오픈스택 기반 프라이빗 클라우드 시스템 재해복구 고려사항

권필주 전문위원(his-pjkwon@hyosung.com)

효성인포메이션시스템

Contents

01

배경

공공/금융시장을 중심으로 한 서비스형 클라우드 수요 증가

대구 클라우드 센터, 지자체별 자체 클라우드 구축

광주센터에, 공공기관의 시스템은 2022년 개소하는 **국가정보자원관리원 대구센터에 클라우드 전환·통합**을 우선 추진할 예정이다. 지자체의 시스템은 **자체 클라우드센터 구축**, 한국지역정보개발원(KLID) 활용 또는 민·관 협력을 통해 추진할 수 있도록 지자체의 지역적 특성, 재정 여건 및 정보화 역량 등 제반 상황을 고려해 다양한 방식으로 클라우드 전환이 가능[출처] 대한민국 정책브리핑(www.korea.kr)

그룹 공동/공용 클라우드 구축

KB금융, 하나금융그룹, 우리금융그룹 등

왜 오픈스택인가?
: 프라이빗 클라우드 IaaS구축을 위한 현실적인 선택지

VMware

상용

외산

왜 오픈스택인가?
: 프라이빗 클라우드 IaaS구축을 위한 현실적인 선택지

VMware

상용

외산

Vendor Lock-in 회피

국내 산업 육성

비용적 고려

왜 오픈스택인가?
: 프라이빗 클라우드 IaaS구축을 위한 현실적인 선택지

VMware

상용

외산

OpenStack

오픈소스

외산 or 국산솔루션업체

Vendor Lock-in 회피

국내 산업 육성

비용적 고려

재해복구관련 국내 규제 / 지침 현황 – 공공

물리적 위치 제약 :
국내클라우드업체 혹은 자체
프라이빗 클라우드 구축

[별표 4] 공공기관용 클라우드컴퓨팅서비스 추가 보호조치

14.2. 물리적 보호조치	14.2.1. 물리적 위치 및 분리	클라우드 시스템 및 데이터의 물리적 위치는 국내로 한정하고, 공공기관용 클라우드컴퓨팅서비스의 물리자원(서버, 네트워크, 보안장비 등), 출입통제, 운영인력 등은 일반 이용자용 클라우드컴퓨팅서비스 영역과 분리하여 운영하여야 한다.
	14.2.2. 중요장비 이중화 및 백업체계 구축	클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.

클라우드에서도
중요 장비 이중화와
백업체계 구축은 필수

재해복구관련 국내 규제 / 지침 현황 - 금융

금융보안연구원, 전자금융감독규정 제 23조

11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것 <개정 2016. 6. 30.>

⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다. <개정 2013. 12. 3.>

⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다. <신설 2015. 6. 24.>

⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다. , <종전의 제9항에서 이동 2015. 6. 24.> <개정 2013. 12. 3.>

금융보안원 금융분야 클라우드컴퓨팅서비스 이용 가이드(2019.1)

⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심업무의 복구목표시간은 3시간 이내로 하되, 「보험업법」에 의한 보험회사의 핵심업무의 경우에는 24시간 이내로 한다.

⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 **매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련**을 실시하여야 한다.

핵심업무(클라우드도 동일 적용): 재해복구목표시간 3시간

오픈스택 환경도 재해복구에 대한 동일한 지침 적용

어떻게 구현할 것인가?

02

재해 복구란?

재해

VS

장애

IT산업에서의 재해라는 것은?

천재 또는 인재로 인해
전산시스템 가동이
전면 중단되고
허용 가능한 중단 시간을
초과하는 경우

하드웨어나 소프트웨어의
오류로 발생한
시스템 불능 상태로서
수분에서 수시간 내에
복구가 가능한 경우

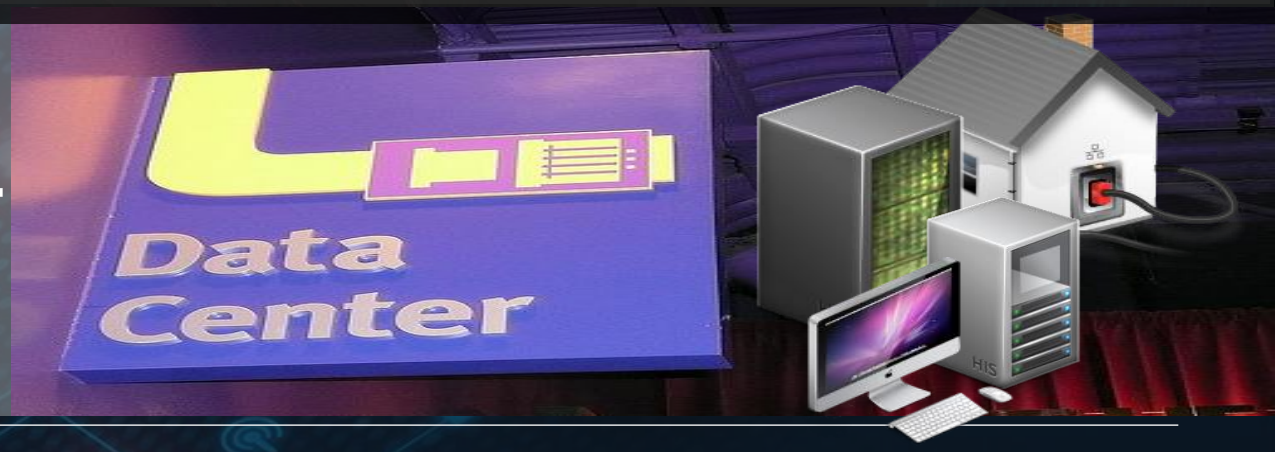
재해 및 장애로 인한
전산서비스 중지가
감내할 수 있는
시간을 초과하여
지속되는 경우

