Table of Contents

Integration of public cloud storage and CDNs into WLCG.................................................................1
Integration of public cloud storage and CDNs into WLCG

The following advice results from a discussion on these matters in March 2020 between the IGTF chair, the WLCG Security Officer and WLCG Ops Coordination.

Using public (cloud) storage and content delivery networks as part of our federated storage solutions can add both resilience as well as capacity in a simple way. To make these ‘truly ours’ requires a bit of thought around their naming, persistency, and authenticity. Many professional solutions offer ready-made solutions for this, of course usually as part of a managed (enterprise-class) solution. These include services like Google Cloud Storage, Cloudflare, &c.

Since you want your storage to be persistent, also choose (DNS) labels that are persistent and are yours. Use a (subdomain of) your own domain name, or register a ‘CDN domain’ that you own. Like "npohosting.nl" if you're "npo.nl", "wpcdn.com" if you're WordPress, or 'ncsa-security.net' if you are NCSA. Some services, including Google Cloud Storage, allow you to use a subdomain you can assign to your Layer-7 load balancer, like "bucketstore.npps.bnl.gov".

Providers of load balancers like GCP also offer you fixed external IP addresses for your loadbalancer. A good idea, since you can port these addresses to different instances and you will not have to deal with the DNS expiration issue (it saves you hours in case you migrate to a different endpoint with the same provider).

Once you have your own dedicated IP address and domain, providers will also allow you to attach your own certificate to it. This gives you organization-validated domains so that your cloud endpoint - which would otherwise be an easy target for phishing, for instance - becomes yours, and becomes interoperable with the rest of the federation. You can request a certificate yourself following your standard process (e.g. get an InCommon IGTF Server CA cert, or a GEANT TCS server cert) and upload that to your cloud provider. Taking Google Cloud Storage and its load balancer as an example, see here. For Cloudflare, you actually host the zone with them, and then upload your custom SSL certificate: see here.

This topic: LCG > CloudStorageIntegration
Topic revision: r1 - 2020-03-30 - MaartenLitmaath