

Storage Technologies

IT403

Prepared by
Dr. Ahmed El-Douh

Lecture 9



Storage Technologies

Lecture 9

IT403

Disaster Recovery Technology and Its Applications

Prepared by
Dr. Ahmed El-Douh

Objectives

Upon completion of this module, you will be able to:

- Describe the concepts and importance of Disaster Recovery.
- Differentiate the Advantages and Disadvantages of common Disaster Recovery solutions.
- Understand the technical principles of Disaster Recovery solutions.
- Learn how to deploy a Disaster Recovery solution through case study of typical application of Disaster Recovery Solution.

Outlines

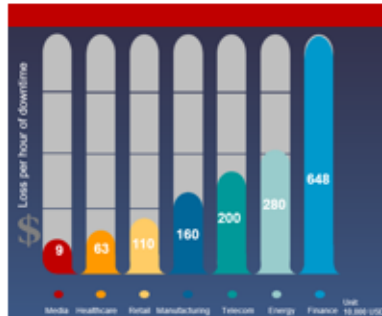
- Overview of Disaster Recovery Solution.
- Architecture of Disaster Recovery Solution.
- Common Disaster Recovery Technologies.

Chapter
09

Overview of Disaster Recovery Solution



Demand For Disaster Recovery



Enterprises: Avoiding major losses and reducing corporate risks.



Enterprises: Comply with laws and regulations and meet industry regulatory requirements.



IT: Simplify operation and maintenance work and avoid major impact of sudden incidents or disaster.

- Three Major Risks: Data Loss, Data Corruption, Service Interruption. Each hour of service interruption can cause losses worth millions of dollars for enterprises.
- Regulatory Compliance: Financial Compliance, Tier 3 Protection, Security Isolation, 3DC, High Business Continuity
- IT Operation and Maintenance: The system is disaster-tolerant and ready for use, simplifies IT operation and maintenance, and avoids the impact of sudden disasters.

Challenges Of Disaster Recovery

Costly Investment

High CAPEX

- High cost of infrastructure, servers, storage and software.
- High cost of building server rooms and facilities.

High OPEX

- Professional O&M Support (Implement/Train/Live Support)
- Long term investments for resources such as water and electricity.



Complex Management

Multiple Devices and Non Unified Management

- Storage media, servers, network management are independent, complex workflows, and low efficiency.

Complex Expansion

- Cycle for online expansion is too long when the capacity is low and requires auto expansion.



Limited DR Capability

Insufficient Safety and DR Capabilities

- Backup data is not out of the data center, and infrastructure failures can easily lead to extreme conditions.

Insufficient Flexibility

- Disaster recovery, data sharing and other capabilities are limited by the physical location of the data. Applications and data cannot be separated, and thus agile applications and better disaster recovery features cannot be built.



What is HA ?

- **HA (High Availability)** refers to the ability to provide continued access to applications in the event of a single component failure in the local system. No matter this fault is a failure of business processes, physical facilities, or IT hardware/software.
- The best high availability is when a machine in the data center is down, but users who use the data center services are completely unaware of it. However, when the data center's machine is down, the service failover for the services running on the machine generally takes some time, which leads to the customer's perception of the downtime.
- The key indicator of **HA** is usability. Its calculation formula is $[1 - (\text{downtime})/(\text{downtime} + \text{uptime})]$. We often use a few 9s for availability measurement:
 - Four 9s: $99.99\% = 0.01\% * 365 * 24 * 60 = 52.56 \text{ minutes/year downtime.}$
 - Five 9s : $99.999\% = 0.001\% * 365 = 5.265 \text{ minutes/year downtime.}$
 - Six 9s : $99.9999\% = 0.0001\% * 365 = 31 \text{ seconds/year downtime.}$
- For HA, shared storage is often used. In this case, **RPO** =0. At the same time, Active/Active (active-active cluster) HA mode is often used to make **RTO** almost 0. If Active/Passive mode HA is used, then the RTO is needed to be reduced to the minimum.

What is Disaster Recovery (DR)?

- **Disaster** is caused by man-made or natural reasons, causing a serious failure or corruption of an information system within a data center, that suspends service functions supported by the information system, or cause unacceptable service levels for a specific period of time that occurred in a sudden event. This often leads to an information system that needs to be switched to an alternate site for operation.
- **Disaster recovery** refers to the ability to recover data, applications, or services in data centers in different locations when a disaster destroys a production center.
- **Disaster recovery** means that, in addition to the production site, redundant sites established by users, when a disaster occurs and the production site is damaged, the redundant sites can take over the normal services of the users and achieve uninterrupted services. In order to achieve higher availability, many users even set up multiple redundant sites.

The Relationship between HA and DR (1)

- The two are related to each other, complement each other, and intercross with each other, but at the same time have with significant differences between them:

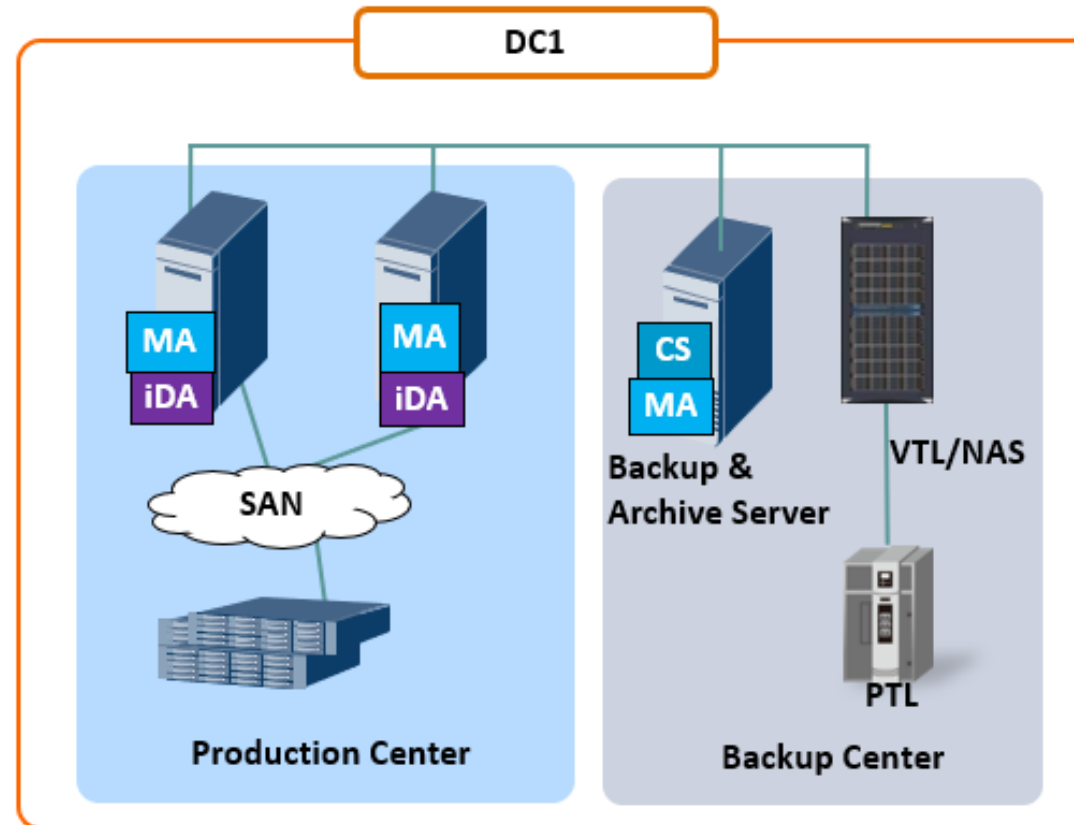
Dimension	HA(High Availability)	DR (Disaster Recovery)
Scenarios	HA refers to the local high availability system, which means that in the case of multiple servers running one or more applications, it should ensure that when any of the server fails, the application it runs won't be interrupted, and the application and system should be able to quickly switch over to operate on another server, which resides within the local system cluster and hot backup.	DR refers to highly available systems in different places (in the same city or different places), indicating the ability to recover data, applications, and services in the event of a disaster.

The Relationship between HA and DR (2)

Dimension	HA(High Availability)	DR(Disaster Recovery)
Storage	HA often uses shared storage, which means there is no lost of data (RPO=0), more considerations are on the RTO due to the time period taken for service switching/failover.	Off-site disaster recovery data recovery uses data replication. According to the different data replication technologies used (synchronous and asynchronous), data loss often results in $RPO > 0$; while off-site application switching often takes longer, so $RTO > 0$.
Faults	Mainly handles single-component failures causing the load to switch between servers in the cluster.	Copes with large-scale failures causing the load to switch between data centers.
Network	LAN scaling tasks are within the category of HA.	WAN scaling tasks are within the category of DR.
Cloud	HA is a mechanism for ensuring business continuity within a cloud environment.	DR is a mechanism for ensuring business continuity among multiple cloud environments.
Objective	HA's main purpose is to ensure that the business/service is highly available.	DR is a business continuity solution that is based on reliable data protection.

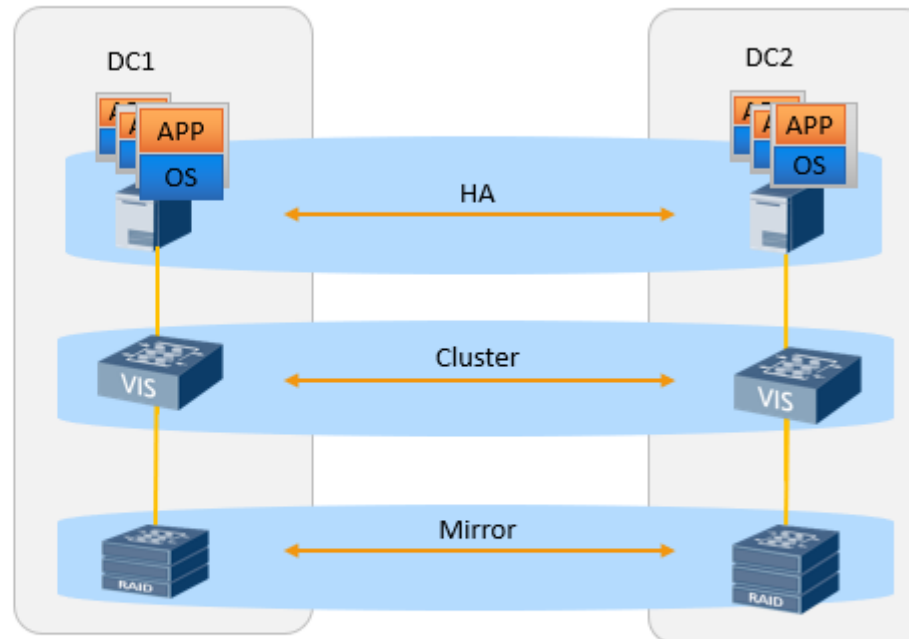
Differences Between DR & Backups (1)

- **Backup:** Backup is the fundamental basis of disaster recovery, it mainly refers to the process where all or part of the data collected from the application host's hard drive or storage arrays are replicated to other storage media.



Differences Between DR & Backups (2)

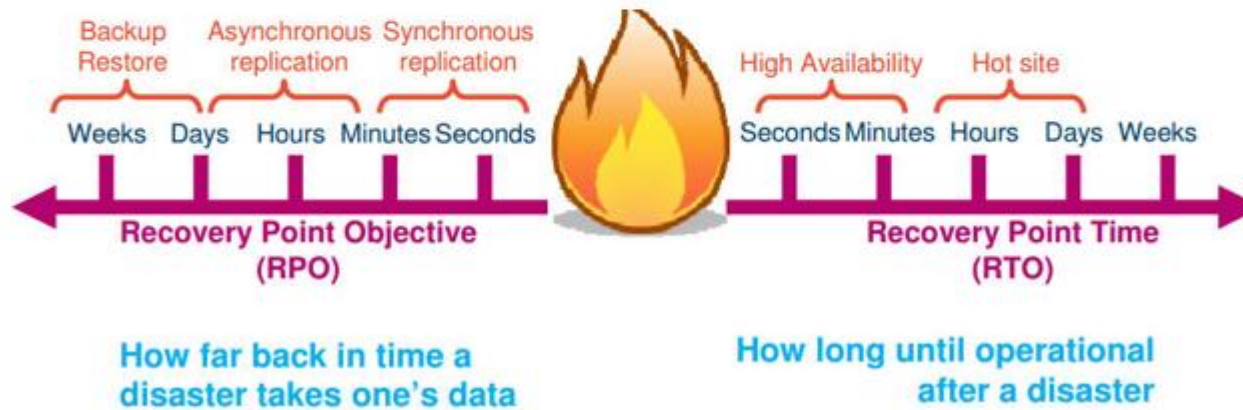
- **Disaster recovery:** Disaster recovery system refers to the establishment of two or more sets of IT systems with the same function in remote locations separated from each other. Health status monitoring and function switching can be performed between them. When a system stops working due to the event of disaster (such as fire, earthquake), the entire application system can be switched to another place so that the system function can continue to work normally.



- Generally, disaster recovery refers to backup of data or application systems that are not in the same server room or location. Backup refers to local data or system backups.
- In general, DR combines disaster recovery with backup, which is, local backup combined with remote data replication to achieve perfect data protection.

