

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 #20011

All Cloud Platform resources in europe-west2-a may be unreachable as of 2020-12-09 18:32 US/Pacific.

Incident began at **2020-12-09 18:31** and ended at **2020-12-09 19:55** (all times are **US/Pacific**).

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



Dec 15, 2020

11:03

ISSUE SUMMARY

On Wednesday 9 December, 2020, Google Cloud Platform experienced networking unavailability in zone europe-west2-a, resulting in some customers being unable to access their resources, for a duration of 1 hour 24 minutes. The following Google services had degraded service that extended beyond the initial 1 hour 24 minute network disruption:

- 1.5% of Cloud Memorystore Redis instances were unhealthy for a total duration of 2 hours 24 minutes
- 4.5% of Classic Cloud VPN tunnels in the europe-west2 region experienced unavailability after the main disruption had recovered and these tunnels remained down for a duration of 8 hours and 10 minutes
- App Engine Flex experienced increased deployment error rates for a total duration of 1 hour 45 minutes

We apologize to our Cloud customers who were impacted during this disruption. We have conducted a thorough internal investigation and are taking immediate action to improve the resiliency and availability of our service.

ROOT CAUSE

Google's underlying networking control plane consists of multiple distributed components that make up the Software Defined Networking (SDN) stack. These components run on multiple machines so that failure of a machine or even multiple machines does not impact network capacity. To achieve this, the control plane elects a leader from a pool of machines to provide configuration to the various infrastructure components. The leader election process depends on a local instance of Google's internal lock service to read various configurations and files for determining the leader. The control plane is responsible for Border Gateway Protocol (BGP) peering sessions between physical routers connecting a cloud zone to the Google backbone.

Google's internal lock service provides Access Control List (ACLs) mechanisms to control reading and writing of various files stored in the service. A change to the ACLs used by the network control plane caused the tasks responsible for leader election to no longer have access to the files required for the process. The production environment contained ACLs not present in the staging or canary environments due to those environments being rebuilt using updated processes during previous maintenance events. This meant that some of the ACLs removed in the change were in use in europe-west2-a, and the validation of the configuration change in testing and canary environments did not surface the issue.

Google's resilience strategy relies on the principle of defense in depth. Specifically, despite the network control infrastructure being designed to be highly resilient, the network is designed to 'fail static' and run for a period of time without the control plane being present as an additional line of defense against failure. The network ran normally for a short period - several minutes - after the control plane had been unable to elect a leader task. After this period, BGP routing between europe-west2-a and the rest of the Google backbone network was withdrawn, resulting in isolation of the zone and inaccessibility of resources in the zone.

REMEDIATION AND PREVENTION

Google engineers were automatically alerted to elevated error rates in europe-west2-a at 2020-12-09 18:29 US/Pacific and immediately started an investigation. The configuration change rollout was automatically halted as soon as the issue was detected, preventing it from reaching any other zones. At 19:30, mitigation was applied to rollback the configuration change in europe-west2-a. This completed at 19:55, mitigating the immediate issue. Some services such as Cloud MemoryStore and Cloud VPN took additional time to recover due to complications arising from the initial disruption. Services with extended recovery timelines are described in the "detailed description of impact" section below.

We are committed to preventing this situation from happening again and are implementing the following actions:

In addition to rolling back the configuration change responsible for this disruption, we are auditing all network ACLs to ensure they are consistent across environments. While the network continued to operate for a short time after the change was rolled out, we are improving the operating mode of the data plane when the control plane is unavailable for extended periods. Improvements in visibility to recent changes will be made to reduce the time to mitigation. Additional observability will be added to lock service ACLs allowing for additional validation when making changes to ACLs. We are also improving the canary and release process for future changes of this type to ensure these changes are made safely.

DETAILED DESCRIPTION OF IMPACT

On Wednesday 9 December, 2020 from 18:31 to 19:55 US/Pacific Google Cloud experienced unavailability for some Google services hosted in zone europe-west2-a as described in detail below. If impact time differs significantly, it will be mentioned specifically.

Compute Engine

~60% of VMs in europe-west2-a were unreachable from outside the zone. Projects affected by this incident would have observed 100% of VMs in the zone being unreachable. Communication within the zone had minor issues, but largely worked normally. VM creation and deletion operations were stalled during the outage. VMs on hosts that had hardware or other faults during the outage were not repaired and restarted onto healthy hosts during the outage.

Persistent Disk

VMs in europe-west2-a experienced stuck I/O operations for 59% of standard persistent disks located in that zone. 27% of regional persistent disks in europe-west2 briefly experienced high I/O latency at the start and end of the incident. Persistent Disk snapshot creation and restore for 59% of disks located in europe-west2-a failed during the incident. Additionally, snapshot creation for Regional Persistent Disks with one replica located in zone europe-west2-a was unavailable.

Cloud SQL

~79% of HA Cloud SQL instances experienced <5 minutes of downtime due to autofailover with an additional ~5% experiencing <25m of downtime after manual recovery. ~13% of HA Cloud SQL instances with legacy HA configuration did not failover because the replicas were out of sync, and were unreachable for the full duration of the incident. The remaining HA Cloud SQL instances did not failover due to stuck operations. Overall, 97.5% of Regional PD based HA instances and 23% of legacy MySQL HA instances had <25m downtime with the remaining instances being unconnectable during the outage. Google engineering is committed to improving the successful failover rate for Cloud SQL HA instances for zonal outages like this.

