






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 Cloud Infrastructure Components Incident #20005

We are investigating an issue with elevated error rates across multiple Google Cloud Platform Services

Incident began at **2020-04-08 06:48** and ended at **2020-04-08 07:42** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION
<div></div> Apr 13, 2020	09:19	<div><h4>ISSUE SUMMARY (All times in US/Pacific daylight time)</h4><p>On Wednesday 08 April, 2020 beginning at 06:48 US/Pacific, Google Cloud Identity and Access Management (IAM) experienced significantly elevated error rates for a duration of 54 minutes. IAM is used by several Google services to manage user information, and the elevated IAM error rates resulted in degraded performance that extended beyond 54 minutes for the following Cloud services:</p><ul style="list-style-type: none">- Google BigQuery's streaming service experienced degraded performance for 116 minutes;- Cloud IAM's external API returned elevated errors for 102 minutes;- 3% of Cloud SQL HA instances were degraded for durations ranging from 54 to 192 minutes.<p>To our Cloud customers whose businesses were impacted during this disruption, we sincerely apologize – we have conducted a thorough internal investigation and are taking immediate action to improve the resiliency, performance, and availability of our service.</p><h4>ROOT CAUSE</h4><p>Many Cloud services depend on a distributed Access Control List (ACL) in Cloud Identity and Access Management (IAM) for validating permissions, activating new APIs, or creating new Cloud resources. Cloud IAM in turn relies on a centralized and planet-scale system to manage and evaluate access control for data stored within Google, known as Zanzibar [1]. Cloud IAM consists of regional and global instances; regional instances are isolated from each other and from the global instance for reliability. However, some specific IAM checks, such as checking an organizational policy, reference the global IAM instance. The trigger of this incident was a rarely-exercised type of configuration change in Zanzibar which also impacted Cloud IAM. A typical change to this configuration mutates existing configuration namespaces, and is gradually rolled out through a sequence of canary steps. However, in this case, a new configuration namespace was added, and a latent issue with our canarying system allowed this specific type of configuration change to propagate globally in a rapid manner. As the configuration was pushed to production, the global Cloud IAM service quickly began to experience internal errors. This resulted in downstream operations with a dependency on global Cloud IAM to fail.</p><p>[1] https://research.google/pubs/pub48190/</p><h4>REMEDIATION AND PREVENTION</h4><p>Google engineers were automatically alerted to elevated error rates affecting Cloud IAM at 2020-04-08 06:52 US/Pacific and immediately began investigating. By 07:27, the engineering team responsible for managing Zanzibar identified the configuration change responsible for the issue, and swiftly reverted the change to mitigate. The mitigation finished propagating by 07:42, partially resolving the incident for a majority of internal services. Specific services such as the external Cloud IAM API, high-availability Cloud SQL, and Google BigQuery streaming took additional time to recover due to complications arising from the initial outage. Services with extended recovery timelines are described in the "detailed description of impact" section below.</p><p>Google's standard production practice is to push any change gradually, in increments designed to maximize the probability of detecting problems before they have broad impact. Furthermore, we adhere to a philosophy of defence-in-depth: when problems occur, rapid mitigations (typically rollbacks) are used to restore service within service level objectives. In this outage, a combination of bugs resulted in these practices failing to be applied effectively. In addition to rolling back the configuration change responsible for this outage, we are fixing the issue with our canarying and release system that allowed this specific class of change to rapidly roll out globally; instead, such changes will in the future be subject to multiple layers of canarying, with automated rollback if problems are detected, and a progressive deployment over the course of multiple days. Both Cloud IAM and Zanzibar will enter a change freeze to prevent the possibility of further disruption to either service before these changes are implemented.