 자동화	
(4단계) DR 시스템 복구(목표: 4hr)	각 업무별 수동 복구 진행 (4hr)	복구 자동화 (2hr / 50%감소)	**정해진** 절차에 따른 복구 병렬 진행을 통한 시간 단축
(5단계) DR 복구 완료 및 서비스 재개	-	-	-

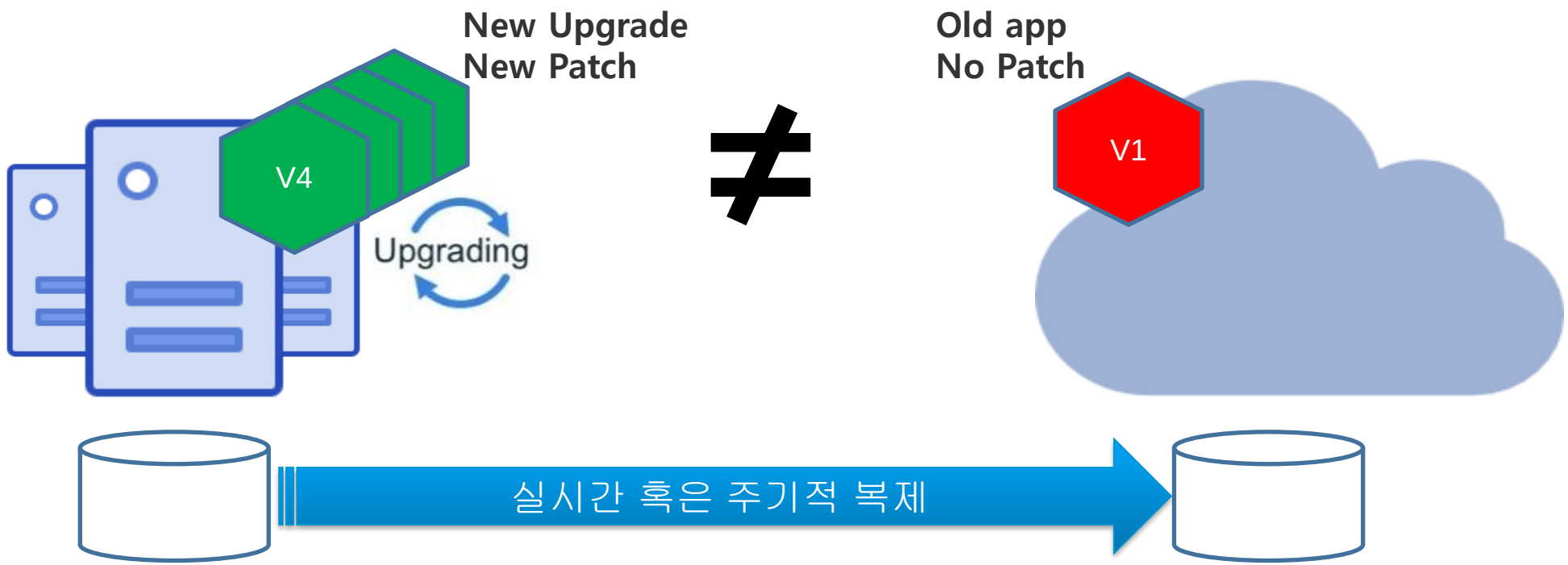


자동화된 모의훈련을 통한 백업본의 가용성 검증



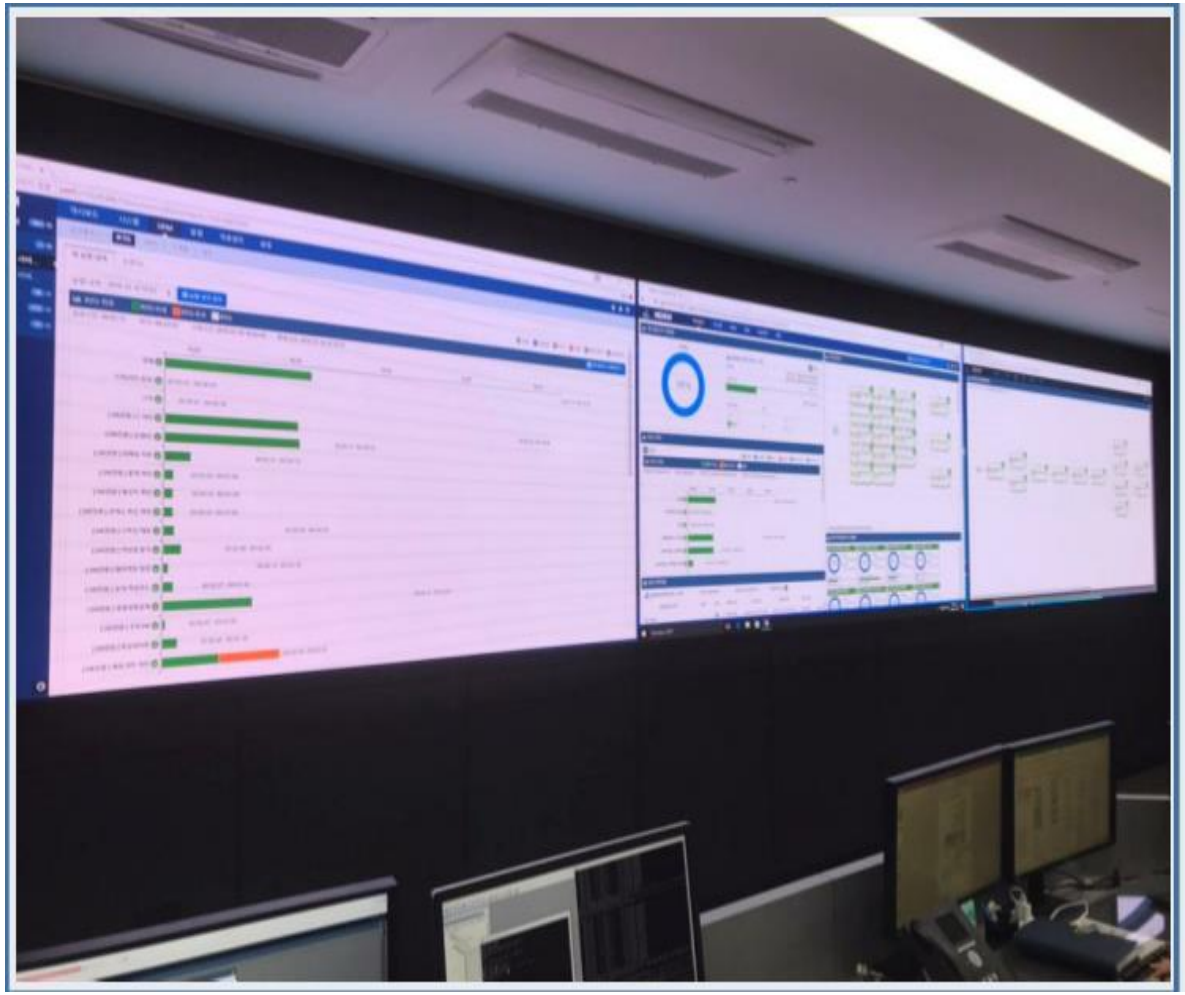


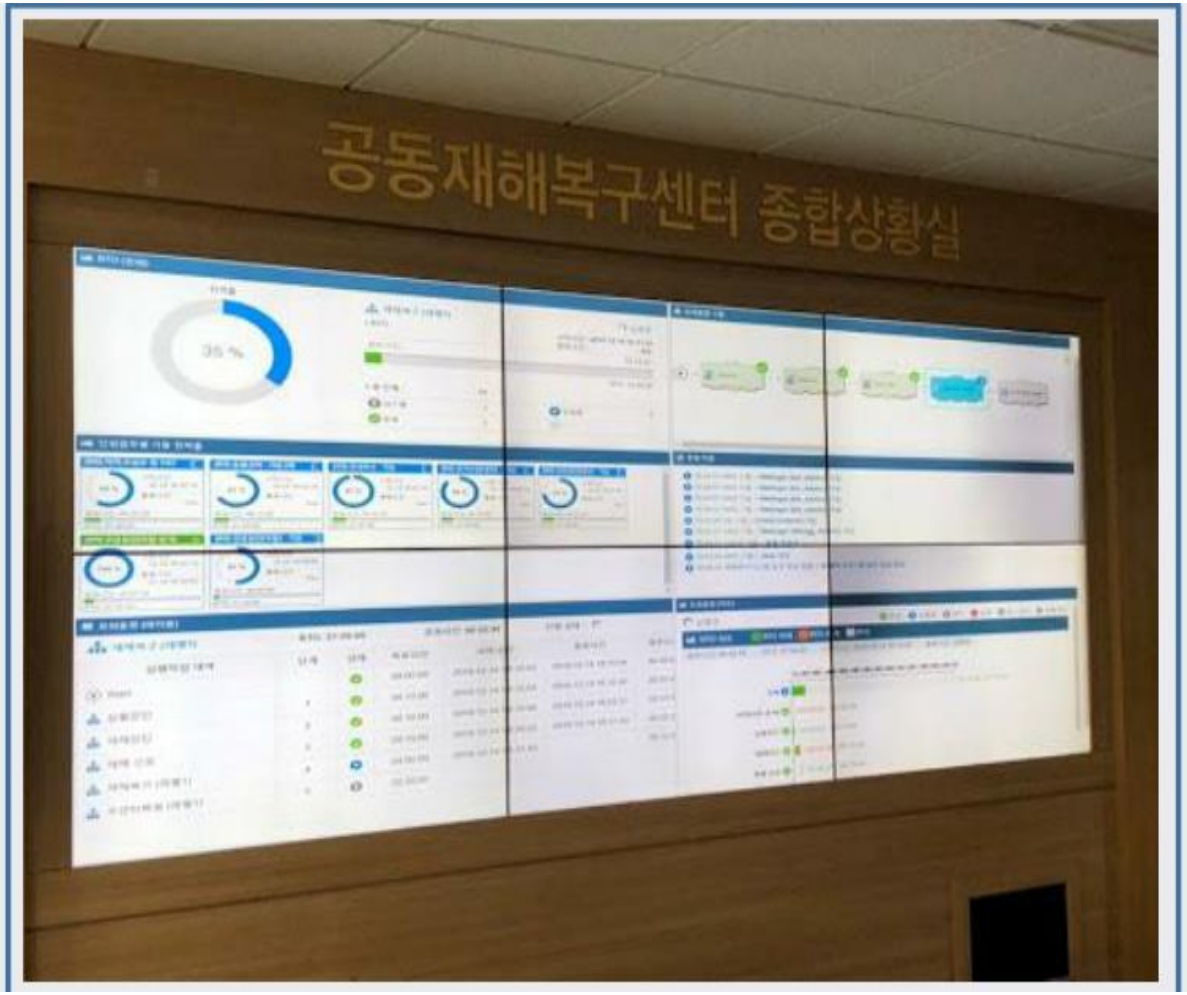
애플리케이션의 변경 유지는 필수



✓ 대부분의 DR의 현실은 데이터 소산에 초점이 맞추어져 있음
✓ 운영과 DR간 앱과 환경의 변경 차이는 DR 기동 실패의 가장 큰 원인 중 하나임
✓ 주기적인 모의훈련을 통해 이를 개선하지만 변경 주기가 매우 빠르게 짧아지고 있음

