Technical Guide

Disaster recovery in a cloud environment

May 2021

SAMSUNG SDS

Contents

1. Overview

This document describes how to establish disaster recovery plans to ensure business continuity and resilience in SDS cloud environments and to design DR according to business needs.
Service interruptions can occur at any time. Network failures, serious bugs in applications, or sometimes even natural disasters occur. In the event of an accident, the importance of a robust and thoroughly tested disaster recovery plan is highlighted. A well-designed and validated disaster recovery scheme can minimize the impact of business in the event of a disaster. SDS Cloud provides materials for constructing a robust, flexible and cost-effective disaster recovery scheme that can be used to build or scale customer-built systems for service continuity.

By definition, a disaster refers to a situation in which IT service is discontinued due to an event that cannot be prevented or controlledor the expected recovery time from the information system failure exceeds the acceptable range, undermining normal performance.
Disaster Recovery aims to resume IT services interrupted by a disaster. In order to recover from a disaster, a plan and a supporting system must be prepared in advance. These are called a Business Continuity Plan (BCP) and Disaster Recovery System (DRS), respectively.
The BCP begins with a business impact analysis that defines two key metrics. Recovery Time Objective (RTO) is the maximum time allowed to restore a service when it is interrupted due to a disaster. Recovery Point Objective (RPO) refers to the point at which loss of data can be sustained when the interrupted service is restored.

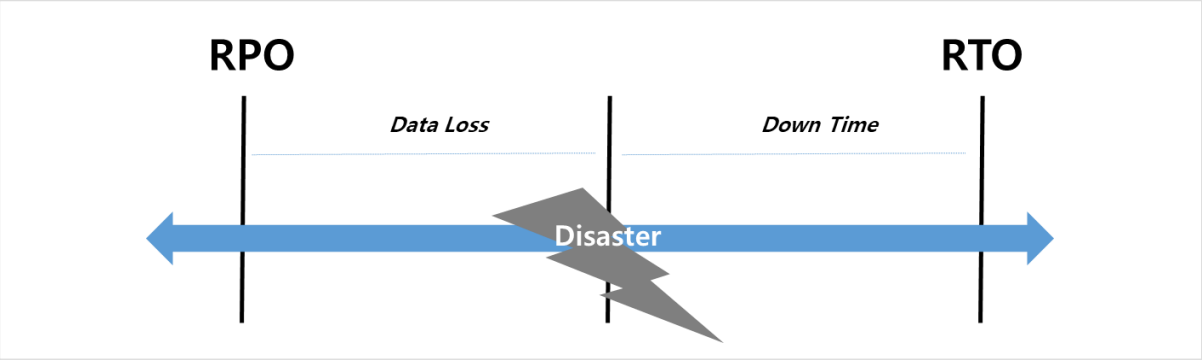

Figure 1. RPO and RTO based on the time of the disaster

In general, the smaller the RTO and RPO values, the faster the application needs to recover from an outage and the higher the cost of running the application.
Smaller RTO and RPO values increase the complexity, which also increases the administrative overhead for this. Highly available applications require managing deployments between the two physically separated data centers, replication management and more.

2. DR plan overview

2.1 Types of DR system by recovery level

Disaster recovery systems are typically divided into mirror sites, hot sites, warmsites, and cold sites, depending on the level of recovery.

1. Mirror sites

- Establish a remote location with the same level of IT resources as the main centerand maintain both centers active (Active-Active) to provide simultaneous service (i.e., theoretical RPO is 0).
- The time required to recover in case of a disaster (RTO) is immediately (theoretically, 0).
- High cost for initial investment and maintenance
- Applicable if the frequency of data updates is not high, such as web application service
- In the case of systems with high frequency of data updates such as database applications, it is not practical to allow simutaneous provision of services from both sites due to the high load of the system. For such cases, it is more common to build a hot site.

2. Hot sites

- A remote center with the same level of IT resources as the main center is in standby status (Active-Standby).
- Keep the data in the latest state through synchronous or asynchronous real-time mirroring.
- In case of disaster, the information system of the disaster recovery center switches to active.
- The time required to recover from a disaster (RTO) is several hours (within about 4 hours).
- High cost is required for initial investment and maintenance.
- For systems with frequent data updates, such as database applications, it is common for the disaster recovery center to maintain a standby status and switch to an active status in case of disaster.

3. Warm sites

- Warm sites are similar to hot sites in some ways, but instead of having IT resources at the same level as the main center in the disaster recovery center, only the highly important IT resources are partially owned by the DR center or the overall scale is smaller.