Key Indicators For Measuring DR System Performance

- RPO (Recovery Point Objective) represents the amount of data that is allowed to be lost when a disaster occurs.
- RTO (Recovery Time Object) represents the system recovery time.
- The smaller the RPO and RTO, the higher the availability of the system and the greater the investment required by the user.



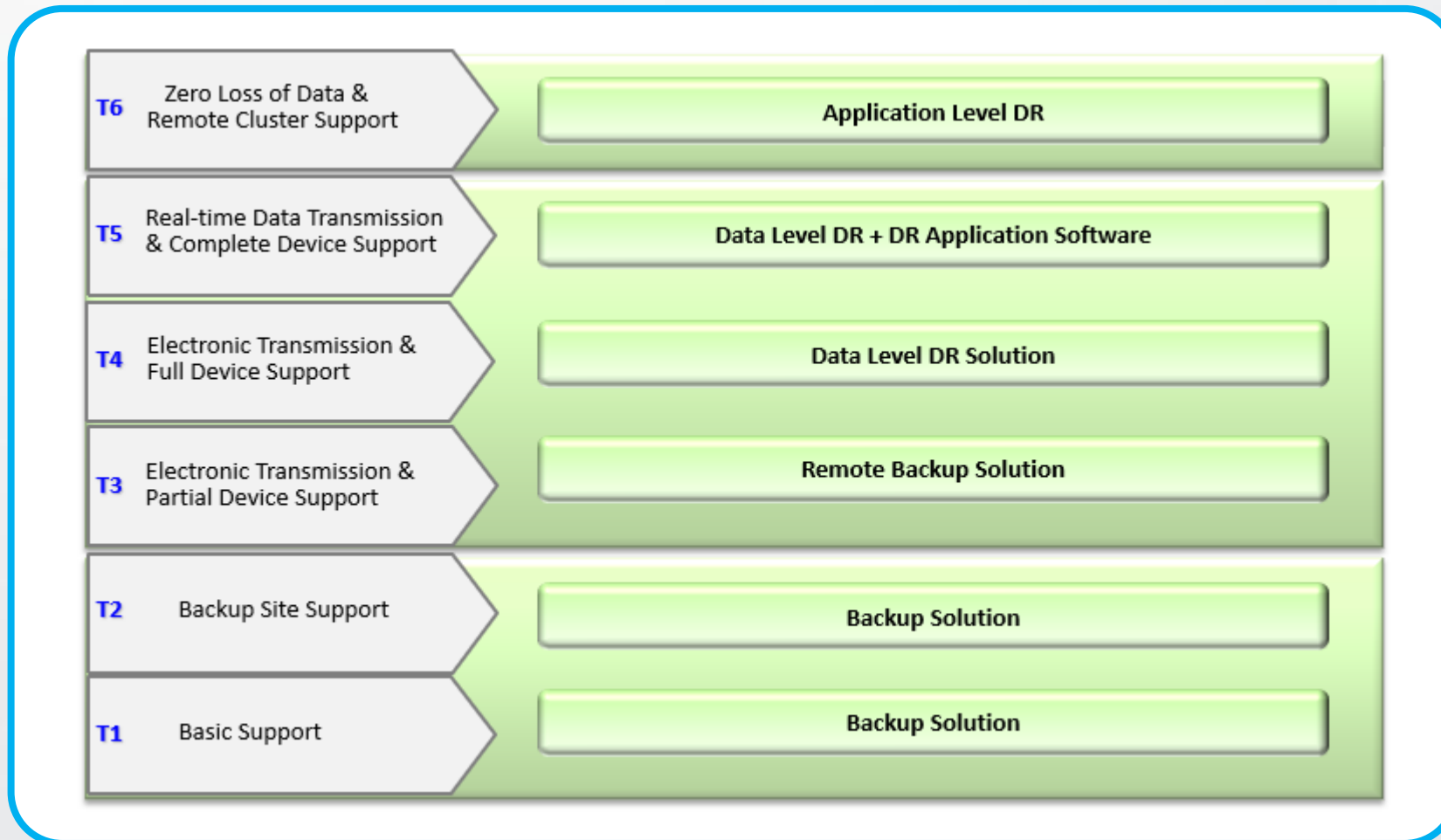
Levels Of DR Systems

Level	Definition	RTO	TCO
Data Level	- Through the establishment of remote disaster recovery centers, remote backup of data will be performed to ensure that the original data will not be lost or destroyed after the disaster. - In the data-level disaster recovery mode, the established disaster recovery center can be simply considered as a remote data backup center. At the data-level disaster recovery level, applications are interrupted when a disaster occurs. - Data-level disaster recovery has a long recovery time, but its cost is lower than other disaster recovery levels, and its implementation is relatively simple. - Data sources are the source of life for all critical business systems, so data-level disaster recovery is essential.	The longest RTO (several days) because after the disaster, the equipment needs to be redeployed to recover the business services using backup data.	Lowest

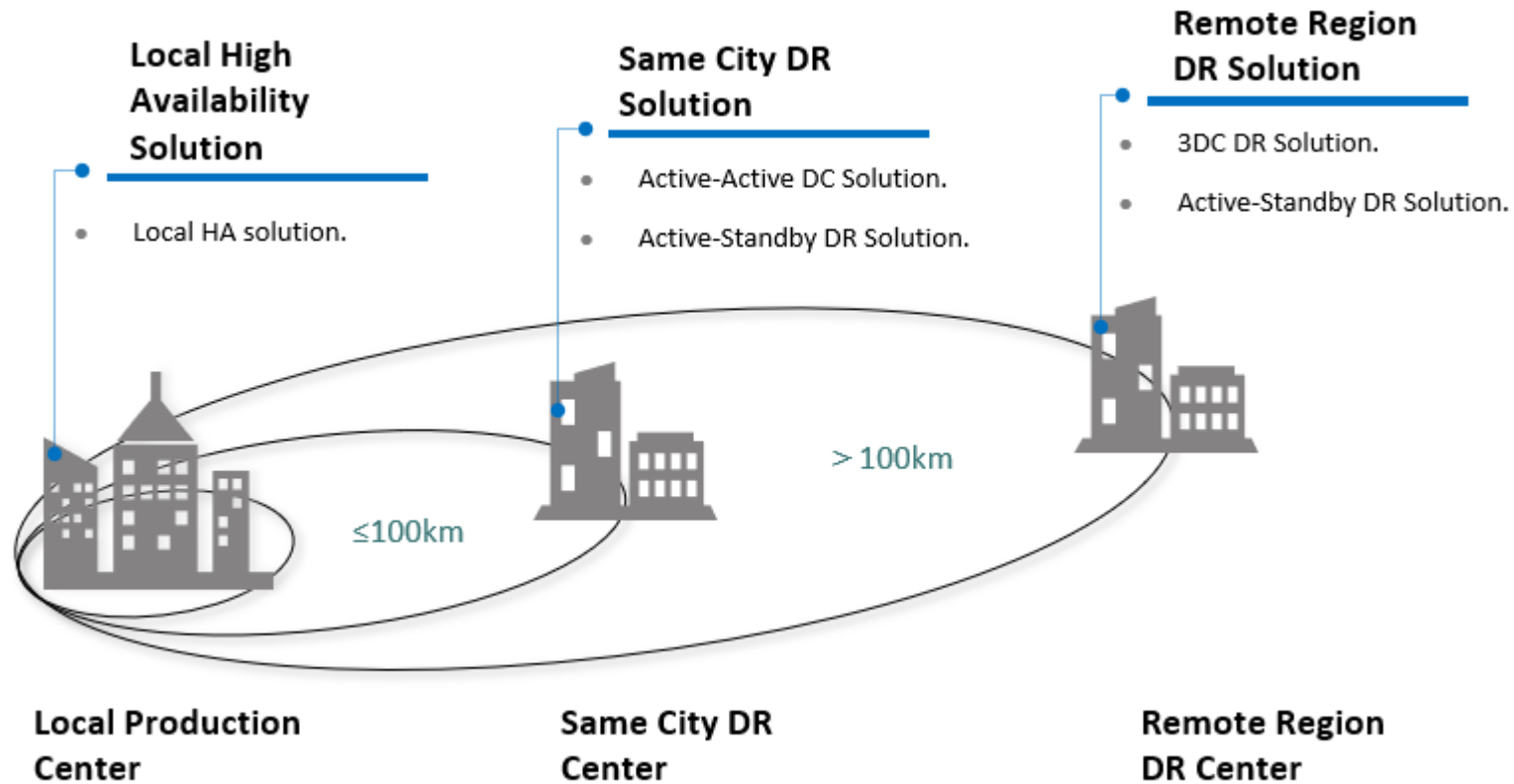
Levels Of DR Systems

Level	Definition	RTO	TCO
Application Level	On the basis of data-level disaster recovery, similar sets of application systems are also built at the backup site. Through synchronous or asynchronous replication technology, key applications can be guaranteed to recover within the allowable time range, minimizing the loss caused by disasters, and allows users to be unaware of the disaster. Thus, the services provided by the system are complete, reliable and safe.	Medium RTO (Few Hours)	Medium. Same or similar system or subsystems is built offsite.
Service Level	In addition to the necessary IT-related technologies, full-service disaster recovery requires full infrastructure. Most of its components are non-IT systems (such as telephones, office locations, etc.). When a catastrophe occurs, the original office space will be destroyed. In addition to the restoration of data and applications, a back-up workplace needs to be provided so business can be conducted as usual.	Smallest RTO (Few Minutes or Seconds)	Highest

Benchmark Analysis Of DR Construction Levels



Panorama Of DR Solution

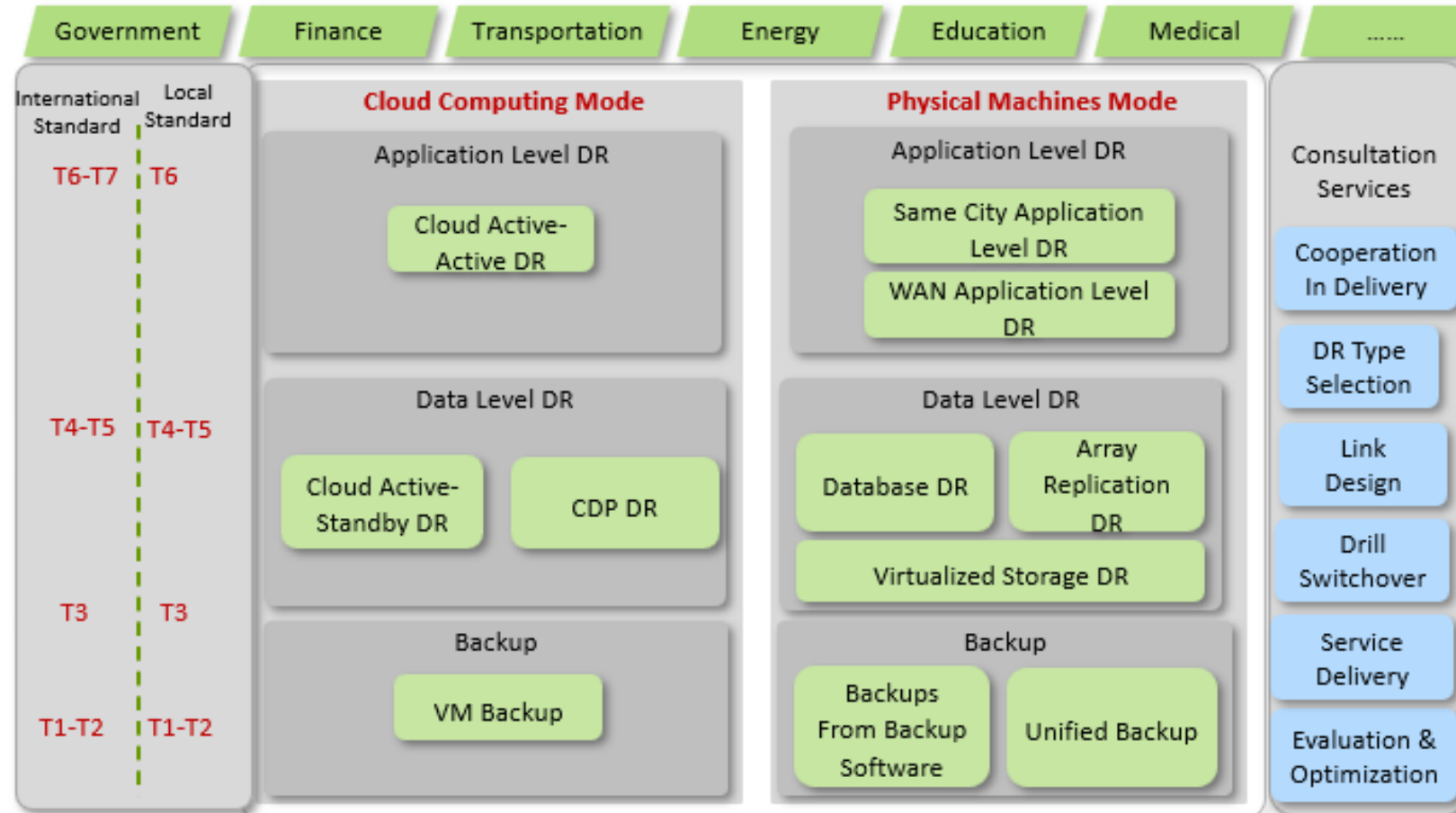


Chapter
09

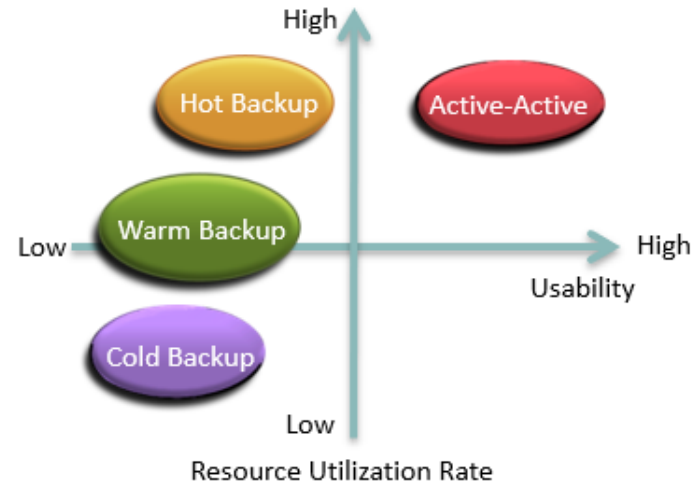
Architecture of Disaster Recovery Solution



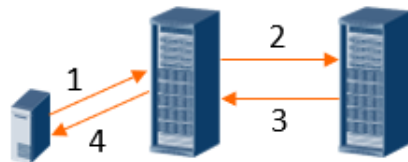
DR Backup Solution Framework



DR Design Model: Combination of Synchronous & Asynchronous



Synchronous DR: Has Distance Limitation



RPO: 0s, 2 identical mirrors.