재해복구 진척도 및 모의훈련 진행사항 대시보드 운영

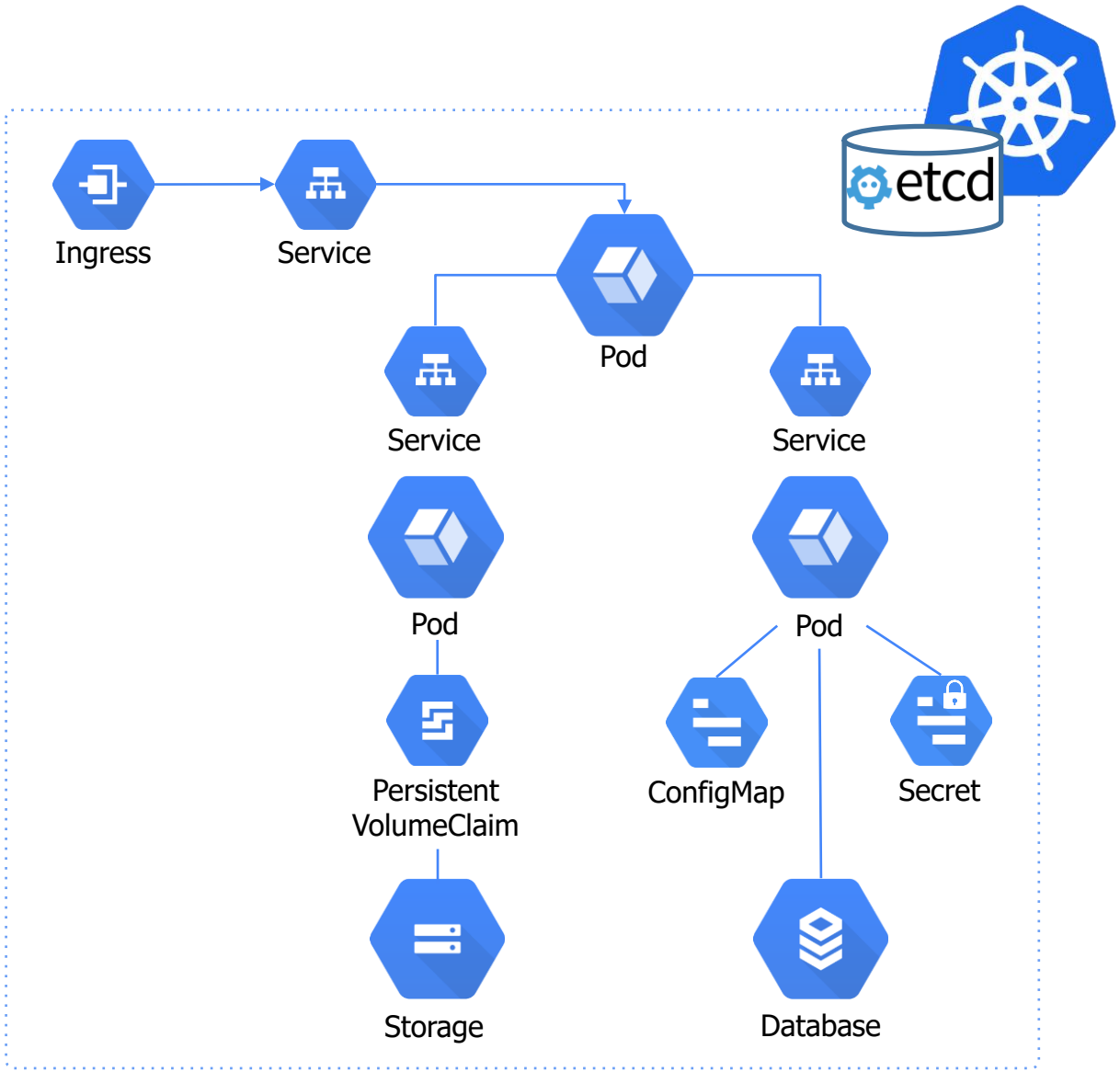




3

“ 쿠버네티스 환경의 DR

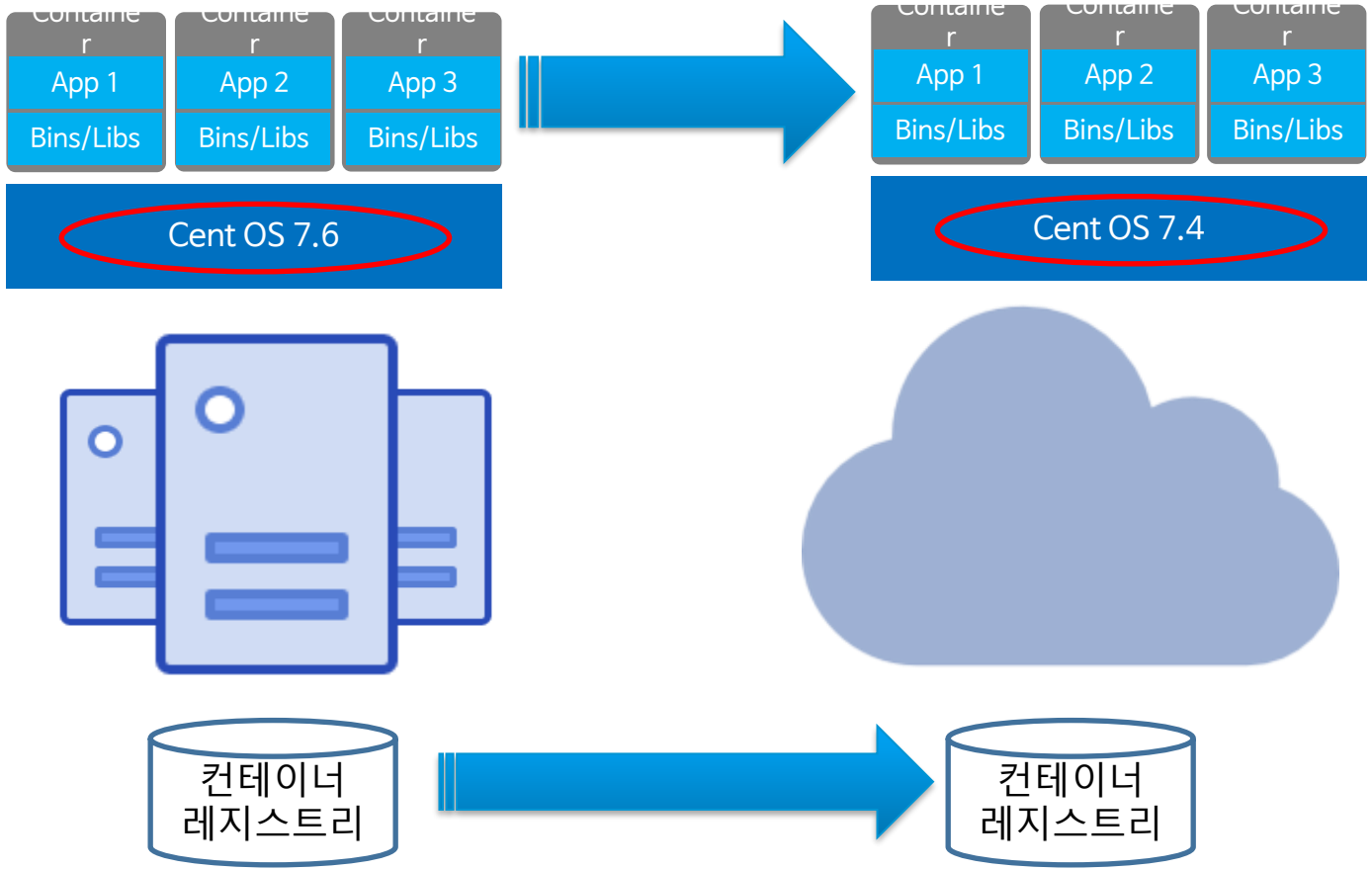
쿠버네티스 환경에서 보호 받아야 될 데이터들



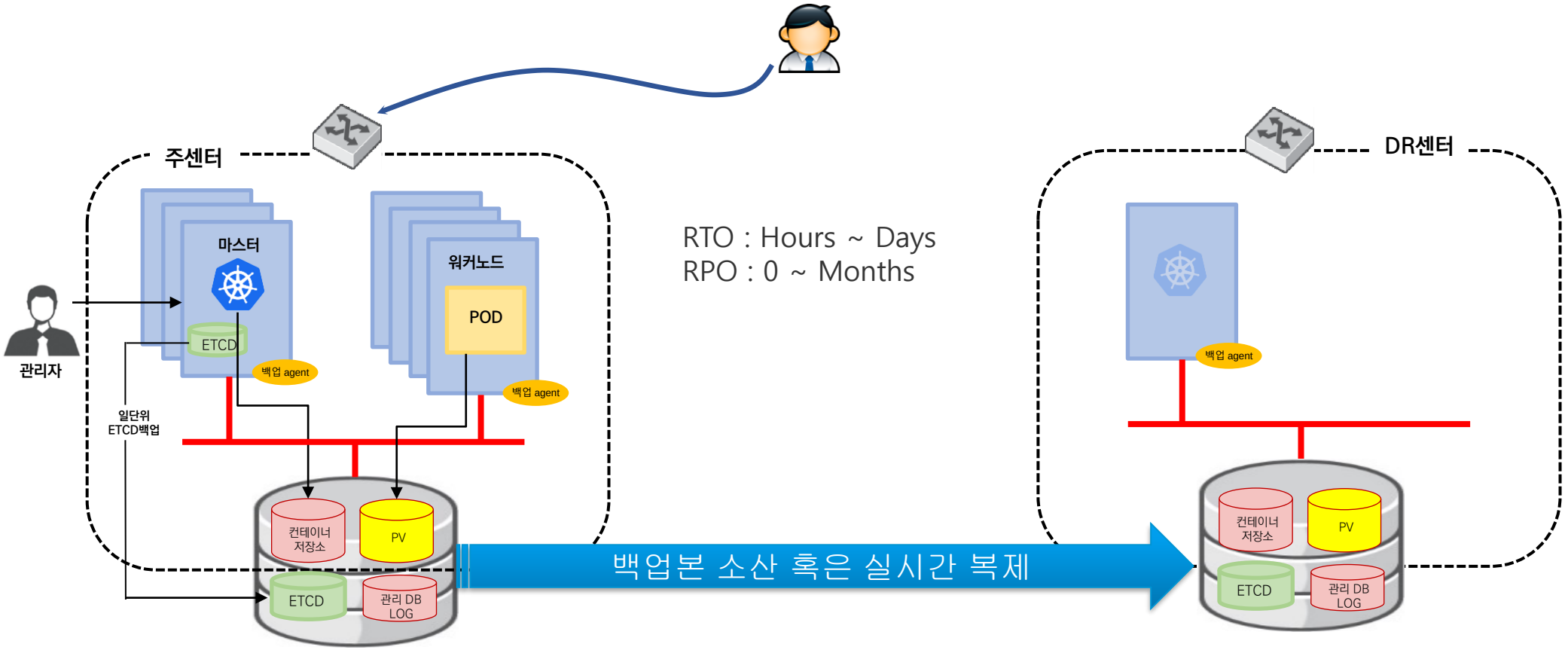
- ✓ ETCD
- ✓ 사용자 계정 DB
- ✓ 모니터링 DB
- ✓ CI/CD Log / Event Log / 감사 Log
- ✓ 컨테이너 레지스트리
