IT 인프라 아키텍처 설계

Session 6
스토리지 · 백업 · DR

Day 2 오후 · 약 180분

6대 스토리지 유형 · SAN 패브릭 · RAID · Snapshot · Tape · 백업 정책 · 랜섬웨어 대응 · DR 4단계

강사 박수현 · 🚀 젠아이랩스(GenAI Labs)

데이터센터 · 서버·OS·DB·GPU · 가상화·컨테이너 · 네트워크 L1~L7 · 스토리지 · 백업·DR · 보안 6대 도메인 · HA · 용량·성능·관찰성 · 설계 워크숍 · RFP · 5종 실전 케이스

왜 스토리지·백업·DR인가 — *국내 백업 실패·랜섬웨어 3선*

🦠 ① 서울대병원 환자정보 83만건 유출

2021.06 (북한 해킹조직)

서울대병원 서버 해킹 → **환자 81만 명 + 직원 1만 7천명** 정보 유출 (북한 해킹조직 소행 확정).

- 의료 업종 보안 투자 8개 산업군 중 최저
- 진료정보·주민번호·진단명
- 의료데이터는 다크웹 고가 거래

💡 **교훈 — Air-Gap·Immutable Backup·SIEM·SAC** + 의료망 분리

> 참고: 「서울대병원 환자정보 유출 2021」 검색

🔥 ② SK C&C 화재 → DR 미흡

2022.10.15 (재인용)

판교 DC 화재 + 카카오의 **DR 사이트 동기화 지연** → 복구가 5일 걸린 핵심 원인.

- DR 안 시 데이터 동기화 미흡
- BCP 시험 부족
- RPO·RTO 사전 정의 부재

💡 **교훈 — 3-2-1-1-0 백업** + DR 분기 시험 + Sync/Async 복제 설계

> 참고: 「카카오 IDC 이중화 보고서」 검색

💾 ③ 2025 국가정보자원관리원 화재

2025.09.26 (금)

대전 본원 화재 → **정부 시스템 709개 마비** · 4주+ 복구. DR 사이트 미흡으로 96개 시스템을 대구 센터로 「긴급 이전 복구」.

- 정부 IT의 DR·이중화 부재 노출
- 운영-DR 동시 영향 (단일 사이트 의존)
- 복구 시험 미실시
- 「공공 IT BCP 점검」 의무화 추진

💡 **교훈 — 3-2-1-1-0 + Sync/Async 복제 설계 + 분기 1회 복구 시험**

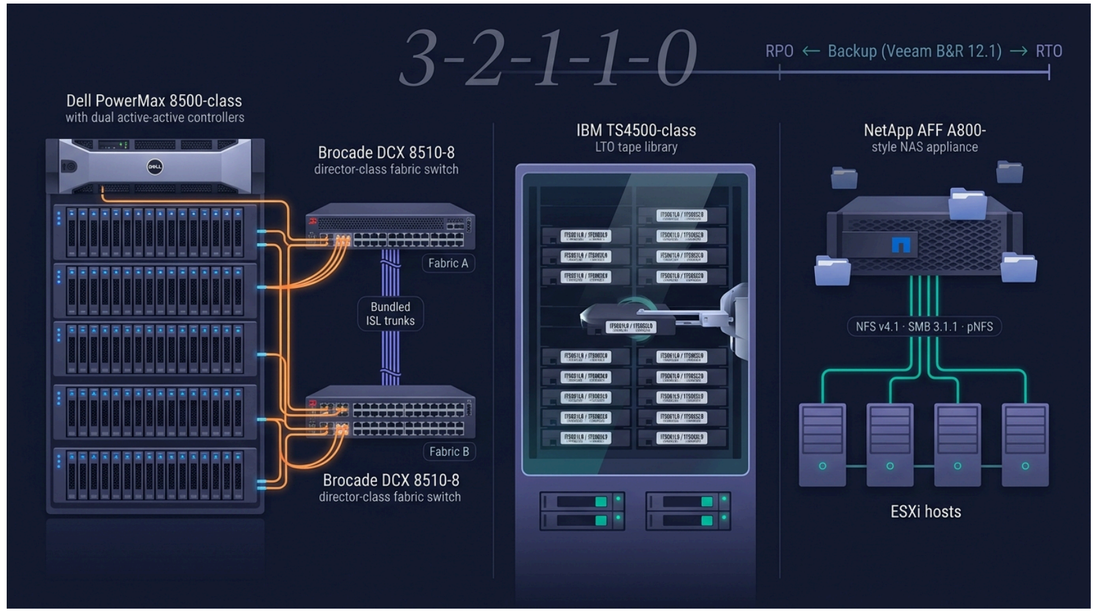
> 참고: 위키백과 「2025년 국가정보자원관리원 화재」

📌 **이번 세션의 시각** — 위 3건은 **「랜섬웨어 → 백업까지 같이 암호화」「DR 동기화 미흡」「복구 시험 누락」** 패턴. **3-2-1-1-0 + Immutable Backup + RPO/RTO 정량화**가 본 세션의 핵심.

🛡️ 3-2-1-1-0 — *백업 황금 원칙(2024+)*

- **3** — 데이터 사본 **3벌** (운영 1 + 백업 2)
- **2** — 서로 다른 **저장 매체 2종** (Disk + Tape·Cloud 등)
- **1** — **1벌은 사외** (Offsite·다른 사이트·Cloud)
- **+1** — **1벌은 Offline / Air-Gap / Immutable** (랜섬웨어 무력화 방지)
- **+0** — **검증 오류 0건** (SureBackup·이상탐지로 무결성 확인)

> "**검증되지 않은 백업은 존재하지 않는 백업**" — Veeam·Rubrik·Cohesity가 사실상의 표준으로 만든 확장판.



Day 2 오후 · 약 180분

회차 메타데이터 — *Session 6 한눈에*

📋 세션 정보

- **회차**: **7 / 18** — Day 2 오후
- **소속**: 스토리지·백업·DR 통합 도메인
- **카테고리**: 인프라 / 데이터 보호
- **예상 분량**: 본문 70 슬라이드 + 일러스트 11장
- **강의 시간**: 약 90분
- **강사**: 박수현 — 젠아이랩스(GenAI Labs) **CEO / CTO**

🎯 핵심 메시지

> "데이터는 **어디에·어떻게 저장**되며, **어떻게 보호**하고, **사라졌을 때 어떻게 되살리는가**" — 스토리지·백업·DR 의사결정의 압축 정리.

🧭 학습 목표 (Learning Objectives)

1. **6대 스토리지 유형** — DAS·NAS·SAN·Object·HCI·SDS를 워크로드별로 매핑한다
2. **SAN 패브릭** — Director·Edge·Zoning·NPIV·WWN의 동작 원리를 설명한다
3. **RAID·Snapshot·Replication** — 안전망 3중 구조를 설계한다
4. **Tape·LTO·LTFS·VTL** — 장기 보존·랜섬웨어 대응의 마지막 방어선을 안다
5. **백업 정책 6종** — Full·Inc·Diff·Synthetic·Forever·Reverse를 비교한다
6. **3-2-1·3-2-1-1-0·Immutable** — 랜섬웨어 시대 백업 황금 원칙을 설계한다
7. **DR 4단계·RPO/RTO** — 사이트 등급과 비용·가용성을 산정한다

PART A

스토리지 6대 유형 — *DAS · NAS · SAN · Object · HCI · SDS*

> 한 줄로 정리: **블록은 SAN·HCI, 파일은 NAS, 객체는 Object, 단일서버는 DAS, 소프트웨어 정의는 SDS.**

스토리지 6대 유형 — *전체 조망 wheel*

1️⃣ DAS

- **Direct Attached**
- SAS/SATA 케이블 직결
- 단일 서버 전용
- 가장 단순·빠름·저렴

2️⃣ NAS

- **Network Attached**
- Ethernet + NFS·SMB
- 다수 클라이언트 파일 공유
- 홈디렉·미디어·백업타깃

3️⃣ SAN

- **Storage Area Network**
- FC·iSCSI·NVMe-oF
- 블록 단위 공유
- DB·VM·미션크리티컬

4️⃣ Object

- **HTTP REST + S3 API**
- 무한 확장·메타데이터
- WORM·버저닝·Object Lock
- 백업·아카이브·CDN 오리진

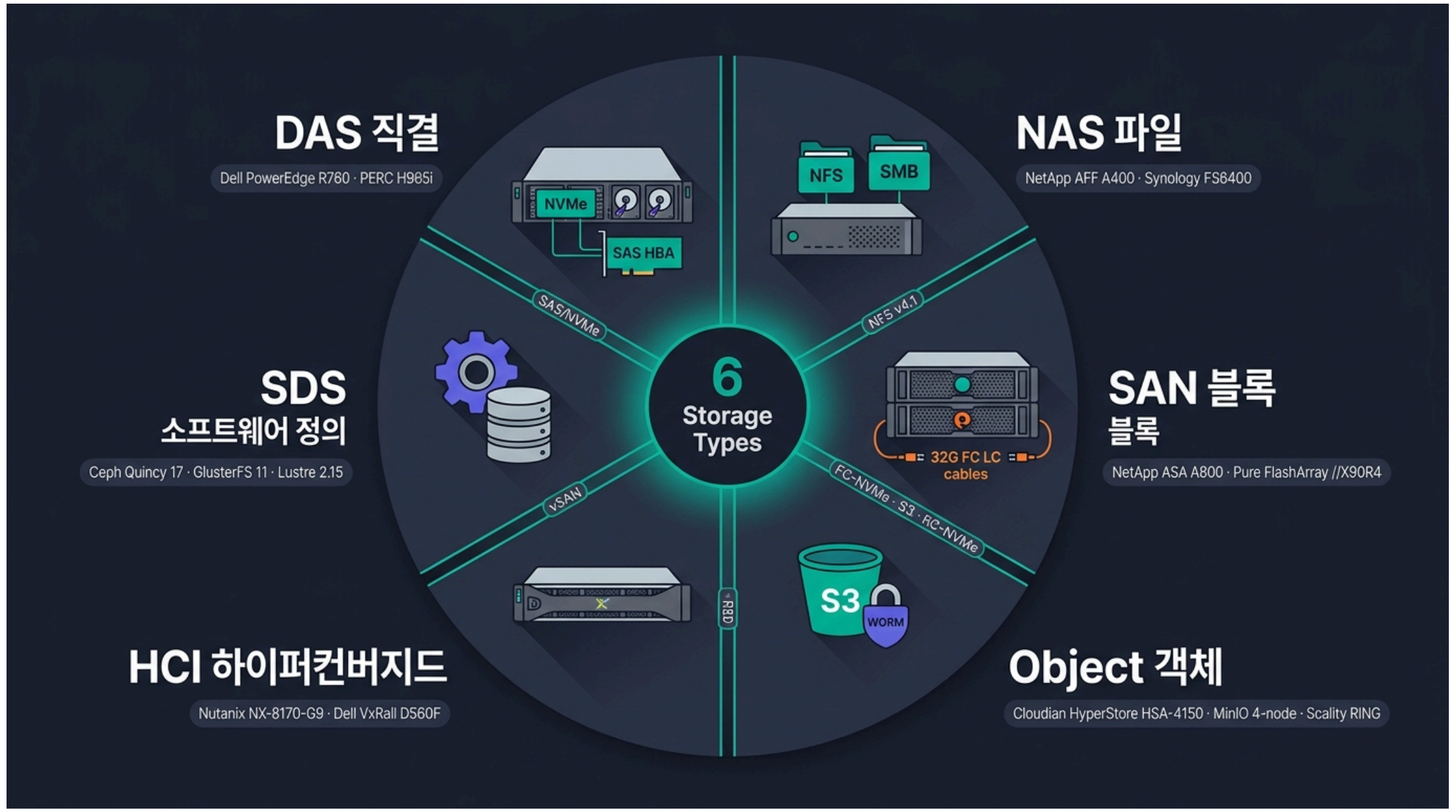
5️⃣ HCI

- **Hyper-Converged**
- Compute + Storage + NW 통합
- vSAN·Nutanix·VxRail
- VDI·중규모 가상화

6️⃣ SDS

- **Software-Defined Storage**
- 범용 HW + 소프트웨어
- Ceph·GlusterFS·Lustre
- 비용·확장성 우선

결정 한 줄 요약: 워크로드의 **공유 단위**(블록·파일·객체)와 **운영 모델**(어플라이언스·HCI·SDS·Object)가 6대 유형을 가른다.



스토리지 6대 유형 — 전체 조망 wheel

① DAS — *서버 안의 디스크, 가장 단순한 형태*

🔧 구성

- 서버 내장 디스크 베이 (2.5"/3.5")
- **RAID 컨트롤러** + 캐시 + BBU/Flash 백업 모듈
- **JBOD** (Just a Bunch Of Disks) 외장 enclosure 연결
- 연결: **SAS** (12Gbps·24Gbps) · **SATA** (6Gbps) · **NVMe** (PCIe Gen4/5)

🔌 SCSI 계보

- **SCSI** (전통 Parallel SCSI)
- **SAS** (Serial Attached SCSI) — 12G·24G
- **SATA** (Serial ATA) — 6G
- **NVMe** (Non-Volatile Memory express) — PCIe 직결

✅ 적합한 용도

- **단일 서버** 워크로드 (Web·WAS)
- 부팅 디스크·로컬 캐시
- 가성비·단순 운영 우선
- 공유가 불필요한 데이터
- AI 학습 데이터 로컬 캐싱 (NVMe)

⚠️ 한계

- 공유·이중화 어려움
- Live Migration 불가 (단일 노드 종속)
- 디스크 장애 = 서버 장애
- 확장성 낮음

> **TA 시각**: DAS는 "없으면 안 되지만, 거기서 멈춰서는 안 되는" 가장 기본 옵션. **부팅 디스크 = DAS RAID 1**이 표준 패턴.