Asynchronous DR: No Distance Limitation

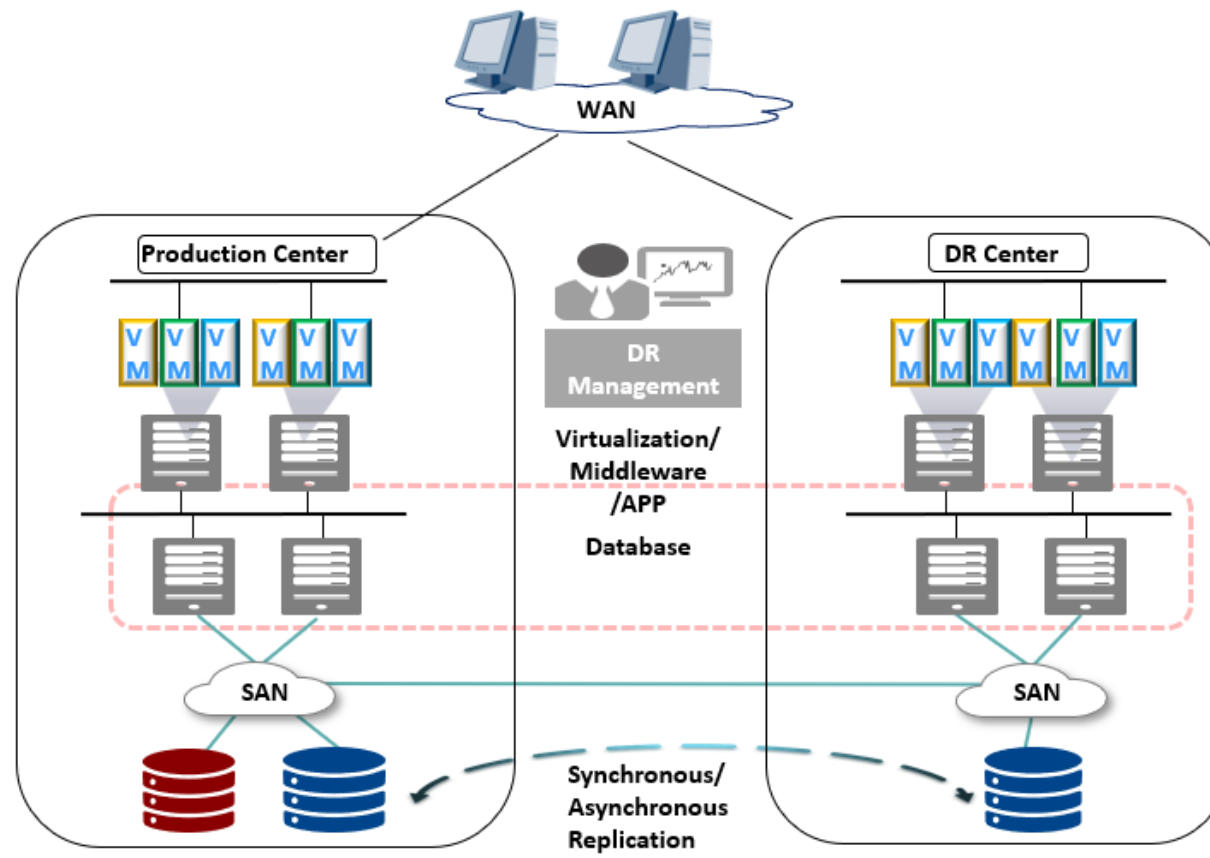


RPO: From 30mins to few hours, periodically updates the target.

DR Design Model: Combination of Synchronous & Asynchronous

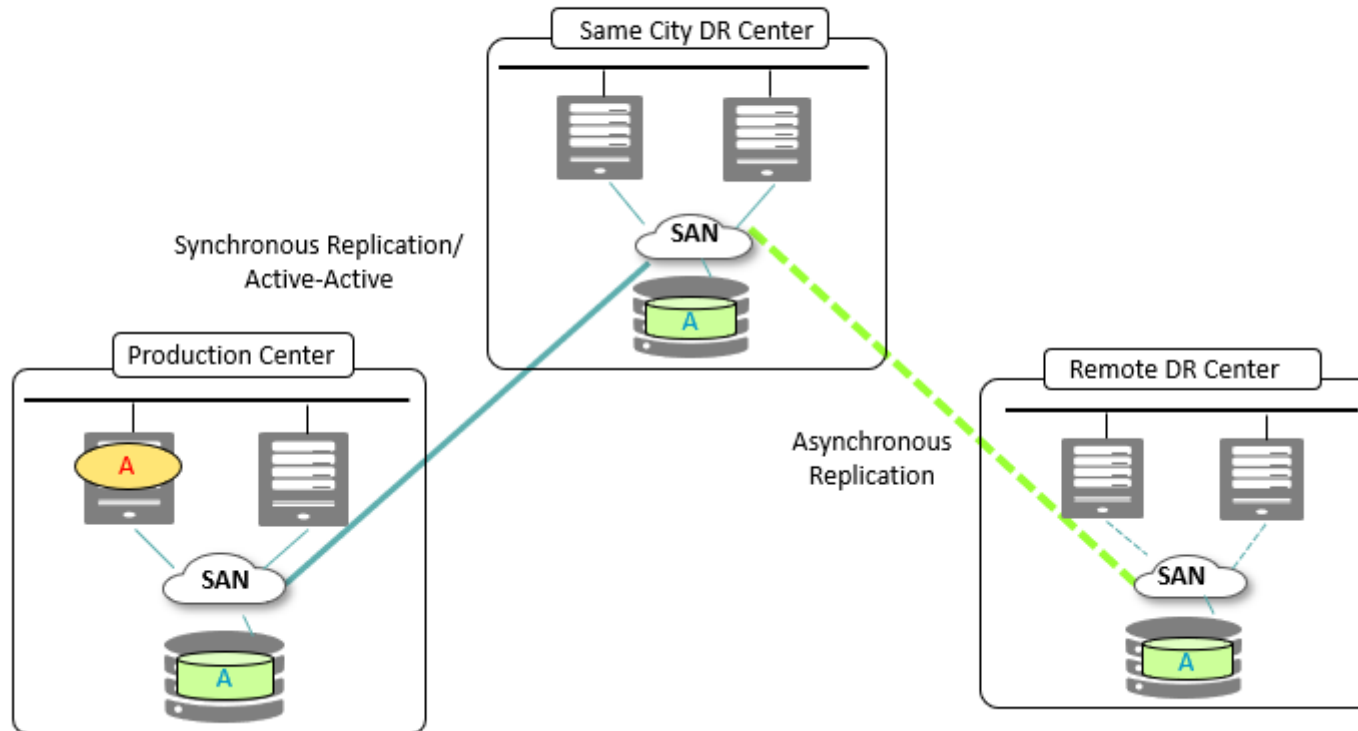
DR Mode	Reliability Solution	DR Recovery	Data Backup Requirements
Active-Active	Cluster + Load Balancing	Automatic	Real-time synchronous replication (<100KM)
Hot Backup	Cluster	Automatic	Real-time synchronous replication (<100KM)
Warm Backup	Manual Intervention	Manual	Asynchronous replication (>100KM)
Cold Backup	Strong Manual Intervention	Manual	Same as above

Active - Standby DR Solution

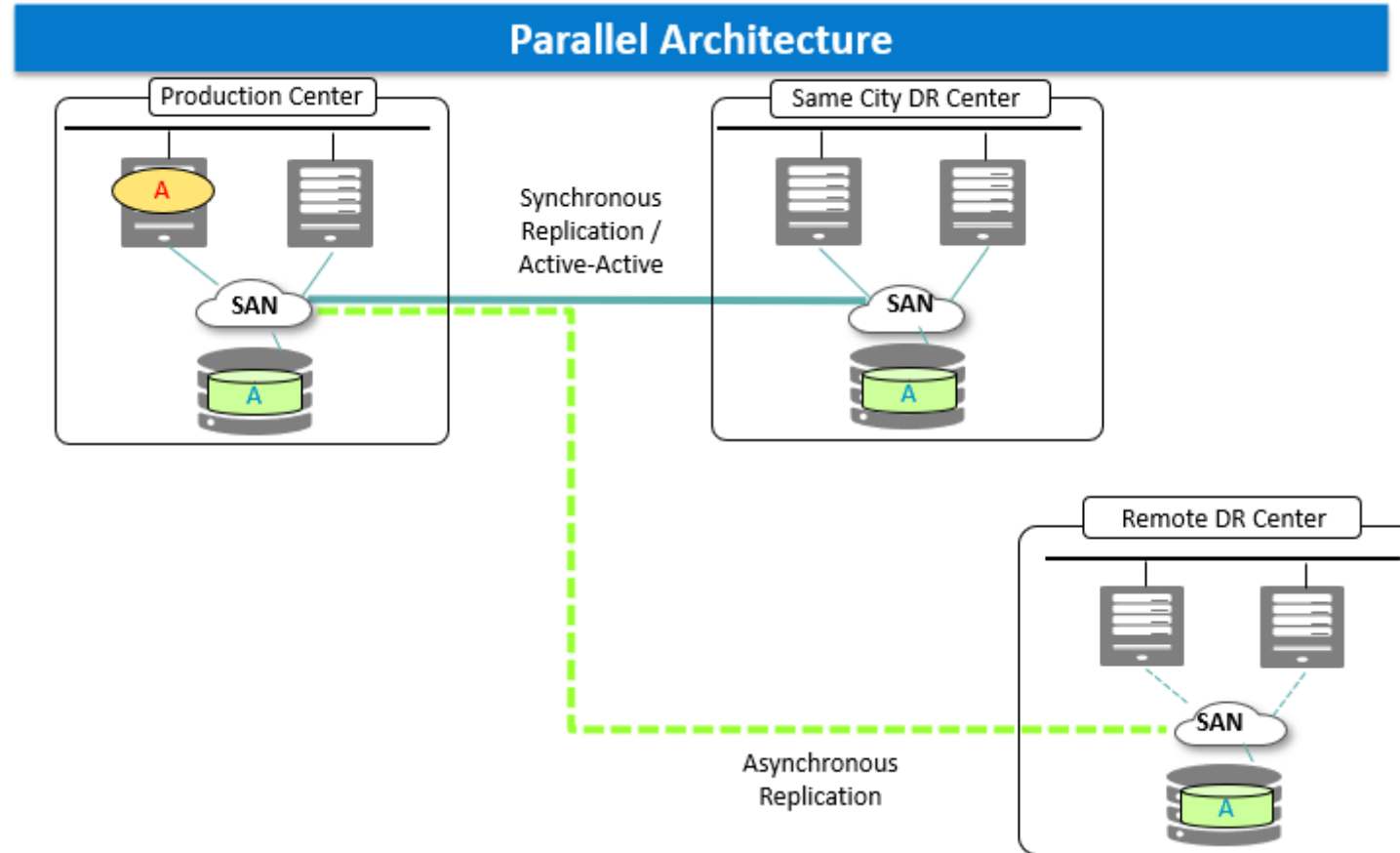


Three Datacenter (3DC) DR Solution (1)

