Google Cloud Status Dashboard

This page provides status information on the services that are part of Google Cloud Platform. Check back here to view the current status of the services listed below. If you are experiencing an issue not listed here, please contact Support. Learn more about what's posted on the dashboard in this FAQ. For additional information on these services, please visit cloud.google.com.

Google App Engine Incident #16009

Networking issue with Google App Engine services

Incident began at **2016-08-22 07:05** and ended at **2016-08-22 07:30** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION
Aug 30, 2016	18:17	SUMMARY: On Monday 22 August 2016, the Google Cloud US-CENTRAL1-F zone lost network connectivity to services outside that zone for a duration of 25 minutes. All other zones in the US-CENTRAL1 region were unaffected. All network traffic within the zone was also unaffected. We apologize to customers whose service or application was affected by this incident. We understand that a network disruption has a negative impact on your application - particularly if it is homed in a single zone - and we apologize for the inconvenience this caused. What follows is our detailed analysis of the root cause and actions we will take in order to prevent this type of incident from recurring. DETAILED DESCRIPTION OF IMPACT: We have received feedback from customers asking us to specifically and separately enumerate the impact of incidents to any service that may have been touched. We agree that this will make it easier to reason about the impact of any particular event and we have done so in the following descriptions. On Monday 22 August 2016 from 07:05 to 07:30 PDT the Google Cloud US-CENTRAL1-F zone lost network connectivity to services outside that zone. App Engine 6% of App Engine Standard Environment applications in the US-CENTRAL region served elevated error rates for up to 8 minutes, until the App Engine serving infrastructure automatically redirected traffic to a failover zone. The aggregate error rate across all impacted applications during the incident period was 3%. The traffic redirection caused a Memcache flush for affected applications, and also loading requests as new instances of the applications started up in the failover zones. All App Engine Flexible Environment applications deployed to the US-CENTRAL1-F zone were unavailable for the duration of the incident. Additionally, 4.5% of these applications experienced various levels of unavailability for up to an additional 5 hours while the system recovered. Deployments for US-CENTRAL Flexible applications were delayed during the incident. Our engineers disabled the US-CENTRAL1-F zone for new deployments during the incident, so that any customers who elected to redeploy, immediately recovered. Cloud Console The Cloud Console was available during the incident, though some App Engine administrative pages did not load for applications in US-CENTRAL and 50% of project creation requests failed to complete and needed to be retried by customers before succeeding. Cloud Dataflow Some Dataflow running jobs in the US-CENTRAL1 region experienced delays in processing. Although most of the affected jobs recovered gracefully after the incident ended, up to 2.5% of affected jobs in this zone became stuck and required manual termination by customers. New jobs created during the incident were not impacted. Cloud SQL Cloud SQL First Generation instances were not impacted by this incident. 30% of Cloud SQL Second Generation instances in US-CENTRAL1 were unavailable for up to 5 minutes, after which they became available again. An additional 15% of Second Generation instances were unavailable for 22 minutes. Compute Engine All instances in the US-CENTRAL1-F zone were inaccessible from outside the zone for the duration of the incident. 9% of them remained inaccessible from outside the zone for an additional hour. Container Engine Container Engine clusters running in US-CENTRAL1-F were inaccessible from outside of the zone during the incident although they continued to serve. In addition, calls to the Container Engine API experienced a 4% error rate and elevated latency during the incident, though this was substantially mitigated if the client retried the request. Stackdriver Logging 20% of log API requests sent to Stackdriver Logging in the US-CENTRAL1 region failed during the incident, though App Engine logging was not impacted. Clients retrying requests recovered gracefully. Stackdriver Monitoring Requests to the StackDriver web interface and the Google Monitoring API v2beta2 and v3 experienced elevated latency and an error rate of up to 3.5% during the incident. In addition, some alerts were delayed. Impact for API calls was substantially mitigated if the client retried the request. ROOT CAUSE: On 18 July, Google carried out a planned maintenance event to inspect and test the UPS on a power feed in one zone in the US-CENTRAL1 region. That maintenance disrupted one of the two power feeds to network devices that control routes into and out of the US-CENTRAL1-F zone. Although this did not cause any disruption in service, these devices unexpectedly and silently disabled the affected power supply modules - a previously unseen behavior. Because our monitoring systems did not notify our network engineers of this problem the power supply modules were not re-enabled after the maintenance event. The service disruption was triggered on Monday 22 August, when our engineers carried out another planned maintenance event that removed power to the second power feed of these devices, causing them to disable the other power supply module as well, and thus completely shut down. Following our standard procedure when carrying out maintenance events, we made a detailed line walk of all critical equipment prior to, and after, making any changes. However, in this case we did not detect the disabled power supply modules. Loss of these network devices meant that machines in US-CENTRAL1-F did not have routes into and out of the zone but could still communicate to other machines within the same zone. REMEDIATION AND PREVENTION: Our network engineers received an alert at 07:14, nine minutes after the incident started. We restored power to the devices at 07:30. The network returned to service without further intervention after power was restored. As immediate followup to this incident, we have already carried out an audit of all other network devices of this type in our fleet to verify that there are none with disabled power supply modules. We have also written up a detailed post mortem of this incident and will take the following actions to prevent future outages of this type: Our monitoring will be enhanced to detect cases in which power supply modules are disabled. This will ensure that conditions that are missed by the manual line walk prior to maintenance events are picked up by automated monitoring. We will change the configuration of these network devices so that power disruptions do not cause them to disable their power supply modules. The interaction between the network control plane and the data plane should be such that the data plane should "fail open" and continue to route packets in the event of control plane failures. We will add support for networking protocols that have the capability to continue to route traffic for a short period in the event of failures in control plane components. We will also be taking various actions to improve the resilience of the affected services to single-zone outages, including the following: App Engine Although App Engine Flexible Environment is currently in Beta, we expect production services to be more resilient to single zone disruptions. We will make this extra resilience an exit criteria before we allow the service to reach General Availability. Cloud Dataflow We will improve resilience of Dataflow to single-zone outages by implementing better strategies for migrating the job controller to a new zone in the event of an outage. Work on this remediation is already underway. Stackdriver Logging We will make improvements to the Stackdriver Logging service (currently in Beta) in the areas of automatic failover and capacity management before this service goes to General Availability. This will ensure that it is resilient to single-zone outages. Stackdriver Monitoring The Google Monitoring API (currently in beta) is already hosted in more than one zone, but we will further improve its resilience by adding additional capacity to ensure a single-zone outage does not cause overload in any other zones. We will do this before this service exits to General Availability. Finally, we know that you depend on Google Cloud Platform for your production workloads and we apologize for the inconvenience this event caused.
Aug 22, 2016	07:58	The issue with network connectivity to Google App Engine applications should have been resolved for all affected users as of 07:20 US/Pacific. We will conduct an internal investigation of this issue and make appropriate improvements to our systems to prevent or minimize future recurrence. We will provide a more detailed analysis of this incident once we have completed our internal investigation.
Aug 22, 2016	07:28	We are investigating an issue with network connectivity. We will provide more information by 08:00 US/Pacific.

All times are US/Pacific