② NAS — *파일 단위 공유 · NFS와 SMB의 두 축*

🐧 NFS (Network File System)

- **Unix·Linux** 표준 파일 공유
- **v3** — 무상태, UDP/TCP, 가장 보편
- **v4** — 상태 유지, TCP만, 보안 강화 (Kerberos), ACL
- **v4.1** — pNFS (병렬 액세스), 세션 multipathing
- **v4.2** — Server-side copy, sparse file

🪟 SMB / CIFS (Server Message Block)

- **Windows** 표준 파일 공유
- **SMB 1.0 / CIFS** — 구식, 보안 취약 (비활성화 권장)
- **SMB 2.x** — Win Vista·2008, 효율 개선
- **SMB 3.x** — Win 2012+, **암호화·Multichannel·Direct (RDMA)**

🧮 비교 매트릭스

항목	NFS v4.1	SMB 3.x
주 OS	Unix·Linux	Windows
인증	Kerberos·sys	NTLM·Kerberos·AD
암호화	TLS·Kerberos	내장 AES-128/256
Multichannel	pNFS	SMB Multichannel
RDMA	NFS over RDMA	SMB Direct
잠금	byte-range	강력한 oplock

🎯 선택 기준

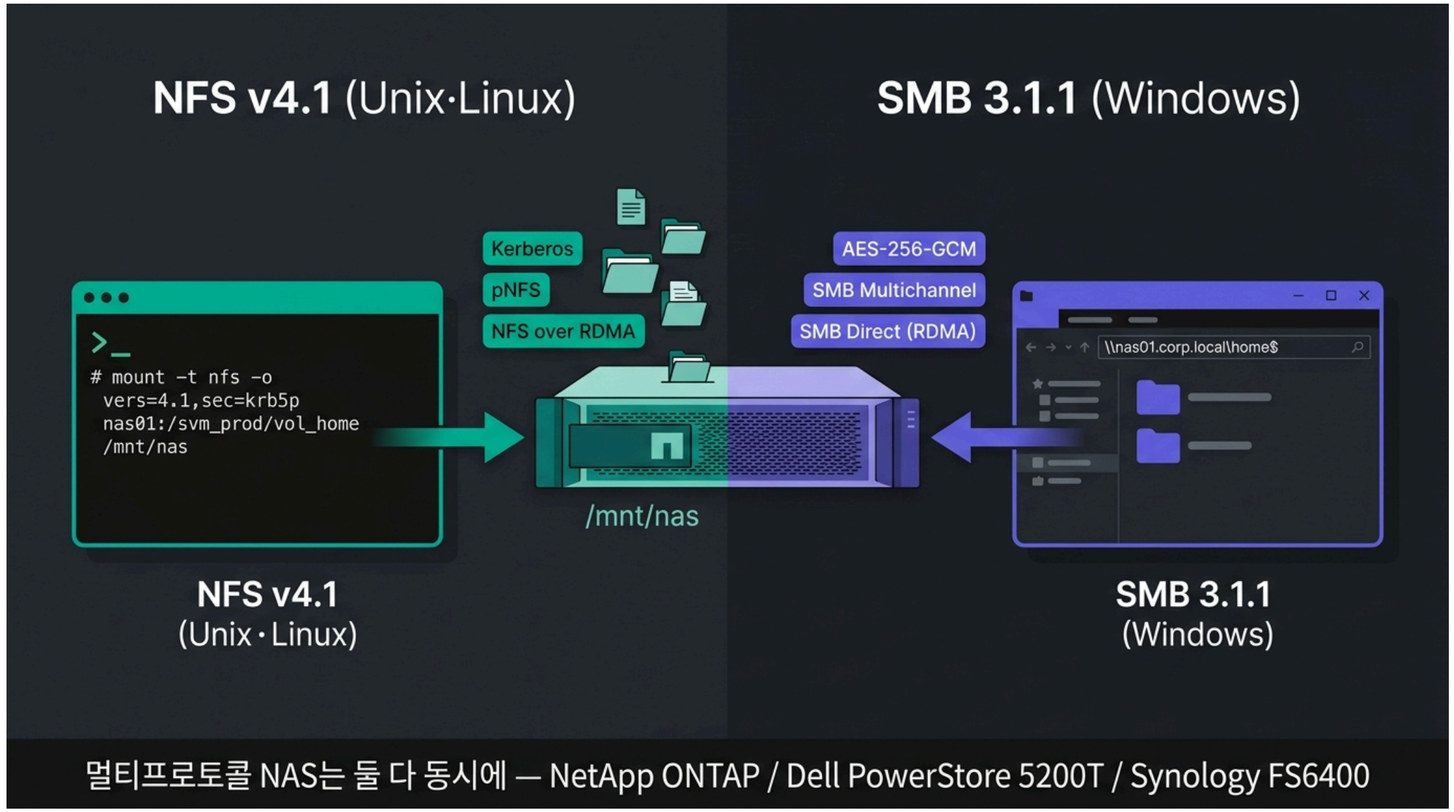
- 운영 서버군 = **NFS** (홈디렉·App 데이터)
- 사무용 PC 공유 = **SMB** (AD 통합)
- 혼용 환경 = **NetApp·TrueNAS** 멀티프로토콜

NAS 솔루션 — *2026 현장 표준*

솔루션	분류	강점	주 사용처
NetApp ONTAP	엔터프라이즈	SnapMirror·SnapVault·멀티프로토콜·중복제거	금융·공공·대기업
Dell EMC Unity / PowerStore	엔터프라이즈	통합 SAN+NAS·Tiering·Inline Dedup	대기업·공공
Dell PowerScale (Isilon)	Scale-Out NAS	단일 네임스페이스·수십 PB	미디어·HPC·AI
IBM Storage Scale (GPFS)	분산 파일시스템	초고성능·병렬	HPC·연구소
Hitachi (HNAS)	엔터프라이즈	FPGA 가속·고성능	통신·제조
Synology DSM	SOHO·중소	가성비·DSM UI·앱 생태	중소·연구실·홈
QNAP QTS	SOHO·중소	확장 모듈·가상화	중소·콘텐츠
TrueNAS (iXsystems)	오픈소스+상용	ZFS 기반·OpenZFS	미디어·중소
OpenZFS	오픈소스	CoW·Snapshot·Send/Receive	자가 구축

국내 도입 패턴: 금융·공공 핵심 = NetApp / Dell, 대용량 분석·미디어 = Isilon, 중소 = Synology·QNAP.

📷 **실제 장비·UI 참조** (벤더 공식) - NetApp AFF / FAS 시리즈 — NetApp 공식 - NetApp ONTAP System Manager — NetApp Docs (관리 UI) - Dell PowerStore — Dell 공식 - Dell PowerScale (Isilon) — Dell 공식 - Synology DiskStation — Synology 공식



NAS 삽화

③ SAN — *블록 단위 · FC와 IP SAN의 진화*

🟧 FC (Fibre Channel)

- 전용 광 패브릭, 가장 안정적
- **세대별 속도**:
- 4 Gbps (2003)
- 8 Gbps (2008)
- 16 Gbps (2011)
- 32 Gbps (2016)
- **64 Gbps (Gen 7, 2019)**
- 128 Gbps (Gen 8, 2025+)
- BB Credit·CRC·In-Order Delivery 보장
- **WWN·WWPN** 식별자

🟦 iSCSI

- IP 위에 SCSI 캡슐화
- 이더넷 + TCP 사용 (저비용)
- **IQN** 식별자 (`iqn.YYYY-MM.com.example:host`)
- 10G·25G·100G NIC + DCB/PFC

🟪 FCoE (Fibre Channel over Ethernet)

- FC 프레임을 이더넷에 캡슐화
- Lossless DCB 필요 (PFC·ETS)
- 2010년대 중반 → 2020년대 쇠퇴
- NVMe/TCP·NVMe/RoCE로 대체

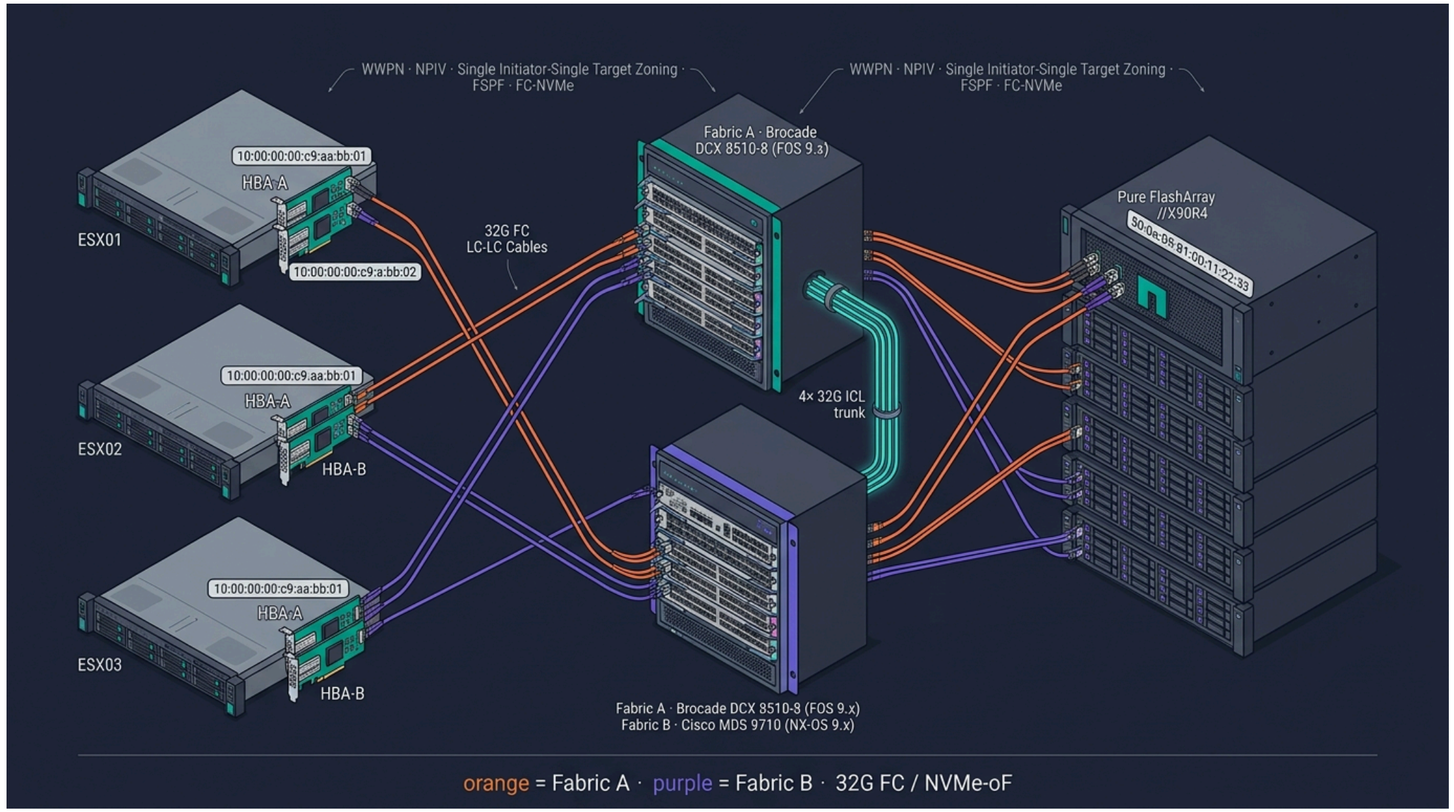
🟩 NVMe-oF (NVMe over Fabrics)

- **차세대 SAN 표준**
- 변종:
- **NVMe/FC** — 기존 FC 패브릭 활용
- **NVMe/TCP** — TCP 위 (저비용)
- **NVMe/RoCE** — RDMA over Ethernet
- **NVMe/IB** — InfiniBand (HPC)
- 지연 < 100µs, IOPS 수백만

📊 비교 한 줄

- FC = 안정·고가, iSCSI = 저비용, NVMe-oF = 차세대

📷 **실제 장비 참조** (벤더 공식) - Brocade (Broadcom) X7 Director — Broadcom 공식 - Brocade G730 / G720 Edge Switch — Broadcom 공식 - Cisco MDS 9710 / 9706 Director — Cisco 공식 - Cisco MDS 9148T / 9396V — Cisco 공식 - Fibre Channel 표준 개요 — Wikipedia



SAN 패브릭 토폴로지 삽화

④ Object Storage — *S3 API의 세계*

📦 Object Storage 특징

- **버킷 → 객체** 2단 구조 (디렉터리 없음)
- **HTTP REST API** (S3·Swift)
- **메타데이터 풍부** — 사용자 정의 가능
- **무한 확장** — 수십 PB·수십 억 객체
- **WORM·버저닝·Object Lock** — 랜섬웨어 대응
- **Erasure Coding** 일반적 (RAID 대체)

🧮 적합한 워크로드

- 백업·아카이브 (장기 보존)
- 로그·이벤트 저장
- 미디어 (이미지·동영상)
- CDN 오리진
- 데이터 레이크·AI 학습 데이터셋
- 정적 웹 콘텐츠