재해로
포괄적으로
인식

데이터 복구

사람/프로세스 복구

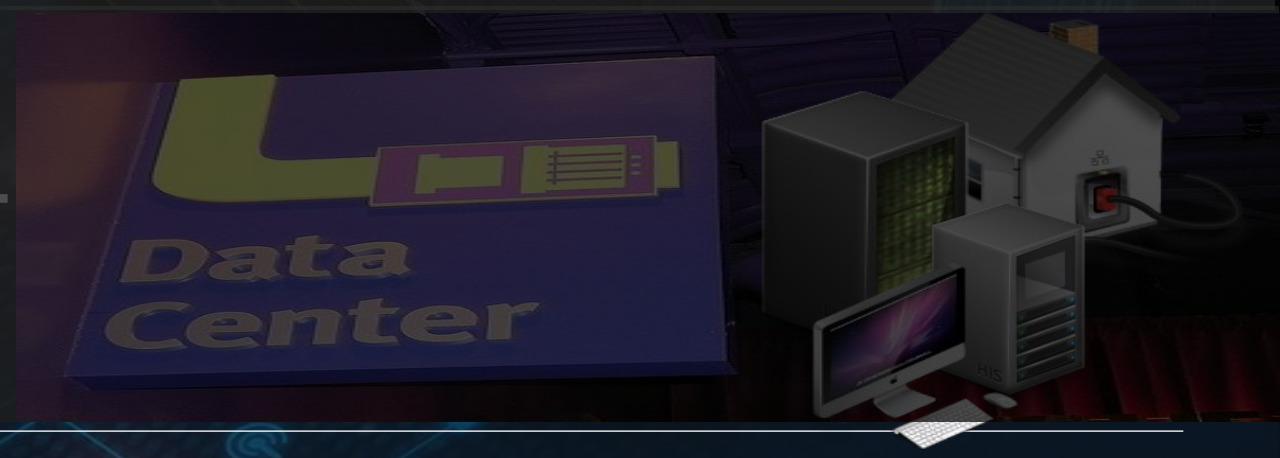
기반시설 복구



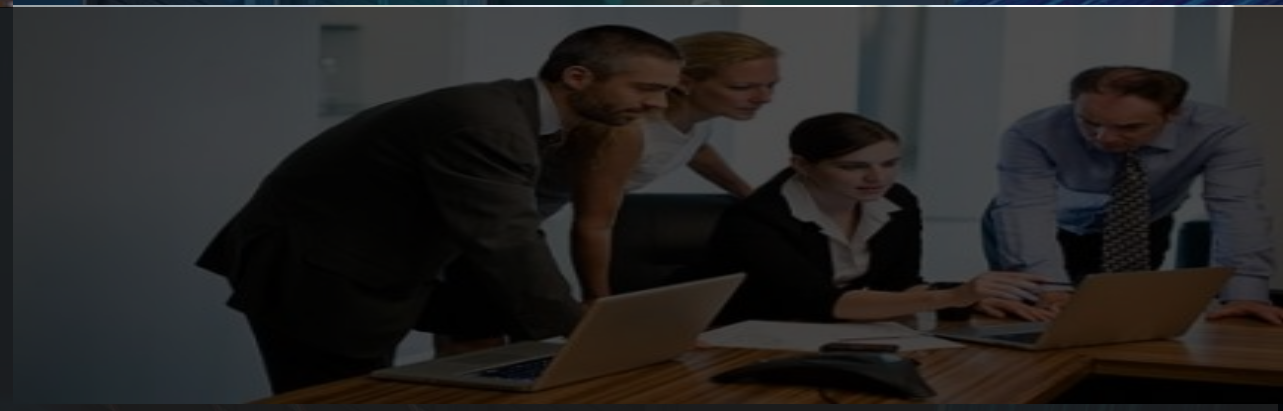
데이터 복구

사람/프로세스 복구

기반시설 복구

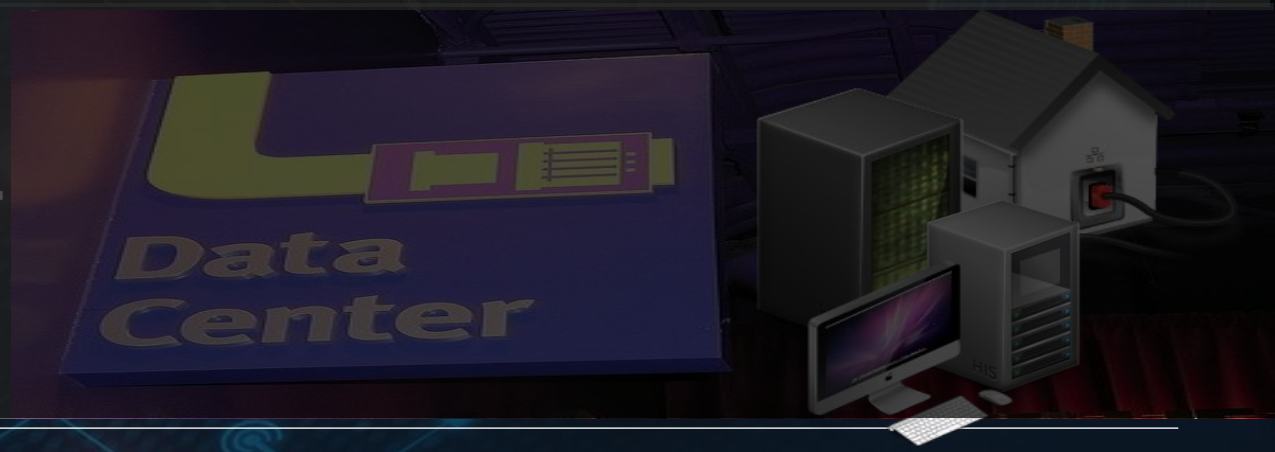


데이터 복구

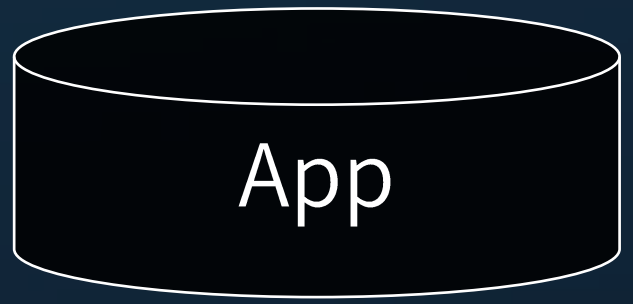


사람/프로세스
복구

기반시설 복구



Stateless vs. Stateful 데이터



Stateless

Stateful

- 데이터 정합성 유지
- 팀 간 복사본 공유
- 재해 복구
- 데이터 관리

Stateless 데이터는 RTO(Recovery Time Objective)가 중요

*빠른 배포 및 기동*이 중요

Stateless 데이터는 RTO(Recovery Time Objective)가 중요

빠른 배포 및 기동이 중요

Stateful 데이터는 RPO가 더 중요

Stateful

- 데이터 정합성 유지
- 팀 간 복사본 공유
- 재해 복구
- 데이터 관리

Stateful 데이터는 RPO가 더 중요

빠른 배포와 기동보다 중요한 데이터 동기화,

어떻게 하면 데이터 손실을 최소화할 것인가?