- Real-time mirroring is not provided and the data backup cycle is from several hours to 1 day, longer than hot sites. The RPO also takes about several hours to 1 day.
- The time required to recover in case of disaster (RTO) ranges from days to weeks.
- Although installation and maintenance costs are lower than mirror sites or hot sites, the initial recovery level is incomplete and it takes longer to complete the recovery.

4. Cold sites

- Data is only stored remotely and information resources for the services are secured only at a minimum level. And in case of disaster, necessary information resources are procured to initiate the restoration process for the information system.
- The data at the main center is backed up at a remote location periodically (from days to weeks) (RPO is the same.)
- The time required to recover from a disaster (RTO) ranges from weeks to months.
- The cost of building and maintanence is the cheapest but ithe recovery is much slower and less reliable.

2.2 DR system implementation technology

Among the DR system methods, cold sites store data that is periodically backed up during system operation in remote storage using remote replication technology via network.

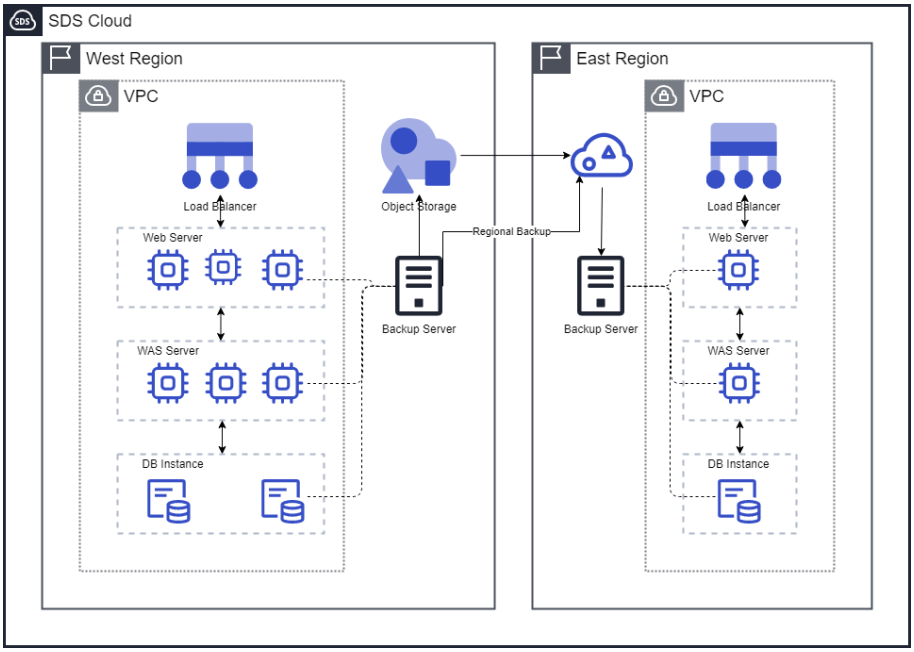

Figure 2. Backup based replication technology

How to organize a disaster recovery system at a hot site level or higher can be classified as follows:

1. Data replication system

- H/W replication method: Physical storage replication

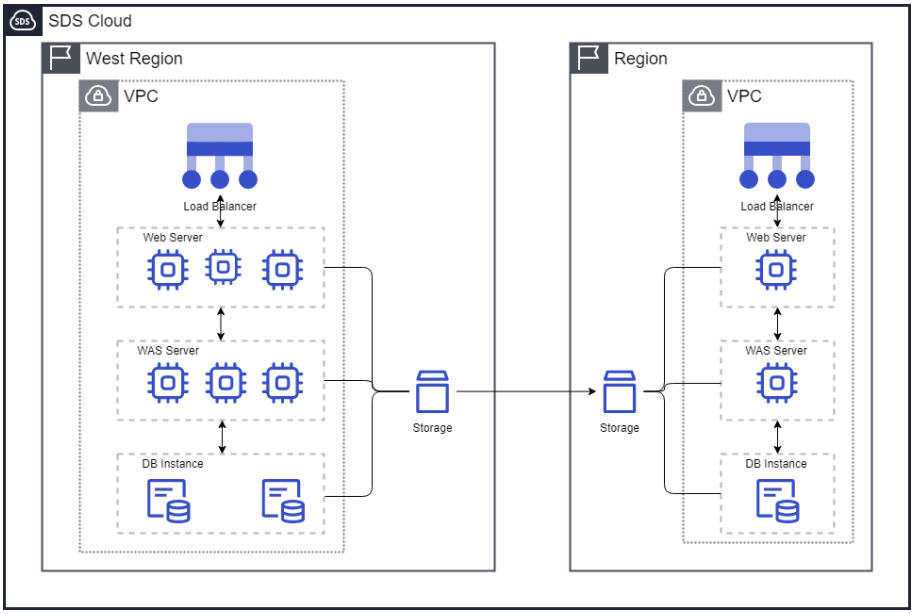

Figure 3. Storage-based replication technology

- Physical storage level: Replication using disk device

- Inter-region storage should provide compatibility at the microcode level.
- Suitable for operational environments using large capacity and high-performance disks, or File Server that need real-time replication

- S/W replication method: Utilizing data replication technology of dedicated replication solution

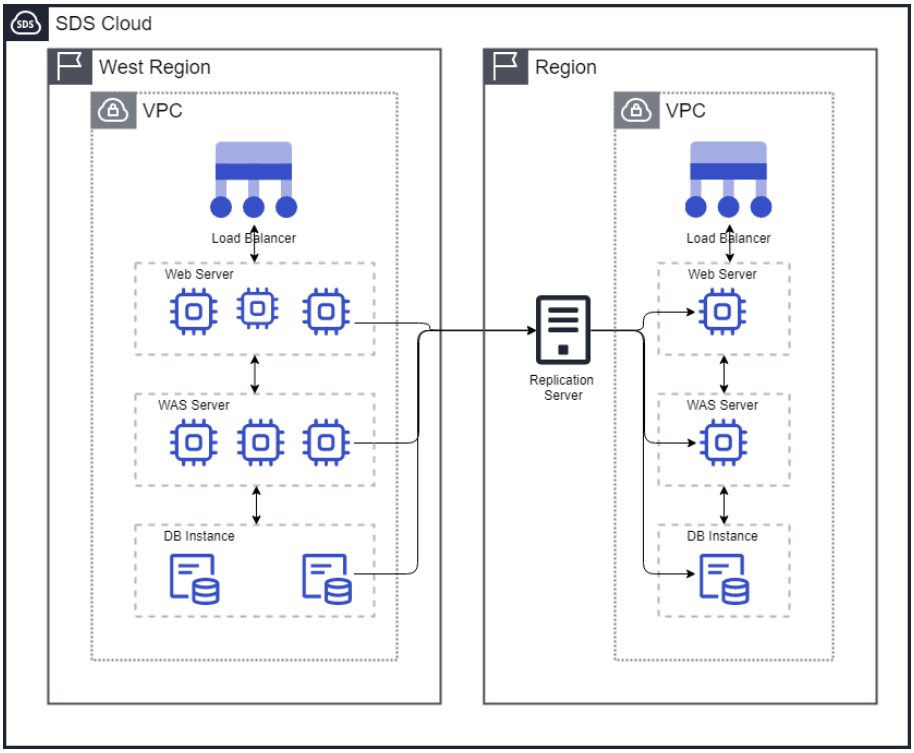

Figure 4. SW-based cloning technology

- Operating system level: Replication using data replication SW solution
- DBMS level: Utilizing functions or dedicated solutions provided by DBMS
- The storage between regions is also possible even if it is heterogeneous.
- The replication solution is executed on the server itself or using a separate replication server's resources. Therefore, the appropriateness of replication server resources according to the capacity and load of the operating environment need to be considered.

