Service Health

This page provides status information on the services that are part of Google Cloud. 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 https://cloud.google.com/.

Incident affecting Google Cloud Networking

global: Elevated HTTP 500s errors for a small number of customers with load balancers on Traffic Director-managed backends

Incident began at **2022-03-08 10:07** and ended at **2022-03-08 12:42** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION
15 Mar 2022	16:23 PDT	**INCIDENT REPORT** **Summary** On Tuesday, 8 March 2022, Traffic Director users, who had service mesh with Traffic Director-managed backends, experienced elevated service errors for 2 hours and 35 minutes. To our Traffic Director customers who were impacted during this service disruption, we sincerely apologize. We have conducted an internal investigation and are taking steps to improve our service. **Root Cause** Traffic Director has a configuration pipeline that distributes customer configurations to Traffic Director infrastructure globally. The configuration pipeline has been undergoing a multi-stage, multi-year architectural rewrite to address a number of limitations in the previous architecture. One step to move to the new architecture has been to migrate existing Traffic Director configurations to a different format. This data migration has been ongoing since November 2021. The Traffic Director code was updated to handle both old and new formats of the configuration. The data format migration was not fully completed; it encountered sporadic failures that were believed to only affect test configurations of new unreleased features. These failures masked the true completion state for full migration of all customer data. As a result, some customer data was an inconsistent state of old and new formats. On 8 March 2022 at 10:05 PT, a change to the Traffic Director code that processes the configuration was updated. The code change assumed that the configuration data format migration was fully completed. In fact, the data migration had not completed. The failures were believed to only affect test configurations of new unreleased features, but they also affected a certain set of customer configurations that met all of the following criteria: 1. The project was part of a Shared VPC. 2. The project had at least one configuration migrated to the new format, which would be true if: a. The customer modified the project configuration after 12 November 2021; or b. The internal migration tool successfully processed the configuration. 3. The project had at least one configuration that was not migrated to the new format: a. The customer had not modified the project since 12 November 2021; or b.The internal migration tool failed to process the configuration. 4. The hostname of interest was part of the migrated configuration or the data plane requested configuration from the Traffic Director based on the migrated configuration. It would inadvertently delete the configurations which caused the downstream clients to lose their programming and deconfigure the data plane. The change was rolled back, the configurations were recovered, and service was restored for all users. **Remediation and Prevention** Google engineers were alerted to the issue through a customer support case on 8 March 2022 at 10:24 US/Pacific and immediately started an investigation. Once the nature and scope of the issue became clear, Google engineers rolled back the Traffic Director configuration rollout to prevent additional customer impact. At 12:42 US/Pacific, engineers forced a reprogramming of configurations, which mitigated the issue. We sincerely apologize for the length and severity of this incident. Our team at Google is taking immediate steps to prevent a recurrence and improve reliability in the future. **Detailed Description of Impact** On Tuesday, 8 March 2022 from 10:07 to 12:42 US/Pacific, customers using Traffic Director-managed backends experienced elevated service errors. Affected customers would have seen their Traffic Director managed clients deprogrammed as the configuration was removed. The effect of the deprogramming for users behind Google Cloud Load Balancers (GCLB) would have been visible as 500 errors. Some affected customers were able to mitigate the issue for themselves through the workaround of moving to backends that were not Traffic Director managed.
9 Mar 2022	09:25 PST	Mini Incident Report (Full Incident Report To Follow) We apologize for the inconvenience this service disruption may have caused. We would like to provide some information about this incident below. Please note, this information is based on our best knowledge at the time of posting and is subject to change as our investigation continues. If you have experienced impact outside of what is listed below, please reach out to Google Support by opening a case using https://cloud.google.com/support. (All Times US/Pacific) **Incident Start:** 08 March 2022 10:07 **Incident End:** 08 March 2022 12:42 **Duration:** 2 hours, 35 minutes **Affected Services and Features:** Traffic Director **Regions/Zones:** Global **Description:** Traffic Director customers who used shared Virtual Private Cloud (VPC) experienced elevated service errors for 2 hours and 35 minutes, due to local proxies, gRPC clients, and other services being unable to retrieve their xDS configurations. From preliminary analysis, the root cause of the issue was related to a bug introduced in a recent Traffic Director programming pipeline rollout. **Customer Impact:** Affected customers would have seen their Traffic Director-managed clients deprogrammed as the configuration was removed. The effect of the deprogramming for users behind GCLB would have been visible as 500 errors. Some affected customers were able to mitigate the issue for themselves through the workaround of moving to backends that were not Traffic Director-managed. **Additional details:** Our engineers rolled back the Traffic Director configuration rollout and forced a reprogramming of configurations, which mitigated the issue.
8 Mar 2022	14:23 PST	The issue with Traffic Director has been confirmed to be caused by a recent release; the release has been rolled back and customers can now start using Traffic Director. We have identified a probable root cause and will be publishing an Incident Report within the next several days. The issue with Cloud Load Balancing, Cloud Networking, Traffic Director has been resolved for all affected projects as of Tuesday, 2022-03-08 12:42 US/Pacific. We thank you for your patience while we worked on resolving the issue.
8 Mar 2022	13:21 PST	Summary: global: Elevated HTTP 500s errors for a small number of customers with load balancers on Traffic Director-managed backends Description: We believe the issue with Traffic Director is mitigated. We do not have an ETA for full resolution at this point. Customers should leave the workaround in place, as the issue could reoccur until the root cause has been determined. We believe the issue is limited to Traffic Director users and does not affect all of Cloud Load Balancing or Cloud Networking. We will provide an update by Tuesday, 2022-03-08 14:30 US/Pacific with current details. Diagnosis: Affected customers will see elevated HTTP 500s errors on load balancers with Traffic Director managed customer-run backends. Thus far, impact has only been observed in us-east1, but customers with multi-regional Traffic Director deployments could be impacted in more regions. Workaround: Customers with Traffic Director managed backends should consider moving to backends that are not Traffic Director-managed.
8 Mar 2022	12:41 PST	Summary: global: Elevated HTTP 500s errors for a small number of customers with load balancers on Traffic Director-managed Envoy backends Description: We are experiencing an intermittent issue with Cloud Load Balancing, Cloud Networking, Traffic Director beginning at Tuesday, 2022-03-08 10:07:51 US/Pacific. Our engineering team continues to investigate the issue. We will provide an update by Tuesday, 2022-03-08 14:00 US/Pacific with current details. We apologize to all who are affected by the disruption. Diagnosis: Affected customers will see elevated HTTP 500s errors on load balancers with Traffic Director managed customer-run Envoy backends. Thus far, impact has only been observed in us-east1, but customers with multi-regional Traffic Director deployments could be impacted in more regions. Workaround: Customers with Traffic Director managing their envoys should consider moving to backends that are not Traffic Director-managed.
8 Mar 2022	12:36 PST	Summary: global: Elevated HTTP 500s errors for a small number of customers with load balancers on Traffic Director-managed Envoy backends Description: Mitigation work is currently underway by our engineering team. We do not have an ETA for mitigation at this point, but a customer self-mitigation is available. We will provide more information by Tuesday, 2022-03-08 14:00 US/Pacific. Diagnosis: Affected customers will see elevated HTTP 500s errors on load balancers with Traffic Director managed customer-run Envoy backends. Thus far, impact has only been observed in us-east1, but customers with multi-regional Traffic Director deployments could be impacted in more regions. Workaround: Customers with Traffic Director managing their envoys should consider moving to backends that are not Traffic Director-managed.