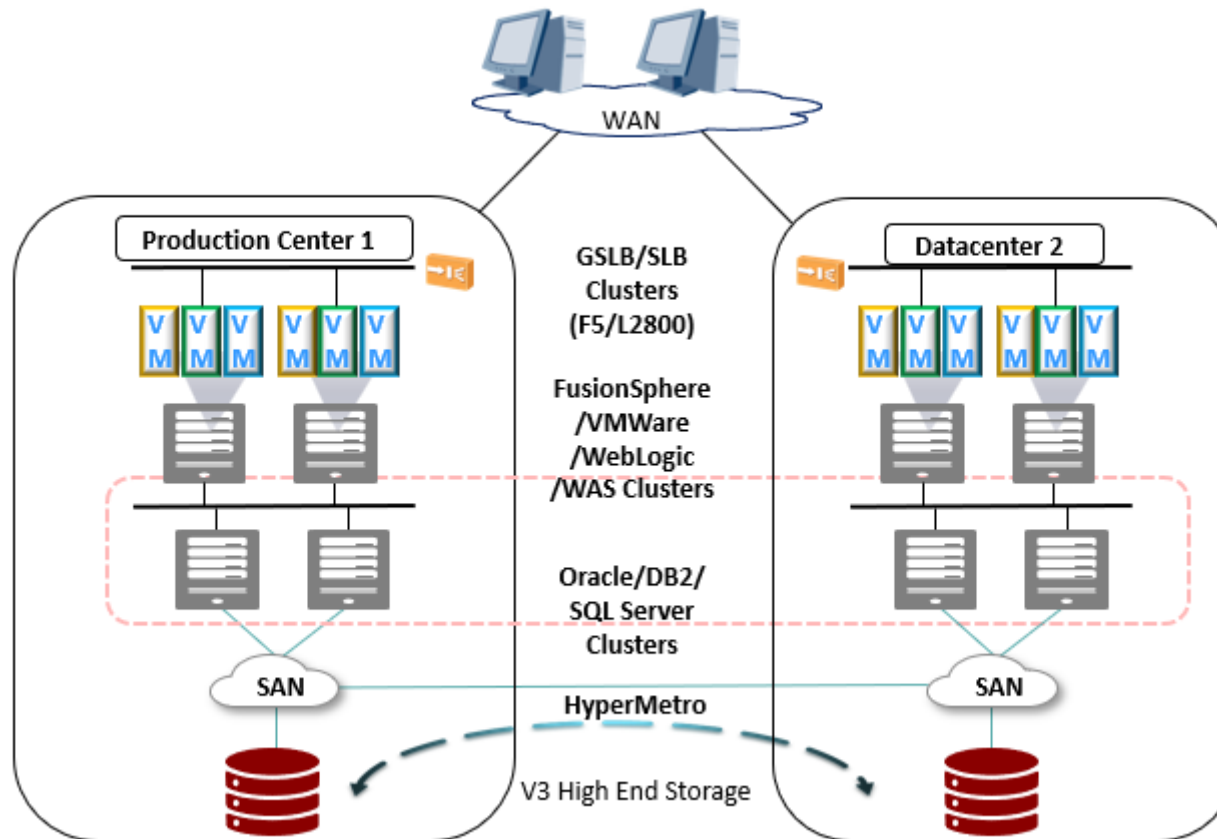
Cascaded Architecture



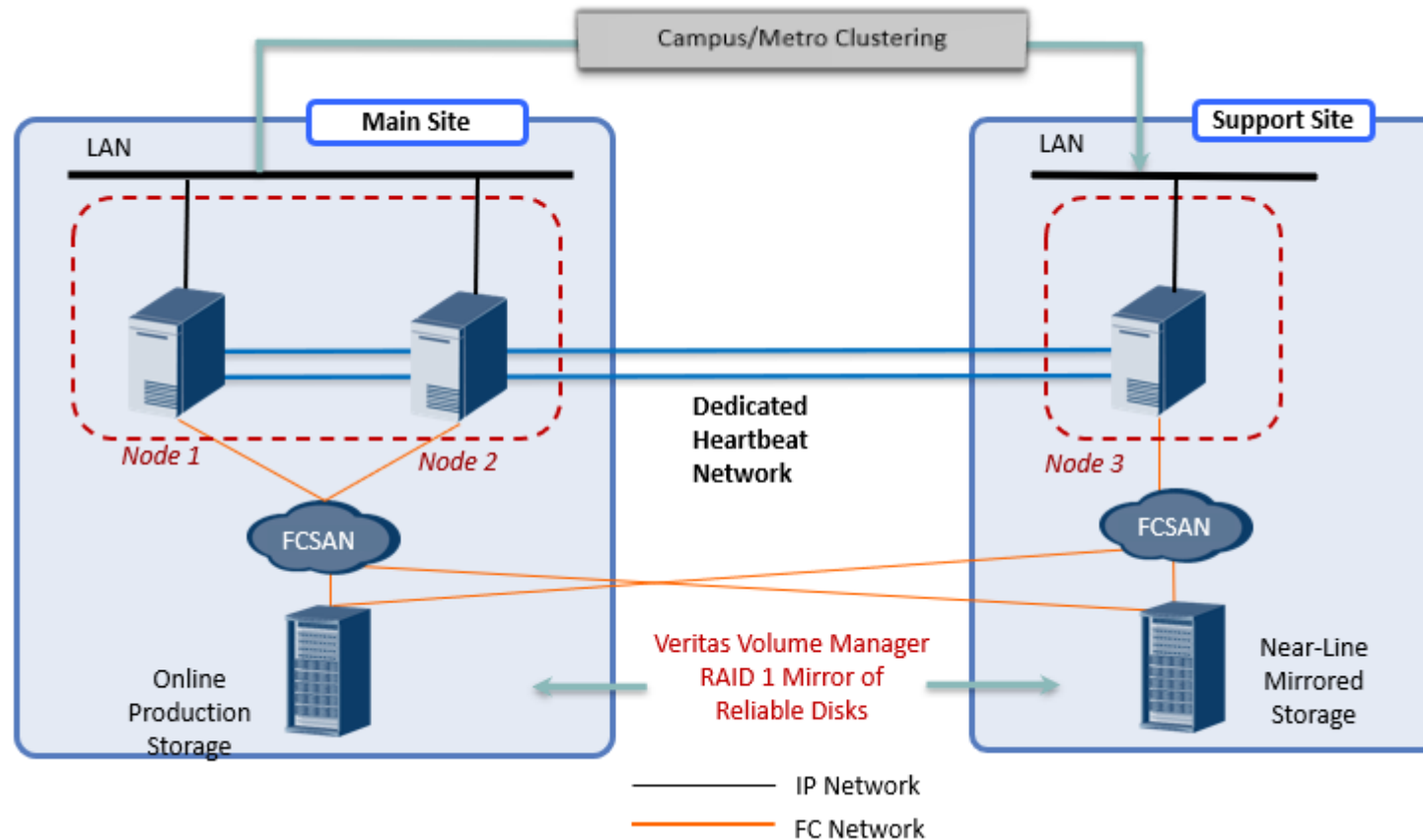
Three Datacenter (3DC) DR Solution (2)



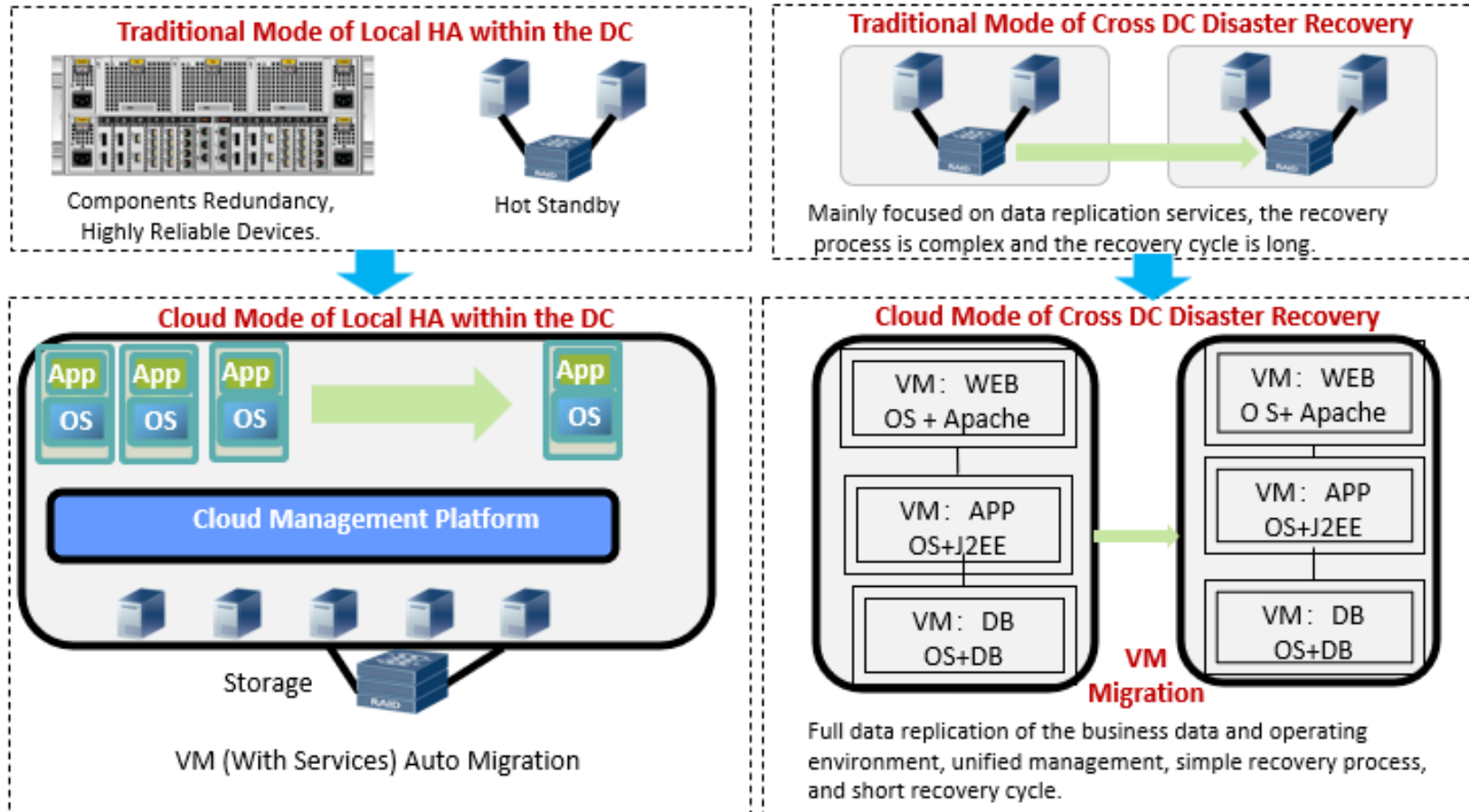
Active - Active DR Solution



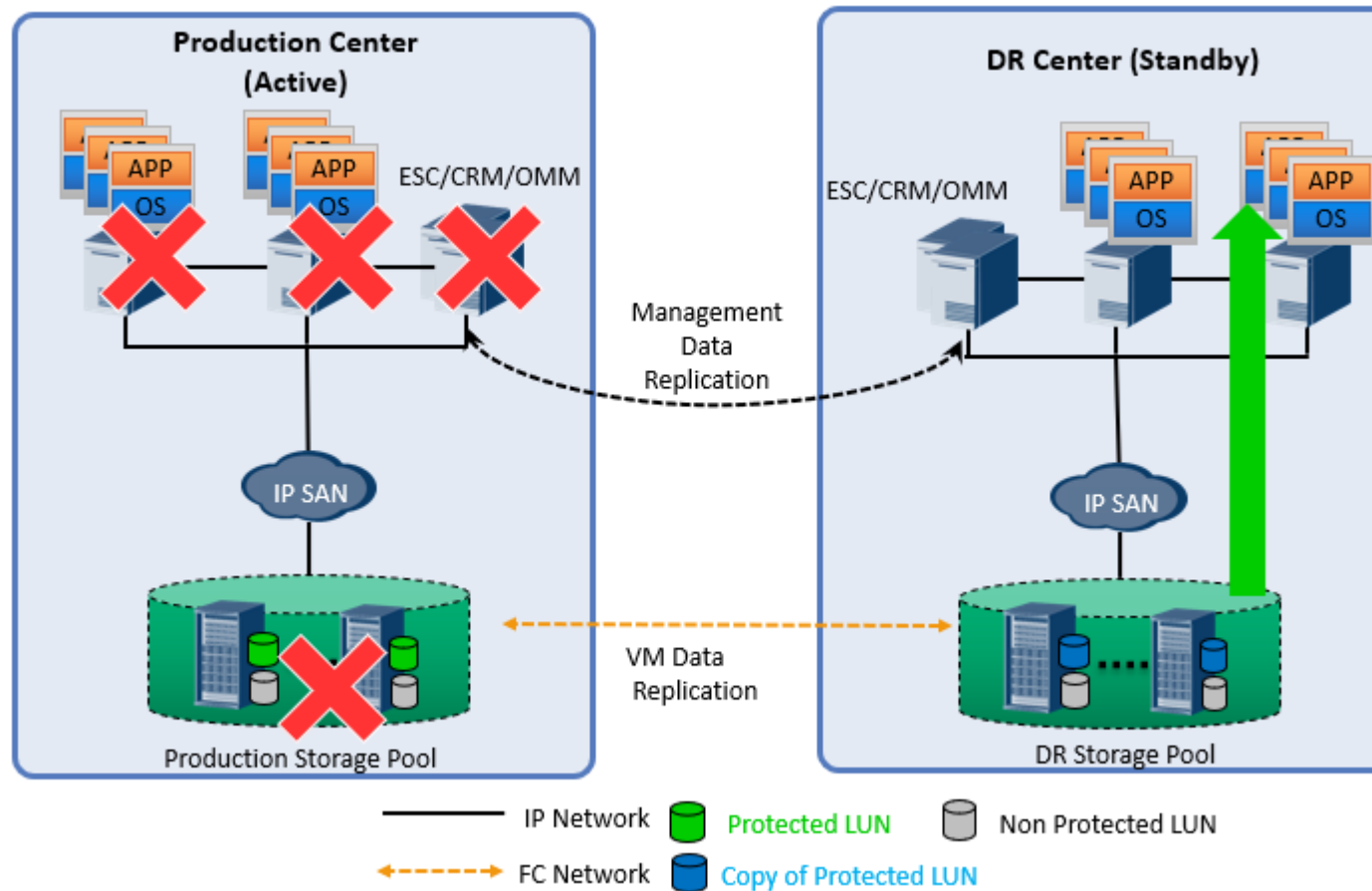
Campus/Same City Application Level DR (Physical Machines Mode)



