

## 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 #20010

We are experiencing an issue with multiple GCP products.

Incident began at **2020-09-24 18:00** and ended at **2020-09-24 18:33** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION
------	------	-------------

Sep 30, 2020

21:55

### BACKGROUND

Google's Global Service Load Balancer (GSLB) is a collection of software and services that load balance traffic across Google properties. There are two main components, a control plane, and a data plane. The control plane provides programming to the data plane on how to handle requests. A key component of the data plane is the Google Front End (GFE). The GFE is an HTTP/TCP reverse proxy which is used to serve requests to many Google properties including: Search, Ads, G Suite (Gmail, Chat, Meet, Docs, Drive, etc.), Cloud External HTTP(S) Load Balancing, Proxy/SSL Load Balancing, and many Cloud APIs.

Google's Global Load Balancers are implemented using a GFE architecture that has two tiers in some cases. The first tier of GFEs are situated as close to the user as possible to minimize latency during connection setup. First tier GFEs route requests either directly to applications, or in some cases to a second tier of GFEs providing additional functionality, before routing to applications. This architecture allows clients to have low latency connections anywhere in the world, while taking advantage of Google's global network to serve requests to backends, regardless of region.

The pool of GFE instances which were impacted in this incident are part of the second tier, handling a subset of Google services. Therefore, this incident only impacted services routed through this specific pool.

### ISSUE SUMMARY

On Thursday 24 September, 2020 at 18:00 US/Pacific, one of Google's several second-tier GFE pools experienced intermittent failures resulting in impact to several downstream services. Almost all services recovered within the initial 33 minutes of the incident; exceptions are outlined in the detailed impact section below. Affected customers experienced elevated error rates and latency when connecting to Google APIs. Existing workloads (i.e. running instances on GCE, or containers on GKE) were not impacted unless they needed to invoke impacted APIs.

Service impact can be divided into two categories, direct and indirect. Services which have a request path that flows through the impacted GFE pool would have been directly impacted. Calls to these services would have experienced higher latency or elevated errors in the form of HTTP 502 response codes. Alternatively, services which did not directly rely on this pool of impacted GFEs may invoke other services, such as authentication, that depend on this shared pool of GFEs. This indirect impact would have varied between customers. One example of this, which we expect to be one of the most common forms of indirect impact, would be use of an oauth token that needed to be refreshed or retrieved. While a service such as Cloud Spanner may not have been serving errors, customers using the Cloud Spanner Client may have seen errors when the client attempted to refresh credentials, depending on the API used to refresh/obtain the credential. A detailed description of impact can be found below.

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 services.

### ROOT CAUSE

For any given pool of tasks, the GFE control plane has a global view of capacity, service configurations, and network conditions, which are all combined and sent to GFEs to create efficient request serving paths. This global view allows requests to be routed seamlessly to other regions, which is useful in scenarios like failover or for load balancing between regions. GFEs are grouped into pools for a variety of traffic profiles, health checking requirements, and other factors; the impacted second-layer GFE pool was used by multiple services.

The GFE control plane picks up service configuration changes and distributes them to GFEs. For this incident, two service changes contained an error that resulted in a significant increase in the number of backends accessed by GFEs in this pool. The particular nature of these changes additionally meant that they would be distributed to all GFEs in this pool globally, instead of being limited to a particular region. While the global aspect was intended, the magnitude of backend increases was not. The greatly increased number of programmed backends caused GFEs to exceed their memory allocation in many locations.

GFE has many internal protections which are activated when there is memory pressure, such as closing idle connections or refusing to accept new connections, allowing them to keep running despite a memory shortage. Tasks which exceeded memory limits were terminated. The combination of a reduced number of available GFEs and a reduction in accepted connections meant that traffic to services behind the impacted GFE pool dropped by 50%.

### REMEDIATION AND PREVENTION

Google engineers were alerted to the outage three minutes after impact began at 2020-09-24 18:03, and immediately began an investigation. At 18:15 the first service change, which significantly increased the number of programmed backends, was rolled back. At 18:18 the second service configuration change was rolled back. Google engineers started seeing recovery at 18:20 and at 18:33 the issue was fully mitigated.