🏆 주요 솔루션

솔루션	분류	특징
AWS S3	퍼블릭	de facto 표준 API
Azure Blob	퍼블릭	호환 SDK
OpenStack Swift	오픈소스	OpenStack 생태
Ceph RGW	오픈소스	S3·Swift 둘 다
MinIO	오픈소스+상용	경량·고성능 S3
Cloudian HyperStore	상용	엔터프라이즈 S3 어플라이언스
Scality RING	상용	대용량·SDS
NetApp StorageGRID	상용	멀티사이트·메타 강력

🔒 핵심 기능

- **Object Lock** (Compliance·Governance 모드)
- **버저닝** — 이전 버전 보존
- **수명 주기 정책** — Hot→Cold→삭제

📷 **실제 솔루션·UI 참조** (벤더 공식) - AWS S3 — AWS 공식 - NetApp StorageGRID — NetApp 공식 - Dell EMC ECS (Elastic Cloud Storage) — Dell 공식 - MinIO Enterprise Object Store — MinIO 공식 - Ceph — Ceph 공식 - Cloudian HyperStore — Cloudian 공식

⑤ HCI — *Hyper-Converged Infrastructure*

🧱 HCI란

- **Compute + Storage + Network을 한 노드에 통합**
- 노드 추가만으로 수평 확장
- 전용 SAN 패브릭 없음 (이더넷만)
- 단일 UI로 통합 관리
- VDI·중소 가상화의 사실상 표준

🛠️ 핵심 아이디어

- 각 노드의 로컬 디스크를 **분산 스토리지 풀**로 묶음
- 데이터 복제 (Replica 2·3) 또는 Erasure Coding
- 메타데이터·캐시는 SSD·NVMe

🏆 주요 솔루션 비교

제품	분류	특징
VMware vSAN	SW + 인증 HW	vSphere 통합·시장 1위
Nutanix	SW + 어플라이언스	Prism UI·AHV 자체 hypervisor
Dell VxRail	어플라이언스	vSAN 기반 검증 HW
HPE SimpliVity	어플라이언스	Dedup 가속 카드 내장
Cisco HyperFlex	어플라이언스	UCS 통합
Azure Stack HCI	SW (MS)	S2D + Hyper-V
Scale Computing HC3	어플라이언스	중소·엣지

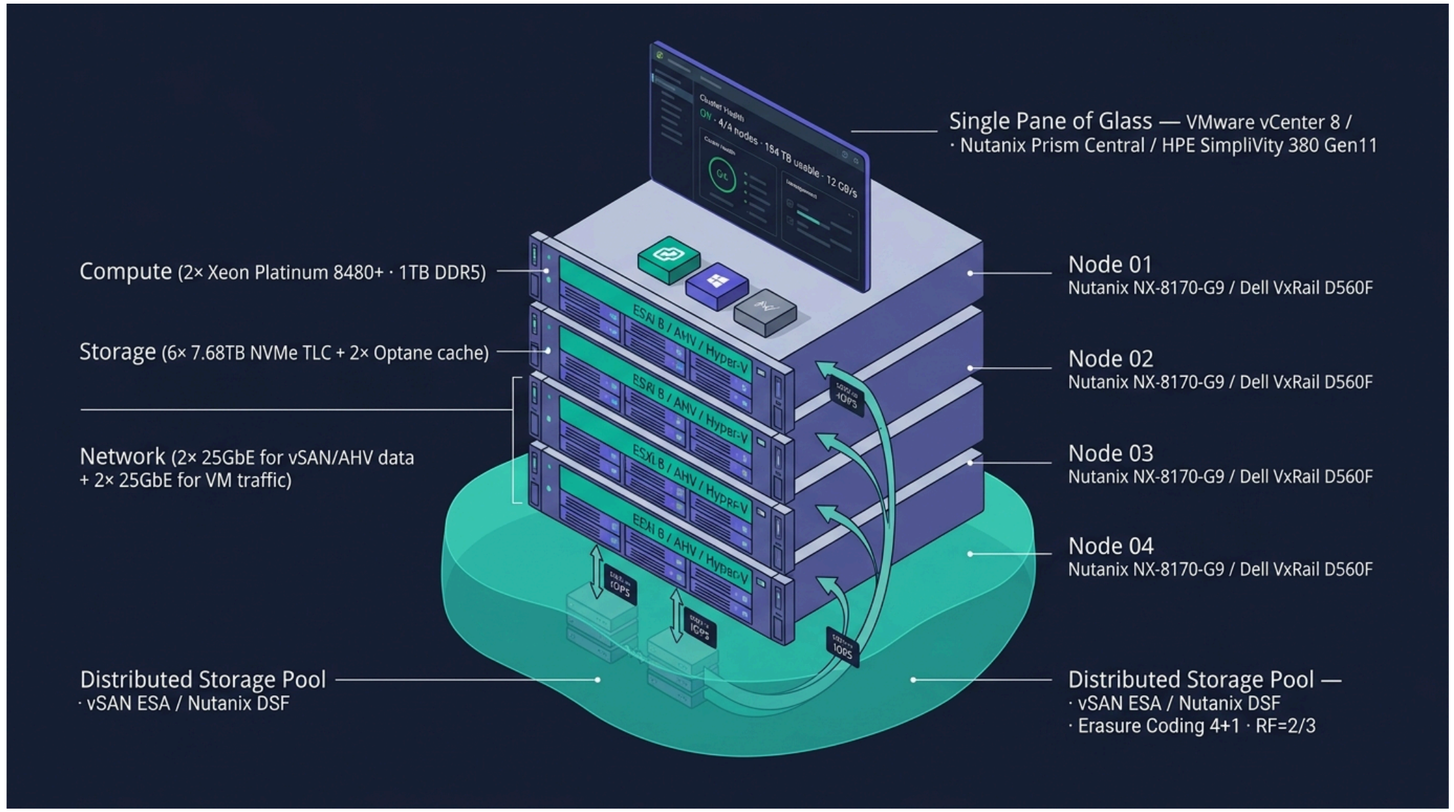
✅ 장점

- 운영 단순화 (단일 UI)
- 빠른 도입 (수일~수주)
- 노드 단위 확장
- 백업·DR 통합 솔루션 풍부

⚠️ 한계

- 대규모 분리 확장(컴퓨트만/스토리지만) 어려움
- 라이센스 비용 (vSAN·Nutanix)
- 특정 워크로드(초대용량 DB)에서는 SAN 우위

📷 **실제 솔루션·UI 참조** (벤더 공식) - VMware vSAN — VMware 공식 - Nutanix Prism (관리 UI) — Nutanix 공식 - Dell VxRail — Dell 공식 - Cisco HyperFlex — Cisco 공식 - Microsoft Azure Stack HCI — Microsoft 공식



HCI 아키텍처 삽화

⑥ SDS — *Software-Defined Storage*

💡 SDS란

- **범용 x86 서버 + 디스크** 위에 **소프트웨어**가 스토리지 기능 제공
- 벤더 종속 탈피·비용 절감
- 블록·파일·객체 통합 가능
- 클러스터로 확장

🏆 주요 솔루션

- **Ceph** — 블록(RBD)·파일(CephFS)·객체(RGW) 통합, 오픈소스 최강
- **GlusterFS** — 분산 파일시스템, Red Hat 인수
- **Lustre** — HPC 병렬 파일시스템, 슈퍼컴퓨터 표준
- **BeeGFS** — HPC·AI 학습용
- **DRBD** — 블록 레벨 복제 (HA Pair)
- **Storage Spaces Direct (S2D)** — MS Windows Server

🆚 SDS vs 어플라이언스

항목	SDS	어플라이언스
HW	범용 (선택 자유)	인증 모델
비용	낮음 (HW만)	높음
운영	자체 책임	벤더 지원
성능 튜닝	자유롭게	벤더 한정
적합 규모	중대형 (전담 인력)	전 규모

🎯 SDS가 빛나는 곳

- HPC·AI 학습 (Lustre·BeeGFS)
- 대용량 백업·아카이브 (Ceph RGW)
- 클라우드 오픈소스 인프라 (Ceph + OpenStack)
- 비용 절감 정책이 강한 공공·연구

⚠️ 운영 부담

- 노드 장애·재구축·확장이 전부 자체 책임
- 사고 시 벤더 책임 한정적

6대 유형 비교 매트릭스 — *한 페이지 결정표*

항목	DAS	NAS	SAN	Object	HCI	SDS
공유 단위	블록	파일	블록	객체	블록	블록·파일·객체
프로토콜	SAS·SATA·NVMe	NFS·SMB	FC·iSCSI·NVMe-oF	S3·Swift	자체 분산	자체 + 표준
성능	최고 (직결)	중	매우 높음	중~높음	높음	가변
확장성	낮음	중	높음	**최고**	높음 (노드 단위)	**최고**
공유 범위	1대	다수 클라이언트	다수 호스트	무제한 (HTTP)	클러스터 내	클러스터 내
비용	낮음	중	높음	낮음~중	중~높음	낮음 (HW만)
운영 난도	낮음	낮음	**높음**	중	중 (단일 UI)	**높음**
대표 워크로드	부팅·캐시	홈디렉·미디어·백업	DB·VM	백업·아카이브·AI	VDI·중소 가상화	HPC·대용량
대표 솔루션	서버 내장	NetApp·Synology	EMC·NetApp·HDS	MinIO·Ceph·StorageGRID	vSAN·Nutanix	Ceph·Lustre·BeeGFS

> **결정 한 줄**: "어떤 공유 단위·어떤 운영 모델인가" 두 축이 6대 유형을 가른다.

PART B

RAID + 데이터 경로 — *디스크 묶음과 경로 이중화*

> RAID는 디스크 결함의 안전망, Multipath는 경로 결함의 안전망.

RAID 0·1·5·6·10·50·60·DP — *비교 매트릭스*

RAID	최소 디스크	용량 손실	결함 허용	읽기	쓰기	Rebuild	용도
0 Stripe	2	없음	**0**	최고	최고	불가	캐시·임시
1 Mirror	2	**50%**	1	빠름	보통	빠름	OS·소용량 중요
5 Parity	3	1 디스크	1	보통	느림	**매우 느림**	구식·소용량
6 Dual Parity	4	2 디스크	**2**	보통	더 느림	느림	**대용량 표준**
10 Mirror+Stripe	4	**50%**	1 디스크/그룹	**최고**	**빠름**	빠름	**DB·고성능**
50	6	그룹별 1	그룹별 1	빠름	중	중	대용량 + 성능
60	8	그룹별 2	**그룹별 2**	빠름	중	중	대용량 + 내결함
DP (NetApp)	4	2 디스크	2	보통	보통	빠름	NetApp 전용

🧮 RAID 5가 사라지는 이유 (URE 문제)

- HDD 용량 증가 (수 TB~수십 TB)
- Rebuild 중 다른 디스크 URE(Unrecoverable Read Error) 확률 ↑
- 8TB HDD 4개 RAID 5 → Rebuild 중 실패 확률 비현실적으로 높음
- → **RAID 6** 또는 **RAID 60** 권장

> "RAID는 백업이 아니다" — 디스크 고장에는 강하지만 사용자 실수·랜섬웨어에는 무력.

Hot Spare · Rebuild — *재구성의 시간 싸움*

🔥 Hot Spare

- 정상 동작 중인 **대기 디스크**
- 장애 발생 시 즉시 자동 재구축 투입
- **Global Hot Spare** — 전 그룹 공유
- **Dedicated Hot Spare** — 특정 그룹 전용
- 권고: **그룹당 1개 + Global 1개**

⏱️ Rebuild Time 예시

- 1TB SAS HDD RAID 6 → **수 시간**
- 8TB SATA HDD RAID 6 → **24~48시간**
- 18TB HDD RAID 6 → **수 일** ⚠️
- SSD/NVMe → 빠름 (수십 분)
- 운영 IO 부하 + Rebuild = 성능 저하

📊 Drive Failure Rate

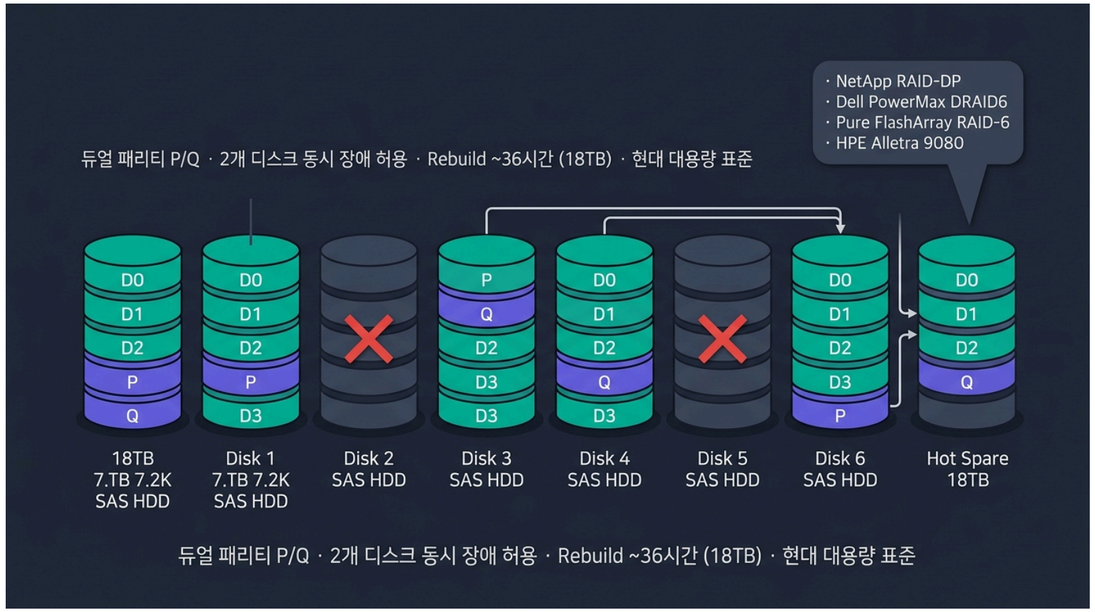
- AFR (Annualized Failure Rate)
- Backblaze 공개 데이터:
- Enterprise HDD: 0.5~1.5%/년
- Consumer HDD: 1.5~3%/년
- Enterprise SSD: 0.2~0.7%/년
- 디스크 100개 운영 시 = 연 1~3개 교체 필요

🛡️ Rebuild 위험 완화

- **RAID 6** 또는 **Triple Parity** 적용
- **Erasure Coding** 도입 (Object·SDS)
- **Rebuild 우선순위 정책** — 운영 부하 시간 회피
- Hot Spare 사전 확보
- 정기 **Scrub** (Patrol Read) — 잠재 오류 사전 발견

RAID 6 — *듀얼 패리티 P/Q*

- **N+2 디스크** 구성 (데이터 N + 패리티 2)
- 두 패리티 **P (XOR) + Q (Reed-Solomon)** 를 디스크 전체에 **분산** 저장
- **2개 디스크 동시 장애**까지 데이터 보존
- Rebuild 중 추가 1개 장애도 견딤 → **대용량 HDD 시대 표준**
- 쓰기 페널티 6배(읽기 2+쓰기 2 = 패리티 갱신)
- 적합: 18TB+ HDD·대용량 NAS·아카이브
- 벤더: NetApp RAID-DP · Dell PowerMax DRAID6 · Pure RAID-6 · HPE Alletra 9080



RAID 6 단면도 — 분산 P/Q 패리티 + Hot Spare Rebuild

PART C

고급 스토리지 기능 — *Snapshot · Replication · Dedup · Tiering · QoS*

> 디스크 박스가 아니라 **소프트웨어 기능**이 곧 엔터프라이즈 스토리지의 가치.