- ✓ StatefulSet의 PV(영구볼륨)
- ✓ configMap
- ✓ Secret
- ✓ Yaml 화일
- ✓ Ingress

재해복구 관점에서 쿠버네티스 환경의 특장점

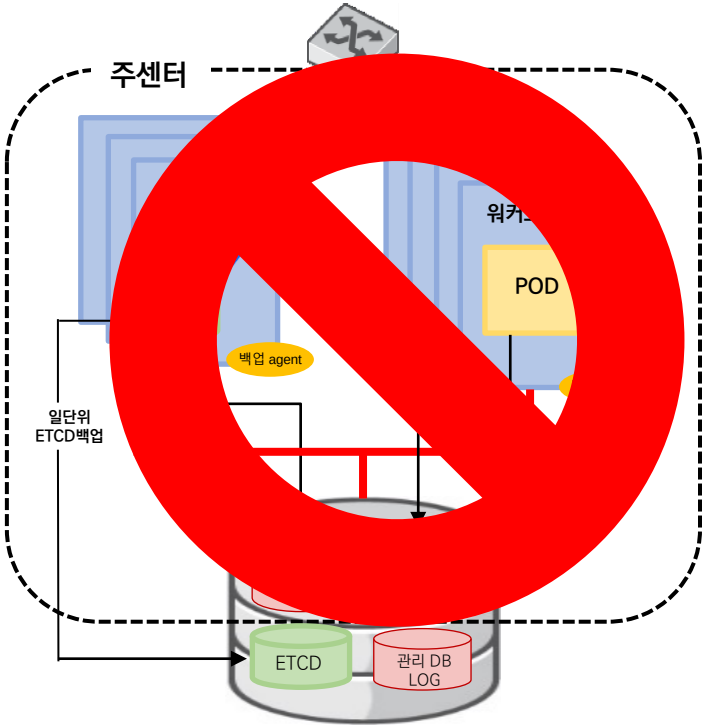
- ✓ 다양한 APP에 대해서도 환경변수는 configmap, secrect 두 개로 관리 가능
- ✓ Hypervisor, OS의 환경이 서로 달라도 컨테이너 이미지의 구동이 가능
- ✓ 운영과 DR간 컨테이너 레파지토리와 버전관리 정보를 상시 동기화를 통해 앱의 변경 관리를 쉽게 해결