GFE is one of the most critical pieces of infrastructure at Google and has multiple lines of defense in depth, both in software and operating procedure. As the result of this outage, we are adding additional protections to both in order to eliminate this class of failure. As an immediate step we have limited the type of configuration changes that can be made until additional safeguards are in place. Those additional safeguards will include stricter validation of configuration changes, specifically, rejecting changes that cause a large increase in backend count across multiple services. In addition to a check in the control plane, we will be augmenting existing protections in the GFE against unbounded growth in any resource dimension, such as backend counts. We will also be performing an audit of existing configurations and converting risky configurations to alternative setups. A restriction will be placed on certain configuration options, only allowing use with additional review and allow lists. Finally, an audit will be performed of services in shared GFE pools, with additional pools being created to reduce impact radius, should an issue in this part of the infrastructure surface again.

### DETAILED DESCRIPTION OF IMPACT

On 2020-09-24 from 18:00 to 18:33 US/Pacific (unless otherwise noted) the following services were impacted globally:

#### OAuth

The following OAuth paths were impacted and returned errors for 50% of requests during the impact period. Impact perceived by customers may have been less as many client libraries make requests to these paths asynchronous to refresh tokens before they expire and retry their requests upon failure, potentially receiving successful responses:

–

oauth2.googleapis.com/token

–

accounts.google.com/o/oauth2/token

–

www.youtube.com/o/oauth2/token

–

www.googleapis.com/o/oauth2/token

–

www.googleapis.com/oauth2/(v3,v4)/token

–

accounts.(google,youtube).com/o/oauth2/(revoke,device/code,tokeninfo)

–

www.googleapis.com/oauth2/v3/authdevice

–

www.googleapis.com/oauth2/v2/IssueToken

–

oauthaccountmanager.googleapis.com

–

The following APIs were NOT affected:

–

www.googleapis.com/oauth2/(v1,v2,v3)/certs

–

contents.googleapis.com/oauth2/(v1,v2,v3)/certs

–

contents6.googleapis.com/oauth2/(v1,v2,v3)/certs

–

iamcredentials.googleapis.com and accounts.google.com (other than specific URIs mentioned above) were not affected.

–

#### Chat

Google Chat experienced an elevated rate of HTTP 500 & 502 errors (averaging 34%) between 18:00 and 18:04, decreasing to a 7% error rate from 18:04 to 18:14, with a mean latency of 500ms. This resulted in affected users being unable to load the Chat page or to send Chat messages.

#### Classic Hangouts

Classic Hangouts experienced an elevated error rate of HTTP 500 errors (reducing Hangouts traffic by 44%) between 18:00 and 18:25. The service error rate was below 1% for Hangouts requests within the product, including sending messages.

#### Meet

Google Meet experienced error rates up to 23% of requests between 18:02 and 18:23. Affected users observed call startup failures which affected 85% of session attempts. Existing Meet sessions were not affected.

#### Voice

Google Voice experienced a 66% drop in traffic between 18:00 and 18:24. Additionally, the service had an elevated error rate below 1% between 18:01 and 18:14, and an average of 100% increase in mean latency between 18:03 and 18:12.

#### Calendar

Google Calendar web traffic observed up to a 60% reduction in traffic, and an elevated HTTP 500 error rate of 4.8% between 18:01 and 18:06, which decreased to and remained below 1% for the remainder of the outage. Calendar API traffic observed up to a 53% reduction in traffic, with an average error rate of 2% for the same period. The traffic reduction corresponded with HTTP 500 errors being served to users.

#### Groups

Google Groups web traffic dropped roughly 50% for the classic UI, and 30% for the new UI. Users experienced an average elevated HTTP 500 error rate between 0.12 and 3%.

#### Gmail

Gmail observed a 35% drop in traffic due to the GFE responding with HTTP 500 errors. The service error rate remained below 1% for the duration of the incident. This affected Gmail page loading and web interactions with the product.

#### Docs

Google Docs witnessed a 33% drop in traffic between 18:00 and 18:23, corresponding with the GFE returning HTTP 500 errors to user interactions. Additionally, between 18:01 and 18:06 the service error rate rose to 1.4%, before decreasing and remaining at approximately 0.3% until 18:23.

#### Drive

Google Drive observed a 60% traffic drop between 18:00 and 18:23, corresponding with the GFE returning HTTP 500 errors to user interactions. The Drive API experienced a peak error rate of 7% between 18:02 to 18:04, and then between 1% and 2% until 18:25. Google Drive web saw up to a 4% error rate between 18:01 and 18:06. 50th percentile latency was unaffected, but 95th percentile rose up to 1.3s between 18:02 and 18:06.

#### Cloud Bigtable

Some clients using the impacted OAuth authentication methods described above were unable to refresh their credentials and thus unable to access Cloud Bigtable. Clients using alternative authentication methods were not impacted. Impacted clients experienced elevated error rates and latency. The main impact was to clients accessing Cloud Bigtable from outside of GCP, there was a 38% drop in this traffic during the impact period.