</p><p>We truly understand how important regional reliability is for our users and deeply apologize for this incident.</p><h4>DETAILED DESCRIPTION OF IMPACT</h4><p>On Wednesday 08 April, 2020 from 6:48 to 7:42 US/Pacific, Cloud IAM experienced an outage, which had varying degrees of impact on downstream services as described in detail below.</p><h5>Cloud IAM</h5><p>Experienced a 100% error rate globally on all internal Cloud IAM API requests from 6:48 - 7:42. Upon the internal Cloud IAM service becoming unavailable (which impacted downstream Cloud services), the external Cloud IAM API also began returning HTTP 500 INTERNAL_ERROR codes. The rate and volume of incoming requests (due to aggressive retry policies) triggered the system's Denial of Service (DoS) protection mechanism. The automatic DoS protection throttled the service, implementing a rate-limit on incoming requests resulting in query failures and a large volume of retry attempts. Upon the incident's mitigation, the DoS protection was removed but took additional time to propagate across the fleet. Its removal finished propagating by 8:30, returning the service to normal operation.</p><h5>Gmail</h5><p>Experienced delays receiving and sending emails from 6:50 to 7:39. For inbound emails, 20% G Suite emails, 21% of G Suite customers, and 0.3% of consumer emails were affected. For outbound emails (including Gmail-to-Gmail) 1.3% of G Suite emails, and 0.3% of consumer emails were affected. Message delay period varied, with the 50th percentile peaking at 3.7 seconds, up to 2580 seconds for the 90th percentile.</p><h5>Compute Engine</h5><p>Experienced a 100% error rate when performing firewall modifications or create, update, or delete instance operations globally from 6:48 to 7:42.</p><h5>Cloud SQL</h5><p>Experienced a 100% error rate when performing instance creation, deletion, backup, and failover operations globally for high-availability (HA) instances from 6:48 - 7:42, due to the inability to authenticate VMs via the Cloud IAM service.</p><p>Additionally, Cloud SQL experienced extended impact from this outage for 3% of HA instances. Such instances initiated failover when upstream health metrics were not propagated due to the Cloud IAM issues. HA instances automatically failed over in an attempt to recover from what was believed to be failures occurring on the master instances. Upon failing over, these instances became stuck in a failed state. The Cloud IAM outage prevented the master's underlying data disk from being attached to the failover instance, leaving the failover instance in a stuck state. These stuck instances required manual engineer intervention to bring them back online. Affected instances impact ranged from 6:48 - 10:00 for a total duration of 3 hours and 12 minutes.</p><p>To prevent HA Cloud SQL instances from encountering these failures in the future, we will change the auto-failover system to avoid triggering based on IAM issues. We are also re-examining the auto-failover system more generally to make sure it can distinguish a real outage from a system-communications issue going forward.</p><h5>Cloud Pub/Sub</h5><p>Experienced 100% error rates globally for Topic administration operations (create, get, and list) from 6:48 - 7:42.</p><h5>Kubernetes Engine</h5><p>Experienced a 100% error rate for cluster creation requests globally from 6:49 - 7:42.</p><h5>BigQuery</h5><p>Datasets.get and projects.getServiceAccount experienced nearly 100% failures globally from 6:48 - 7:42. Other dataset operations experienced elevated error rates up to 40% for the duration of the incident. BigQuery streaming was also impacted in us-east1 for 6 minutes, us-east4 for 20 minutes, asia-east1 for 12 minutes, asia-east2 for 40 minutes, europe-north1 for 11 minutes, and the EU multi-region for 52 minutes. With most of the above regions experiencing up to a maximum of 30% average error rates, The EU multi-region, US multi-region, and us-east2 regions specifically experienced higher error rates, reaching nearly 100% for the duration of their impact windows.