2. Data transmission system

- Synchronous replication

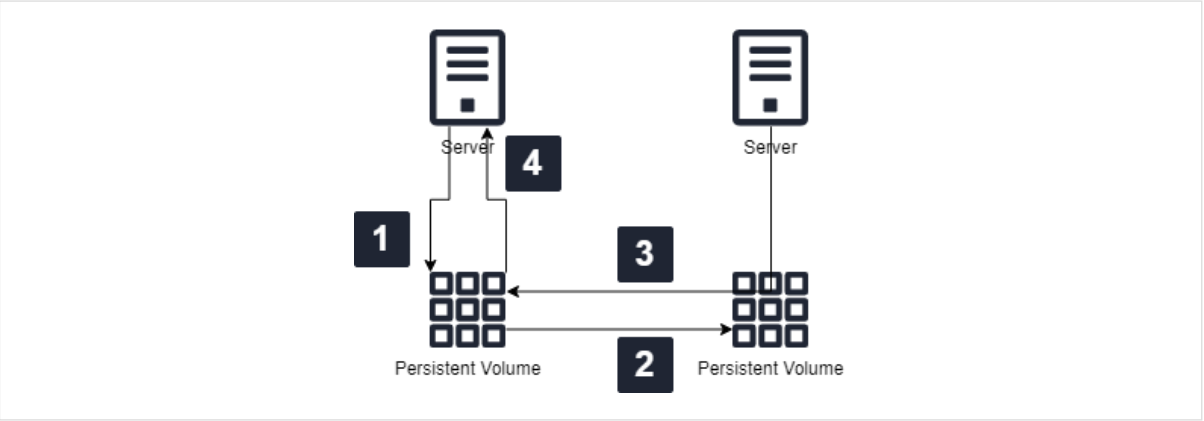

Figure 5. Real-time synchronous replication

- Main storage I/O is not completed until data is written in the remote storage.
- Data replication of remote replicas is always proportional to the distance from the main storage source, and storage service response time can somewhat increase due to the replication work.
- Data recovery and quick service resumption is possible without RPO loss.
- System service impact is sensitive to the transmission distance and I/O pattern.

o Asynchronous replication

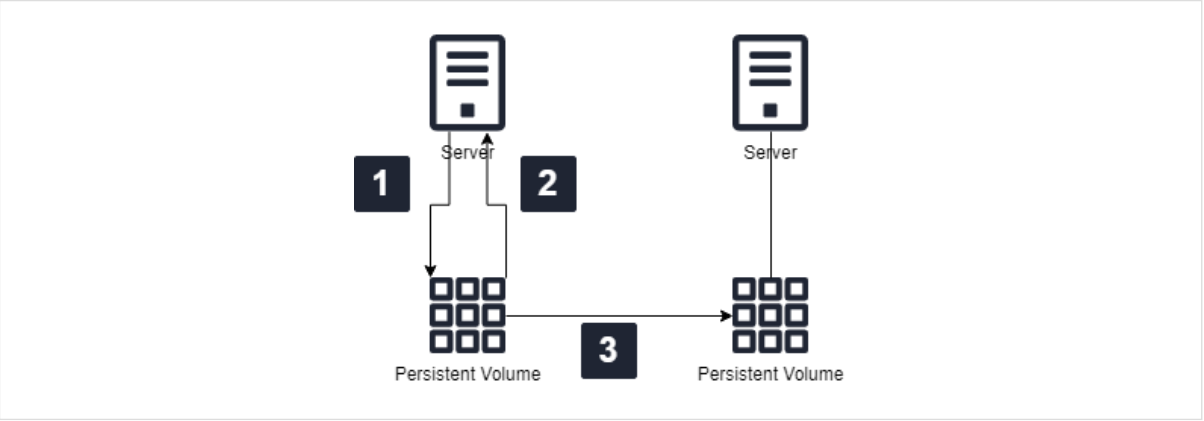

Figure 6. Near 0 asynchronous replication

- Data can be replicated in real time in several milliseconds in the asynchronous method.
- Data in the DR site can be matched using timestamp and sequence numbers.
- RPO/RTO have little data loss (near 0) for data recovery and can quickly resume services.

- System service impact has little effect on operating services due to data replication configuration, and therefore is suitable for long distance data transmission or insensitive to I/O patterns.
- Regular replication can be scheduled and in this case, RPO and RTO can be affected by the replication period.

3. DR configuration options from SDS Cloud

SDS cloud provides 3 replication measures to fit the disaster recovery strategy, including the real-time replication method for the region's entire resources and low-complexity, low-cost backup method.
For example, for data that follows previous compliance rules,, a backup/recovery DR pattern with higher RTO value was appropriate because it did not require quick access to the data. However, if today's online service breaks down, you must be able to recover both customer-related applications and the data as quickly as possible. In such cases, the hot standby pattern is appropriate. For general non-business email notification systems, on the other hand, may be more suitable with warm standby patterns.

3.1 Backup and restore

Backup and recovery is the easiest approach to preventing data loss and corruption.
It establishes a self backup policy through SDS backup and backs up VM images, DB, and file storage snapshots based on schedule, and securely stores them in the Object Storage within the same region. During backup, you can directly back up to Object Storage in other regions.
Object Storage replicates objects in buckets into different regions in an asynchronous and scheduled manner.
In a DR situation, the data can be recovered with the backup data replicated in other regions.