Google App Engine

App Engine Flex apps in europe-west2 experienced increased deployment error rates between 10% and 100% from 18:44 to 20:29. App Engine Standard apps running in the europe-west2 region experienced increased deployment error rates of up to 9.6% that lasted from 18:38 to 18:47. ~34.7% of App Engine Standard apps in the region experienced increased serving error rates between 18:32 and 18:38.

Cloud Functions

34.8% of Cloud Functions served from europe-west2 experienced increased serving error rates between 18:32 and 18:38.

Cloud Run

54.8% of Cloud Run apps served from europe-west2 experienced increased serving error rates between 18:32 and 18:38.

Cloud MemoryStore

~10% of Redis instances in europe-west2, were unreachable during the outage. Both standard tier and basic tier instances were affected. After the main outage was mitigated, most instances recovered, but ~1.5% of instances remained unhealthy for 60 minutes before recovering on their own.

Cloud Filestore

~16% of Filestore instances in europe-west2 were unhealthy. Instances in the zone were unreachable from outside the zone, but access within the zone was largely unaffected.

Cloud Bigtable

100% of single-homed Cloud Bigtable instances in europe-west2-a were unavailable during the outage, translating into 100% error rate for customer instances located in this zone.

Kubernetes Engine

~67% of cluster control planes in europe-west2-a and 10% of regional clusters in europe-west2 were unavailable for the duration of the incident. Investigation into the regional cluster control plane unavailability is still ongoing. Node creation and deletion operations were stalled due to the impact to Compute Engine operations.

Cloud Interconnect

Elevated packet loss for zones in europe-west2. Starting at 18:31 packets destined for resources in europe-west2-a experienced loss for the duration of the incident. Additionally, interconnect attachments in europe-west2 experienced regional loss for 7 minutes at 18:31 and 8 minutes at 19:53.

Cloud Dataflow

~10% of jobs in europe-west2 failed or got stuck in cancellation during the outage. ~40% of Dataflow Streaming Engine jobs in the region were degraded over the course of the incident.

Cloud VPN

A number of Cloud VPN tunnels were reset during the disruption and were automatically relocated to other zones in the region. This is within the design of the product, as the loss of one zone is planned. However once zone europe-west2-a reconnected to the network, a combination of bugs in the VPN control plane were triggered by some of the now stale VPN gateways in the zone. This caused an outage to 4.5% of Classic Cloud VPN tunnels in europe-west2 for a duration of 8 hours and 10 minutes after the main disruption had recovered.






Cloud Dataproc

~0.01% of Dataproc API requests to europe-west2 returned UNAVAILABLE during the incident. The majority of these requests were read-only requests (ListClusters, ListJobs, etc.)

SLA CREDITS

If you believe your paid application experienced an SLA violation as a result of this incident, please submit the SLA credit request: 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/>

	Dec 09, 2020	20:43	<p>The issue with Google Cloud infrastructure components is believed to be resolved for all services, however a small number of Compute resources may still be affected and our Engineering Team is working on it.</p> <p>If you have questions or are impacted, please open a case with the Support Team and we will work with you until this issue is resolved.</p> <p>No further updates will be provided here.</p> <p>We thank you for your patience while we're working on resolving the issue.</p>
	Dec 09, 2020	20:30	<p>Description: We believe the issue with Google Cloud infrastructure components is resolved for most services as of approximately 2020-12-09 20:21.</p> <p>We do not have an ETA for full resolution at this point.</p> <p>We will provide an update by Wednesday, 2020-12-09 22:07 US/Pacific with current details.</p> <p>Diagnosis: None at this time.</p> <p>Workaround: Moving resources to another zone temporarily.</p>
	Dec 09, 2020	20:11	<p>Description: Mitigation work is still underway by our engineering team. We are starting to see recovery for some Google Cloud infrastructure components.</p> <p>We do not have an ETA for full resolution at this point.</p> <p>We will provide an update by Wednesday, 2020-12-09 21:40 US/Pacific with current details.</p> <p>Diagnosis: None at this time.</p> <p>Workaround: Moving resources to another zone temporarily.</p>
	Dec 09, 2020	19:51	<p>Description: Mitigation work is currently underway by our engineering team.</p> <p>We do not have an ETA for mitigation at this point.</p> <p>We will provide more information by Wednesday, 2020-12-09 21:32 US/Pacific.</p> <p>Diagnosis: None at this time.</p> <p>Workaround: None at this time.</p>
	Dec 09, 2020	19:17	<p>Description: We are experiencing an issue with Google Cloud infrastructure components affecting resources located in europe-west2-a.</p> <p>Our engineering team continues to investigate the issue.</p> <p>We will provide an update by Wednesday, 2020-12-09 20:46 US/Pacific with current details.</p> <p>We apologize to all who are affected by the disruption.</p> <p>Diagnosis: None at this time.</p> <p>Workaround: None at this time.</p>