</p><p>Additionally, BigQuery streaming in the US multi-region experienced issues coping with traffic volume once IAM recovered. BigQuery streaming in the US multi-region experienced a 55% error rate from 7:42 - 8:44 for a total impact duration of 1 hour and 56 minutes.</p><h5>App Engine</h5><p>Experienced a 100% error rate when creating, updating, or deleting app deployments globally from 6:48 to 7:42. Public apps did not have HTTP serving affected.</p><h5>Cloud Run</h5><p>Experienced a 100% error rate when creating, updating, or deleting deployments globally from 6:48 to 7:42. Public services did not have HTTP serving affected.</p><h5>Cloud Functions</h5><p>Experienced a 100% error rate when creating, updating, or deleting functions with access control [2] globally from 6:48 to 7:42. Public functions did not have HTTP serving affected.</p><p>[2] https://cloud.google.com/functions/docs/concepts/iam</p><h5>Cloud Monitoring</h5><p>Experienced intermittent errors when listing workspaces via the Cloud Monitoring UI from 6:42 - 7:42.</p><h5>Cloud Logging</h5><p>Experienced average and peak error rates of 60% for ListLogEntries API calls from 6:48 - 7:42. Affected customers received INTERNAL_ERRORS. Additionally, create, update, and delete sink calls experienced a nearly 100% error rate during the impact window. Log ingestion and other Cloud Logging APIs were unaffected.</p><h5>Cloud Dataflow</h5><p>Experienced 100% error rates on several administrative operations including job creation, deletion, and autoscaling from 6:55 - 7:42.</p><h5>Cloud Dataproc</h5><p>Experienced a 100% error rate when attempting to create clusters globally from 6:50 - 7:42.</p><h5>Cloud Data Fusion</h5><p>Experienced a 100% error rate for create instance operations globally from 6:48 - 7:42.</p><h5>Cloud Composer</h5><p>Experienced 100% error rates when creating, updating, or deleting Cloud Composer environments globally between 6:48 - 7:42. Existing environments were unaffected.</p><h5>Cloud AI Platform Notebooks</h5><p>Experienced elevated average error rates of 97.2% (peaking to 100%) from 6:52 - 7:48 in the following regions: asia-east1, asia-northeast1, asia-south1, australia-southeast1, europe-west1, europe-west6, northamerica-northeast1, southamerica-east1, and us-west1.</p><h5>Cloud KMS</h5><p>Experienced a 100% error rate for Create operations globally from 6:49 - 7:40.</p><h5>Cloud Tasks</h5><p>Experienced an average error rate of 8% (up to 15%) for CreateTasks, and a 96% error rate for AddTasks in the following regions: asia-northeast3, asia-south1, australia-southeast1, europe-west1, europe-west6, northamerica-northeast1, southamerica-east1, us-central1, us-east4, and us-west3. Delivery of existing tasks were unaffected, but downstream services may have experienced other issues as documented.</p><h5>Cloud Scheduler</h5><p>Experienced 100% error rates for CreateJob and UpdateJob requests globally from 6:48 - 7:42.</p><h5>App Engine Task Queues</h5><p>Experienced an average error rate of 18% (up to 25% at peak) for UpdateTask requests from 6:48 - 7:42.</p><h5>Cloud Build</h5><p>Experienced no API errors, however, all builds submitted between 6:48 and 7:42 were queued until the issue was resolved.</p><h5>Cloud Deployment Manager</h5><p>Experienced an elevated average error rate of 20%, peaking to 36% for operations globally between 6:49 and 7:39.</p><h5>Data Catalogue</h5><p>Experienced a 100% error rate for API operations globally from 6:48 - 7:42.</p><h5>Firebase Real-time Database</h5><p>Experienced elevated average error rates of 7% for REST API and long-polling requests (peaking to 10%) during the incident window.</p><h5>Firebase Test Lab</h5><p>Experienced elevated average error rates of 85% (peaking to 100%) globally for Android tests running on virtual devices in Google Compute Engine instances. Impact lasted from 6:48 - 7:54 for a duration of 1 hour and 6 minutes.</p><h5>Firebase Hosting</h5><p>Experienced a 100% error rate when creating new versions globally from 6:48 - 7:42.</p><h5>Firebase Console</h5><p>Experienced a 100% error rate for developer resources globally. Additionally, the Firedata API experienced an average error rate of 20% for API operations from 6:48 - 7:42</p><p>Affected customers experienced a range of issues related to the Firebase Console and API. API invocations returned empty lists of projects, HTTP 404 errors, affected customers were unable to create, delete, update, or list many Firebase entities including (Android, iOS, and Web Apps), hosting sites, Real-time Database instances, Firebase-linked GCP buckets. Firebase developers were also unable to update billing settings. Firebase Cloud Functions could not be deployed successfully. Some customers experienced quota exhaustion errors due to extensive retry attempts.