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 Networking Incident #21002

The issue with network configuration propagating for Cloud Networking VPN, Network Load Balancer VIPs, and VM Instances in multiple regions is resolved.

Incident began at **2021-02-12 14:51** and ended at **2021-02-12 18:55** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION
Feb 19, 2021	09:02	**ISSUE SUMMARY** On Friday, 12 February 2021, Google Cloud Networking experienced elevated packet loss for newly created, updated, deleted or migrated virtual machines (VMs) and network endpoints for a duration of 4 hours, 4 minutes. Network programming for VMs and network endpoints was also affected for the duration. To our customers whose businesses were impacted during this service disruption, we sincerely apologize – this is not the level of quality and reliability we strive to offer you, and we are taking immediate steps to improve the platform's performance and availability. **ROOT CAUSE** Google Cloud's networking control plane has global components that are responsible for fanning-out network configurations that can affect an entire Virtual Private Cloud (VPC) network to downstream (regional/zonal) networking controllers. Work has been ongoing to better isolate global networking control plane components to limit scope of impact for issues that affect these global components. Cloud Networking also relies on a suite of automation tools to manage and enforce the quota of resources allocated to VPC networks. Some quotas are enforced with logic that will automatically remove resources when the quota is decreased, and reprocess previous resource operations when quota is increased. The circumstances that led to this was a latent issue in the control plane quota enforcement logic. During routine handling of peering quota change requests, previous operations that were rejected due to a lack of available quota were being re-evaluated and re-processed by the networking control plane. While doing this re-evaluation, the networking control plane encountered the latent issue and could not process other incoming network programming operations, triggering timeouts for those requests. As VPC resources are multi-regional in nature, this also meant that newly created, updated, deleted or migrated VM resources in regions that required programming on the network control plane were not able to establish connectivity, resulting in elevated packet loss. **REMEDIATION AND PREVENTION** Once the nature and scope of the issue became clear, Google engineers paused VM migrations globally to prevent existing instances from being impacted. Networking quota changes were also paused to prevent a recurrence until a fix had been rolled out. The issue trigger was isolated to update operations, not initial load operations, so a rolling restart of the networking control plane was triggered to mitigate the issue. Teams worked through the weekend to ensure that recurrence was not possible by rolling out a fix globally. In addition to fixing the underlying cause, we will be implementing changes to prevent and reduce the impact of this type of failure in several ways: 1. Add health checks and automated restarts when the networking control plane responsible for peering operations becomes unresponsive 2. Continue work to regionalize network control plane components to reduce scope of impact for future issues of this type 3. Automatically pause VM migrations when high numbers of VMs are exhibiting networking issues 4. Improve monitoring of network control plane operations to decrease time to mitigation for issues of this type 5. Improve networking data plane resilience when the networking control plane is unresponsive **DETAILED DESCRIPTION OF IMPACT** On Friday 12 February, 2021 from 14:51 to 18:55 US/Pacific, Cloud Networking control plane operations experienced increased error rates, and experienced elevated packet loss for both inter- and intra-region traffic. **Cloud Networking** Elevated control plane operation error rates of up to 15% in most regions except for us-central1. Region us-central1 experienced elevated control plane error rates of up to 50% between 15:00 and 16:15, dropping to values similar to other regions by 16:45. VM to VM traffic experienced up to 2.5% packet loss for intra-region traffic, and up to 3.5% loss for inter-region traffic. **Cloud VPN** 1.4% of Cloud VPN tunnels in us-central1 lost connectivity from 15:12 to 17:00. **Cloud Interconnect** Changes to Cloud Interconnect resources experienced delayed propagation or failures during the incident. **Compute Engine (GCE)** Newly created, updated, deleted or migrated VMs failed to have networking set up during the incident. Existing instances that were not migrated or updated during the incident were not impacted. **Kubernetes Engine (GKE)** Approximately 1000 clusters were affected by the inability to provision new clusters or nodes. Node availability was impacted due to the impact to Cloud Networking and GCE instances for the duration of the incident. **Cloud Dataproc** Cluster creation and update operations that created new nodes experienced failures during the incident due to the impact to GCE VM networking. **Cloud Shell** Cloud Shell users assigned to us-central1 were unable to connect to Cloud Shell. Existing sessions were unaffected. **Cloud SQL** 6.3% of instance creation operations failed globally between 14:55 and 17:52. Maintenance operations failed or timed out during the incident, but did not impact data plane availability on existing instances. Replica creation during the incident resulted in instances in a failed state, and were automatically recovered within 24 hours. **Cloud Memorystore** Up to 100% of instance creations failed between 15:15 and 18:20. Instances that were being live-migrated came up on new hosts without networking and faced connectivity issues until they recovered automatically. **Cloud Data Fusion** Cloud Data Fusion instance creations failed during the incident due to failure to create GKE and Cloud SQL instances. **Filestore** A small number of Filestore instances were live-migrated during the incident. These newly migrated instances lost networking after the live migration before recovering on their own. **Cloud Load Balancing** Create and update requests for global L7 external load balancers experienced up to 98% error rate between 15:17 and 18:15, and error rates up to 50% between 18:15 and 18:33. Create and update requests for regional L7 internal load balancers experienced up to 10% error rates, with us-central1 experiencing up to 70% error rates between 15:10 and 17:02. **App Engine Flex** Up to 80% of new deployments to App Engine Flex failed during the incident.