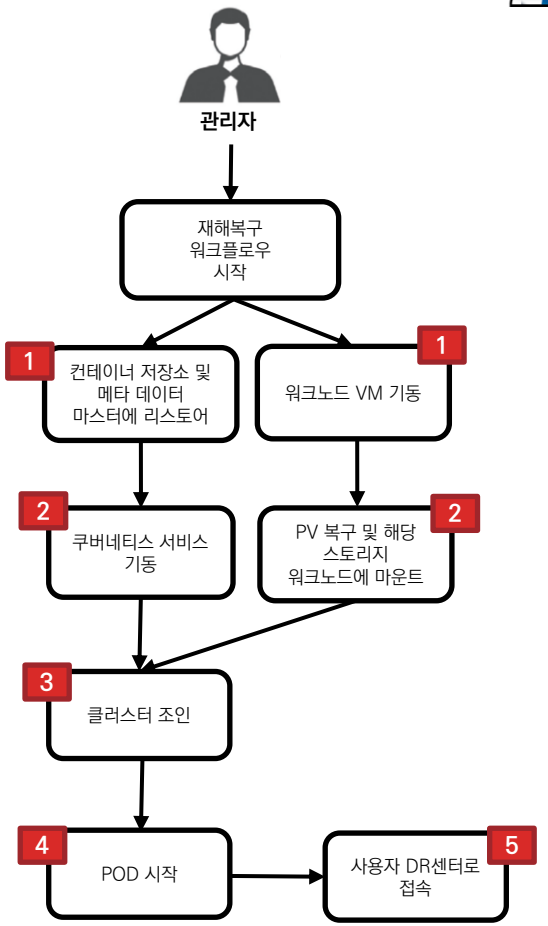


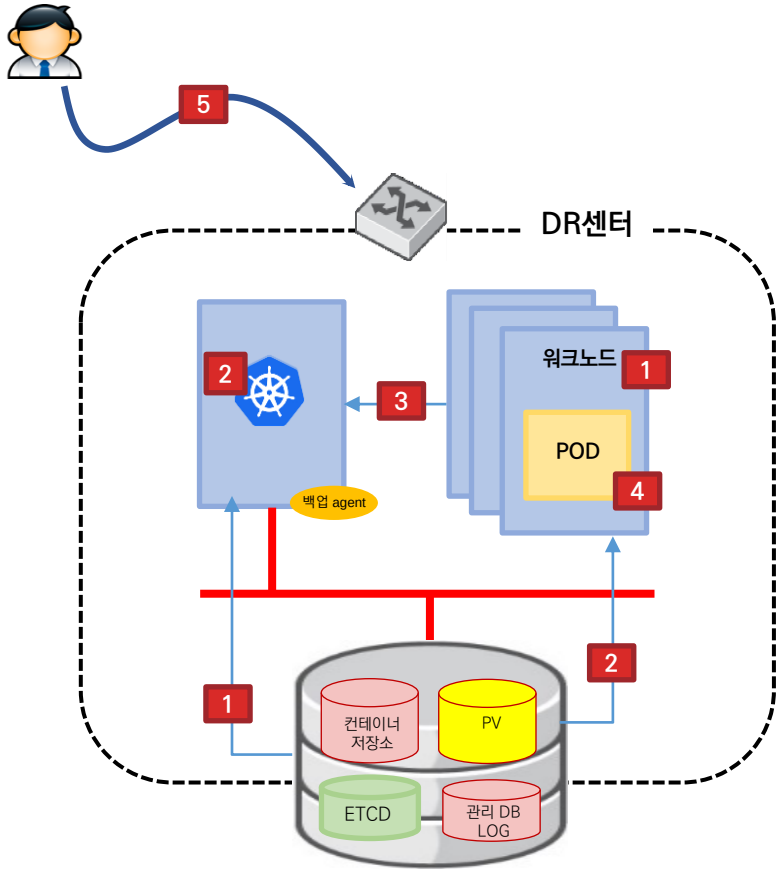
K8S환경의 Warm Site



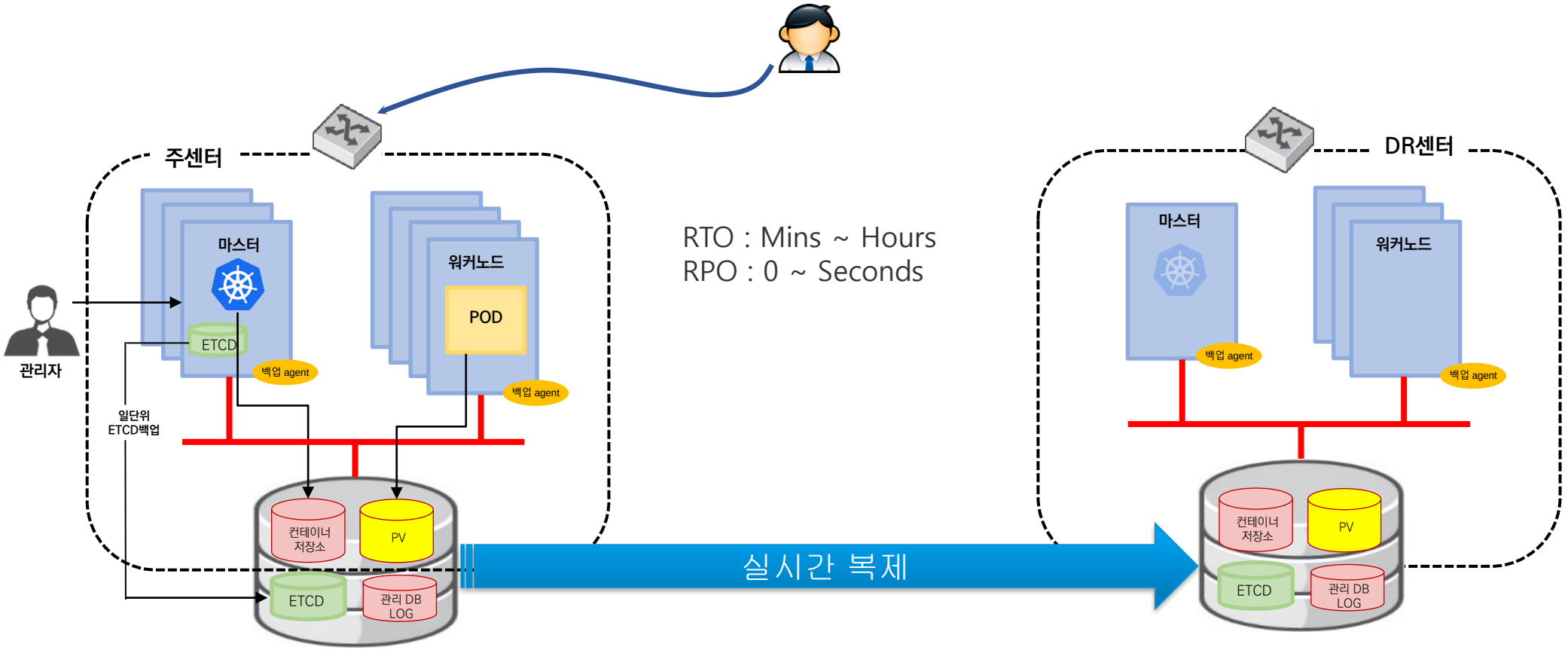
K8S환경의 Warm Site 재해복구 과정



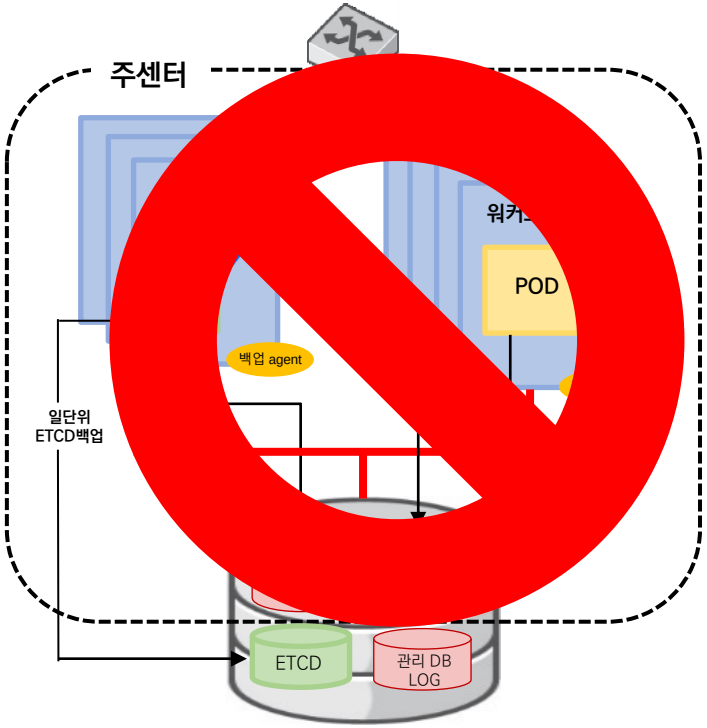