Snapshot — *CoW와 RoW 두 가지 방식*

🖊️ CoW (Copy-on-Write)

- Snapshot 시점에 **원본 데이터 위치 그대로 유지**
- 변경 발생 시: **이전 데이터를 별도 영역에 복사** → 그 후 원본 덮어쓰기
- 읽기 성능 우수, **쓰기 성능 저하** (1회 쓰기 = 1읽기 + 1쓰기 + 1쓰기)
- 채택: 전통 SAN (Dell EMC·HPE·일부 IBM)

🔁 RoW (Redirect-on-Write)

- Snapshot 시점부터 **새 쓰기를 새 위치에 기록**
- 원본 블록은 변경되지 않음
- **쓰기 성능 우수** (1회 쓰기 = 1쓰기)
- 메타데이터 관리 복잡 (가비지 컬렉션)
- 채택: NetApp WAFL·ZFS·대부분 현대 시스템

🔗 Clone

- Snapshot을 **읽기·쓰기 가능한 새 볼륨**으로 노출
- 처음엔 원본 공유, 변경분만 별도
- DB 테스트·개발 환경 신속 복제에 활용

⚠️ Snapshot의 한계

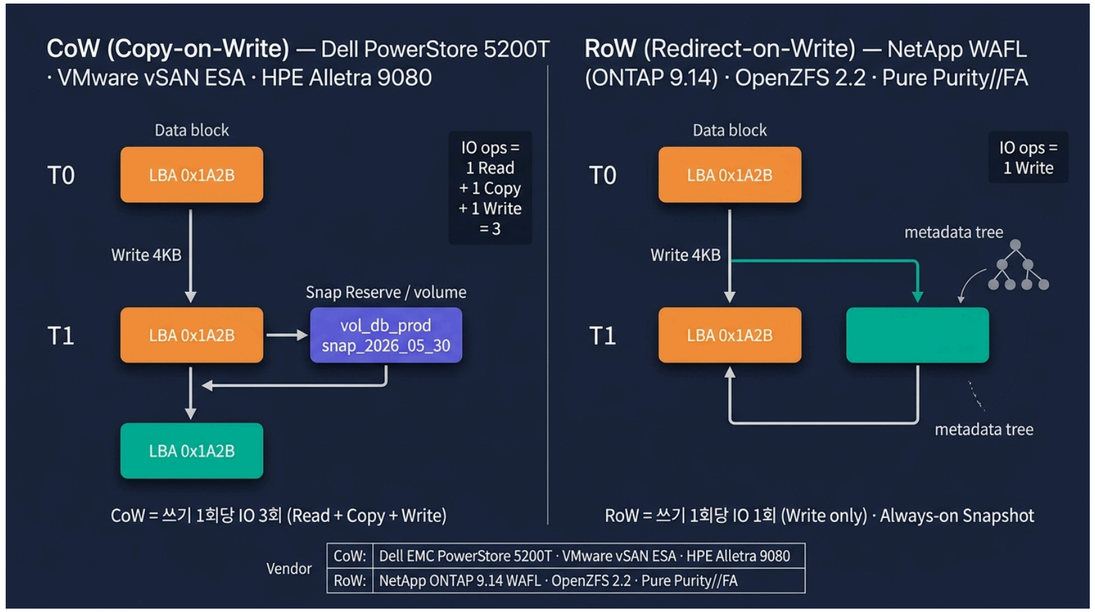
- **백업이 아니다** — 동일 어레이에 종속
- 어레이 자체 장애 시 Snapshot도 함께 손실
- 원본 데이터 부분 손상이면 Snapshot도 영향
- 메타데이터 의존 → 파일시스템 손상 시 무력

🎯 활용 패턴

- 패치·업그레이드 전 안전장치
- 시간별 정기 (RPO 단축 수단)
- Clone으로 테스트 DB 신속 생성
- **백업의 보조 수단**으로 위치 잡기

🧊 CoW vs RoW — *Snapshot 두 갈래*

- **CoW (Copy-on-Write)** — 쓰기 발생 시 **원본을 복사 후 덮어쓰기**
- 쓰기 1회 = **IO 3회** (Read + Copy + Write)
- Dell PowerStore · vSAN ESA · HPE Alletra
- **RoW (Redirect-on-Write)** — 쓰기를 **신규 위치로 리다이렉트**, 원본은 유지
- 쓰기 1회 = **IO 1회** (Write only)
- NetApp WAFL · OpenZFS · Pure Purity//FA
- 핵심: **Snapshot ≠ 백업** — 어레이가 죽으면 Snapshot도 죽는다



Snapshot CoW vs RoW — IO 경로 차이

Replication — *동기 vs 비동기*

🔄 Synchronous Replication

- **원본·복제본 동시 쓰기** 후 응답
- **RPO = 0** (데이터 손실 0)
- 거리 한계 ~ **100km** (지연 < 5ms 권고)
- 비용 높음 (전용 회선·동등 사양)
- 사이트 간 응답시간 지연이 운영에 영향
- 미션크리티컬 (금융 코어·결제)

⏳ Asynchronous Replication

- 원본 쓰기 응답 → 일정 주기로 복제본에 적용
- **RPO 수 초 ~ 수 분**
- 거리 무제한 (대륙 간 가능)
- 운영 성능 영향 최소
- 일반 기업 DR의 표준

🏆 주요 솔루션

솔루션	벤더	모드
SnapMirror	NetApp	Sync·Async (분 단위)
SnapVault	NetApp	백업 복제
SRDF	Dell EMC	Sync·Async·SRDF/Star
HyperSwap	IBM	Sync (Active-Active)
MetroCluster	NetApp	Sync (Stretched)
PowerStore Metro	Dell	Sync
Hitachi GAD	Hitachi	Sync (Active-Active)
VPLEX	Dell EMC	Sync (Active-Active)

🌐 Stretched Cluster

- 두 사이트가 **단일 클러스터**로 동작
- LUN이 양쪽에서 동시 활성 (Active-Active)
- VMware vMSC·Hyper-V Stretch
- 거리·지연 제약 엄격

NetApp ONTAP 9.14.1 · cluster1 · AFF A800

SSH

NetApp AFF A800 · cluster1 (2-node HA pair) · ONTAP 9.14.1 · RAID-DP

```
cluster1::> cluster show
cluster1-01 / cluster1-02 — Health: true · Eligibility: true
cluster1::> storage aggregate show
aggr_ssd_01 · 92TB · 38TB Available · 59% Used · online · cluster1-01
```

```
cluster1::> volume create -vserver svm_prod -volume vol_db_prod -aggregate aggr_ssd_01
-size 4TB -junction-path /db_prod -security-style unix
cluster1:> snapshot show -vserver svm_prod -volume vol_db_prod
Vserver · Volume          · Snapshot  · State · Size
------------------------ ----------- -------- ------
hourly.2026-05-30_0905    · valid     · 812MB
daily.2026-05-30_0010     · valid     · 4.2GB
before_patch_2026_05_30   · valid     · 0B
```

```
cluster1:> snapmirror create -source-path cluster1://svm_prod:vol_db_prod -destination-path
cluster_dr://svm_dr:vol_db_prod_dr -type XDP -policy MirrorAllSnapshots -schedule hourly
cluster1:> snapmirror show
svm_prod:vol_db_prod → svm_dr:vol_db_prod_dr · Snapmirrored · Idle
Last Transfer 2026-05-30 09:00:12 · Lag 00:05:48
cluster1:>
```

XDP = Extended Data Protection · Async DR · RPO ≈ 1h

NetApp ONTAP CLI — Volume·Snapshot·SnapMirror 실제 명령

Dedup · Compression — *공간 효율의 두 축*

🗜️ Deduplication (중복제거)

- **동일한 블록을 1번만 저장**, 나머지는 참조
- **Inline** — 쓰기 시점에 즉시 처리 (성능 영향 ↑)
- **Post-Process** — 일단 기록 후 백그라운드 처리

📦 Compression (압축)

- LZ4·Snappy·Zstd·Deflate 알고리즘
- Inline·Post-Process 동일 구분
- 텍스트·로그에서 효과 큼, 영상·암호화 파일은 효과 적음

🎯 효과가 큰 곳

- **VDI** (동일 OS 이미지 수십~수백) — 10:1 이상
- **백업 데이터** — 5:1 ~ 30:1
- **DB 로그·텍스트** — 2:1 ~ 5:1

⚖️ 트레이드오프

항목	Inline	Post-Process
쓰기 성능	낮음 (CPU 부하)	높음
디스크 사용	즉시 절감	일시 점유 후 절감
운영 단순성	단순	복잡 (스케줄)
대표	현대 All-Flash·Veeam	전통 SAN·일부 NAS

📊 실효 절감률 측정

- Veeam 백업: 5~10:1 일반적
- VDI 부팅 이미지: 10~20:1
- DB: 2~3:1
- 영상·암호화 파일: 1.1:1 (효과 미미)

⚠️ 주의

- **암호화 후 Dedup·Compression 불가** — 순서 중요
- 메타데이터 손상 = 전체 데이터 손실 가능
- CPU·메모리 사양 충분히 확보

Tiering · Thin Provisioning — *공간과 성능의 자동 분배*

🎚️ Tiering (자동 계층화)

- 데이터 접근 빈도에 따라 자동 이동
- 일반 계층:

```
🔥 Tier 0: NVMe  (Hot)
🟧 Tier 1: SSD
🟨 Tier 2: SAS HDD
🟦 Tier 3: SATA HDD
☁️ Tier 4: Cloud Cold (S3 Glacier·Deep Archive)
```

- **Cloud Tier** — 자동 클라우드 오프로드 (NetApp FabricPool·Pure Cloud Block Store)
- 정책: 30일·90일·1년 미사용 → 다음 Tier로 이동

📦 Thin vs Thick Provisioning

항목	Thick	Thin
할당	즉시 전체 점유	사용분만 점유
성능	일정 (예측 가능)	가변
효율	낮음	높음
위험	없음	**과할당 시 일제 중단**
적합	DB·미션크리티컬	일반·VDI

⚠️ Thin Provisioning 과할당

- 가상 1TB 할당 × 100개 = 100TB 가상
- 실제 디스크 50TB → 사용량 50TB 도달 시 **모든 LUN 일제 정지**
- 실사용량 모니터링 + 알람(70%·80%·90%) 필수
- 정기 회수 (UNMAP) 운영

📋 운영 권고

- DB·미션크리티컬 = **Thick**
- VDI·일반 = **Thin** + 강한 모니터링

PART D

Tape · 아카이브 — *랜섬웨어 시대에 다시 빛나는 매체*

> Tape는 과거 기술이 아니다 — **오프라인의 마지막 방어선**이자 장기 보존의 최저 비용 수단.