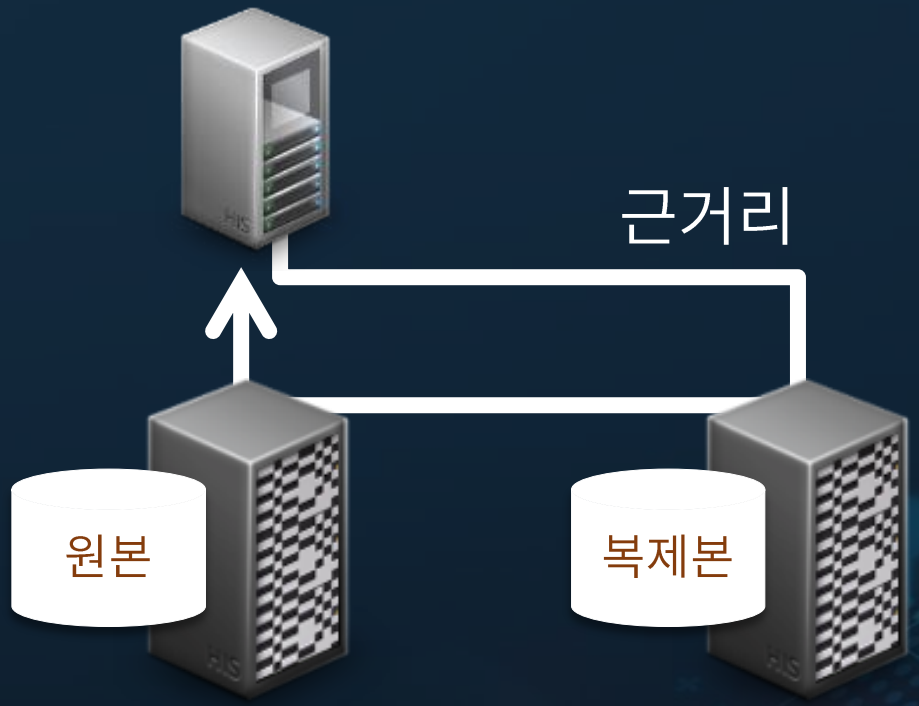
Stateful

- 데이터 정합성 유지
- 팀 간 복사본 공유
- 재해 복구
- 데이터 관리

03

데이터 동기화 검토

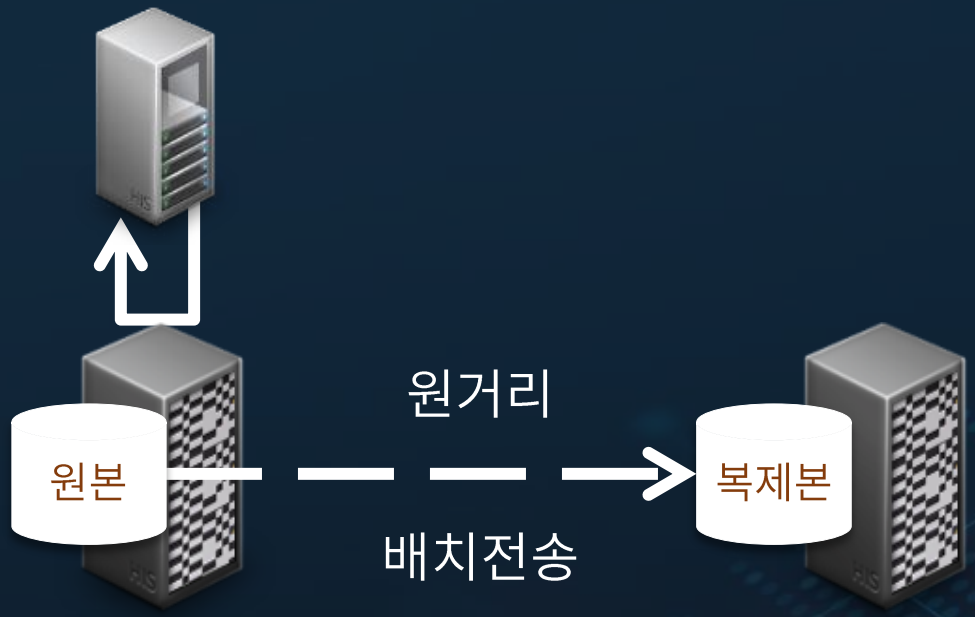
데이터 동기화 방법 – Sync, RPO = 0



응답성능 영향 최소화가 중요

- Low latency Protocol : Fiber Channel, DWDM …
- 거리 : 100km 이내 권고

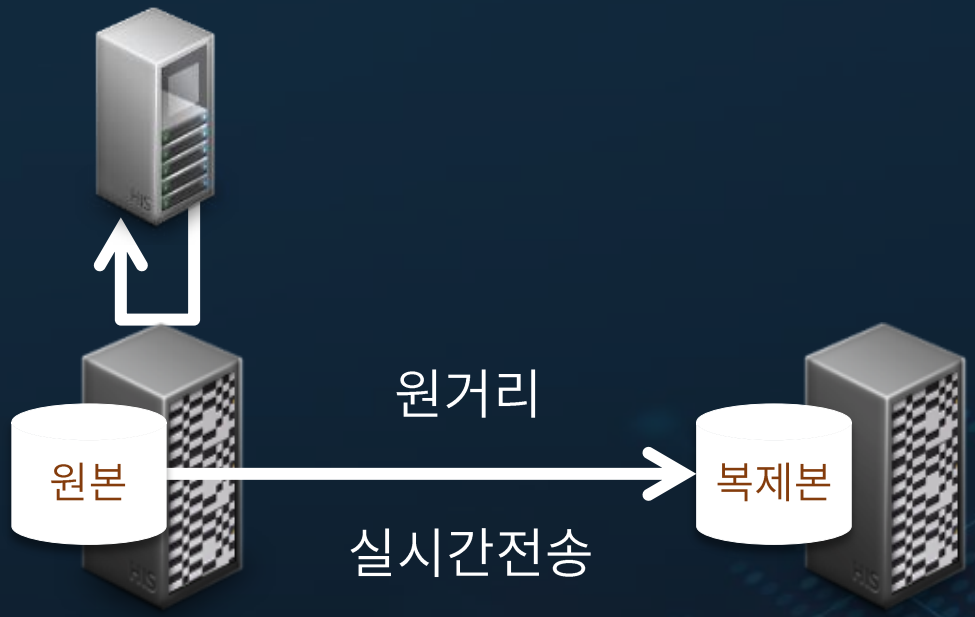
데이터 동기화 방법 – Async, 거리제약 해소 : 배치방식



데이터 손실 최소화 기술 중요

- 배치 방식,
  - 수분 이상의 데이터 손실 가능

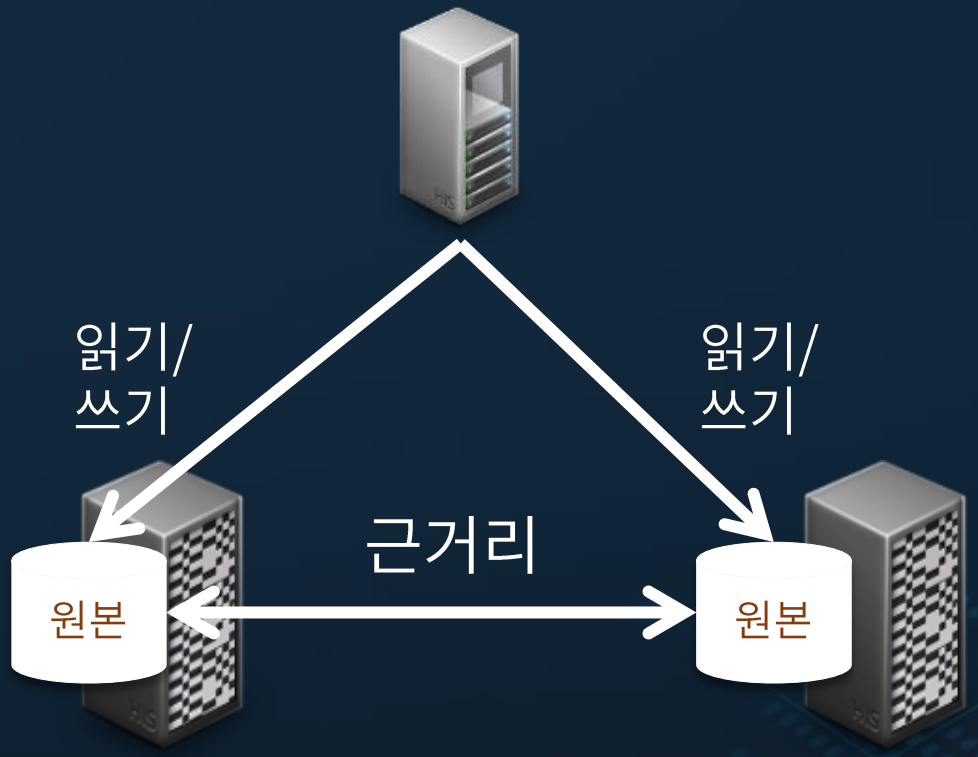
데이터 동기화 방법 – Async, 거리제약 해소 : 실시간전송



데이터 손실 최소화 기술 중요

- 실시간 전송 방식
  - ✓ 예) Hitachi Universal Replicator

데이터 동기화 방법 – Active-Active Mirroring



동시 읽기/쓰기 중요 ✔

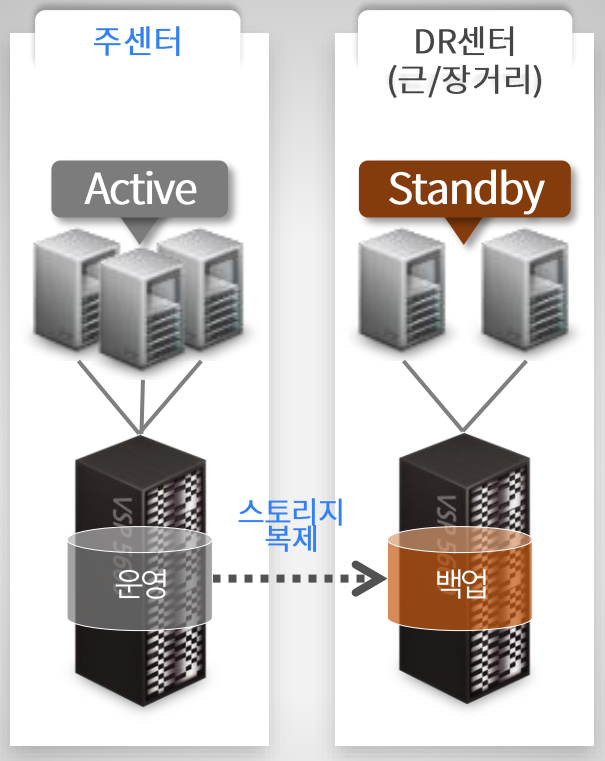
- RTO/RPO=0 지원 가능
- 무중단 운영

04

국내 재해센터 구축 현황

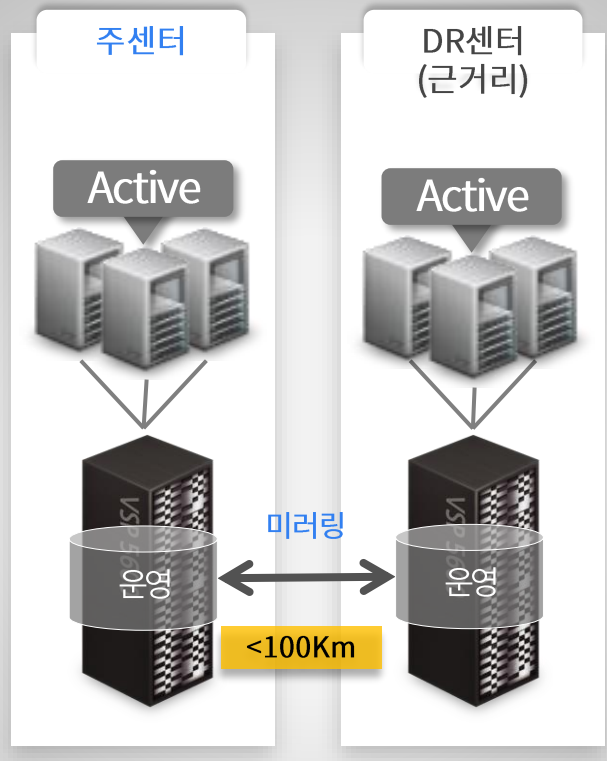
기존 주요 시스템 재해 센터 구축 현황

Case 1 (2DC)



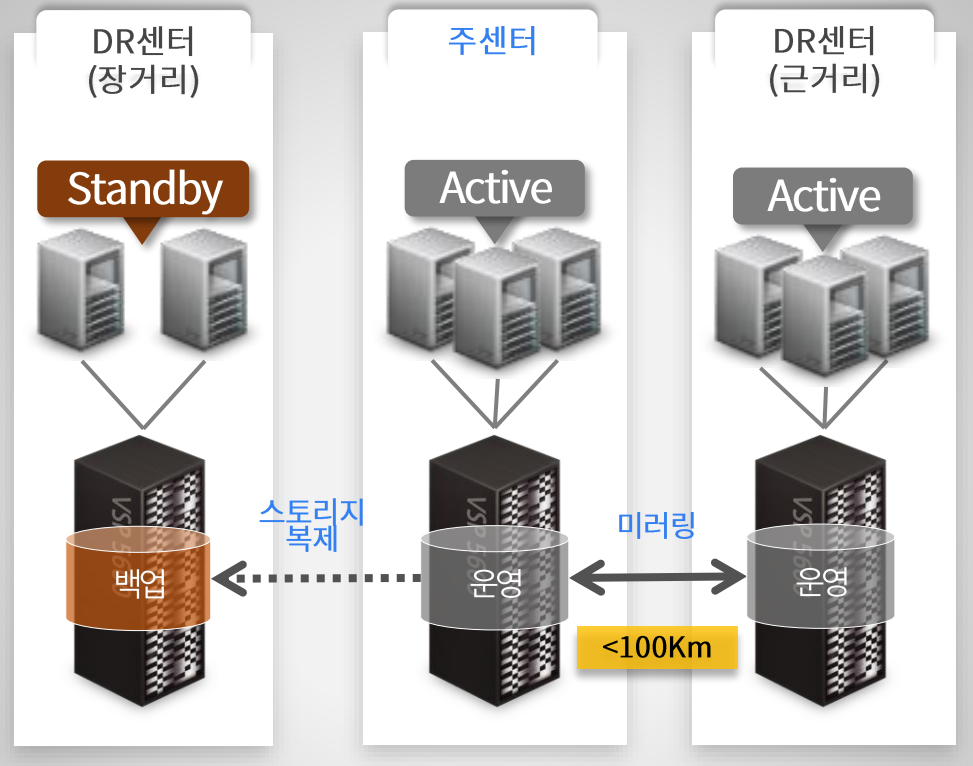
- 데이터 복제 중심 재해복구 시스템
- 복구목표시간(RTO) 최대 3Hr 이내
- 성능 고려 근거리 또는 장거리 DR

Case 2(2DC)



- 서비스 가용 중심 재해복구 시스템
- 복구목표시간(RTO)이 필요치 않음
- 성능 고려 근거리 DR만 구성 권고

Case 3 (3DC)



- 단거리 DR은 서비스 가용 중심의 재해복구시스템 구성
- 장거리 DR은 데이터 복제 중심의 재해복구시스템 구성
- 복구목표시간(RTO)이 무중단에서 최대 3Hr 이내 가능

업무중요도별 재해복구 솔루션 적용 가이드라인 (예시)

구 분	Platinum	Gold	Silver	Bronze