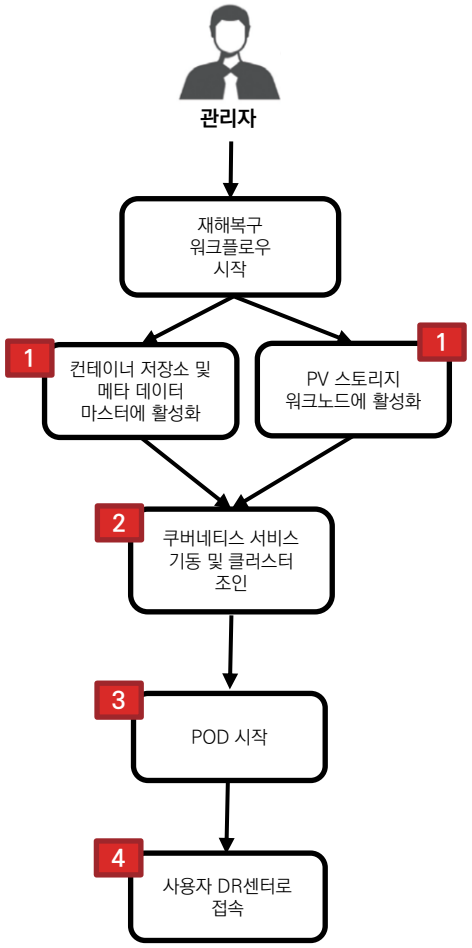


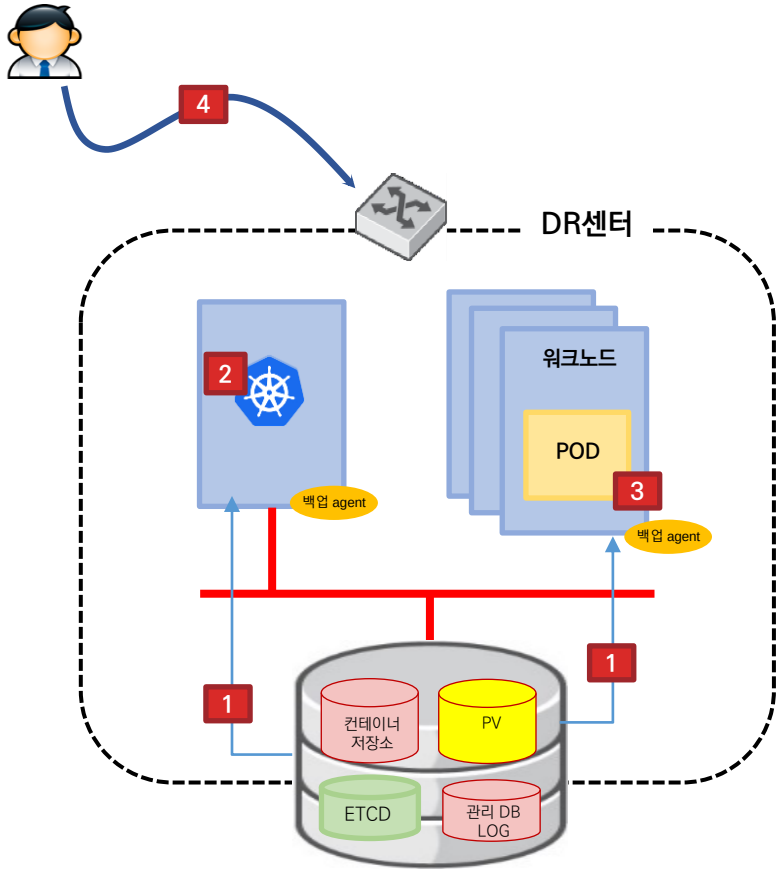
K8S환경의 Hot Site



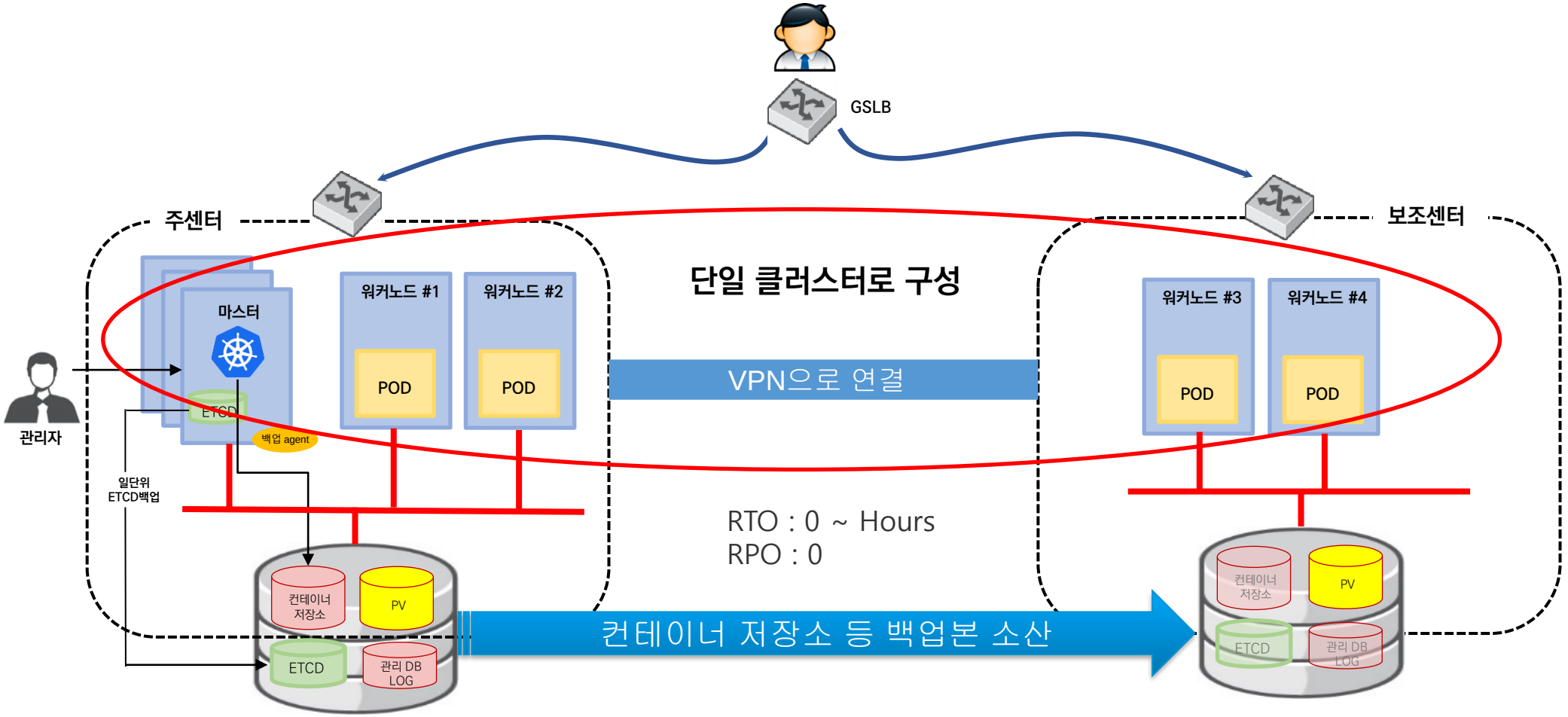
K8S환경의 Hot Site 재해복구 과정





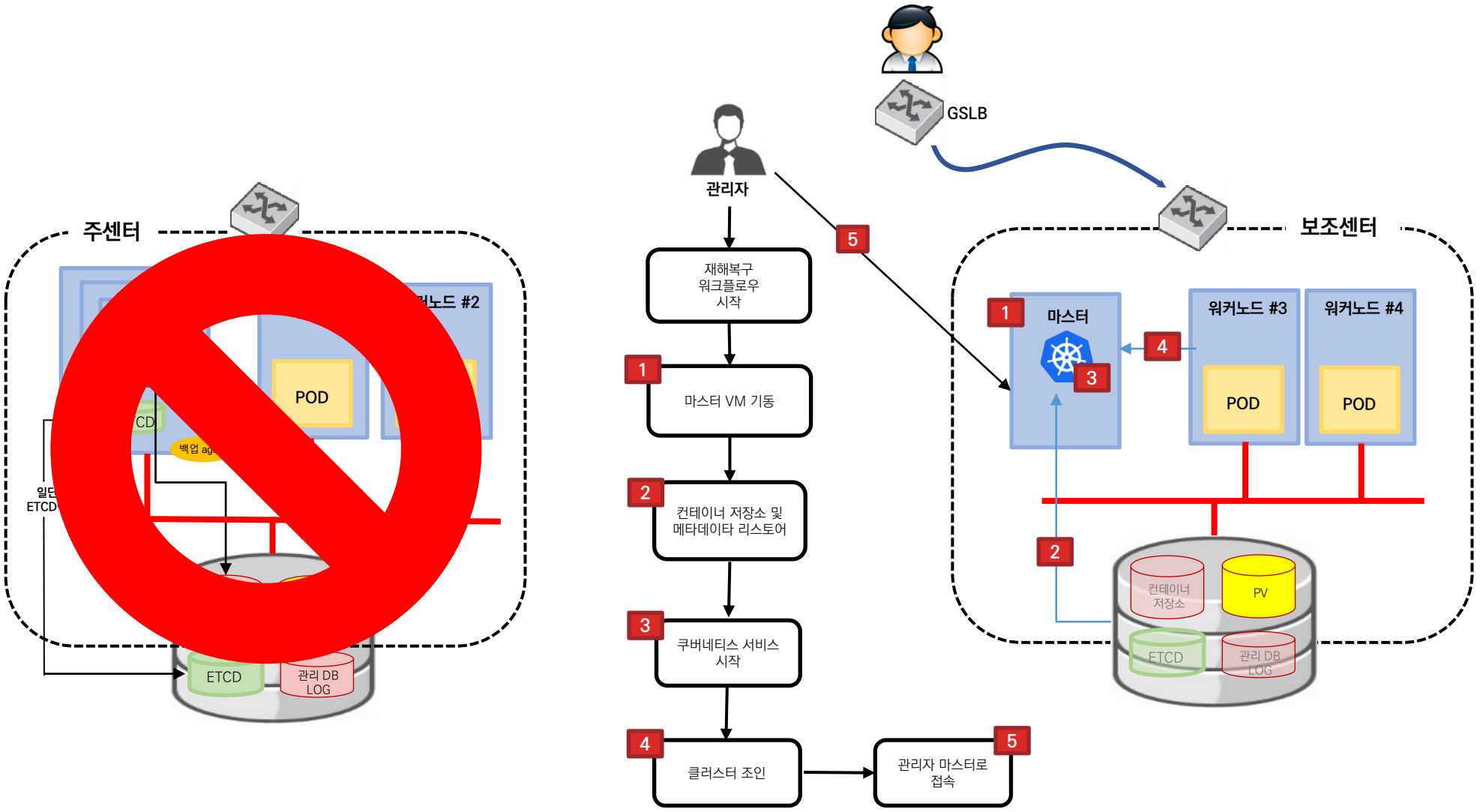


