Disaster recovery

Overview

The service provides IT service recovery using cloud resources located in other regions in the event of a failure or disaster such as an earthquake or fire, which is difficult to be recovered in a short period of time in the cloud infrastructure. Disaster recovery (DR) is an essential element that must be implemented to ensure business continuity in an enterprise.

Customers can build a cost-effective DR system by utilizing cloud resources. SDS Cloud configures different levels of service according to the level of disaster recovery targets, including RPO (Recovery Point Objective) and RTO (Recovery Time Objective). The backup & restore method is available for RPO of 24 hours and the warm standby method is available for RPO of 30 minutes. The level of RTO depends on the customer's DR policy.

Architecture Diagram

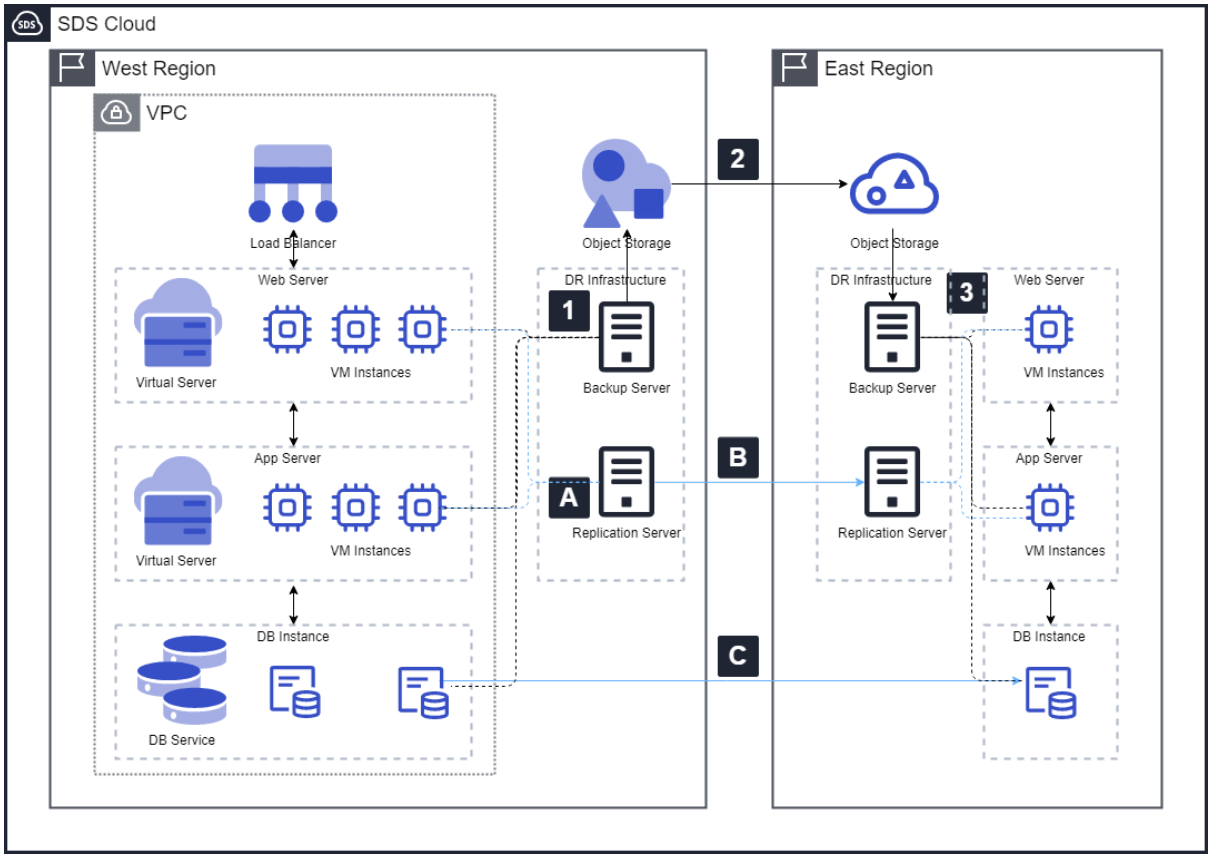

Figure 1. Backup and replication between regions

For RPO of 24 hours

1. Install the backup agent on the server to be backed up and set the backup policy on each server.
2. Synchronize the data in **Object Storage** between regions through a dedicated line for replication.
3. When a disaster occurs, request a **Virtual Server** resource, restore the server using the OS images backed up in **Object Storage**, and resume the service.

For RPO of 30 minutes

A. Install a synchronization software on the web server and application servers then set the synchronization policy.

B. Synchronize servers between regions through a dedicated line for replication.

C. **DB Service** synchronizes data through an asynchronous replication solution.

Use Cases

A. Service recovery in case of SDS Cloud west region failure

When IT resources of the region cannot be used due to a data center disaster (earthquake or fire), services can resume by using the resources that have been backed up or replicated in other regions.

If the RPO is low, low-cost **Object Storage** is used instead of separate **Virtual Server** resources, dramatically reducing overall DR cost.

B. Service transfer in case of public Cloud Service Provider(CSP) failure

For customers who choose a public CSP with services only in a single region, the service provider itself cannot configure the DR Site.

In the event of a failure in the Seoul region that prolongs without fast recovery, the service can be restored using SDS Cloud backup/replication resources.

SDS Cloud east region is geographically far enough away from the Seoul region and can be operated as a DR site even in disasters such as earthquakes.

Pre-requisites

Application for **Object Storage** resources is required.

Customers must pre-build backup infrastructure and a replication infrastructure for DR. This includes backup agent S/W licenses, master servers, proxy servers, replication S/W licenses, DB replication S/W licenses, and replication servers.

Limitations

The current **Backup** only provides agentless snapshot-based backup, and separate infrastructure must be installed for agent-based backup.

A separate service request is required to use **Object Storage** replication between regions.

Considerations

When DR is configured using interregional replication, you need to calculate the traffic usage to estimate the total network costs.

In addition, policies such as backup cycles should be properly configured to meet the RPO goals.

In particular, DR configuration for public cloud service requires decisions based on the analysis of outbound replication traffic volume and the applicable network cost.

Related Products

- Virtual Server
- Block Storage
- Object Storage
- Backup
- Load Balancer
- DB Service