LTO (Linear Tape-Open) — *9세대·10세대로 가는 진화*

세대	출시	Native	Compressed	전송속도
LTO-1	2000	100 GB	200 GB	20 MB/s
LTO-2	2003	200 GB	400 GB	40 MB/s
LTO-3	2005	400 GB	800 GB	80 MB/s
LTO-4	2007	800 GB	1.6 TB	120 MB/s
LTO-5	2010	1.5 TB	3 TB	140 MB/s
LTO-6	2012	2.5 TB	6.25 TB	160 MB/s
LTO-7	2015	6 TB	15 TB	300 MB/s
LTO-8	2017	12 TB	30 TB	360 MB/s
LTO-9	2021	**18 TB**	**45 TB**	**400 MB/s**
LTO-10	2025~2026 예정	36 TB (예정)	90 TB (예정)	1100 MB/s (예정)
LTO-11	미래	72 TB (계획)	180 TB	—

🔑 핵심 특징

- WORM 매체 옵션 (LTO-3+) — Write Once Read Many
- AES-256 하드웨어 암호화 (LTO-4+)
- 30년+ 보존 (적정 환경)
- 호환성: **n세대 드라이브는 n-1 읽기·쓰기, n-2 읽기 가능**

LTFS (Linear Tape File System) — *Tape을 디스크처럼 사용*

📂 LTFS란

- Tape에 **파일시스템 메타데이터**를 별도 파티션으로 저장
- 일반 OS 마운트 가능 (Linux·Windows·macOS)
- 파일 단위 접근 — `cp`, `mv`로 직접 다룸
- LTO-5+ 지원, 산업 표준 (ISO/IEC 20919)

🎯 활용 패턴

- **방송·미디어** — 영상 마스터 보관
- **연구·과학** — 측정 데이터 장기 보존
- **공공·아카이브** — 법정 보관
- **클라우드 백업** — AWS S3 Glacier 기반

🆚 LTFS vs 전통 Tape

항목	전통 Tape	LTFS
접근	백업 SW 필수	OS 마운트로 직접
메타데이터	백업 SW 카탈로그	Tape 자체에 보관
호환	백업 SW 종속	표준
용도	백업	아카이브

⚠️ 주의

- **순차 매체** — 임의 접근 느림 (수십 초~수 분 탐색)
- 헤드 위치 이동 비용 큼
- 쓰기 후 자주 수정하는 데이터에는 부적합

Tape의 현대적 가치 — *랜섬웨어 시대에 다시 부상*

🛡️ Tape의 본질적 강점

- **오프라인 매체** — 네트워크에서 분리되면 사이버 공격 불가능
- **WORM** — 본질적으로 한 번 쓰면 변경 불가
- **장기 보존** — 30년+ (적정 환경)
- **저비용** — GB당 단가 가장 낮음
- **에너지 효율** — 보관 중 전력 소모 0

📊 비용 비교 (대략, GB 당)

- HDD: $0.02 / GB / 월 (전력 포함)
- Object Cold: $0.004 / GB / 월
- Tape: **$0.001 / GB / 월 + 초기 HW**

🦠 랜섬웨어 대응 가치

- 운영망·관리망·백업망 다 침해되어도
- **오프라인 Tape**은 격리되어 살아남음
- 실제 사건: 2020+ 다수 기업이 백업까지 암호화당해 몸값 지불
- 이후 **Tape 복귀**가 보안 권고로 부상

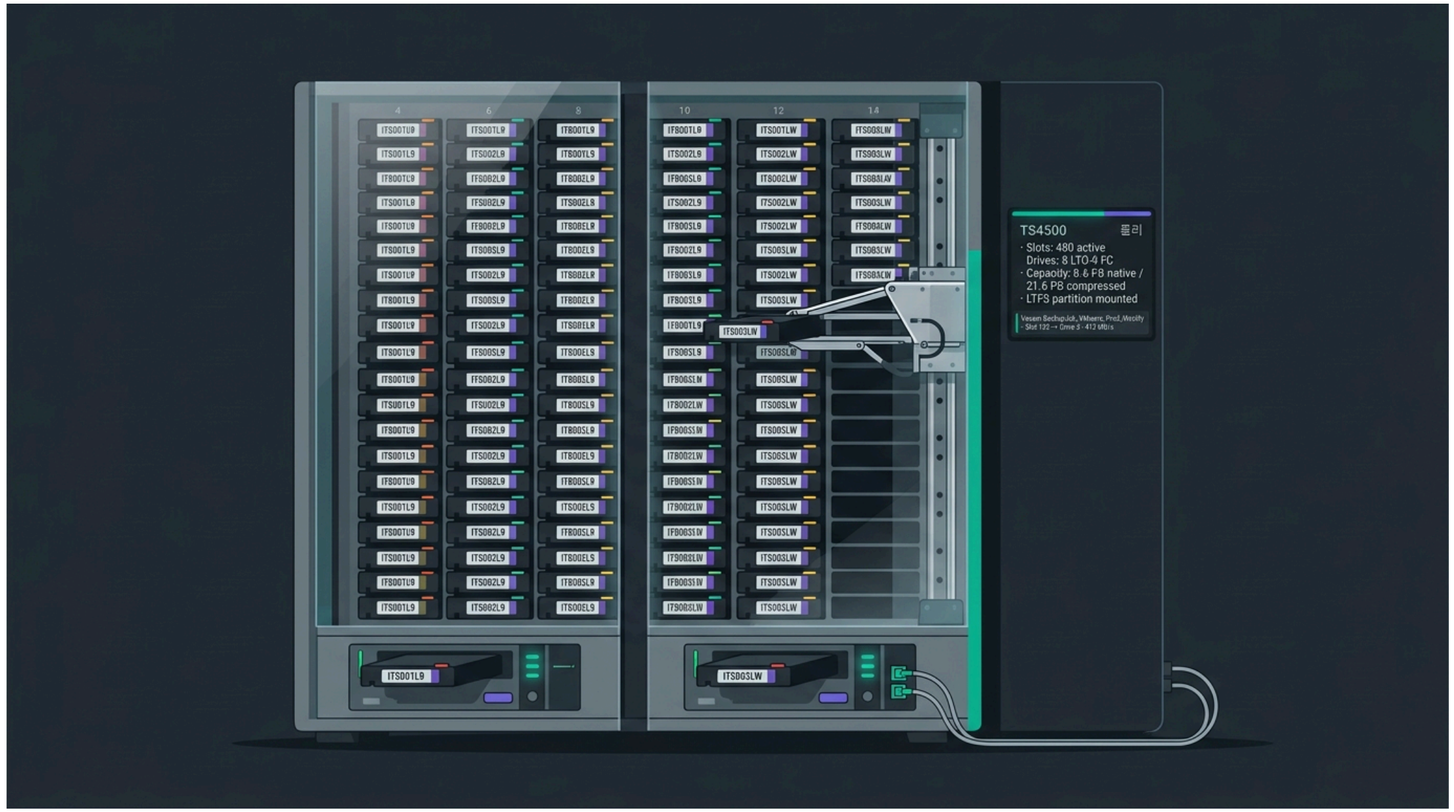
⚠️ Tape의 한계

- **복구 시간 길다** — 수 시간~수 일
- **순차 매체** — 부분 복구 비효율
- **물리 보관·운반 비용**
- **카트리지·드라이브 노후화 관리**

🎯 권장 운영

- **일별 Inc → 디스크, 주별 Full → Tape**
- Tape는 오프사이트 보관 (사외 보관소)
- 분기 1회 복구 시험

📷 **실제 장비 참조** (벤더 공식·Wikipedia) - IBM TS4500 Tape Library — IBM 공식 - IBM TS1170 / LTO-9 Drive — IBM 공식 - Dell PowerVault ML3 — Dell 공식 - HPE StoreEver MSL Series — HPE 공식 - Quantum Scalar i6 / i6000 — Quantum 공식 - LTO Ultrium 표준 — LTO Program 공식 (로드맵·사양서)



Tape Library 삽화

PART E

백업 정책 · 솔루션 — *6종 정책 · GFS · 7대 솔루션*

> "검증되지 않은 백업은 백업이 아니다."

백업 정책 6종 — *비교 매트릭스*

정책	첫 백업	이후	복구 시 필요	용량	백업 속도	복구 속도
Full	전체	**전체**	마지막 Full 1개	**큼**	느림	**빠름**
Incremental	Full	변경분 (이전 Inc 이후)	Full + 모든 Inc	**작음**	**빠름**	느림
Differential	Full	변경분 (마지막 Full 이후)	Full + 마지막 Diff	중간	중간	중간
Synthetic Full	Full	Inc + 가상 합성	마지막 Synthetic Full	큼	빠름 (Inc 백업)	빠름
Forever Incremental	Full	Inc만 지속	Forever Inc 체인	작음	빠름	중간
Reverse Incremental	Full	직전 백업이 Full, 이전이 Reverse Inc	최근 Full만	중간	중간	**매우 빠름** (최근 우선)

🧮 정책 선택 가이드

- 일반 환경: **Synthetic Full** (Inc로 빠르게, 복구는 Full처럼)
- 대용량·고빈도: **Forever Incremental** (Veeam 표준)
- 오프사이트 Tape: **Weekly Full + Daily Inc** (전통)
- 빠른 최근 복구: **Reverse Incremental**

Hot · Cold · Warm Backup — *서비스 상태별 백업*

🔥 Hot Backup

- **서비스 운영 중** 백업
- DB Online Backup (Oracle RMAN·MS SQL VSS)
- Snapshot + 백업 SW 통합
- 응용 일관성 (Application-Consistent)
- **무중단 필수 환경**

❄️ Cold Backup

- **서비스 중단 후** 백업
- 가장 안정적 (정합성 100%)
- 야간 점검 윈도 활용
- 현대 거의 사용 안 함

🌤️ Warm Backup

- 단시간 일시 정지 후 백업
- 짧은 점검 윈도 활용
- 일부 DB·중요도 중간

🧬 일관성 수준

- **Crash-Consistent** — 디스크 상태만 (응용 미인지)
- **File-System-Consistent** — FS sync
- **Application-Consistent** — DB·App 협력 (VSS·Agent)

📌 VSS (Volume Shadow Copy Service)

- Windows 표준 Snapshot 프레임워크
- Exchange·SQL·SharePoint·AD 응용 일관성

🎯 권장 패턴

- **Hot Backup + Application-Consistent** = 현대 표준
- DB는 **Native Backup Tool** + 백업 SW 연계
- Oracle RMAN
- MS SQL Native Backup
- PostgreSQL pg_basebackup
- MongoDB mongodump
- 트랜잭션 로그 별도 백업 → 시점 복구

⚠️ 흔한 실수

- DB 파일을 일반 파일 백업하면 깨질 위험
- VSS Writer 비정상 → 백업 실패
- 트랜잭션 로그 백업 누락

백업 검증 · 복원 테스트 — *검증 없는 백업은 백업이 아니다*

🧪 검증 단계

1. **Job 성공 확인** — 백업 SW의 status (기본)
2. **체크섬 검증** — SHA-256·CRC
3. **샘플 복구 시험** — 정기 무작위
4. **전체 복구 시험** — 분기·반기
5. **자동화된 검증** — 백업 후 자동 부팅·테스트

🛠️ 자동 검증 솔루션

- **Veeam SureBackup** — 격리 샌드박스에서 자동 부팅·테스트
- **Commvault DASH** — 자동 복구 시험
- **Rubrik Live Mount** — 즉시 마운트 검증
- **Cohesity TestDev** — 격리 환경 자동 생성

📋 정기 점검 체크리스트

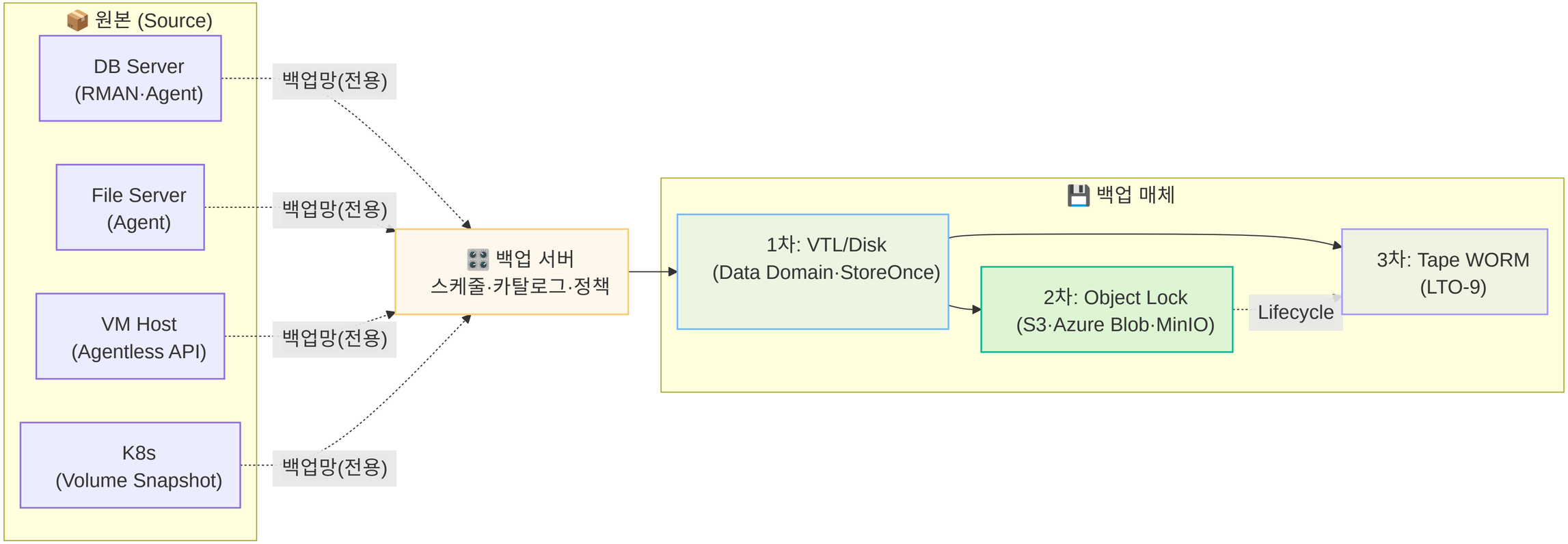
- [ ] 일별: Job 성공률 100%인가
- [ ] 주별: 무작위 1건 복구 시험
- [ ] 월별: 보고서 + 실측 RTO 기록
- [ ] 분기별: 전체 DR 전환 시뮬레이션
- [ ] 반기별: Live DR 훈련
- [ ] 연: 정책·매체·솔루션 재검토

🚨 흔한 실패 패턴

- 백업 Job은 성공인데 **데이터는 실제 백업되지 않은 경우** (Agent 오류)
- Tape 카트리지 자체 불량
- 복구 시 의존 라이브러리·DB 누락
- 비밀번호·인증서 정보가 없어 복구 불가

> **"백업이 정상 수행되고 있습니다"는 의미 없는 보고**. "복구 시험 분기 1회 + 최근 실측 RTO + 검증된 복구 절차서"가 실질적 답.