</p><h5>Cloud IoT</h5><p>Experienced a 100% error rate when performing DeleteRegistry API calls from 6:48 - 7:42. Though DeleteRegistry API calls threw errors, the deletions issued did complete successfully.</p><h5>Cloud Memorystore</h5><p>Experienced a 100% error rate for create, update, cancel, delete, and ListInstances operations on Redis instances globally from 6:48 - 7:42.</p><h5>Cloud Filestore</h5><p>Experienced an average error rate of 70% for instance and snapshot creation, update, list, and deletion operations, with a peak error rate of 92% globally between 6:48 and 7:45.</p><h5>Cloud Healthcare and Cloud Life Sciences</h5><p>Experienced a 100% error rate for CreateDataset operations globally from 6:48 - 7:42.</p><h4>SLA CREDITS</h4><p>If you believe your paid application experienced an SLA violation as a result of this incident, please populate the SLA credit request: https://support.google.com/cloud/contact/cloud_platform_sla</p><p>A full list of all Google Cloud Platform Service Level Agreements can be found at https://cloud.google.com/terms/sla/.</p><p>For G Suite, please request an SLA credit through one of the Support channels: https://support.google.com/a/answer/104721</p><p>G Suite Service Level Agreement can be found at https://gsuite.google.com/intl/en/terms/sla.html</p></div>
<div></div> Apr 08, 2020	08:57	<p>As of 08:36 US/Pacific, the issue affecting multiple Google Cloud services has been resolved for all users.</p> <p>We will publish an analysis of this incident once we have completed our internal investigation.</p> <p>We thank you for your patience while we've worked on resolving the issue.</p>
<div></div> Apr 08, 2020	08:10	<p>Description: We are experiencing an issue in Cloud IAM which is impacting multiple services.</p> <p>Mitigation work is currently underway by our engineering team. We believe that most impact was mitigated at 07:40 US/Pacific, allowing many services to recover. Impact is now believed to be limited more directly to use of the IAM API.</p> <p>We will provide an update by Wednesday, 2020-04-08 09:00 US/Pacific with current details.</p> <p>Diagnosis: App Engine, Cloud Functions, Cloud Run, Dataproc, Cloud Logging, Cloud Monitoring, Cloud Build, Cloud Pub/Sub, BigQuery, Compute Engine, Cloud Tasks, Cloud Memorystore, Firebase Test Lab, Firebase Hosting, Cloud Networking, Cloud Data Fusion, Cloud Kubernetes Engine, Cloud Composer, Cloud SQL, and Firebase Realtime Database may experience elevated error rates.</p> <p>Additionally, customers may be unable to file support cases.</p> <p>Workaround: Customers may continue to file cases using https://support.google.com/cloud/contact/prod_issue or via phone.</p>
<div></div> Apr 08, 2020	07:49	<p>Description: We are experiencing an issue with Google Cloud infrastructure components beginning on Wednesday, 2020-04-08 06:52 US/Pacific.</p> <p>Symptoms: elevated error rates across multiple products.</p> <p>Customers may be experiencing an issue with Google Cloud Support in which users are unable to create new support cases.</p> <p>Customers may continue to file cases using a https://support.google.com/cloud/contact/prod_issue or via phone.</p> <p>Our engineering team continues to investigate the issue.</p> <p>We will provide an update by Wednesday, 2020-04-08 08:15 US/Pacific with current details.</p> <p>We apologize to all who are affected by the disruption.</p> <p>Diagnosis: Customers may be unable to create new support cases.</p> <p>Workaround: Customers may continue to file cases using a https://support.google.com/cloud/contact/prod_issue or via phone.</p>
<div></div> Apr 08, 2020	07:44	<p>Description: We are experiencing an issue with Google Cloud infrastructure components.</p> <p>Symptoms: elevated error rates across multiple products.</p> <p>Our engineering team continues to investigate the issue.</p> <p>We will provide an update by Wednesday, 2020-04-08 08:15 US/Pacific with current details.</p> <p>We apologize to all who are affected by the disruption.</p> <p>Workaround: None at this time.</p>