K8S환경의 Mirror Site 1 (Active-Active)

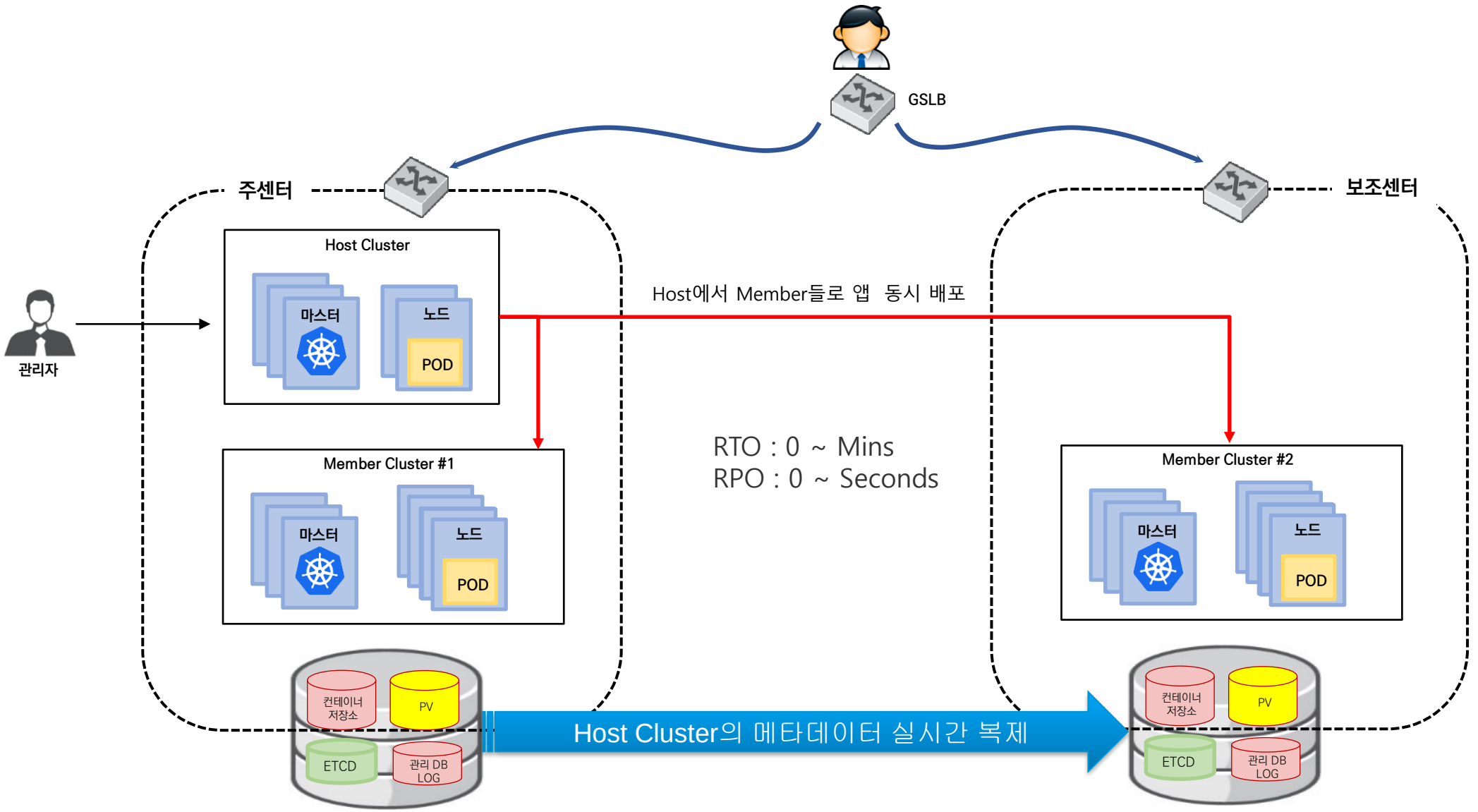


✓ POD 배포 시 워크노드 총합 이상으로 균등 배포해야 함
✓ 주센터 재해 시 DR센터에서 이미 기동중인 POD는 서비스 가능
✓ VPN 속도 느릴 시 평상 시 보조센터쪽 POD들의 응답이 느려짐