대상 업무	기업의 생산, 판매 및 영업활동에 직접적인 영향을 주는 업무	기업의 대고객 서비스에 영향을 주는 업무	기업의 내부 운영에 영향을 주는 업무	기업의 내부 업무 지원을 위한 개발, 테스트 업무
RPO(복구시점목표)	Near 0	Near 0	< 2Days	< 2Days
RTO(복구시간목표)	< 3Hr	< 24Hr	< 7Days	< 30Days
권장 거리	근거리+장거리	근거리, 장거리	근거리, 장거리	근거리, 장거리
권장 DR 형태	3DC 이상	2DC	2DC	2DC
권장 DR 솔루션	디스크 복제	디스크 복제	S/W 복제	S/W 복제, 백업
업무 성능 저하 허용여부	불가	불가	허용	허용

05

오픈스택기반 프라이빗 클라우드 재해복구 구축하기

오픈스택 환경에서 주요 백업/복구 대상

	데이터 변동성	데이터량	고려사항
Controller node의 구성정보	낮음	소량	재해센터환경 맞는 일부 설정 변경
Glance의 가상 머신 템플릿 이미지	낮음	소량	빠른 배포를 위한 Cinder backed image 구성
Cinder 볼륨	높음	대량 (XXTB이상)	실시간 동기화

오픈스택 환경에서 주요 백업/복구 대상

Controller node의 구성정보

Glance의 가상 머신 템플릿 이미지

Cinder 볼륨

데이터 변동성	데이터량	고려사항
낮음	소량	재해센터환경 맞는 일부 설정 변경
낮음	소량	빠른 배포를 위한 Cinder backed image 구성
높음	대량 (XXTB이상)	실시간 동기화

Stateless

오픈스택 환경에서 주요 백업/복구 대상

Controller node의 구성정보

Glance의 가상 머신 템플릿 이미지

Cinder 볼륨

데이터 변동성	데이터량	고려사항
낮음	소량	재해센터환경 맞는 일부 설정 변경
낮음	소량	빠른 배포를 위한 Cinder backed image 구성
높음	대량 (XXTB이상)	실시간 동기화

Stateless

오픈스택 환경에서 주요 백업/복구 대상

	데이터 변동성	데이터량	고려사항
Controller node의 구성정보	낮음	소량	재해센터환경 맞는 일부 설정 변경
Glance의 가상 머신 템플릿 이미지	낮음	소량	빠른 배포를 위한 Cinder backed image 구성
Cinder 볼륨	높음	대량 (XXTB이상)	실시간 동기화

