Zesty.io Incident Report

Date: 01/06/2025
Affected Instance: All
Zesty.io Service: WebEngine

Introduction

On the morning of Jan 6, 2025 the Zesty service responsible for webpage rendering, WebEngine, experienced downtime. The downtime was due to an internal network change by our Infrastructure as a Service (IaaS) vendor, Google Cloud Platform (GCP). GCP changed local private cloud IP addresses to databases which the Zesty WebEngine service relied on for over 6 years. The IP change by GCP was unexpected and made without notification and caused a service interruption to the Zesty WebEngine service. The service interruption affected non-cached webpages from 6:55 AM PST to 10:20AM PST. During this time, Zesty Cloud customers experienced intermittent issues depending on webpage cache status at the CDN. Zesty Private Cloud(customer managed CDN) customers would have experienced origin downtime throughout this period.

All other Zesty services were operating normally. Applications built upon the instance api, accounts api, auth api, and/or media api all functioned properly. During this service disruption, all content manager user interfaces operated as normal.

Resolution

Zesty.io provisions a cluster of read-only content instance databases which are used for rendering customer pages per non-cached web request. Each database in the cluster has a unique internal network IP addresses which are stored in a dynamically accessed configuration file managed by Zesty, the address stored in this file enables the WebEngine service to make internal private cloud connections to the GCP managed databases. This architecture and connection process has been in place and operating without issue since 2018.

Our service provider, GCP, made no notice that these IP addresses would change. There are no logs from the service provider (GCP) which indicate that the IP addresses had changed.

The Zesty.io Engineering team went through standard incident response protocols which included attack vector identification, cloud scale health, abnormal service consumption rate checks, CDN health, and, but not limited to, log investigation. The team determined there was not an attacker, cloud scale was operating correctly, service consumption was normal, CDN was under normal loads, and logs were showing consistent timeouts. The team then began investigating novel concerns around logs showing timeouts to determine the root cause which

led to the IP change discovery. This was abnormal as downtimes are often due to attacks, not internal private cloud provider changes (which were unknown to the team).

Future Prevention

Our learning from this event has led to a series of changes to our internal protocol, technical implementation, and provider configuration. These changes are being made to prevent this type of incident from occurring again as well as implementing additional fault tolerances to prevent downtime from any related events that could cause customer downtime on the WebEngine service. Entailed below is the high-level approach to different areas of the system that will be improved in response to this incident.

Service Discovery

Currently the WebEngine service uses a standard process of making a database connection via an IP address. This method, as highlighted by this incident, is fragile as in the fine print of GCP's terms of service outlines that they do not provide a guarantee the IP address will retain. At the time we set up the Zesty WebEngine configuration, using local IP's from GCP was the most optimal option for setup. In order to prevent this issue from occurring in the future we will be exploring options for a service discovery type of connection to the database. Doing so will detach the database IP value from the service which relies on the database connection. Allowing IP values to change without affecting a service's ability to connect with the database.

IP Value Change Alerts

As noted in public reports of similar incidents the changing of GCP CloudSQL private IP address is an uncommon occurrence. Consistent with our experience of not seeing this type of incident occur over the past 6 years of this configuration. In order to reduce the potential impact of a change like this we need a monitor and alert in place which will notify us of this exact type of change. This will be implemented in health endpoints that are hit on the WebEngine service every second.

Stale If Error

Zesty.io Cloud customers are configured with a managed CDN service. This service should have served stale cache objects while receiving errors from the downstream origin(Zesty.io WebEngine). This behavior did not occur, causing errors to be served to end users instead of stale cache objects.

We will be working with our service provider to determine why this function did not operate properly and to ensure this proper functionality in the future. When 'stale if error' functions correctly, the Zesty CDN will fall back to the last cache served object rather than showing an error to a consumer. This behavior would ensure data availability during origin downtime failure due to dynamic connections or scale times.

Enhanced Health Checks for WebEngine

Existing health checks for WebEngine were designed to inform Google AppEngine when a pod is alive and available to receive new traffic. This code path does not include logic for database or cache connections. Meaning the WebEngine service currently responds healthy when pods support connection but does not ensure database connection availability. Health checks will be changed in the future to ensure database and cache connections are successfully created before reporting health.

Disabling Publishing and Extended Cache Times

The Zesty team has discussed the possibility of extending the cache duration (currently set to 24 hours or refreshed upon content publish) to a longer period, such as 14–30 days. This adjustment could help reduce the likelihood of cache objects expiring at inopportune times while still allowing for instant content updates whenever a user publishes new content.

A new feature is also being considered where the publish button in the content manager would disable itself if it detected an unhealthy state of the page rendering service WebEngine.

Incident Timeline

A summarized timeline highlighting key events related to Zesty support responses, engineering actions, service notifications, and customer reports. Please note, this is not a comprehensive list of all activities.

- **6:55 AM PST:** Internal incident notifications of elevated 500 class responses started from the WebEngine service
- **7:26 AM PST:** Incident is escalated internally by the Zesty.io support team
- **7:29 AM PST:** First customer report of service interruption
- **7:46 AM PST:** Zesty.io engineering team begins investigation based on protocol
- **7:58 AM PST:** Incident response call is started
- **8:12 AM PST:** Redeployment of service is initiated
- **8:47 AM PST**: Potential culprit traffic patterns are identified and blocked in an attempt to restore service
- **8:49 AM PST:** Ticket is opened with service provider (GCP/DOIT) support
- **9:05 AM PST:** Redeployment of service is initiated
- **9:14 AM PST:** Service provider support is invited to internal response call
- **9:22 AM PST:** Collaborated with DoIT on investigation of logs, customer coordination, and downtime protocol checks
- **9:50 AM PST:** Databases are restarted. In discussion with service provider support, restarting databases is theorized as a solution.

- **9:56 AM PST:** Engineering begins stepping through each point in the infrastructure to determine potential failure points
- **10:03 AM PST:** Database IP addresses are identified as having changed
- **10:07 AM PST:** Database IP addresses are updated, service starts to restore
- **10:20 AM PST:** Service determined as fully restored

Summary

On January 6, 2025, Zesty's WebEngine service experienced downtime from 6:55 AM PST to 10:20 AM PST due to an unnotified change in private database IP addresses by Google Cloud Platform (GCP), disrupting non-cached webpage rendering. While APIs and user interfaces remained operational, customers experienced intermittent issues depending on CDN cache status. The engineering team identified the root cause after standard incident response protocols and restored service by updating the IP addresses that GCP rotated without notification to the Zesty engineering team. To prevent recurrence, Zesty will implement dynamic service discovery, IP change monitoring, enhanced health checks, improved CDN cache handling, extended cache durations, and safeguards against publishing during outages. These measures aim to enhance fault tolerance and ensure greater service reliability.