Evolution of New DR Model Under Cloud Computing



Cloud Active - Standby Data Level DR Implementation Method

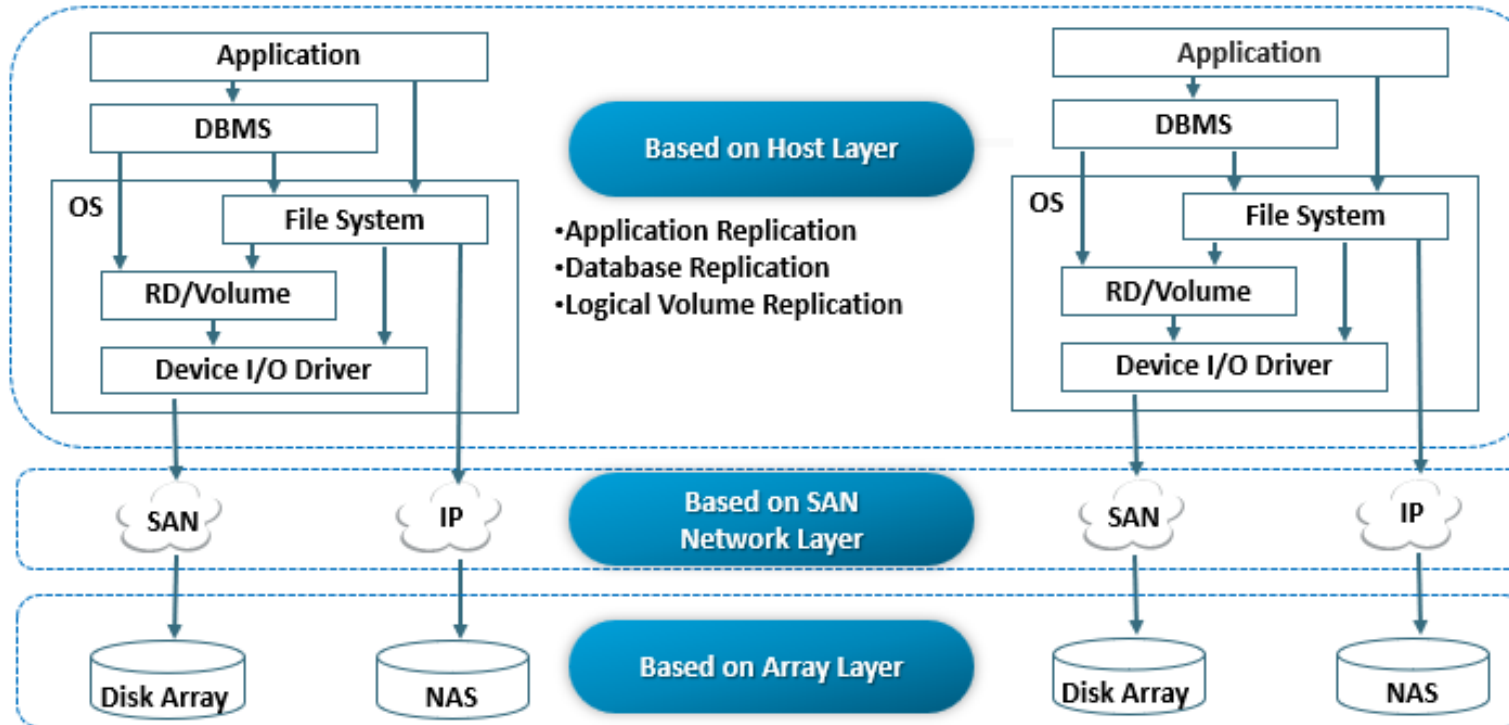


Chapter
09

Common Disaster Recovery Technologies



Main Technologies For DR

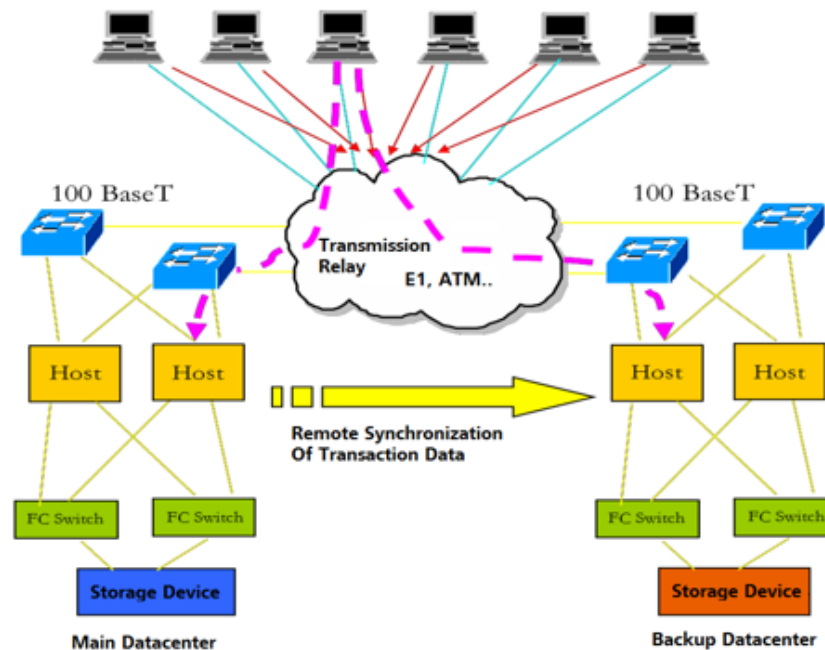


RD: Raw Device

DBMS: Database Management System

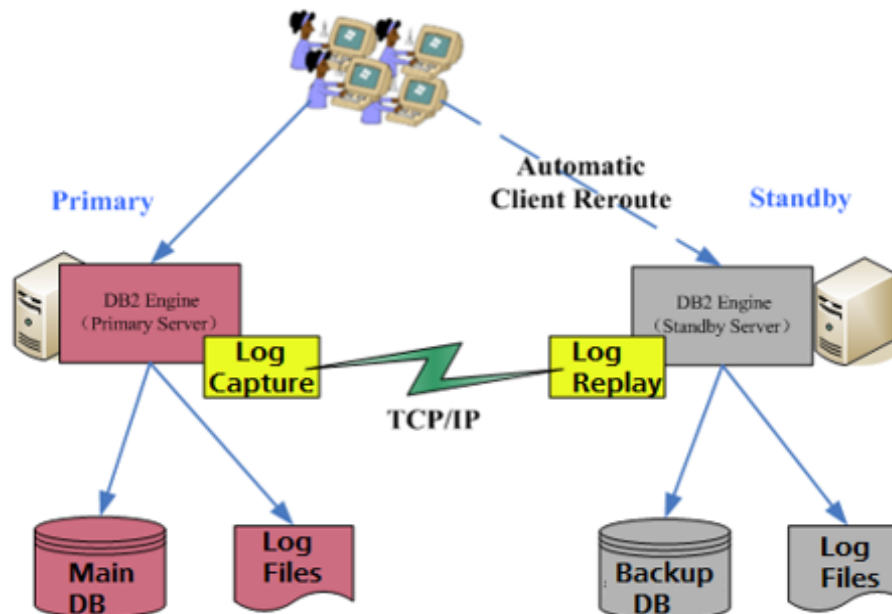
Host Layer DR Technology - Application Level

- **Application-level** disaster recovery technology enables remote replication and synchronization of data by application software. When the primary center fails, the application software system of the disaster recovery backup center resumes operation and takes over the services of the primary center.



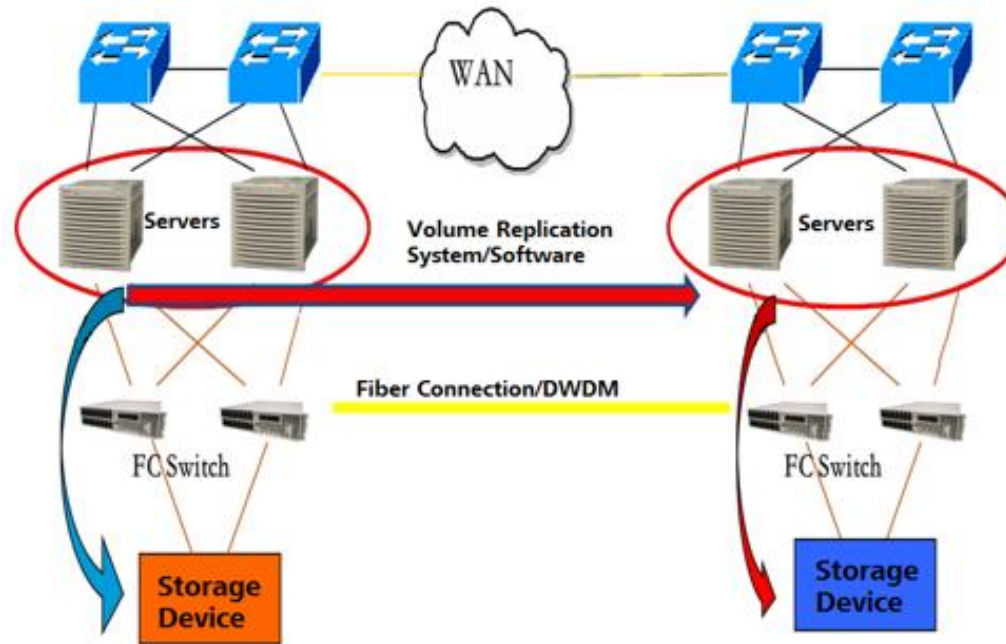
Host Layer DR Technology - Data Level

- Database-level** disaster recovery technology is a disaster recovery solution for specifically designed for databases. A typical database usually has database-level disaster recovery. For example: Oracle Data Guard, DB2 HADR etc. Disaster recovery at the database level is mainly achieved by transferring database logs and performing replay at disaster recovery sites. Database-level disaster recovery technology can be smoothly switched in the event of a disaster.



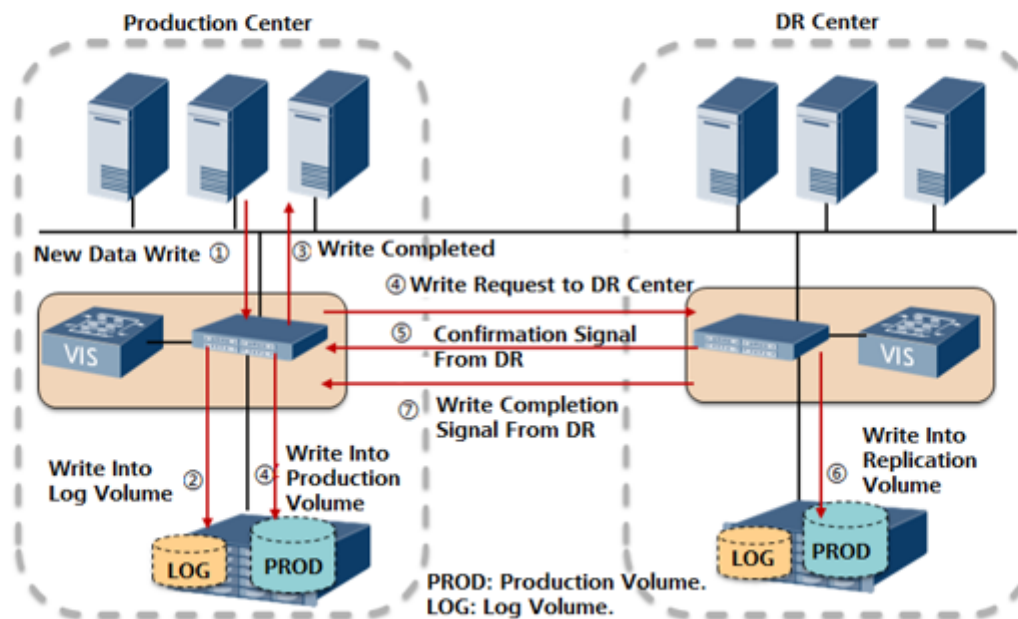
Host Layer DR Technology - Logical Volume Level

- Logical disk volume-based remote data replication refers to the remote synchronous (or asynchronous) replication of one or more volumes based on demand. The implementation of this solution is usually done through software.

