Private Cloud Storage Access Through Load Balancer

Clean technical case study prepared by Hariharan J

Executive Summary

This case study shows a static-content access pattern using a private Cloud Storage bucket behind a global external application load balancer. The design focuses on controlled access, HTTPS delivery, backend bucket configuration, and validation of content routing.

Primary services	Cloud Storage, Backend Bucket, Global External Application Load Balancer, HTTPS
Goal	Serve content through a controlled load balancer path rather than direct public bucket access
Operational focus	Bucket setup, upload, routing, certificate readiness, and validation

Architecture

```
Client -> HTTPS load balancer frontend -> URL map -> backend bucket -> Cloud Storage object.
Access is validated through the load balancer endpoint.
```

Implementation Steps

- Create a Cloud Storage bucket and upload static website content.
- Configure backend bucket behavior and connect it to a URL map.
- Create frontend IP, target proxy, forwarding rule, and HTTPS certificate workflow.
- Test content delivery through the load balancer endpoint.
- Keep bucket access and routing aligned with the intended security model.

Validation

- Confirm bucket objects are reachable through the load balancer URL.
- Check HTTPS behavior and response headers.
- Verify that routing maps requests to the correct backend bucket.

Risks and Controls

- Misconfigured bucket permissions can expose content directly; mitigate with access review.
- Certificate or DNS mismatch can break HTTPS; mitigate with domain validation checks.
- Wrong URL map/backend binding can route traffic incorrectly; mitigate with endpoint tests.

Interview Talking Points

- Difference between direct bucket access and load-balancer-mediated access.
- How backend buckets work with application load balancers.

- Why HTTPS and DNS validation matter for production readiness.