Content sharing between multiple web instances with object storage

Overview

If there is a requirement for sharing images, videos, or other file content between web systems connected to the Internet, you can use a predefined, traditional web system interface. For files with simple requirements, it is also possible to use Object Storage to provide functions such as file downloads after checking the content list.

Object Storage is an object-based storage space with Internet access. Unlike Block Storage or File Storage, files can be uploaded/downloaded using Amazon S3 API anywhere by obtaining an access URL and key. Access from other CSPs (Cloud Service Providers) as well as on-premises are also allowed as long as the network path is secured.

This document describes how to share file contents between multiple web Instances through **Object Storage** endpoint URL and public access control, as well as Amazon S3 API among clients.

Architecture Diagram

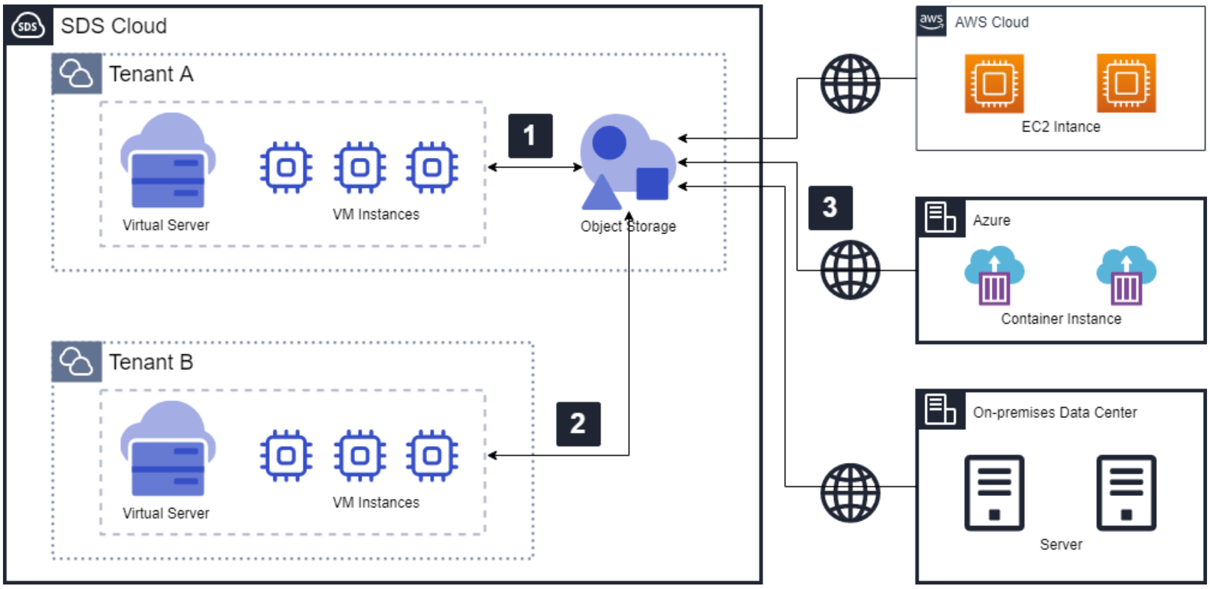

Figure 1. Content sharing between multiple web instances with object storage

Object Storage enables free content sharing between internal systems of SDS Cloud. Contents can also be shared with other external CSPs or on-premises systems through endpoint URL.

1. A tenant creates resources such as a **Virtual Server** in SDS Cloud and creates **Object Storage** to store/share content. After creating a bucket, an endpoint URL is obtained to access key/secret key.
2. If another tenant in the SDS Cloud wants to use a bucket in **Object Storage** used by Tenant A, the tenant requests the bucket owner to grant access to the endpoint URL and key.
3. In addition to SDS Cloud, it is also possible to access the bucket through the endpoint URL of another CSP or on-premises environments.

Use Cases

A. Linkage with applications using S3 API

SDS Cloud's Object Storage innately supports the Amazon S3 API. In the case of an application developed based on the S3 API, you can enjoy the effect of saving multi-cloud data without major code changes by simply adding a URL.

B. Content linkage using CDN and **Object Storage**

When distributing content through CDN, you can specify the bucket of **Object Storage** with static website hosting enabled as the source server for static content such as html and css.

Even if you do not use a CDN, you can distribute the deployment path by content with an application load balancer. For example, if a request is made with a basic content type such as /*.*, it is requested to the Web Application Server(WAS), and requests such as /images/* or /*.css can be set to go to the S3 bucket.

Pre-requisites

In order to read/write **Object Storage**, the access key and secret key of the corresponding bucket must be inquired to the bucket owner and notified in advance.

When connecting only with the endpoint URL (with active public access), only reading (GET) of the file is allowed.

Limitations

None

Considerations

A. Application aspect

Communication with **Object Storage** is done through S3 API, which means that all applications can communicate in the same way by simply changing the URL and key without changing the code. However, in the case of a client that did not previously use the S3 API, it is necessary to configure a library environment to use the S3 API in the client program.

B. Network environment aspect

Sites with strict network policies such as on-premises environments may require preliminary procedures such as opening a firewall to communicate with the endpoint URL IP address of Object Storage.

C. Security aspect

The transmitted file is encrypted and stored, and users who access without an access/secret key can only read the object. Still, the assignment manager to which the bucket belongs needs to manage the access key and secret key of the bucket to prevent exposure to unintended users.

Related Products

- Virtual Server
- Bare Metal Server
- Block Storage
- Object Storage
- Backup

- DB Service