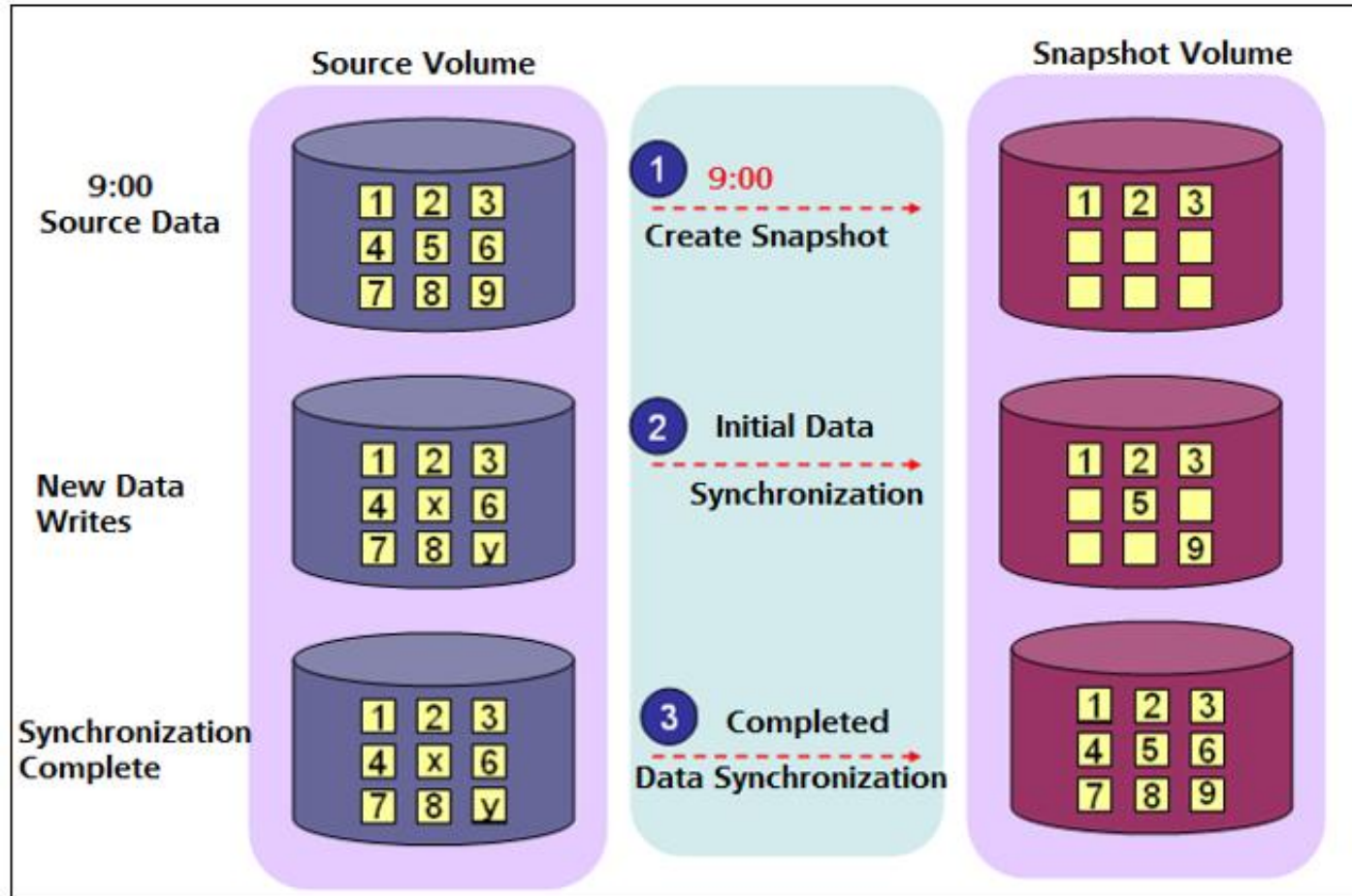


Network Layer DR Technology

- The SAN-based data replication technology is a storage area network (SAN) between the front-end application server and the back-end storage system. A layer of intelligent switches is added, where the front-end is connected to server and hosts, and the back-end is connected to the storage devices.

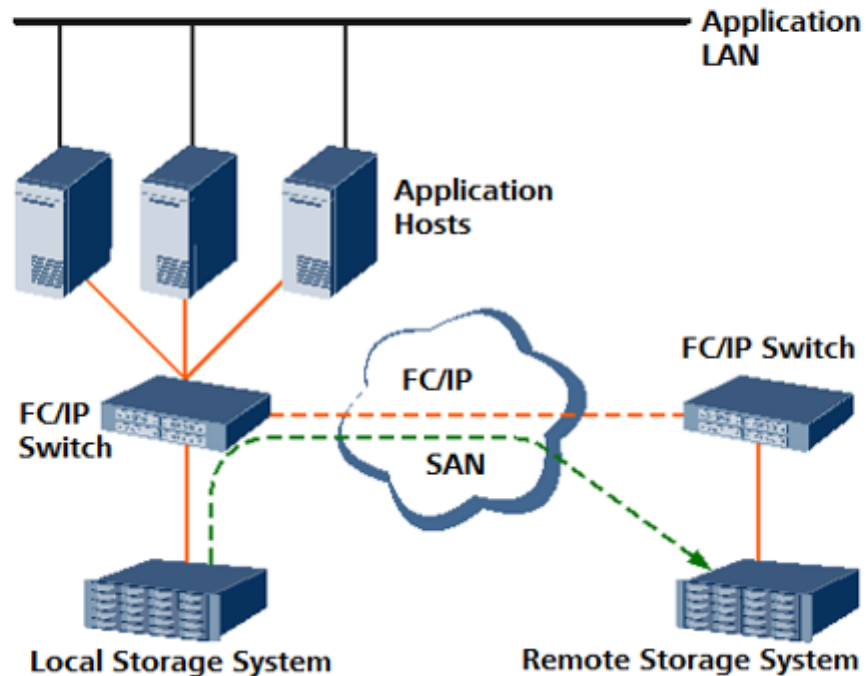


Network Layer Full Space Snapshot Working Principle

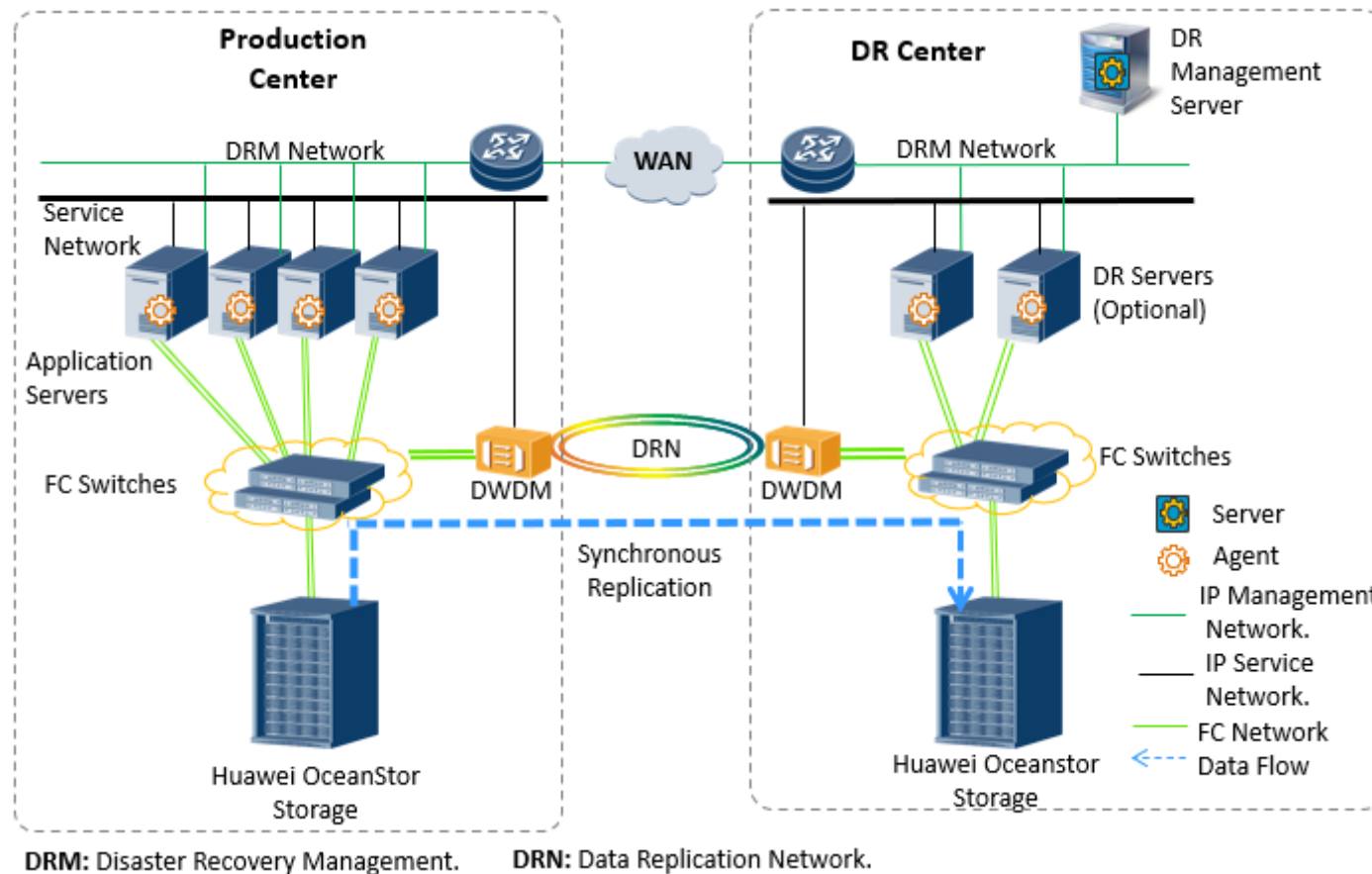


Array Level DR Technology

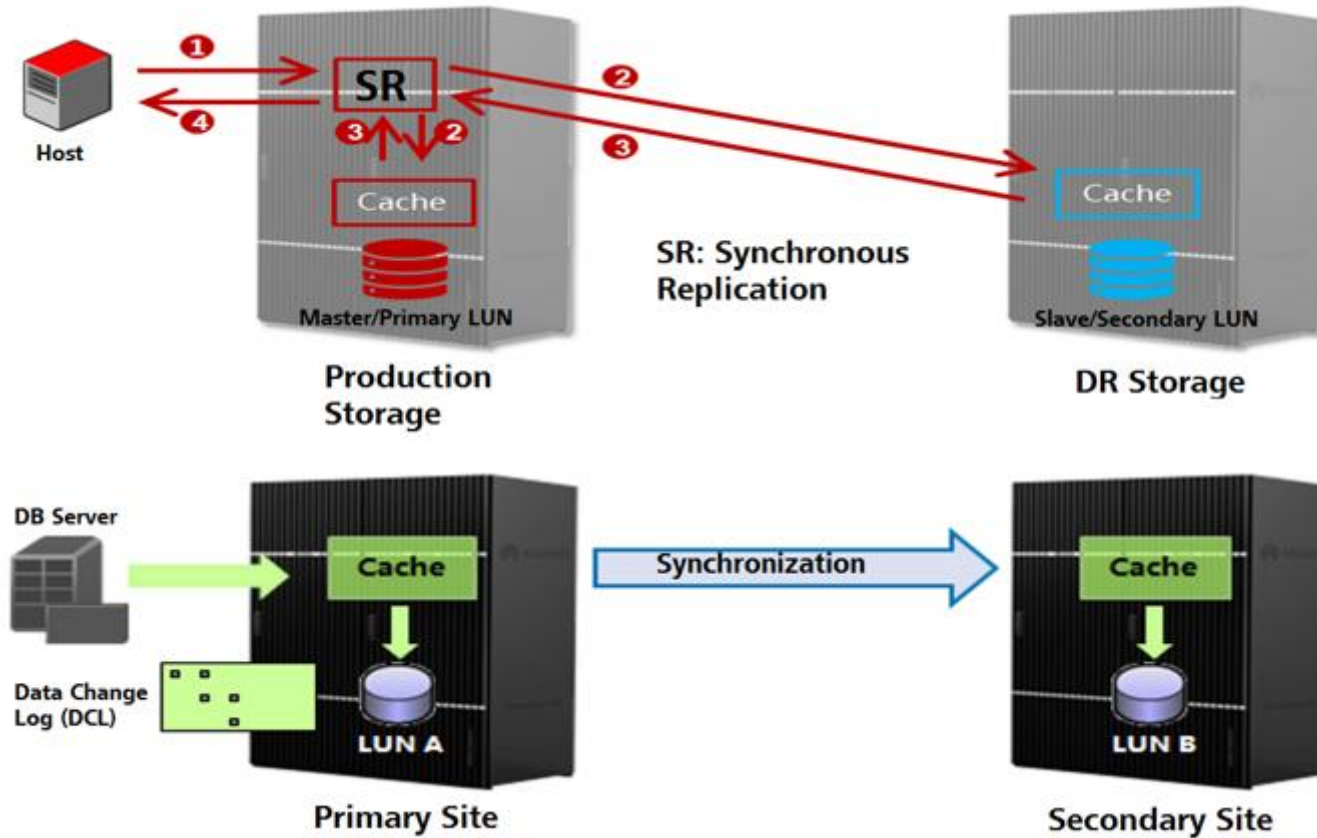
- Array-level disaster recovery is mainly implemented using inter-array replication technology. Since the array's replication does not pass through the host, there is minimal effect on the performance of the host.