백업 시스템 아키텍처 — *전형적 구조*



> 1차(빠른 복구) · 2차(Immutable) · 3차(오프라인) = **2024+ 표준 3계층**.

PART F

데이터 무결성 · 랜섬웨어 대응 — *3-2-1-1-0과 Immutable*

> 모든 백업은 결국 "복구할 수 있는가 + 변경되지 않는가" 두 질문에 답해야 한다.

Air-Gapped · Immutable Backup — *공격자가 접근할 수 없는 백업*

🌬️ Air-Gapped (에어갭)

- **물리적·논리적으로 운영망과 분리된 백업**
- 평시 분리 → 백업 시점에만 연결 → 다시 분리
- 종류:
- **물리 에어갭** — Tape 카트리지 오프라인 보관
- **논리 에어갭** — VLAN 분리 + 일시 활성화
- **시간 에어갭** — 백업 윈도 외 차단
- 자동화: **백업 SW + NW 자동화** 연동

🪨 Immutable Backup

- **한 번 기록되면 변경·삭제 불가**
- 보존 기간 동안 그대로 보존
- 시스템 관리자도 삭제 불가 (Compliance 모드)
- 랜섬웨어가 접근해도 데이터 보존

🔐 구현 방법

매체	메커니즘
S3 Object Lock	Compliance / Governance 모드
Azure Blob Immutable	Time-based / Legal Hold
Veeam Hardened Linux Repository	변경 불가 OS 설정
Dell PowerProtect Cyber Vault	격리·Immutable 통합
Linux WORM (XFS·ZFS)	파일시스템 옵션
LTO WORM 카트리지	물리적 WORM

🎯 권장 조합

- 1차: **Veeam Hardened Repository** (즉시 복구)
- 2차: **S3 Object Lock** (Immutable 클라우드)
- 3차: **LTO WORM** (오프라인 최종 방어)
- → **3중 Immutable**

WORM · S3 Object Lock — *법적·물리적 변경 불가*

🪨 WORM (Write Once Read Many)

- **물리적 또는 논리적으로 한 번만 쓰기 가능**
- 금융·의료·공공 법정 보관에 사용
- 매체별 구현:
- **CD-R·DVD-R·BD-R** — 광 매체 (구식)
- **LTO WORM 카트리지** — 별도 모델
- **WORM Disk** — 어플라이언스
- **WORM Object Storage** — S3 Object Lock

🔐 S3 Object Lock 모드

Governance 모드 - 일반 사용자는 삭제 불가 - 특별 권한(`s3:BypassGovernanceRetention`) 보유자는 가능 - 운영 유연성 + 보안

Compliance 모드 - **누구도 삭제 불가** (Root 계정조차) - 보존 기간 동안 100% 보존 - 법정 요건·랜섬웨어 최고 방어

📋 Object Lock 설정 예시

```
Retention:
  Mode: COMPLIANCE
  RetainUntilDate: 2027-12-31
LegalHold:
  Status: ON
```

- **Retention** — 시간 기반 (만료 후 삭제 가능)
- **Legal Hold** — 무기한 (수동 해제 전까지)
- 동시 적용 가능

🎯 활용 패턴

- 금융: **Compliance 모드** + 5~10년 보관
- 공공: **Compliance** + 법정 보관 기간
- 일반 기업: **Governance** + 90일~1년
- 의료: **Compliance** + 10년+

⚠️ 주의

- 보존 기간 동안 **저장 비용 청구 지속**
- 잘못 설정하면 **수정 불가** — 신중히 적용
- 버킷 단위·객체 단위 모두 가능

3-2-1 원칙 — *백업의 황금 규칙*

3

사본 3개 보유
(원본 + 백업 2개)

2

서로 다른 매체 2종
(Disk + Tape · Disk + Cloud)

1

오프사이트 1부
(다른 건물·다른 도시·클라우드)

🧮 적용 예시 (일반 기업)

- **원본**: 운영 서버 (DAS·SAN·NAS)
- **백업 ①**: 1차 디스크 (VTL·Backup Appliance) — 사내
- **백업 ②**: Tape WORM — **사외 보관** (오프사이트)

🎯 매체 다양화의 이유

- 동일 매체는 동일 결함을 공유 (펌웨어 버그·환경 영향)
- 디스크 어레이가 전부 죽어도 Tape이 살아 있어야 함

3-2-1-1-0 — *랜섬웨어 시대의 확장판*

🔢 추가된 1과 0

+ 1 (Offline) - 오프라인·에어갭 1부 - Tape 카트리지 오프라인 보관 - 또는 Immutable Object Lock - **랜섬웨어 격리**의 최종 방어선

+ 0 (Zero Errors) - 백업 후 **검증 시 오류 0** - 자동화된 복구 시험 통과 - 체크섬 무결성 확인 - "**검증된 백업만 백업**"

🛡️ 시각화

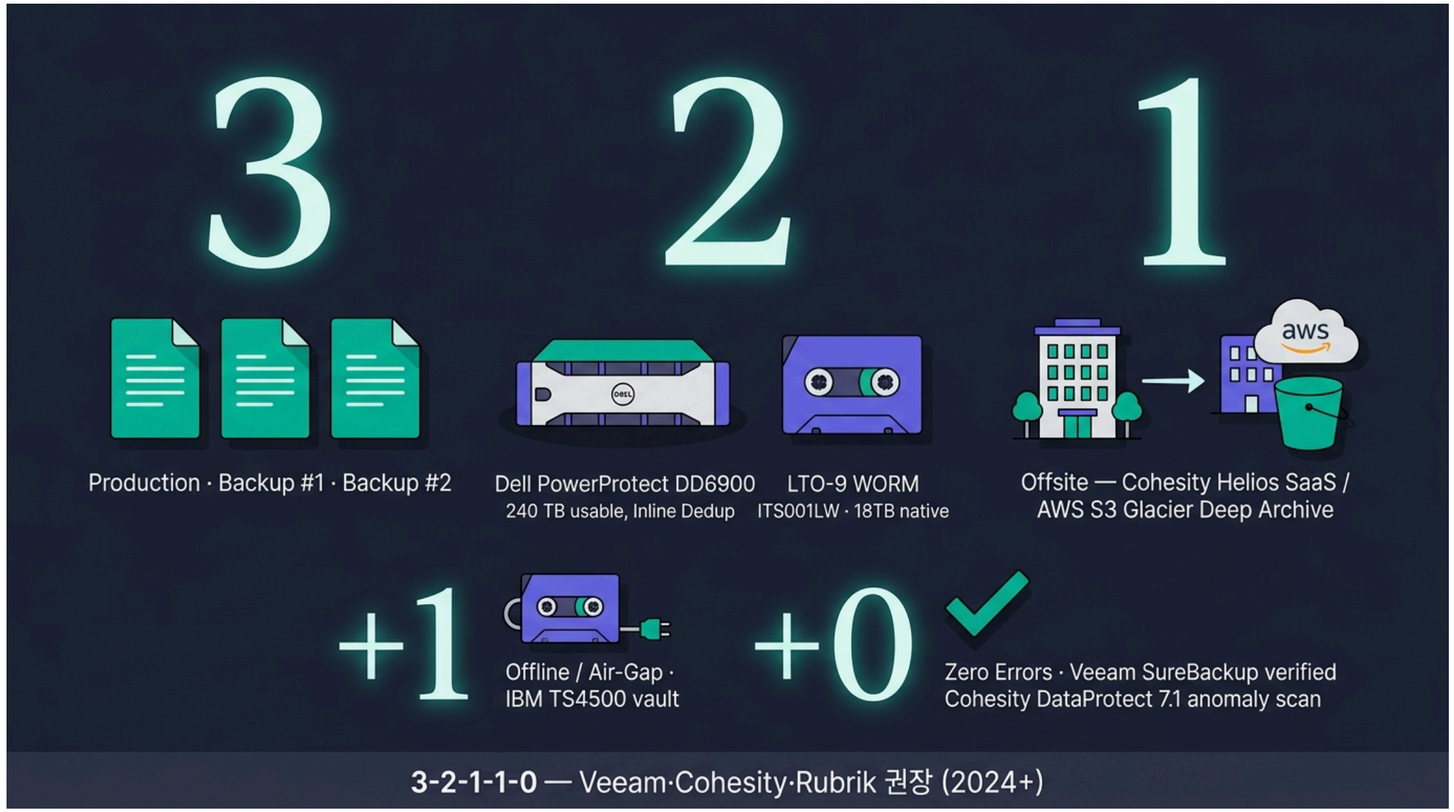
```
3 — Copies (원본+2)
2 — Different Media (Disk+Tape·Disk+Cloud)
1 — Offsite (다른 건물·도시·클라우드)
1 — Offline (Tape WORM·Immutable)
0 — Errors (검증 통과)
```

🎯 실무 매핑

- **3-2-1-1-0** 충족 = ISMS-P·금융 점검 통과 수준
- 핵심 시스템은 모두 이 수준 필수
- 일반 시스템은 **3-2-1** 만으로 충분할 수 있음

📋 점검 질문 (TA 면접 단골)

- "당신 환경의 3-2-1-1-0 수준은?"
- "마지막 검증 복구 시험 일자는?"
- "Immutable 백업 보유 여부?"



3-2-1 삽화

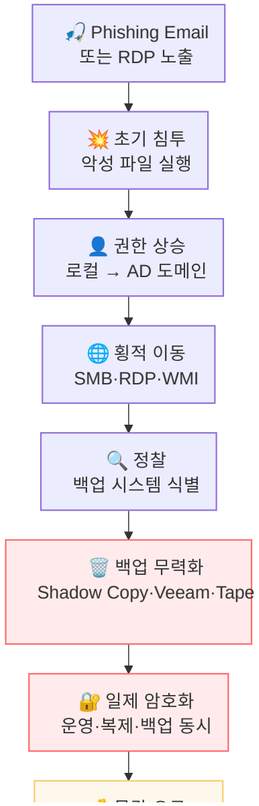
랜섬웨어 공격 시나리오 — *전형적 침투 흐름*

🦠 2020+ 사건의 공통 패턴

- 평균 잠복 기간 **수 주~수 개월**
- 백업 시스템 무력화가 **암호화보다 우선**
- AD 관리자 권한 탈취가 핵심 단계
- "백업이 있어도 **백업 시스템이 살아 있어야** 효력"

🎯 2단 공격의 본질

- 1단 — **백업 무력화** (Shadow Copy 삭제·Veeam 콘솔 침투·Tape 카탈로그 파괴)
- 2단 — **일제 암호화** (운영·복제·온라인 백업 동시)
- → Immutable·Air-Gap·Hardened Repo 가 마지막 보루



랜섬웨어 대응 SOP — *발견 시 5단계*

🚨 1단계 — Detection (탐지)

- EDR·SIEM·NDR 경보
- 사용자 신고 (파일 열리지 않음)
- 백업 Job 비정상

🛑 2단계 — Containment (격리)

- 감염 호스트 즉시 **네트워크 분리**
- AD 관리자 계정 비활성화
- 백업망 **물리 차단** (운영 영향 격리)
- 외부 인터넷 차단 (C2 통신 차단)

🔍 3단계 — Investigation (조사)

- 침투 경로·시점·범위 식별
- 감염 시점 이전 백업 확보
- 포렌식 (디스크 이미지·메모리)
- 법적 절차 (경찰·KISA 신고)

🛠️ 4단계 — Recovery (복구)

- **Immutable·Offline 백업** 확보 확인
- 깨끗한 환경(새 서버) 준비
- 백업 시점 이전으로 복구
- 시스템 단계적 재구축
- 응용 검증 후 서비스 재개

📝 5단계 — Lessons Learned

- 사고 보고서 작성
- 침투 경로 차단 (패치·정책)
- 백업 정책 강화
- 직원 보안 교육
- 모의 침투 정기화

❌ 절대 하지 말아야 할 것

- 몸값 지불 → 복호화 보장 없음
- 백업 검증 없이 운영 망 재연결
- 사건 미보고 (법적 의무)

PART G

DR (재해 복구) — *4단계 · RPO/RTO · BCP · 훈련*

> "데이터를 잃지 않는 것"이 백업이라면, "**서비스를 잃지 않는 것**"이 DR.

