Google Cloud Platform

March 29, 2018 **All services available**

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 #16003

Authentication issues with Google Cloud Platform APIs

Incident began at **2016-04-19 07:30** and ended at **2016-04-19 07:48** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION
Apr 25, 2016	22:57	SUMMARY: On Tuesday 19th April 2016, 1.1% of all requests to obtain new Google OAuth 2.0 tokens failed for a period of 70 minutes. Users of affected applications experienced authentication errors. This incident affected all Google services that use OAuth. We apologize to any customer whose application was impacted by this incident. We take outages very seriously and are strongly focused on learning from these incidents to improve the future reliability of our services. DETAILED DESCRIPTION OF IMPACT: On Tuesday 19 April 2016 from 06:12 to 07:22 PDT, the Google OAuth 2.0 service returned HTTP 500 errors for 1.1% of all requests. OAuth tokens are granted to applications on behalf of users. The application requesting the token is identified by its client ID. Google's OAuth service looks up the application associated with a client ID before granting the new token. If the mapping from client ID to application is not cached by Google's OAuth service, then it is fetched from a separate client ID lookup service. The client ID lookup service dropped some requests during the incident, which caused those token requests to fail. The token request failures predominantly affected applications which had not populated the client ID cache because they were less frequently used. Such infrequently-used applications may have experienced high error rates on token requests for their users, though the overall average error rate was 1.1% measured across all applications. Once access tokens were obtained, they could be used without problems. Tokens issued before the incident continued to function until they expired. Any requests for tokens that did not use a client ID were not affected by this incident. ROOT CAUSE: Google's OAuth system depends on an internal service to lookup details of the client ID that is making the token request. During this incident, the client ID lookup service had insufficient capacity to respond to all requests to lookup client ID details. Before the incident started, the client ID lookup service had been running close to its rated capacity. In an attempt to prevent a future problem, Google SREs triggered an update to add capacity to the service at 05:30. Normally adding capacity does not cause a restart of the service. However, the update process had a misconfiguration which caused a rolling restart. While servers were restarting, the capacity of the service was reduced further. In addition, the restart triggered a bug in a specific client's code that caused its cache to be invalidated, leading to a spike in requests from that client. Google's systems are designed to throttle clients in these situations. However, the throttling was insufficient to prevent overloading of the client ID lookup service. Google's software load balancer was configured to drop a fraction of incoming requests to the client ID lookup service during overload in order to prevent cascading failure. In this case, the load balancer was configured too conservatively and dropped more traffic than needed. REMEDIATION AND PREVENTION: Google's internal monitoring systems detected the incident at 06:28 and our engineers isolated the root cause as an overload in the client ID lookup service at 06:47. We added additional capacity to work around the issue at 07:07 and the error rate dropped to normal levels by 07:22. In order to prevent future incidents of this type from occurring, we are taking several actions. 1. We will improve our monitoring to detect immediately when usage of the client ID lookup service gets close to its capacity. 2. We will ensure that the client ID lookup service always has more than 10% spare capacity at peak. 3. We will change the load balancer configuration so that it will not uniformly drop traffic when overloaded. Instead, the load balancer will throttle the clients that are causing traffic spikes. 4. We will change the update process to minimize the capacity that is temporarily lost during an update. 5. We will fix the client bug that caused its client ID cache to be invalidated.
Apr 19, 2016	07:49	The issue with Authentication Services should have been resolved for all affected projects as of 07:24 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.
Apr 19, 2016	07:30	We are still investigating the issue with Authentication services for Google Cloud Platform APIs. We will provide another status update by 08:00 US/Pacific with current details.

All times are US/Pacific

Send Feedback