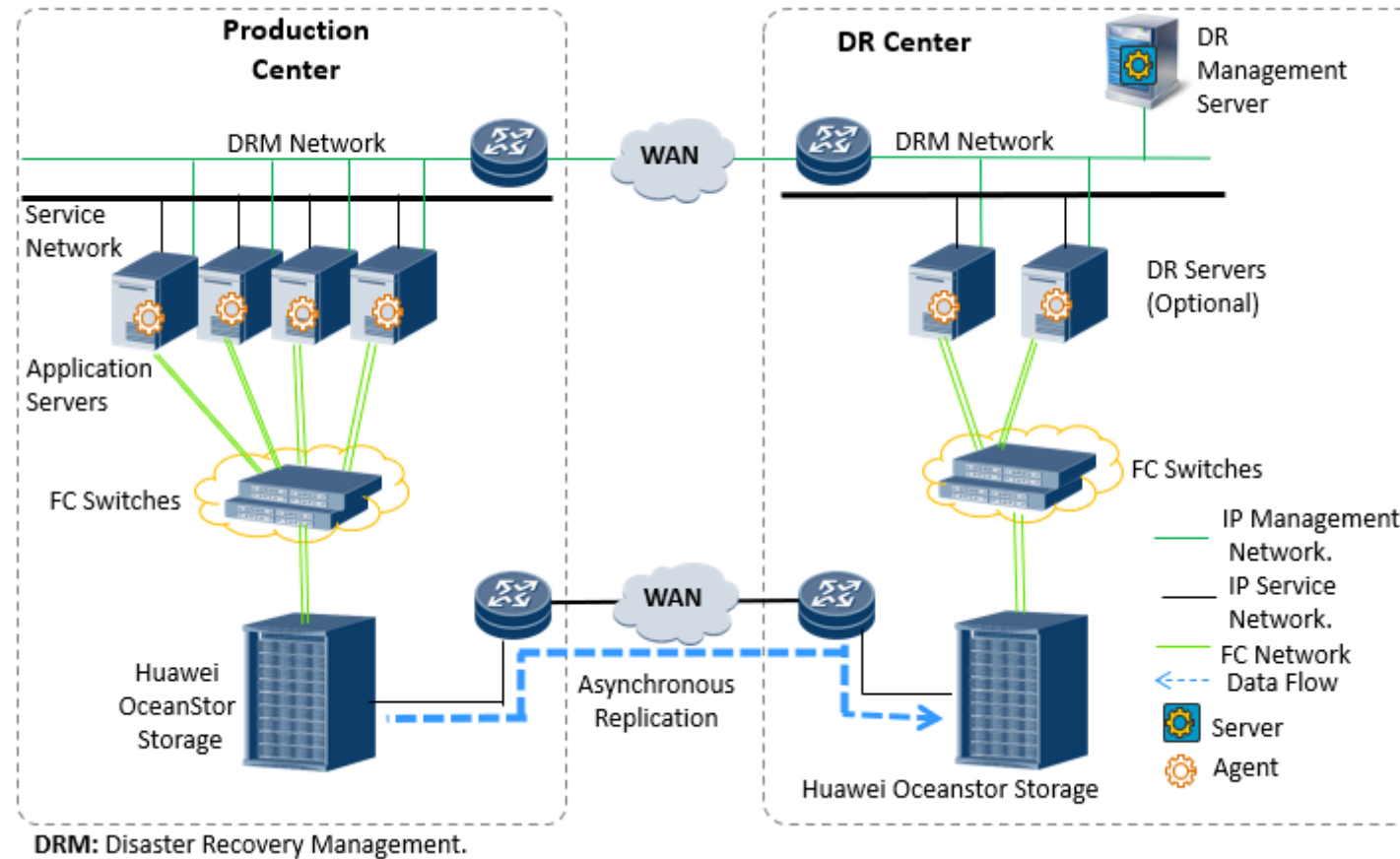
SAN Synchronous Replication DR



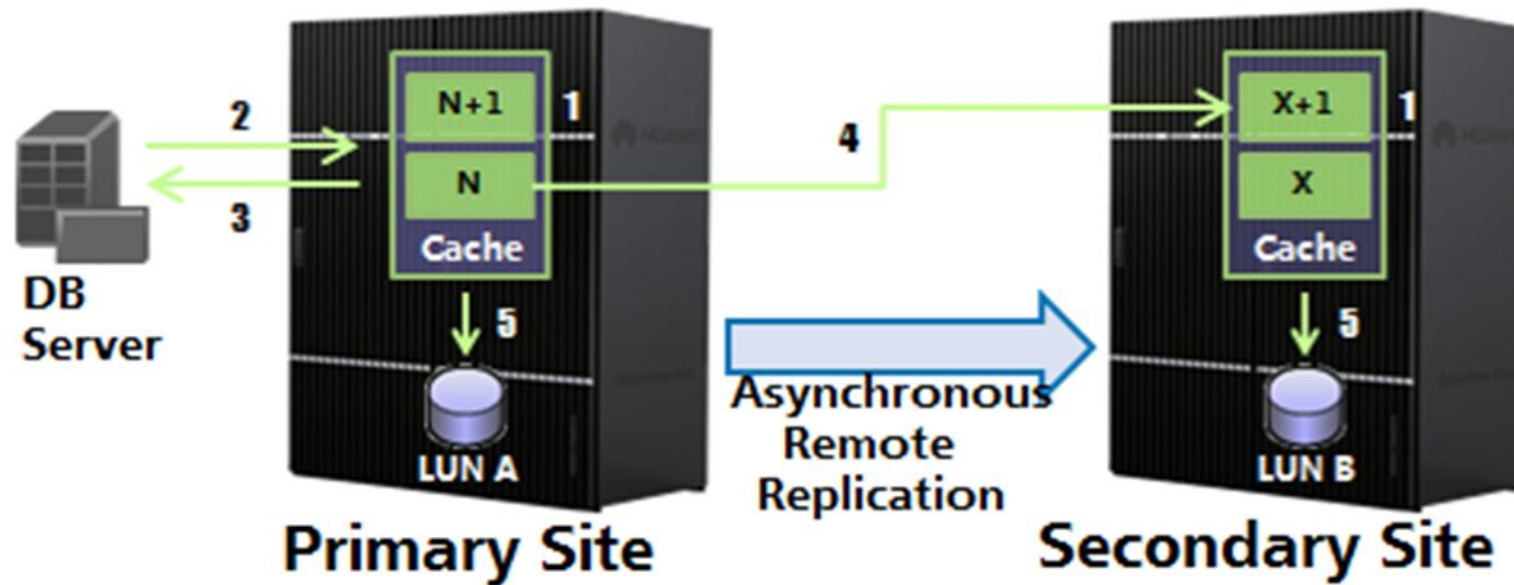
Working Principles of SAN **Synchronous** Replication



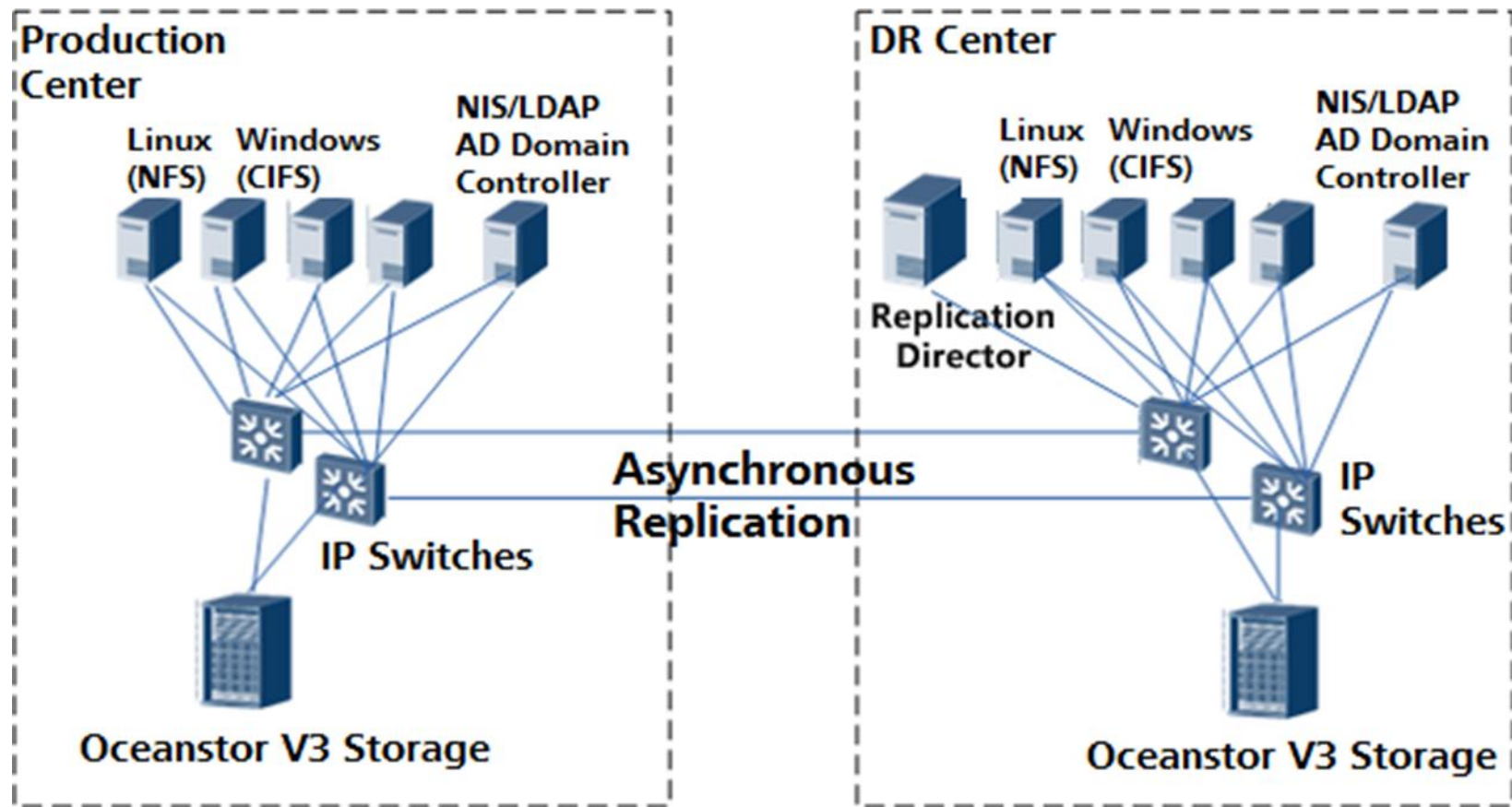
SAN Asynchronous Replication DR



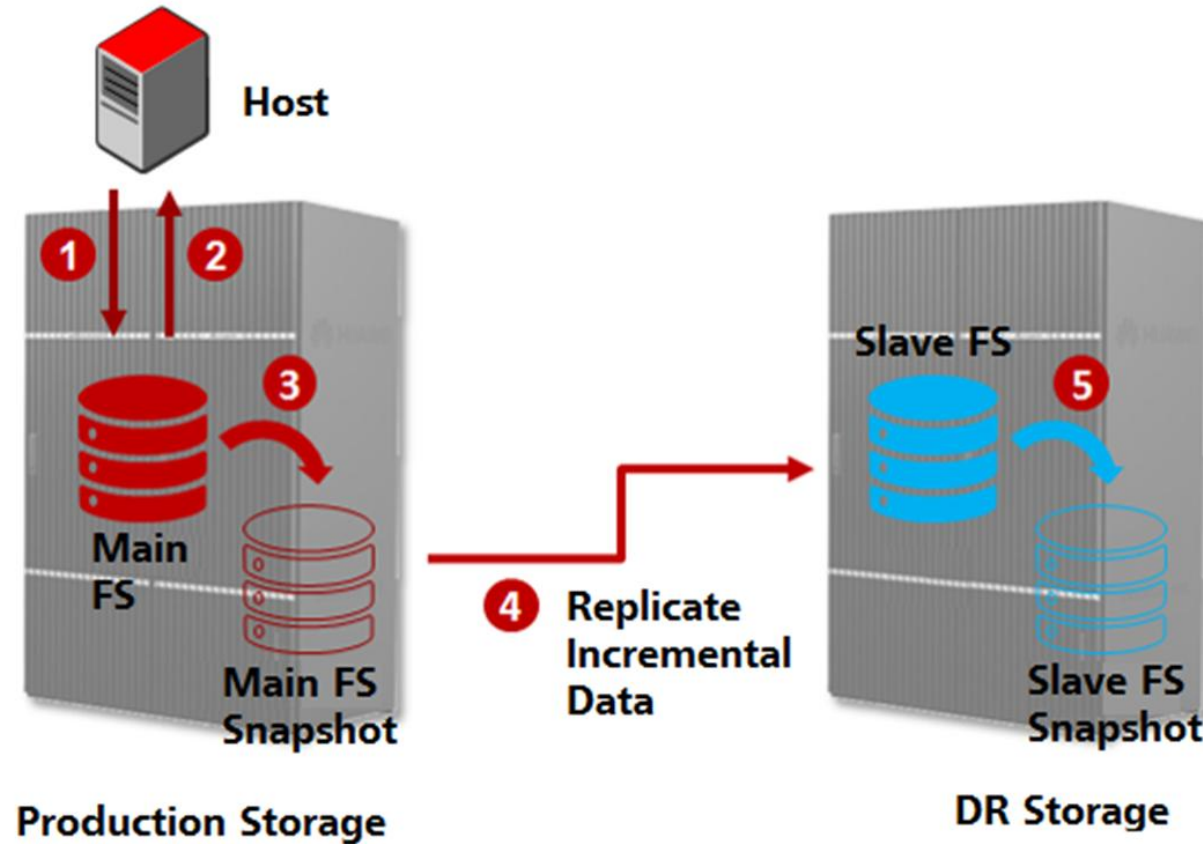
Working Principle Of SAN Asynchronous Replication