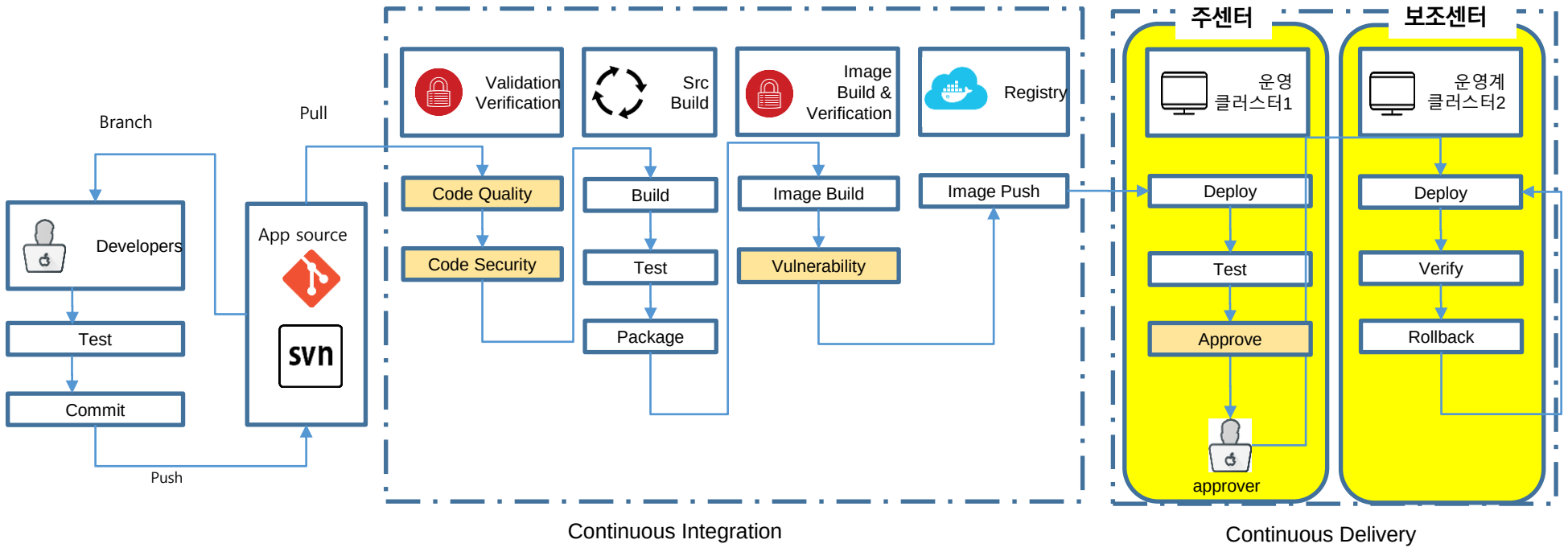
K8S환경의 Mirror Site 1 재해복구 과정

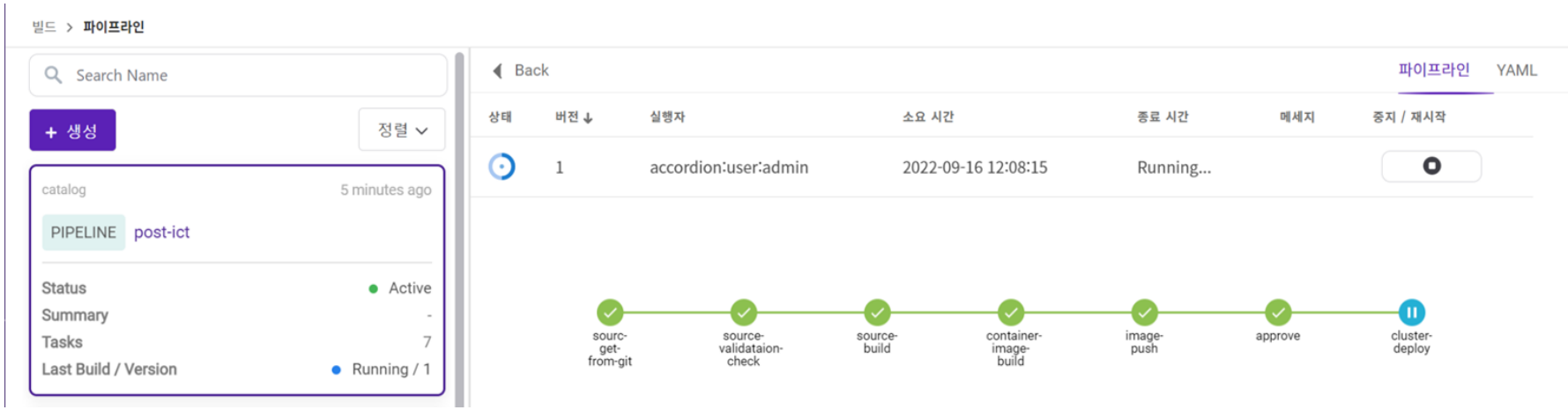


K8S환경의 Mirror Site 2 (Active-Active)

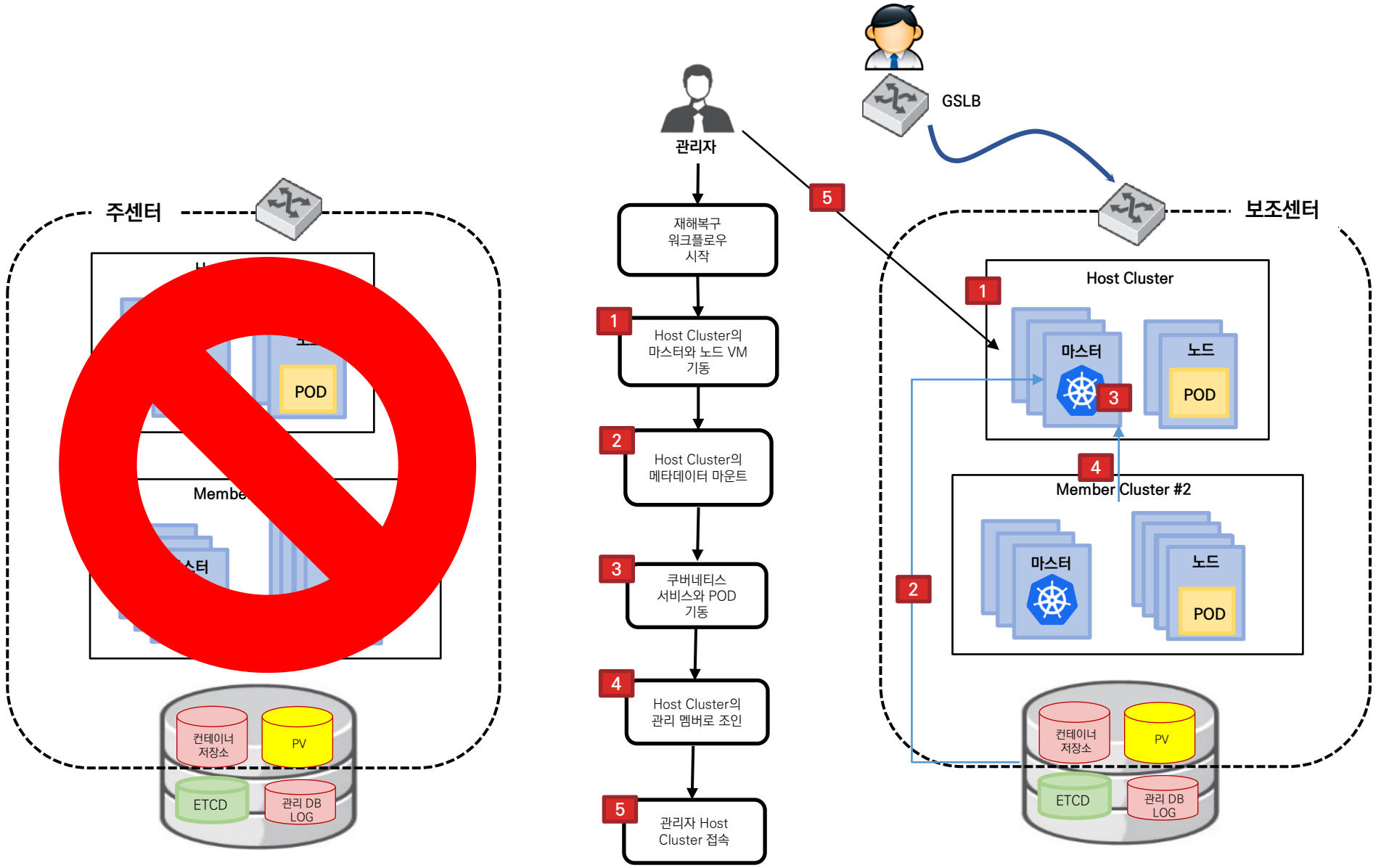


CI/CD Pipeline을 통해 멀티 사이트 간 앱의 변경 분 배포 자동화





K8S환경의 Mirror Site 2 Host Cluster복구 과정



재해복구 비교

	Warm site	Hot site	Mirror site
구성 방식	Active – Standby	Active – Standby	Active - Active
초기 구성 복잡도	매우 간단	간단	복잡
목표 RTO	일주일 이내	24시간 이내	0~3시간 이내
목표 RPO	한달 이내	0~하루	0~1시간 이내
비용	저	중	고
애플리케이션 가용성	낮음	높음	매우 높음

4

“ 국내 사례

K 중견기업

1. Challenge

- 10여년 전 외주로 개발한 ERP가 인사, 급여, 회계, 영업 중심의 경영 관리 시스템 이었음
- 이후 개발 요구사항에 의해 SCM, CRM, 그룹웨어, 배차, 운행 시간 관리 시스템, 차량 정비 시스템, 구매 시스템, 식자재 관리, 유니폼 생산 공정 관리 시스템 등의 서비스가 점진적으로 추가
- 서비스의 확장성, 유연성, 효율성의 한계에 봉착

2. Solution

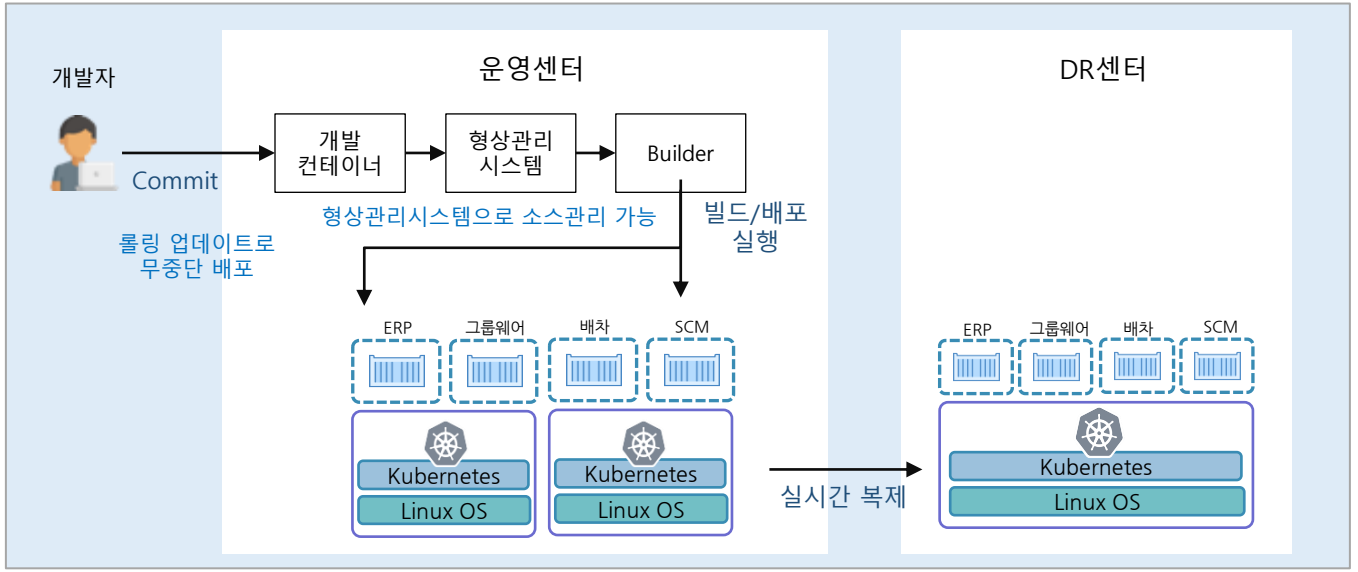
- 벤더 의존적인 환경에서 오픈 환경으로 전환 (Unix → x86/Linux, 상용 WAS → 오픈소스 WAS)
- 업무별로 서비스 인스턴스 분할 (미니 아키텍처)
- 잦은 업무 변화에 대응하기 위한 DevOps 체계 구축
- 재해에 대비하여 자동화된 DR 구축