#### Cloud Build API

Cloud Build API experienced elevated error rates due to a 50% loss of incoming traffic over 26 minutes before reaching the service front end. Additionally, 4% of Cloud Builds failed due receiving errors from other Google services

#### Cloud Key Management Service (KMS)

Cloud KMS was unable to receive API requests from GFE for ~33 minutes starting at 18:00 impacting non-Customer Managed Encryption Key (CMEK) customers. CMEK customers were not impacted.

#### Cloud Logging

Cloud Logging experienced increased error rates (25% average, up to 40% at peak) from 18:05 to 18:50. Customers would have experienced errors when viewing logs in the Cloud Console. Data ingestion was not impacted.

#### Cloud Monitoring

Cloud Monitoring API experienced elevated error rates (50% average, up to 80% at peak) of uptime checks and requests from 18:00 - 18:26. This affected cloud uptime workers running uptime checks.

#### Cloud Networking API

Cloud Networking API experienced up to 50% error rate for Network Load Balancer Creation from 18:00 to 18:20 due to downstream service errors. Additionally up to 35% of HTTP(S) Load Balancer or TCP/SSL Proxy Load Balancer creation requests failed from 18:00 - 18:28 due to downstream service errors. Traffic for existing load balancers was unaffected.

#### Google Compute Engine API

The Google Compute Engine (GCE) API experienced an error rate of up to 50% from 18:00 - 18:25 with affected users experiencing HTTP 502 error response codes. This would have prevented loading the GCE portion of the Cloud Console as well listing, modifying, and creating GCE resources via other API clients. This applies only to the GCE API. GCE instance connectivity and availability was not impacted. Please note that some GCP services were served by the impacted GFE pool, so customer workloads running inside compute instances may have seen impact if they depend on other GCP services that experienced impact. Autoscaler continued to function nominally during the outage window.

#### Cloud Profiler

Cloud Profiler API experienced an elevated rate of HTTP 502 errors due to an up to 50% reduction in global traffic for all requests.

#### Cloud Run API

Cloud Run API experienced an elevated rate of HTTP 502 errors up to 70% from 18:00 to 18:30. Existing Cloud Run deployments were unaffected.

#### Cloud Spanner

Cloud Spanner clients experienced elevated error rates due to authentication issues which caused a 20% drop in traffic. Impacted customers saw increased latency and errors accessing Cloud Spanner. Clients using alternative authentication methods, such as GKE Workload Identity, were not impacted.

#### Game Servers

Game Servers experienced elevated request latencies of up to 4x normal levels during the incident window, resulting in some clients experiencing connection timeouts and increased retry attempts. The service did not experience elevated error rates.

#### Google Cloud Console

4.18% of customers experienced "The attempted action failed" error messages when attempting to load pages in the Cloud Console during the incident window. This prevented some customers from viewing the UI of networking, compute, billing, monitoring, and other products and services within the Cloud Console platform.

#### Google Cloud SQL

0.08% of Cloud SQL's fleet experienced instance metrics and logging delays from 18:07 - 18:37 for a duration of 30 minutes. The Cloud SQL API did not serve errors during the outage, but incoming traffic dropped by ~30%. No spurious auto-failovers or auto-repairs were executed as a result of the incident. There were no actual Instance failures.

#### Google Kubernetes Engine

Requests to the Google Kubernetes Engine (GKE) control plane experienced increased timeouts and HTTP 502 error. Up to 6.6% of cluster masters reported errors during the time of the incident. Up to 5.5% of newly added nodes to clusters may have experienced errors due to issues communicating with impacted cluster masters.

#### Firebase Crashlytics

66% of Crashlytics imports from AWS were impacted from 18:01 - 19:01 US/Pacific for a duration of 60 minutes. This created an import backlog which was quickly worked through 10 minutes after the incident ended.

#### Dialogflow and Speech-to-text API

Requests to Dialogflow returned up to 72% errors in the form of HTTP 502 response codes. Requests to Google Speech API may have seen up to 68% errors in the form of HTTP 502 response codes.

#### Cloud Firestore and Datastore

Cloud Firestore saw 80% of listen streams become disconnected and up to 50% error rates for query/get requests across all regions except nam5 and eur3.