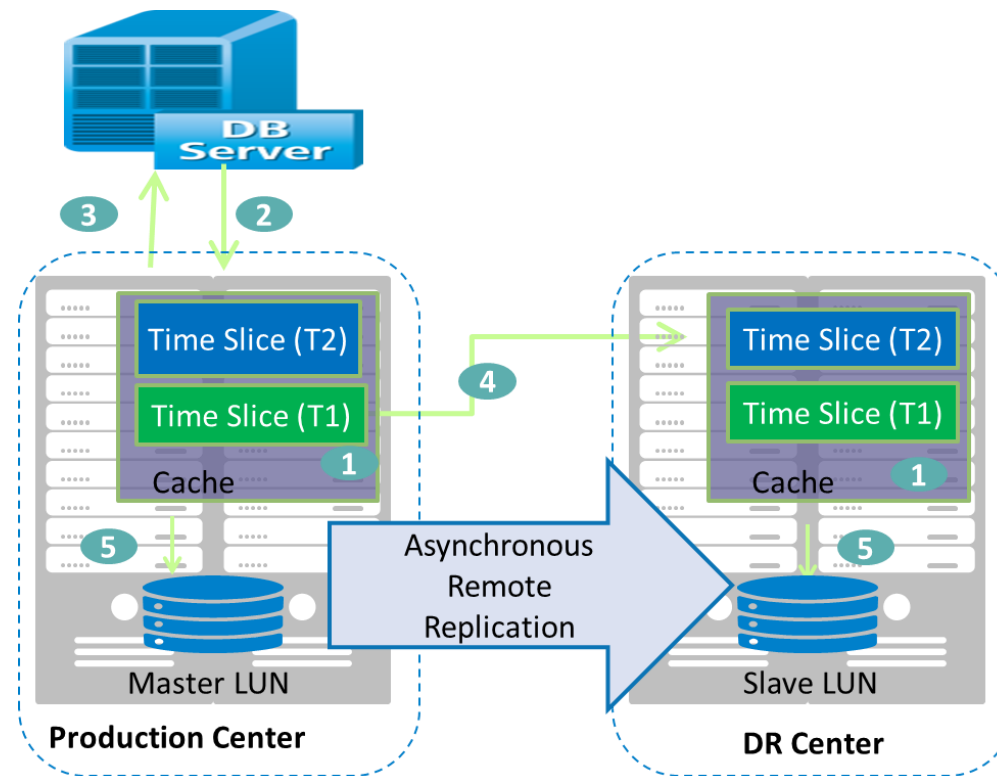
NAS Asynchronous Replication DR



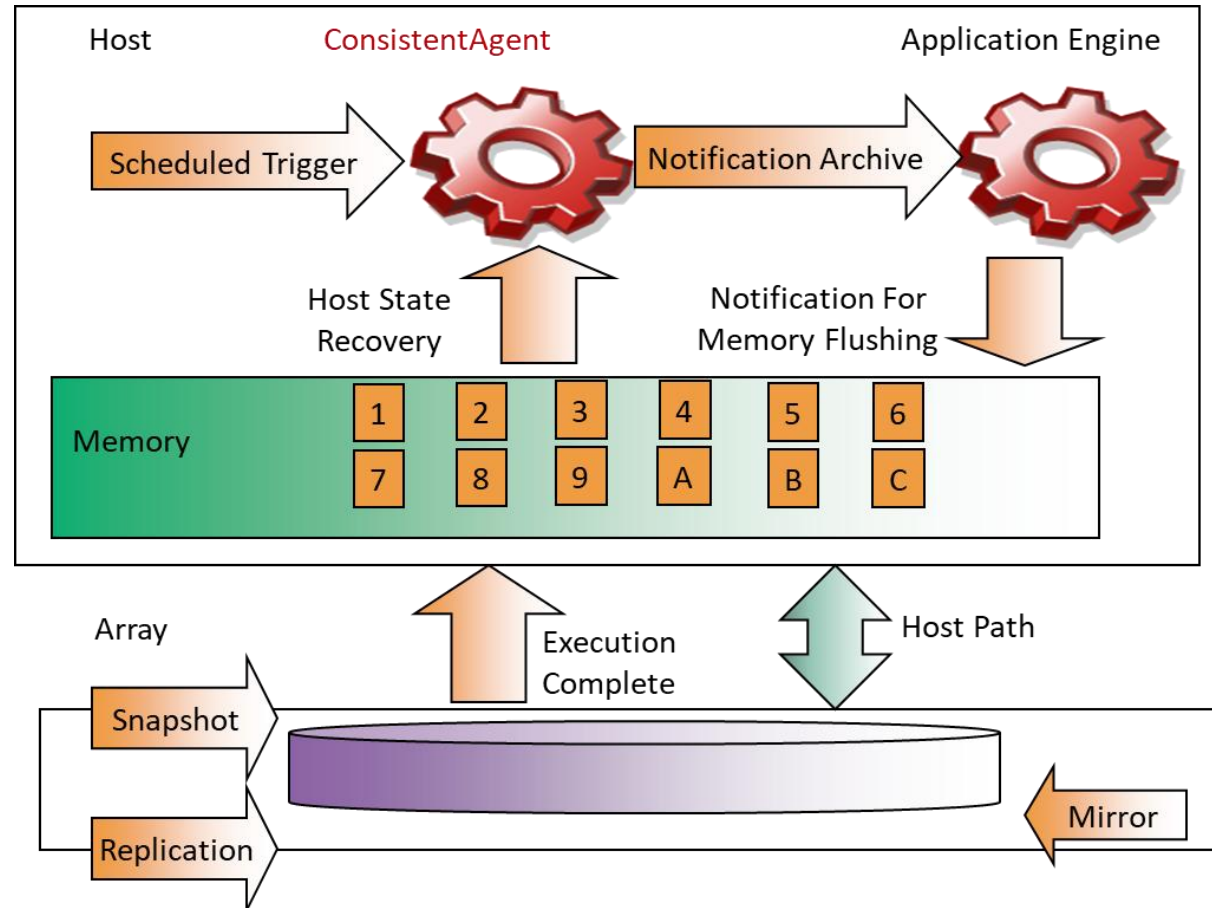
Working Principles Of NAS Asynchronous Replication



Multi Time Point Asynchronous Remote Replication – Seconds Level RPO

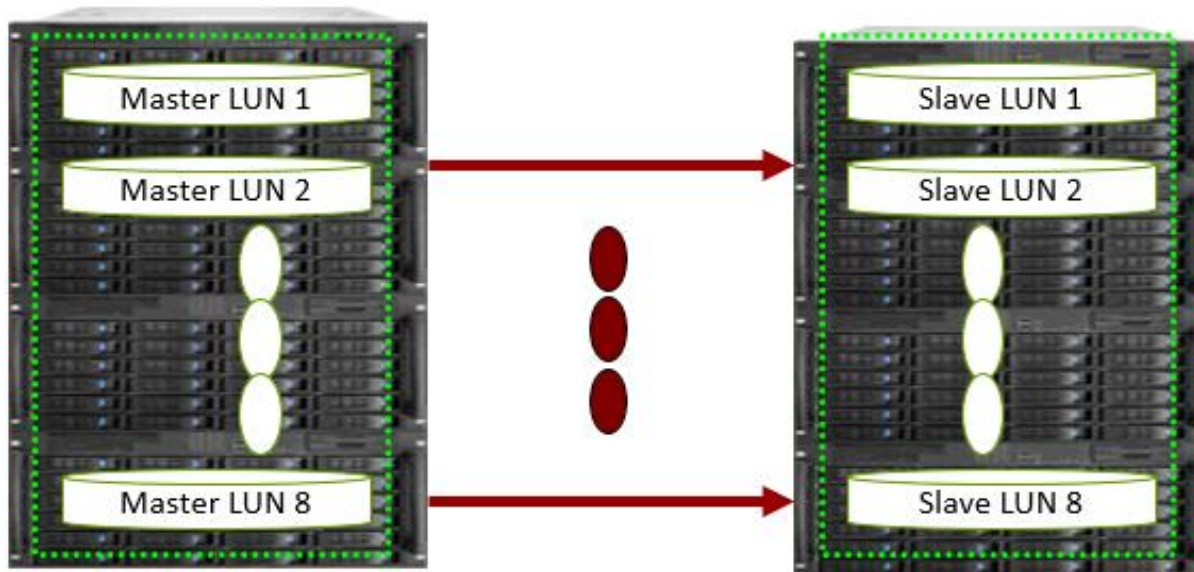


Remote Replication - Application Consistency

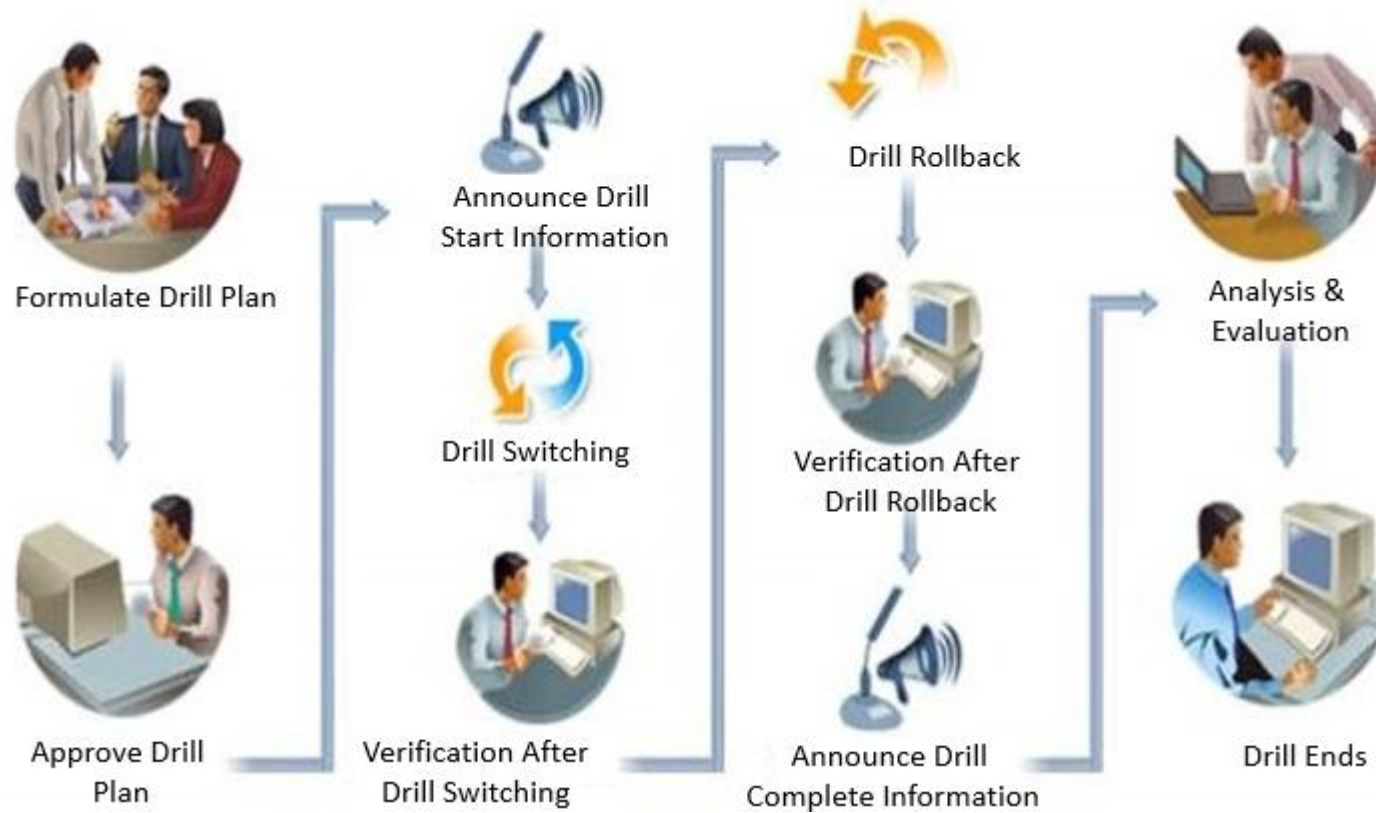


Remote Replication - Consistency Group

- Used to maintain the time consistency of the mirrored data of multiple LUNs.
- All the members are synchronized, split, break and switched between primary to secondary together at the same time.



Typical DR Drill Solution





Thank You