Stateful

오픈스택에서 실시간 동기화 대상을 외장스토리지 저장

Active – Standby DataCenter 구성

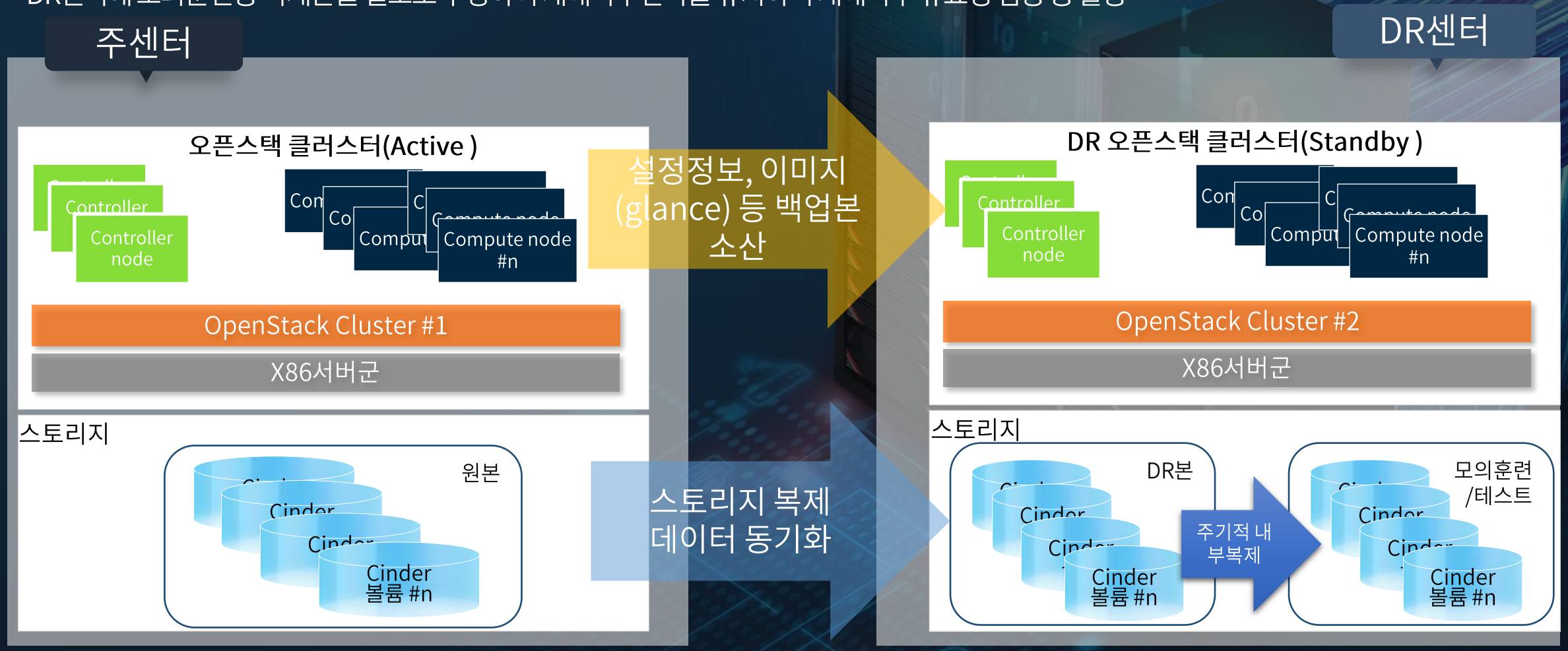
- *RTO<3시간, RPO=0목표*

재해 복구에 사용된 솔루션 정보

OpenStack Release version	Train release
Cinder Driver	Hitachi Block Storage Driver for OpenStack
원격 복제 솔루션	Hitachi Universal Replicator
스토리지 하드웨어	VSP Family (VSP 5000, VSP E시리즈, VSPG 시리즈, VSP F시리즈)

재해복구 목표 구성 – 2DC Active – Standby – RTO<3, RPO=0

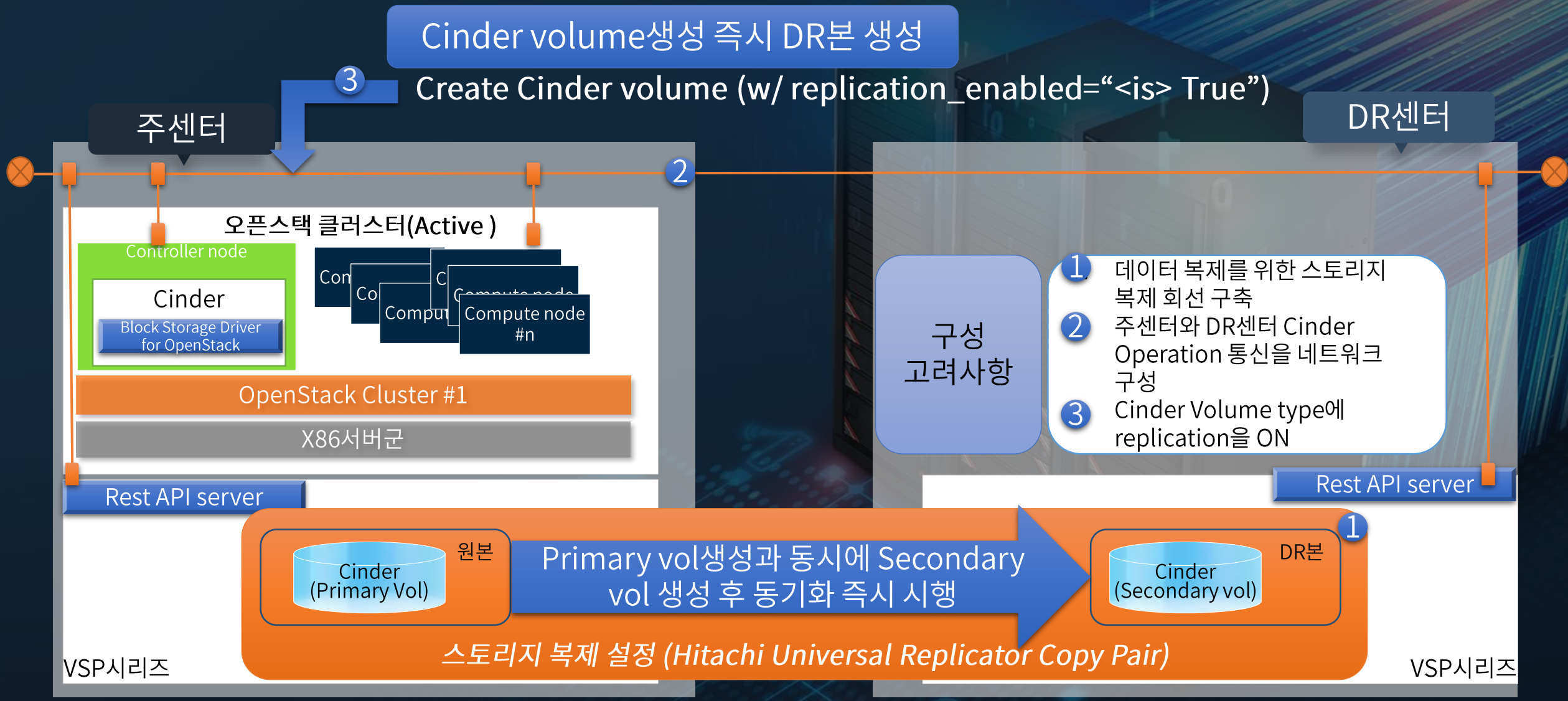
- DR센터에 오픈스택 클러스터는 주센터와 연동이 안된 완전한 Standby 클러스터이며 재해 시 구성 정보를 복구하여 서비스 재개 목표
- 실시간으로 변동되는 Cinder 주요 볼륨에 대해서는 실시간 데이터 동기화를 적용하여 RPO=0를 유지함
- DR센터에 모의훈련용 복제본을 별도로 구성하여 재해복구연속을 유지하며 재해복구 유효성 검증 용 활용