3. Results

- 전체 운영 TCO 40% 절감
- 경영 손익 계산 결과 성능 8개 증가
- 실시간 배차와 운행 관리 체계로 전환
- 자동화된 가용성 관리와 재해복구로 인한 운영 스트레스 감소

4. Next

- 현대화된 운송 ERP로 패키징하여 타 운송사에 판매와 컨설팅을 진행



H 공기업

1. Challenge

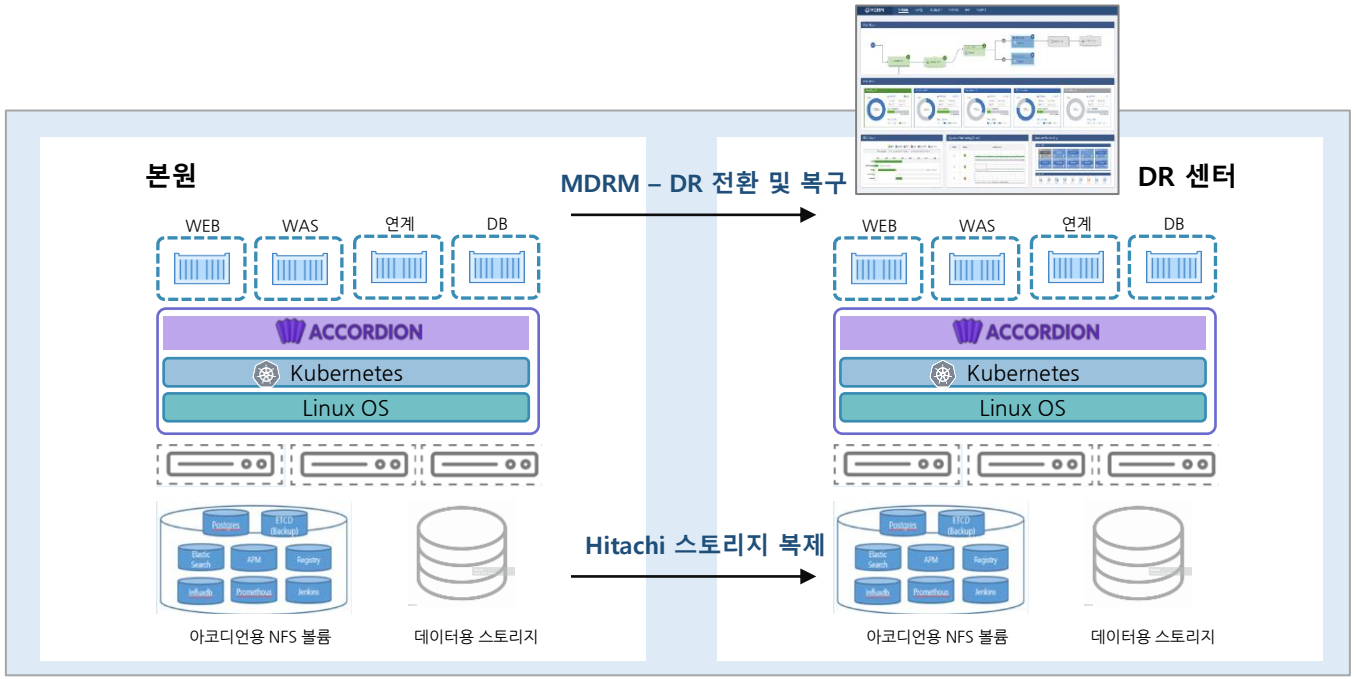
- 기존 레거시 환경에 대하여 스크립트 방식으로 수작업으로 재해복구 진행
- 스크립트를 통한 반자동 복구의 경우 복구 단계별 진행 상황 가시화 불가
- DR전환 및 모의훈련 시 장시간 소요됨에 따라 목표 RTO 도달이 불가

2. Solution

- 쿠버네티스 기반의 대내외 포털에 대한 재해복구 자동화 구현
- 백업 복구를 통한 쿠버네티스 구성 파일 복구
- 재해 전환 시 자동화된 애플리케이션 재배포

3. Results

- 복구 전환의 모든 과정을 가시화하여 Risk 판별
- 자동화된 복구를 통한 RTO 충족
- 레파지토리 복제를 통한 자동화된 변경관리
- 복구에 대한 위험부담도와 스트레스 감소



E 공공부처

1. Challenge

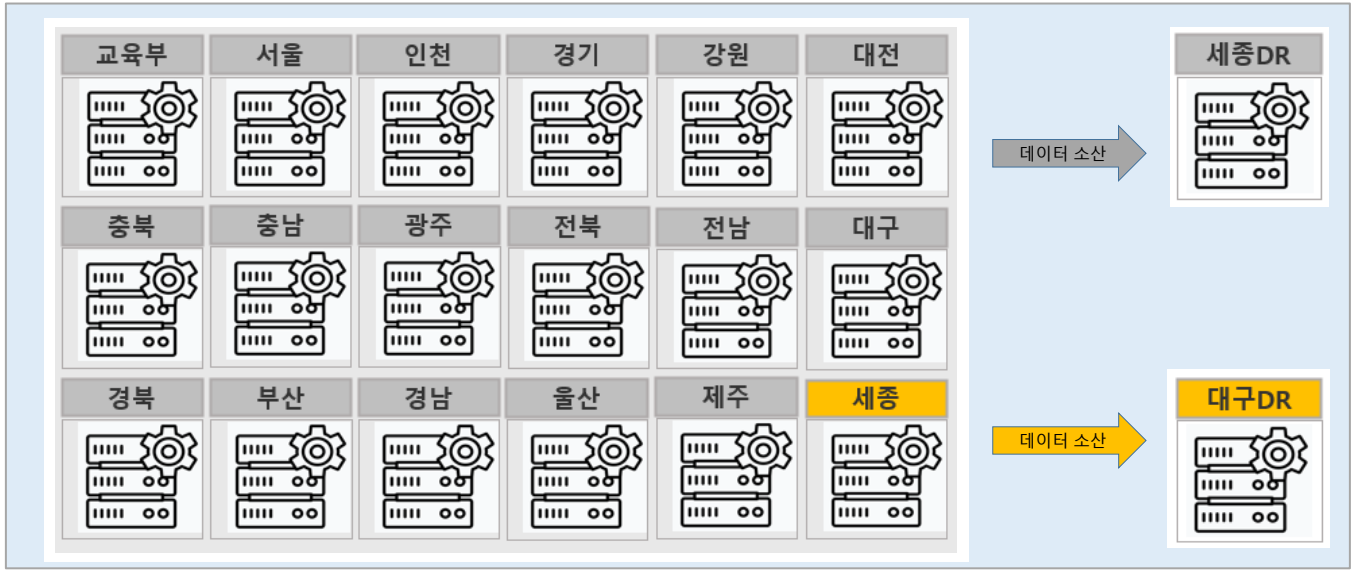
- 차세대 사업에 의해 구축될 클라우드 플랫폼에 대한 통합적인 재해복구 체계마련 필요
- 산재한 17개 시도교육청에 대한 복구 현황의 중앙집중 방식의 관제 필요
- 재난/재해로 나이스 정보자원이 유실되더라도 24시간 이내 서비스를 재개할 수 있도록 재해복구시스템 구축

2. Solution

- 교육부 총괄센터를 중심으로 전국 센터에 대한 통합 제어 시스템 구축
- 데이터 소산대상은 환경정보(ETCD, Yaml 파일), 플랫폼 데이터(모니터링 DB, 컨테이너 저장소, CI/CD Log, 시스템 Log, 감사 Log 등)
  영구 볼륨(Pod에 할당된 데이터 볼륨)
- 재해 사항에 대하여 24시간 이내 서비스 복구 목표

3. Results

- 세종시를 제외한 16개 시도교육청과 교육부 총괄센터는
  세종DR센터로 데이터 소산
- 세종시 교육청은 대구DR센터로 데이터 소산
- 재해복구 및 모의훈련은 재해복구 자동화 툴을 활용하여 수행



Thank You