DR 4단계 — *Backup&Restore부터 Multi-Site Active-Active까지*

단계	명칭	핵심	RTO	RPO	비용
1	**Backup & Restore**	백업 데이터만 사외 보관, 사이트 0	**시간~일**	시간~일	**저**
2	**Pilot Light**	DR 사이트에 핵심 인프라만 가동, 데이터 복제	시간	분~시간	중
3	**Warm Standby**	축소된 운영 사이트 가동, 데이터 비동기 복제	분~시간	분	중~고
4	**Hot Standby**	운영과 동일 사양, 동기 복제	**분 단위**	**0~수 초**	고
5	**Multi-Site Active-Active**	두 사이트가 동시 운영 (트래픽 분산)	**0**	**0**	**최고**

🎯 등급별 채택 패턴

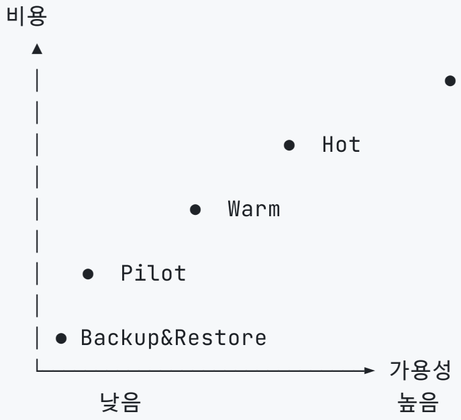
- **일반 기업**: 1~2단계 (Backup+Restore 또는 Pilot Light)
- **중요 시스템**: 3단계 (Warm)
- **금융 코어·통신**: 4단계 (Hot)
- **결제·119·재난·국방**: 5단계 (Active-Active)

> AWS 백서가 정리한 4단계 + Active-Active를 더한 **5단계 모델**이 현재 표준.

RPO · RTO 매트릭스 — *비용과 가용성의 결정표*

등급	RTO	RPO	일반 수단	추가 비용 (대략)
일반	4~24시간	24시간	일 1회 백업 (Backup&Restore)	**기본**
중요	1~4시간	1~4시간	백업 + 시간별 Snapshot (Pilot Light)	+30%
준 미션	15~60분	분 단위	비동기 복제 + 백업 (Warm Standby)	**+100%**
미션크리티컬	분 단위	0~수 초	동기 복제 + HA (Hot Standby)	**+200~400%**
무중단	**0**	**0**	사이트 이중화 + Active/Active	**+400%+**

💰 비용 vs 가용성 그래프 (개념)



BCP · DR 사이트 위치 — *지리적 거리의 의미*

🏢 BCP (Business Continuity Plan)

- DR은 IT 인프라 영역
- **BCP는 업무 연속성** — 사람·프로세스·외부 통신·물리 공간 포함
- BCP > DR > 백업·복구

📐 BIA (Business Impact Analysis)

- 업무별 중단 시 영향도 분석
- MTPD (Maximum Tolerable Period of Disruption)
- 등급별 우선순위
- → DR 등급 결정의 출발점

🏗️ DR 사이트 위치 결정 변수

- **거리** — 동일 재해 영향 회피
- **네트워크 비용** — 거리 ∝ 회선료
- **법규** — 금융 30km+ (전자금융감독규정)
- **인력 가용성** — 원격 운영 가능 여부

🗺️ 한국 DR 사이트 표준

등급	거리 권고	예시
일반	도시 내	서울 강남 ↔ 강서
중요	**30km+**	서울 ↔ 일산·분당
미션크리티컬	**수도권 분산**	서울 ↔ 천안·대전
국가 핵심	**전국 분산**	서울 ↔ 부산·광주
글로벌	**국가 간**	한국 ↔ 일본·싱가포르

⚖️ 거리의 트레이드오프

- 동기 복제 가능 한계 = **~100km** (지연 5ms 이내)
- 100km+ → 비동기 복제 필수
- 1000km+ → 회선 비용 폭증

🎯 권고

- 동일 지진대·동일 전력망·동일 통신망 회피
- 통신 회선 **물리적 이중화** (2개 통신사·2개 경로)

DR 훈련 5단계 — *Tabletop부터 Full Interruption까지*

훈련	정의	운영 영향	비용	주기 권고
1. Tabletop	회의실에서 시나리오 토론·점검	**없음**	매우 낮음	분기 1회
2. Walkthrough	절차서 따라 단계별 시뮬레이션 (실행 X)	없음	낮음	반기 1회
3. Simulation	격리 환경에서 일부 시스템 실제 절체 시뮬레이션	낮음	중	반기~연 1회
4. Parallel	DR 사이트 동시 운영, 트래픽은 운영에만	낮음	중~높	**연 1회+**
5. Full Interruption	운영 중단 + DR로 완전 절체	**있음**	매우 높음	**2~5년 1회**

🎯 권장 운영

- 분기: **Tabletop** (가벼운 검토)
- 반기: **Walkthrough** + 부분 **Simulation**
- 연: **Parallel** + 산출물 갱신
- 2~5년: **Full Interruption** (대형 변경 시)

📋 훈련 시 점검 항목

- 실측 RTO·RPO (vs 목표)
- 절차서 일치도
- 인력 가용성 (휴가·교대)
- 통신·이해관계자 알림 절차

재해 시나리오 — *우리가 대비해야 할 7가지*

🔥 화재

- 가장 흔한 데이터센터 재해
- 진압 후에도 **수증기·연기·연쇄 누전**
- 화재진압 가스 (FM-200·Inergen·Novec-1230) 후 환기 필요
- **수 시간~수일** 복구 불가
- → DR 사이트 절체 필요

💧 침수

- 1층·지하 데이터센터 위험
- 누수 감지기 필수
- 폭우·태풍·내부 배관 파열
- 한 번 침수되면 장비 거의 폐기

🌍 지진

- 한국도 안전지대 아님 (포항·경주)
- 진동 차단·내진 설계 필수
- 동일 지진대 회피 → **DR 거리 결정 요인**

⚡ 정전 (장기)

- UPS·발전기로 단기 대응
- 디젤 발전기 연료 = 보통 **8~24시간분**
- 장기 정전(수일+) = 운영 중단
- 한전 2회선·자가발전 + DR 필요

📡 통신 케이블 단절

- 광케이블 굴착 사고
- 통신사 1개 의존 = 리스크
- **2개 통신사·2개 물리 경로** 필수
- 수 시간~수일 복구

🦠 랜섬웨어

- 21세기 가장 빈번한 "재해"
- 기술 사고가 아닌 **공격**
- Immutable·Air-Gap 필수
- BCP 시나리오 1순위

🦠 팬데믹·인력 불가

- COVID-19 사례
- 원격 운영 체계 필수
- 출입 인력 격리·교대
- 데이터센터 운영 BCP 별도

🏗️ 건물·시설 재해

- 천장 누수·에어컨 고장
- 전력 분전반 사고
- 시설 노후화

🎯 시나리오별 대응 매트릭스

재해	백업	복제	DR 사이트
화재	△	○	◎
침수	△	○	◎
지진	△	△ (거리)	◎
정전	△	○	◎
통신 단절	×	×	◎
랜섬웨어	◎	×	△
팬데믹	×	×	△

DR 비용 산정 사례 — *현실적 숫자로 보기*

🎯 가상 사례: 중규모 SaaS 기업

- 운영 사이트: 서울 (자체 데이터센터)
- 핵심 워크로드: 웹 + DB(Oracle) + 파일 + 백업
- 목표 RTO 1시간 · RPO 5분 → **Warm Standby + Async 복제**

💰 초기 구축 비용 (CapEx)

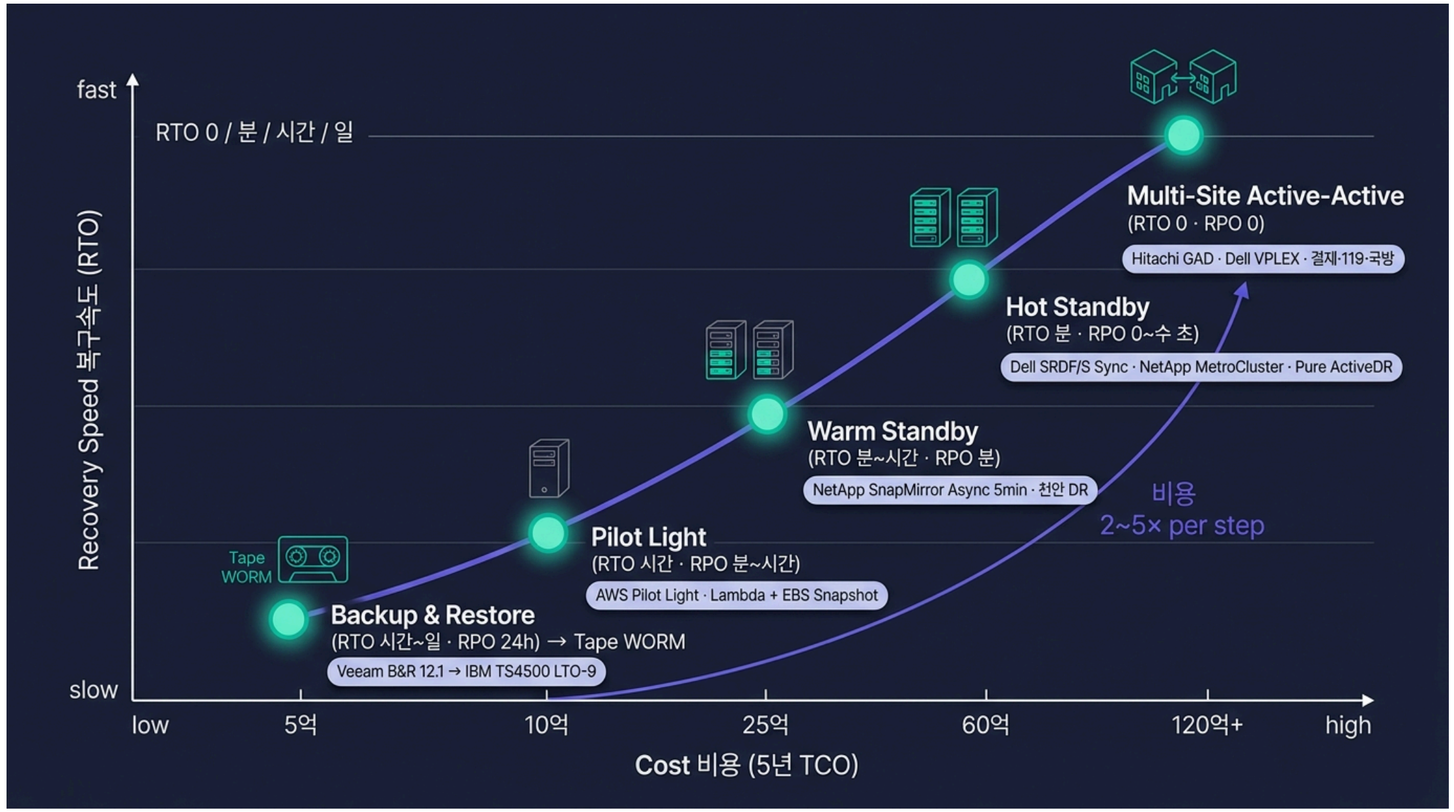
항목	비용 (대략)
DR 사이트 임대 (코로케이션)	5,000만 원 (랙 5개)
DR 서버 (운영의 60% 사양)	3억 원
DR 스토리지 (운영의 70% 용량)	2억 원
DR NW 장비 (FW·SW·LB)	1억 원
사이트 간 회선 (전용선 100Mbps)	초기 3,000만 원
DR 백업 (Immutable·Tape)	1억 원
DR 솔루션·라이센스	1억 원
합계	**약 8억 5천**

🔁 운영 비용 (OpEx, 연간)

항목	비용 (대략)
코로케이션 임대 + 전력	6,000만 원/년
회선료 (전용선 100Mbps)	4,800만 원/년
유지보수 (HW·SW)	1.5억 원/년
DR 훈련 비용	2,000만 원/년
인력 (DR 운영 0.5명)	5,000만 원/년
연 합계	**약 3.5억**

📊 5년 TCO

- 초기 8.5억 + 운영 17.5억 = **약 26억**
- 동일 가용성 클라우드 DR = 약 20~25억 (지속)
- 비교: 자체 DR vs AWS DR vs DRaaS



DR 4단계 매트릭스 삽화

PART H

산출물 · 결정 — *TA가 만들고 결정하는 것*

> 스토리지·백업·DR 설계는 결국 **숫자와 정책의 문서화**.

TA가 스토리지·백업 설계에서 내리는 12가지 결정

1️⃣ 스토리지 유형

- 워크로드별 6대 유형 매핑
- SAN vs HCI vs Object

2️⃣ 프로토콜

- FC vs iSCSI vs NVMe-oF
- NFS vs SMB

3️⃣ RAID 레벨

- DB = RAID 10
- 대용량 = RAID 6 / EC

4️⃣ Snapshot 정책

- 주기·보관 기간
- CoW vs RoW (벤더 종속)

5️⃣ Replication 모드

- Sync vs Async
- 거리·RPO

6️⃣ Dedup·Compression

- Inline vs Post
- 실효 절감률 보수적 산정

7️⃣ Thin vs Thick

- 워크로드별
- 모니터링 정책

8️⃣ 백업 정책

- Full·Inc·Synthetic·Forever
- GFS 보관 기간

9️⃣ 백업 매체 3계층

- 1차 Disk/VTL · 2차 Object Lock · 3차 Tape WORM

🔟 Immutable·Air-Gap

- 매체별 구현
- Compliance vs Governance

1️⃣1️⃣ DR 단계 결정

- 4단계 + Active-Active 중 선택
- BIA 기반

1️⃣2️⃣ 훈련 정책

- Tabletop·Walkthrough·Simulation·Parallel·Full
- 주기 + KPI

> 이 12가지가 곧 **스토리지·백업·DR 설계서의 목차**.