#### SLA CREDITS

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](https://support.google.com/cloud/contact/cloud_platform_sla)

A full list of all Google Cloud Platform Service Level Agreements can be found at <https://cloud.google.com/terms/sla/>

For G Suite, please request an SLA credit through one of the Support channels: <https://support.google.com/a/answer/104721>

G Suite Service Level Agreement can be found at <https://gsuite.google.com/intl/en/terms/sla.html>

Sep 25, 2020

14:48

With all services restored to normal operation, Google's engineering teams are now conducting a thorough post-mortem to ensure we understand all the contributing factors and downstream impact to GCP and G Suite from this incident. The root cause of this disruption is well understood and safeguards have been put in place to prevent any possible recurrence of the issue.

At this time we have determined that the following products were affected:

#### Cloud Build API

Google Front End (GFE) prevented API requests from reaching the service. CreateBuild requests that did make it to the servers were more likely to fail due to user code calling other GCP services.

#### Cloud Firestore and Datastore

Cloud Firestore saw 80% of listen streams become disconnected and a 50% drop in query/get requests across all regions except nam5 and eur3.

#### Cloud Key Management Service (KMS)

Google Front End (GFE) prevented API requests from reaching the service.

#### Cloud Logging

Unavailable for viewing in the Cloud Console, but data ingestion was not impacted.

#### Cloud Monitoring

Elevated error rates of uptime checks and audits to the Cloud Monitoring API

#### Cloud Compute Engine

Requests to compute.googleapis.com would have seen an increase in 502 errors. Existing instances were not impacted.

#### Cloud Spanner

Cloud Spanner experienced elevated latency spikes which may have resulted in connection timeouts.

#### Game Servers

Minor impact to cluster availability due to dependencies on other services.

#### Google Cloud Console

Multiple pages and some core functionality of the Cloud Console impacted.

#### Google Cloud SQL

Minor connectivity problems. Instance log reporting to stackdriver was delayed. There was a ~50% drop in SqlInstancesService.List API requests.

#### Google Kubernetes Engine

Minor impact to cluster availability due to dependencies on other services.

#### Firebase Crashlytics

From 18:00 - 18:24, Crashlytics imports from AWS were impacted. This created an import backlog which was quickly worked through 10 minutes after the incident ended.

We are conducting an internal investigation of this issue and will make appropriate improvements to our systems to help prevent or minimize future recurrence. We will provide a detailed report of this incident, including both GCP and G Suite impact, once we have completed our internal investigation. This detailed report will also contain information regarding SLA credits.

Sep 24, 2020

19:31

We believe the issue with multiple GCP products has been resolved for most traffic at 2020-09-24 18:33 US/Pacific.

Affected products include: Cloud Run, Firestore Watch, Cloud SQL, Cloud Spanner, GKE, Cloud Logging, Cloud Monitoring, Cloud Console, Cloud KMS, Game Server

We thank you for your patience while we worked on resolving the issue.

Sep 24, 2020

19:19


Description: We are experiencing an issue with multiple GCP products, beginning at Thursday, 2020-09-24 17:58 US/Pacific.

Symptoms: Increased error rate

Affected products include: Cloud Run, Firestore Watch, Cloud SQL, Cloud Spanner, GKE, Cloud Logging, Cloud Monitoring, Cloud Console, Cloud KMS, Game Server

Mitigation work is currently underway by our engineering team.

We will provide an update by Thursday, 2020-09-24 20:00 US/Pacific with current details.

Sep 24, 2020

19:05


Description: We are experiencing an issue with multiple GCP products, beginning at Thursday, 2020-09-24 17:58 US/Pacific.

Symptoms: Increased error rate.

Affected products include: Cloud Run, Firestore Watch, Cloud SQL, Cloud Spanner, GKE, Cloud Logging, Cloud Monitoring, Cloud Console, Cloud KMS, Game Server

Our engineering team continues to investigate the issue.

We will provide an update by Thursday, 2020-09-24 20:00 US/Pacific with current details.

Sep 24, 2020

18:46


Description: We are experiencing an issue with multiple GCP products, beginning at Thursday, 2020-09-24 17:58 US/Pacific.

Symptoms: Increased error rate.

Affected products include: Cloud Run, Firestore Watch, Cloud SQL, Cloud Spanner, GKE, Cloud Logging, Cloud Monitoring, Cloud Console

Our engineering team continues to investigate the issue.

We will provide an update by Thursday, 2020-09-24 19:30 US/Pacific with current details.

Sep 24, 2020

18:28

Description: We are experiencing an issue with multiple GCP products.

Our engineering team continues to investigate the issue.

We will provide an update by Thursday, 2020-09-24 19:00 US/Pacific with current details.