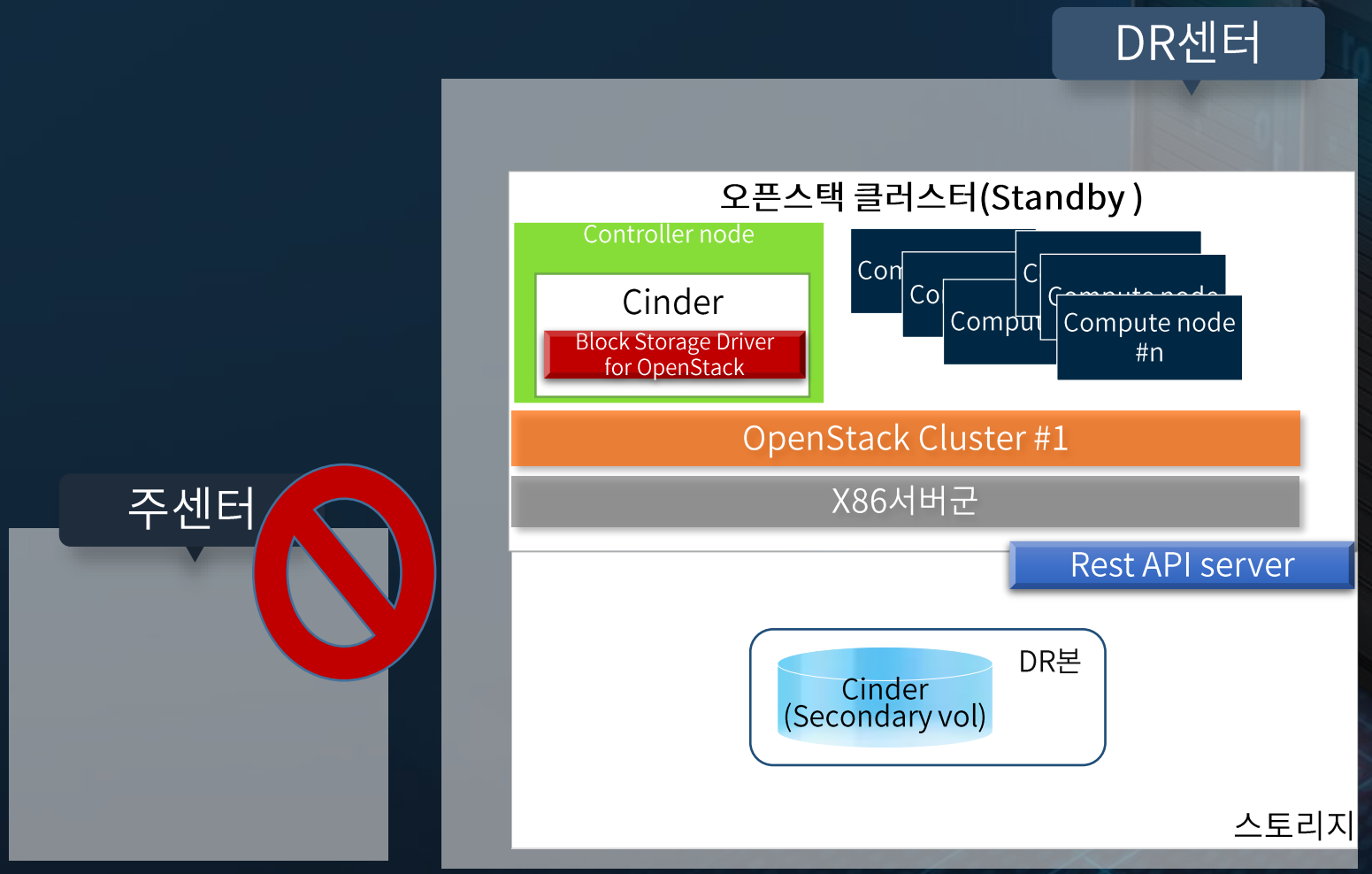
구축방안 – Cinder Remote Replication 구성(1/3)

구축방안 – Cinder Remote Replication 구성(2/3)

구축방안 – Cinder Remote Replication 구성(3/3)



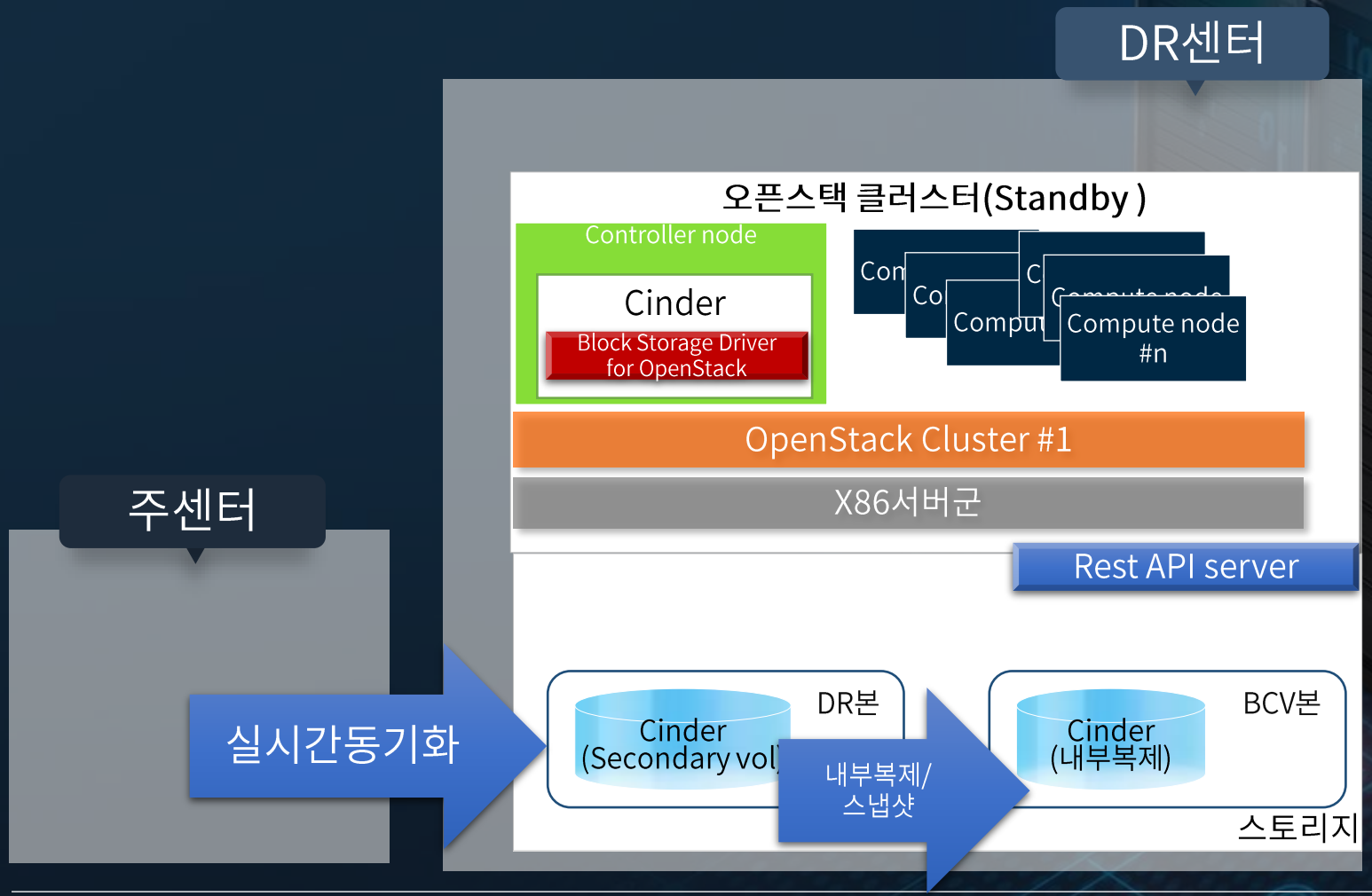
재해 시 DR센터에서 복구 방안



복구절차

- Controller node와 compute node 구성 사전 준비
- Controller node에서 Secondary vol에 대한 인식
- Compute node에서 정상 mount 확인
- 네트워크 구성 등 기타 설정 복구 후 서비스 재개

재해복구 모의훈련방안



모의훈련절차

- Controller node와 compute node 구성 사전 준비
- Controller node에서 내부복제 볼륨에 대한 인식
- Compute node에서 정상 mount 확인
- 네트워크 구성 등 기타 설정 복구 후 모의훈련 검증

오픈스택 기반 클라우드 재해 복구를 위한 가이드

데이터 백업 방안	주요 볼륨에 대한 실시간 동기화 구성
네트워크 구성	Cinder 원격복제 자동추가를 위해 주센터와 백업센터와 통신 가능할 것 I/O 부하를 고려해서 적절한 스토리지 복제 회선 구축 (DWDM, FCIP…)
모의훈련	사전 모의훈련을 위해 재해 센터에 추가 내부복제볼륨 구성