산출물 ① — *스토리지 BOM (Bill of Materials)*

분류	모델	수량	단가	합계	비고
SAN 어레이	Dell PowerStore 1200T	1	4억 원	4억	이중 컨트롤러
디스크 (NVMe SSD)	1.92TB NVMe TLC	24	200만	4,800만	RAID 6 (22+2)
디스크 (SAS HDD)	8TB 7.2K SAS	36	50만	1,800만	RAID 6 (16+2) × 2
SAN Switch (Director)	Brocade X7-4	2	1.5억	3억	Fabric A/B 이중화
HBA	Emulex LPe35002 32G FC	16	80만	1,280만	호스트당 2개 × 8호스트
광 케이블·SFP+	32G FC LC-LC 5m	32	5만	160만	양단 결선
VTL/백업 어레이	Dell DD6900 (240TB usable)	1	2.5억	2.5억	Inline Dedup
Tape Library	Dell TL4000 (LTO-9, 48슬롯)	1	8,000만	8,000만	WORM 카트리지 24매
백업 SW 라이센스	Veeam Universal License (VUL)	50	100만/VM	5,000만	5년
유지보수 (5년)	HW·SW 통합	—	—	4억	24×7 4hr 응대
합계				**약 17억**	—

📋 BOM 작성 체크리스트

- 모델·세대·펌웨어 명시
- 수량·단가·합계
- 유지보수 기간·SLA 등급
- 케이블·광 모듈 등 부속품 누락 방지
- 라이센스 모델 (Per-Capacity·Per-VM·Per-Node)

산출물 ② — *백업 정책표*

시스템	등급	정책	주기	보관	매체	RTO	RPO	검증
핵심 DB (Oracle)	Tier-1	Hot+RMAN	일별 Inc, 주 1 Full	30일/90일/연	VTL+Object Lock+Tape	1h	5m	일 1회 자동
VM (운영)	Tier-1	Veeam Forever Inc	매 4시간 Inc	30일/52주/7년	VTL+Object Lock	30m	4h	일 1회 SureBackup
파일 서버	Tier-2	Full + Diff	주 1 Full, 일 Diff	30일/12주/3년	VTL+Tape	4h	24h	주 1회
로그·아카이브	Tier-3	Inc	일별 Inc	90일/3년	Object Cold	24h	24h	월 1회
개발·테스트	Tier-4	Full	주 1 Full	4주	VTL only	24h	7d	월 1회

📋 정책표 구성 요소

- **시스템·등급**
- **백업 정책** (방식 + 솔루션)
- **주기 + 보관 기간** (GFS)
- **매체** (3계층 매핑)
- **RTO/RPO** (목표)
- **검증 주기·방법**

🎯 권고

- 핵심 시스템은 **3계층 매체 + 자동 검증**
- 일반 시스템은 **2계층 + 수동 분기 검증**
- 정책표는 **분기 1회 갱신**

산출물 ③ — *DR 설계서 (목차)*

📑 DR 설계서 목차

1. **사업 개요·범위**
2. **BIA (Business Impact Analysis)** - 핵심 업무 목록 - 중단 시 영향도 - MTPD·RTO·RPO 도출
3. **DR 등급 결정** - 4단계 중 선택 근거 - 비용 산정
4. **DR 사이트 위치·계약** - 거리·통신·접근성 - 코로케이션 vs 자체
5. **DR 아키텍처** - 인프라 구성도 - 복제·동기화 방식 - 네트워크 토폴로지
6. **절체 절차** - Failover 절차 - Failback 절차 - 의사결정자·승인자
7. **데이터 동기화 모니터링** - 복제 지연·오류 알람 - RPO 실측
8. **DR 훈련 계획** - 5단계 훈련 주기 - 실측 결과 기록
9. **이해관계자 통신** - 사고 시 알림 흐름 - 외부 통신 (고객·언론·당국)
10. **사후 검토·개선**
    - 훈련 결과 반영
    - 설계서 갱신

🎯 산출물 권고 분량

- 본문: 80~150 페이지
- 별첨: 절차서·연락처·점검표

산출물 ④ — *랜섬웨어 대응 SOP*

📜 SOP 구성

1. **목적·범위**
2. **역할 정의** - CISO·CIO·TA·운영팀·홍보팀·법무팀 - 외부 연락처 (KISA·경찰·MSSP)
3. **탐지 기준** - EDR·SIEM 경보 조건 - 사용자 신고 채널
4. **초동 격리 절차** - 호스트 분리·계정 비활성화 - 백업망 차단 의사결정자
5. **조사·증거 보전** - 디스크 이미지·메모리 덤프 - 로그 보존
6. **복구 절차** - Immutable 백업 식별 - 복구 우선순위 - 단계별 시스템 재구축
7. **외부 통신** - KISA 신고 (24시간 내) - 개인정보 유출 시 통지 - 고객·언론 응대
8. **사후 조치** - RCA 보고서 - 정책·인프라 강화 - 직원 교육
9. **체크리스트·점검표**
10. **연락처·에스컬레이션 매트릭스**

🎯 SOP 권고

- **분기 1회 검토·갱신**
- 모의 침해 훈련 시 SOP 따라가기
- 인쇄본도 비치 (NW 차단 시 디지털 접근 불가)

케이스 미니 ① — *DB 데이터 손실 시나리오*

🚨 상황

- 운영자 실수로 핵심 테이블 DELETE
- **동기 복제본도 함께 삭제** (사이트 B에도 적용됨)
- 백업: 전일 야간 Full (자정)
- 사고 시점: **당일 14:00**

❓ TA가 던지는 질문

1. RTO·RPO 등급은?
2. **시점 복구(PiTR) 가능한 DB**인가?
3. 트랜잭션 로그 보관 여부
4. 백업 + 로그로 14:00 직전 복구 가능?
5. 전체 롤백 vs 부분 복구?

✅ 대응 절차

1. **격리** — 추가 변경 차단 (운영 일시 중지)
2. **Snapshot** 확보 (있다면)
3. **복구 결정** - Full + Archive Log → 13:59 시점 복구 - 별도 인스턴스에 복구 후 데이터만 추출 → 운영 인스턴스에 INSERT
4. **검증** — 데이터 정합성
5. **서비스 재개**
6. **사후 보고** — 사용자 권한 재검토·감사 로그 강화

📌 교훈

- **복제 ≠ 백업** — 본 시나리오가 정답
- 트랜잭션 로그 백업이 PiTR의 전제
- DB Native Backup이 일반 백업보다 우선

케이스 미니 ② — *랜섬웨어로 백업까지 암호화*

🦠 상황

- 운영 서버·파일·NAS 일제 암호화
- 백업 디스크도 함께 암호화 (네트워크 마운트 상태)
- 동기 복제본도 암호화 상태로 복사됨
- → 일반 백업·복제 전부 무력화

🛡️ 보존된 자원

- **오프라인 Tape WORM** (격리 보관)
- **S3 Object Lock (Compliance)** Immutable
- **Veeam Hardened Linux Repository** (변경 불가)
- → 3중 Immutable 중 일부 살아남음

✅ 대응 절차

1. **격리** — 전체 NW 차단, 외부 인터넷 차단
2. **조사** — 침투 시점 파악 (감염 이전 백업 확보)
3. **깨끗한 환경 준비** — 신규 서버·OS·NW 분리
4. **복구**: - Tape 또는 Object Lock에서 마지막 정상 백업 복구 - 감염 시점 이전 데이터로 환원
5. **검증** — 악성코드 잔존 검사
6. **단계적 서비스 재개**
7. **KISA·경찰 신고** (의무)

📌 교훈

- "복제 + 백업 디스크"만 있으면 무력
- **Immutable + Offline** 2중이 최종 방어선
- 사후 침투 경로 차단·직원 교육·정기 훈련

케이스 미니 ③ — *전력 장기 정전으로 DR 절체*

⚡ 상황

- 강남 운영 사이트 인근 변전소 화재
- 한전 2회선 모두 동시 차단
- UPS 30분 + 자가발전기 가동
- 발전기 연료 12시간분 → **장기화 우려**
- 운영팀 DR 절체 결정

🎯 RTO/RPO 목표

- 운영 RTO 1시간 / RPO 5분
- DR 사이트: 천안 (Warm Standby + 비동기 복제)

✅ 절체 절차

1. **결정** — CIO 승인 (사전 정의된 의사결정 매트릭스)
2. **고객 통지** — 점검 안내 (전화·SMS·홈페이지)
3. **DB 비동기 복제 종료** — 마지막 복제분 적용
4. **DR DB 활성화** — Read-Only → Read-Write 전환
5. **DNS 변경 / GSLB 전환** — 트래픽 DR로
6. **응용 서비스 가동** — 미리 준비된 인스턴스
7. **검증** — 헬스체크·기본 트랜잭션
8. **서비스 재개** — 30분 내
9. **사후**: - 실측 RTO/RPO 기록 - Failback 일정 수립 - 운영 사이트 복전·검증 후 Failback

📌 교훈

- 절체 자체보다 **Failback**이 어려움
- 정기 훈련이 실측 시간 단축의 유일한 방법

워크로드별 권장 매핑 — *한 페이지 결정표*

워크로드	스토리지	RAID	백업	DR
OS 부팅 디스크	DAS NVMe	RAID 1	이미지 백업 (월)	DR 사이트 동일 구성
Web/WAS 로컬	DAS SSD	RAID 10	VM 백업 (일)	Pilot Light
DB (Oracle/MSSQL) — 핵심	**SAN FC**	**RAID 10**	RMAN + Veeam, 매 4시간	**Hot Standby + Sync**
DB (NoSQL·Cassandra·Mongo)	DAS NVMe·HCI	RAID 10 / EC	Native + Snapshot	Multi-DC Replication
VMware 데이터스토어	SAN / HCI	RAID 6/10	Veeam VBR (일)	Warm Standby
파일 공유 (홈디렉·문서)	NAS NFS/SMB	RAID 6	NDMP (일)	Async Replication
미디어·영상 마스터	Scale-Out NAS·Object	EC	LTFS Tape (월)	Backup&Restore
로그·이벤트	Object Cold	EC	Lifecycle (자동)	Object Replication
백업 1차 매체	VTL/Backup Appliance	RAID 6	—	Tape + Object Lock
백업 2차 매체	Object Lock	EC	—	Cros6-Region Replication
백업 3차 매체	LTO WORM	—	—	Offsite 보관
캐시·임시	DAS NVMe	RAID 0 (or none)	백업 안 함	재생성
AI 학습 데이터	Scale-Out NAS·Lustre·BeeGFS	EC	데이터셋 백업 (Object)	별도 정책

> 표 한 장이 곧 **워크숍·면접·실무**의 기준점.

자주 보는 안티패턴 — *피해야 할 8가지*

❌ 1. RAID = 백업

- RAID는 디스크 결함 대응만
- 사용자 실수·랜섬웨어 무력

❌ 2. 복제 = 백업

- 동기·비동기 모두 실수도 함께 복제
- 시점 복구 불가

❌ 3. Snapshot = 백업

- 어레이 자체 장애 시 함께 손실

❌ 4. 백업 = 복구 검증

- 백업 Job 성공 ≠ 실제 복구 가능
- 분기 1회 복구 시험 필수

❌ 5. Thin Provisioning 무한 과할당

- 실사용량 모니터링 누락
- 100% 도달 시 일제 정지

❌ 6. 모든 시스템 = 미션크리티컬

- 비용 비현실적
- BIA로 등급 분류 필수

❌ 7. 백업 디스크에만 의존

- 랜섬웨어가 NW 마운트 백업 같이 암호화
- Immutable + Offline 1중 이상 필수

❌ 8. DR 사이트 = 백업·복구의 끝

- 정기 훈련 없는 DR은 무용
- 절체 절차·인력 가용성 동반 필요

외부 규제 · 표준 — *백업·DR이 요구되는 근거*

📜 국내 규제

- **전자금융감독규정** (금융위)
- 금융 DR 사이트 30km+
- 일 1회 이상 백업
- 분기 1회 모의 훈련
- **개인정보보호법**
- 백업·복구 가능한 수단
- 안전한 보관·파기
- **정보통신망법**
- 침해사고 24시간 내 신고
- **공공 SW 사업 데이터 요구사항**
- 백업·보관 기간 명시

🏆 국내 인증

- **ISMS-P** — 정보보호·개인정보보호 관리체계
- 백업·복구 항목 점검
- **CSAP** — 클라우드 보안
- 백업·DR 요건

🌍 국제 표준

- **ISO 27001** — 정보보호 관리체계
- 2.9.3 백업
- A.17 BCP
- **ISO 22301** — BCM (사업연속성 관리)
- **NIST SP 800-34** — Contingency Planning
- **NIST CSF** — Recover 기능
- **PCI-DSS** — 카드사 보안
- **HIPAA** — 의료 데이터 보안
- **GDPR** — 데이터 보호

🎯 TA의 점검 포인트

- 자사 적용 규제 목록 작성
- 규제별 백업·DR 요건 매트릭스
- 정기 점검 (분기·연)
- 인증 갱신 일정 관리

Session 6 정리 — *오늘 확보한 시야 7가지*

① 스토리지 6대 유형

DAS·NAS·SAN·Object·HCI·SDS — 워크로드별 매핑

② SAN 패브릭

Director·Edge·Zoning·NPIV·WWN

③ RAID + 안전망

RAID 6/10·Hot Spare·Rebuild = 디스크 결함 안전망

④ 고급 기능

Snapshot·Replication·Dedup·Tiering·Thin Provisioning

⑤ Tape 르네상스

LTO-9·LTFS·VTL·WORM·D2D2T·D2D2C

⑥ 백업 정책 + 3-2-1-1-0

6종 정책·GFS·Immutable·Hardened·Air-Gap

⑦ DR 4단계 + 훈련 5단계

BIA → 등급 → 사이트 → 절체 → 훈련 → 사후

🎯 핵심 메시지

- **RAID + 백업 + 복제 + Immutable + DR = 5중 안전망**
- **검증되지 않은 백업은 존재하지 않는 백업**
- **RPO/RTO는 요건, 수단은 TA가 설계**