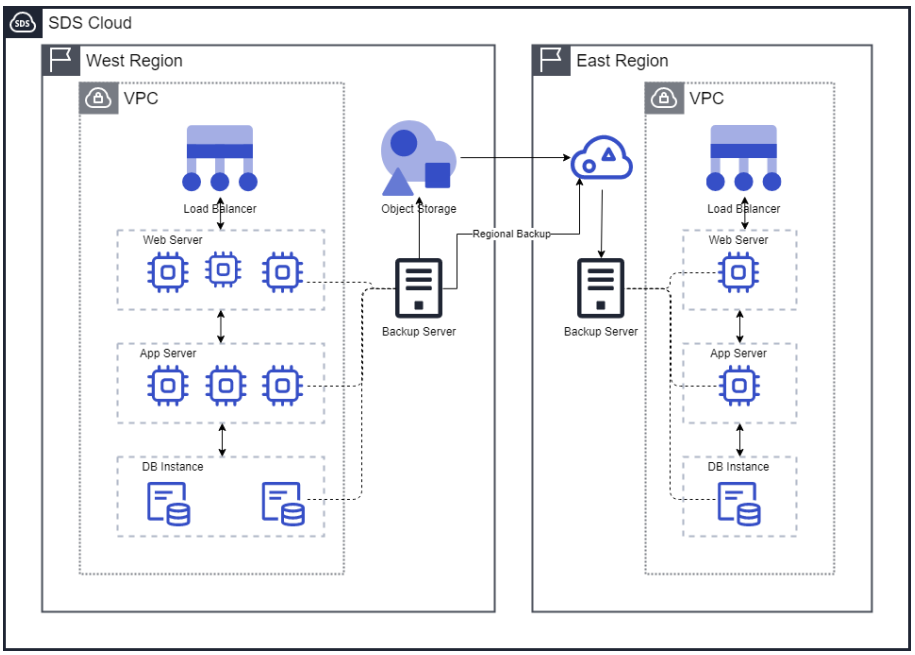

Figure 7. Disaster recovery using backup and restore methods

1. Install an agent on a server that needs backup and set up a backup policy (schedule backup) for each server.
2. Synchronize the Object Storage data using the replication lines between regions.
3. When a disaster occurs, virtual server resources are applied and the OS images backed up in the Object Storage are used to restore the server to resume service.

3.2 Warm standby

DB data, the core system of the business, takes a long time to recover, so backup and recovery methods cannot match higher levels of RPO and RTO.
SDS Cloud securely protects the DB system through real-time replication in the same region and can guarantee continuity of service with high availability HA solutions. In addition, async-based real-time replication is performed in other regions to provide replication at the near-zero RPO level. Web/WAS applications shorten the backup period using SDS backup solutions, to range from several minutes to several hours, depending on the amount of backup data and conducts recovery from DR sites.

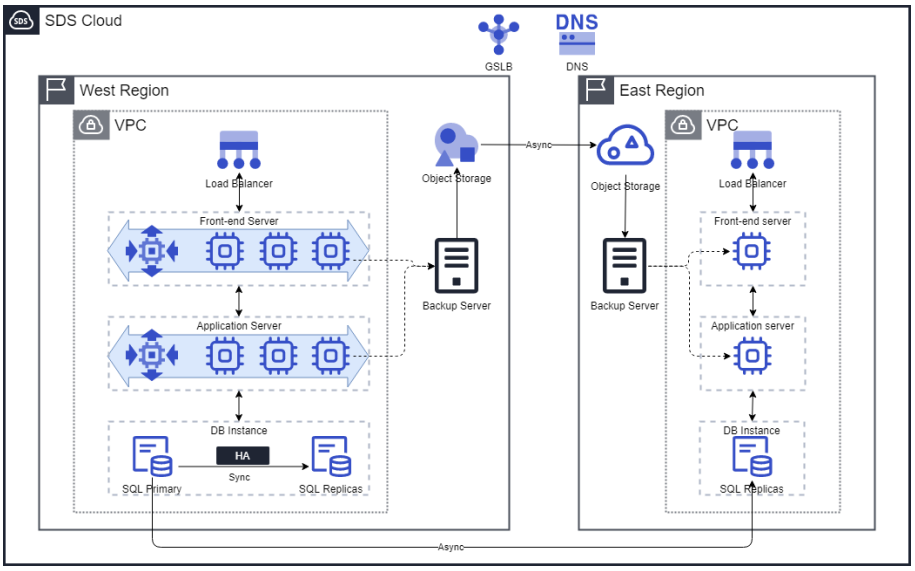

Figure 8. Disaster recovery using backup/restore and software-based replication solutions

1. Install the agent on the server that needs backup and set the backup policy (schedule backup) for each server. Synchronize the server through the replication lines between regions.
2. Synchronize the Object Storage data through the replication lines between regions.
3. DB service synchronizes data using the asynchronous replication solution among S/W replication methods.
4. When a disaster occurs, the Web/WAS recovers the OS images backed up in the Object Storage in the prepared Virtual Server, and the DB service is recovered using the asynchronous replicated data.