하나 더…

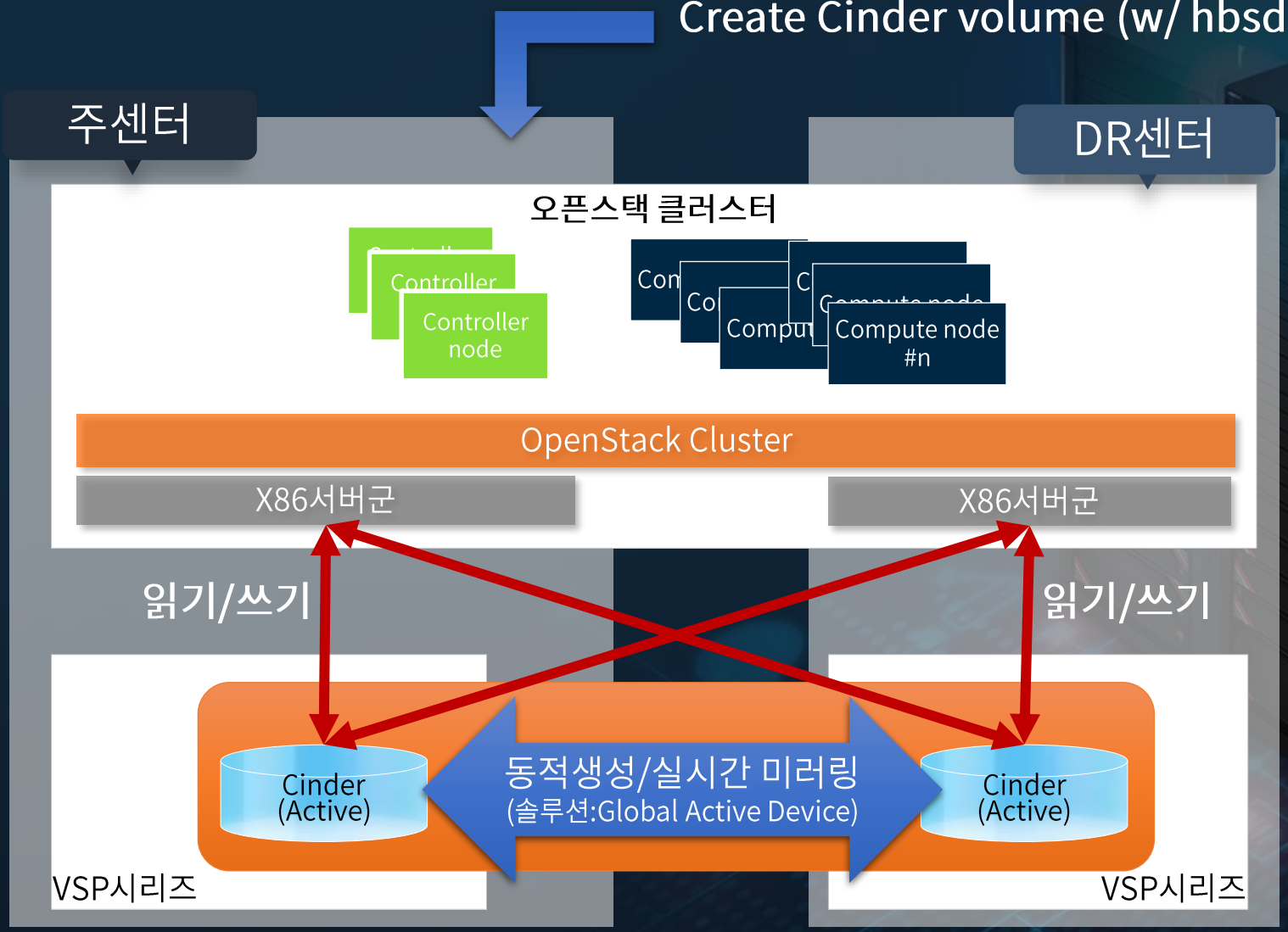
Active-Active Mirroring

-RTO/RPO=0

Active-Active Mirroring 구성을 위한 솔루션 정보

OpenStack Release version	Train release
Cinder Driver	Hitachi Block Storage Driver for OpenStack
Active-Active Mirroring 솔루션	Hitachi Global Active Device
스토리지 하드웨어	VSP Family (VSP 5000, VSP E시리즈, VSPG 시리즈, VSP F시리즈)

목표 구성도



고려사항

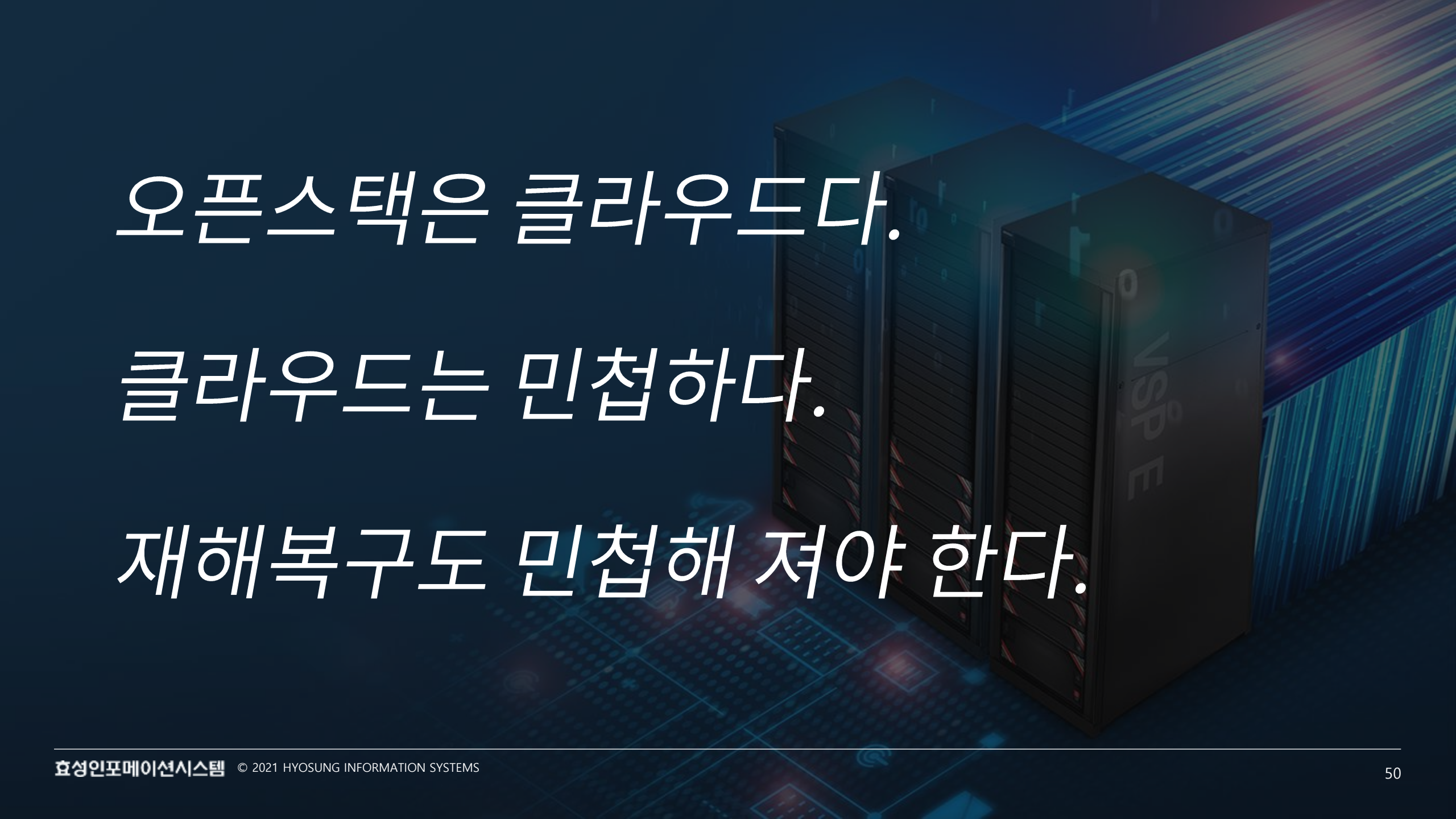
센터 장애 대비 적절한 Controller/Compute node 배분

주센터와 DR센터가 하나의 네트워크로 연결

응답시간을 고려 근거리 구성
- Campus DR (건물간 혹은 층간)
- 전원, 화재에서 분리된 지역

06

마무리



오픈스택은 클라우드다.

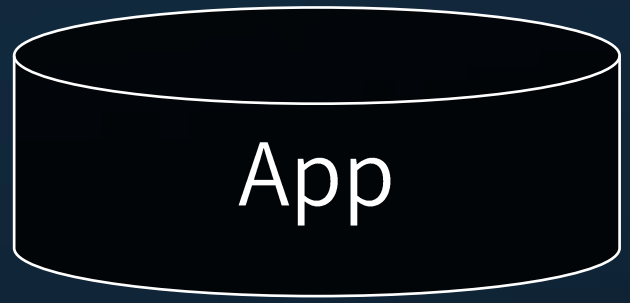
클라우드는 민첩하다.

재해복구도 민첩해 져야 한다.

첫째, 재해 복구는 데이터의 복구다.
백업방법과 복구범위를 확장해야 할 것

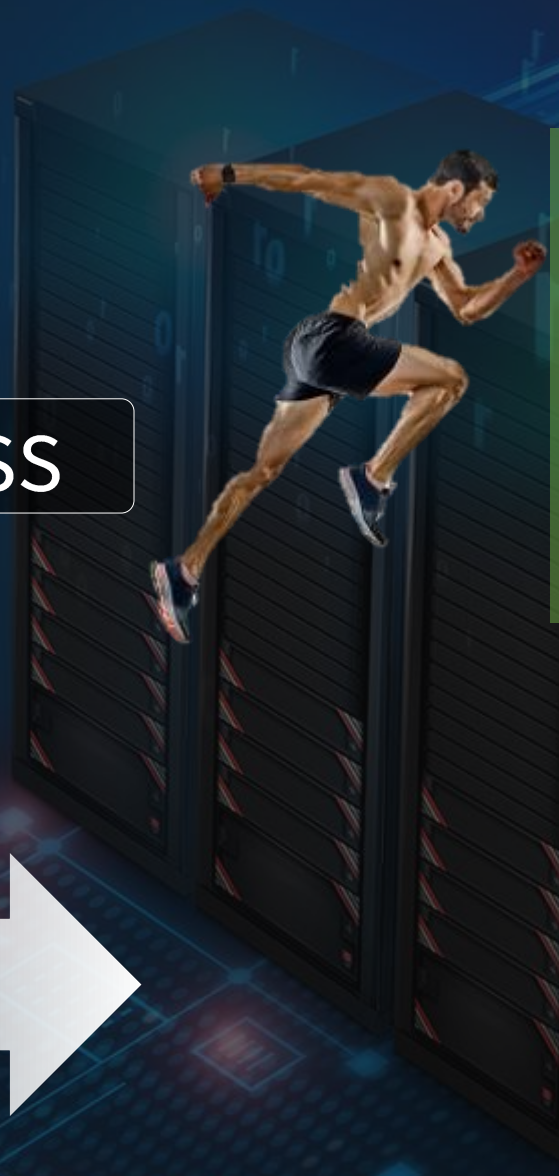
최신 이미지 확보를 데이터 백업 방안 필요
데이터 손실 최소화 (RPO=0)

둘째, 진보와 보수 사이에 적절한 중도적인 접근법 사용



Stateless

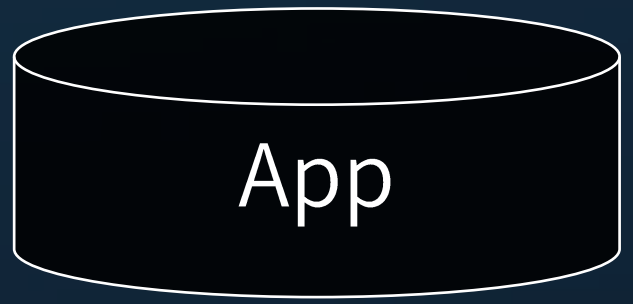
Stateful



좀더 Agile한 혁신 기술 도입

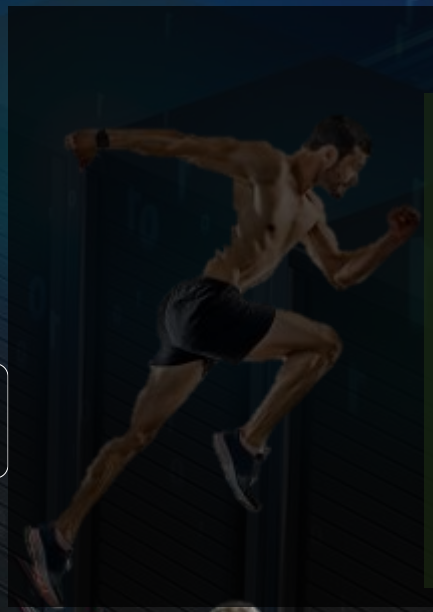
- 가상화/컨테이너
- AutoScaling
- Serverless …

둘째, 진보와 보수 사이에 적절한 중도적인 접근법 사용



Stateless

Stateful



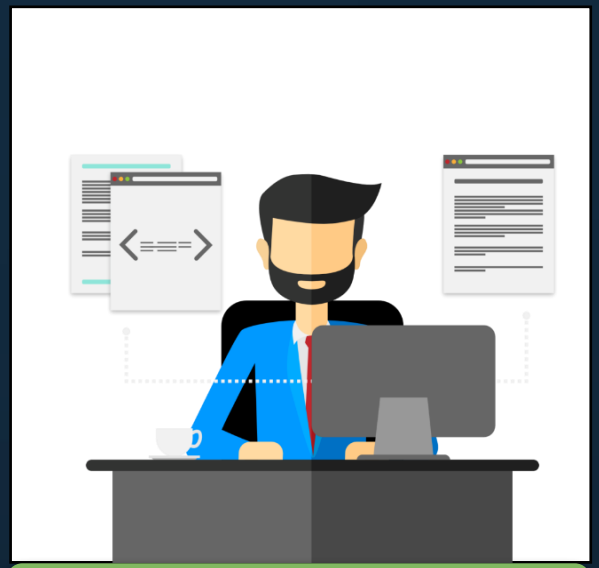
좀더 Agile한 혁신 기술 도입

- 가상화/컨테이너
- AutoScaling
- Serverless …

검증된 안정적 솔루션 선택

- 외장 스토리지 기반 재해 복구…

마지막으로 개발자와 IT인프라 담당자 협업 환경이 필요



개발자

인프라 프로비저닝에 코딩 능력 필요
하지만,

인프라 이해 부족

openstack™ kubernetes

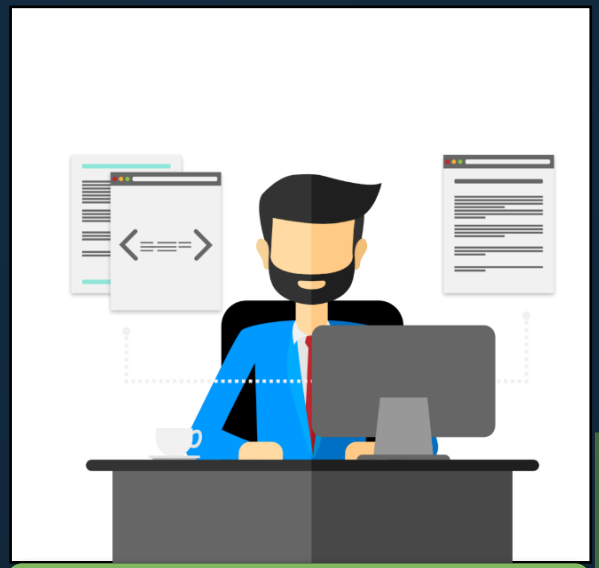
인프라 담당

기존 인프라 운영에 대한 코드화 제공 필요
하지만,

코딩이 약함

마지막으로 개발자와 IT인프라 담당자 협업 환경이 필요

재해복구 자동화



개발자

인프라 프로비저닝에 코딩 능력 필요 하지만,

인프라 이해 부족

인프라 이해

코딩 이해

openstack

kubernetes

인프라 담당

기존 인프라 운영에 대한 코드화 제공 필요 하지만,

코딩이 약함


Thank
you