3.3 Hot standby

We provide the highest level of data protection and recovery through real-time replication for the entire business. We perform SW-based real-time replication for DB and file data stored in Block Storage as well as VM OS. The real-time replication for File Storage and Object Storage is based on physical storage. By providing real-time replication for the entire resource in the region, data is protected at the near-zero RPO level and fast recovery within 4hr is enabled.

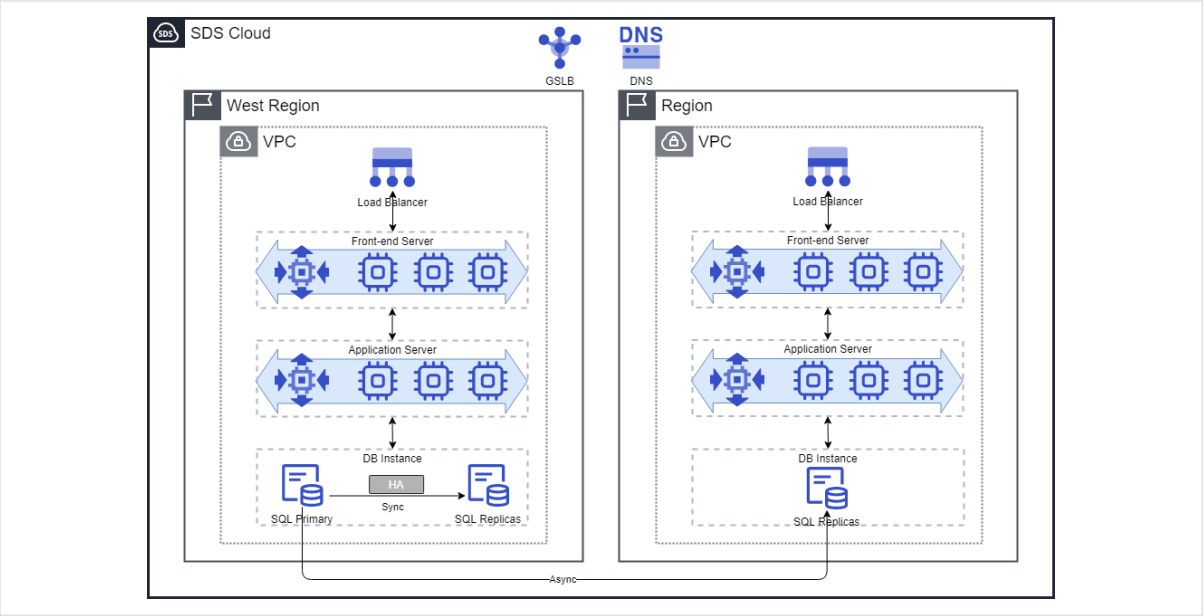

Figure 9. Disaster recovery using S/W based asynchronous replication

1. Set policy through S/W-based synchronization solutions for DB, web servers, and application servers. You can directly install and configure Virtual Servers and Bare Metal Servers after request in the main or DR sites.
2. File Storage and Object Storage set policy using a synchronization solution of physical storage. Apply for replication service when applying for initial storage offering or by making changes later.
3. Synchronize servers using the replication lines between regions. Apply for a dedicated replication network offering between main and DR sites and configure them directly.
4. When a disaster occurs, the service is restored with resources that have already been replicated in other regions.

SDS Cloud provides optimized high availability and disaster recovery solutions for enterprises and service continuity with validated solution partners.

3.4 Considerations

When DR is configured through interregional replication, you need to calculate the traffic usage to estimate the total network costs. In addition, policies such as backup cycles and replication periods should be properly configured to meet the RPO goals.
In particular, DR configuration with SDS Cloud resources for public cloud service requires analysis of the outbound replication traffic volume and network cost accordingly to make decisions.