Feb 12, 2021	19:55	The issue with network configuration propagating for Cloud Networking VPN, Network Load Balancer VIPs, and VM Instances in multiple regions has been resolved for all affected projects as of Friday, 2021-02-12 18:55 US/Pacific. We thank you for your patience while we worked on resolving the issue.
Feb 12, 2021	19:10	Description: The mitigation has rolled out to all regions. We will continue to monitor the situation to ensure the issue does not recur before declaring full resolution. All affected products should be recovered. We will provide an update by Friday, 2021-02-12 20:00 US/Pacific Diagnosis: None at this time. Workaround: Customers should now be able to continue using products as normal.
Feb 12, 2021	18:26	Description: Mitigation work is progressing as expected and we are continuing to see recovery. Mitigation is continuing to roll out in other regions. Mitigation is still expected to complete by 19:00 US/Pacific. Network connectivity within us-central1 should be fully recovered, however, some connectivity issues to other regions may persist while the mitigation completes roll out. Current known impacted products: Compute Engine Cloud SQL Dataproc Memorystore App Engine Flex Cloud Composer Kubernetes Engine Cloud Data Fusion We will provide an update by Friday, 2021-02-12 19:00 US/Pacific with current details. We apologize to all who are affected by the disruption. Diagnosis: Customers using Cloud VPN, creating new Network Load Balancer VIPs, and new VM Instances may not be able to achieve external connectivity. Existing configurations should be unaffected. Instances that have live-migrated within the impact period may experience connectivity loss. Cloud VPN tunnels may have been impacted between 14:50 and 15:31 This issue would impact services that rely on instances to function, dataproc cluster creation, new dataflow jobs, and App Engine Flex deployments may also be impacted. Workaround: No workaround at this time. However, to reduce the likelihood of impact customers should pause autoscalers and other systems which may cause changes such as upgrades or deployments.
Feb 12, 2021	17:50	Description: Mitigation work is still underway by our engineering team and we are continuing to see recovery. We believe that mitigation has fully completed rolling out in the us-central1 region, and we are monitoring for recovery. Mitigation is continuing to roll out in other regions. We estimate mitigation to be fully complete by 19:00 US/Pacific. Network connectivity within us-central1 should be fully recovered, however, some connectivity issues to other regions may persist while the mitigation completes roll out. Current known impacted products: Compute Engine Cloud SQL Dataproc Memorystore App Engine Flex Cloud Composer Kubernetes Engine Cloud Data Fusion We will provide an update by Friday, 2021-02-12 18:15 US/Pacific with current details. We apologize to all who are affected by the disruption. Diagnosis: Customers using Cloud VPN, creating new Network Load Balancer VIPs, and new VM Instances with external IPs may not be able to achieve external connectivity. Existing configurations should be unaffected. Instances that have live-migrated within the impact period may experience connectivity loss. Cloud VPN tunnels may have been impacted between 14:50 and 15:31 This issue would impact services that rely on instances to function, dataproc cluster creation, new dataflow jobs, and App Engine Flex deployments may also be impacted. Workaround: No workaround at this time. However, to reduce the likelihood of impact customers should pause autoscalers and other systems which may cause changes such as upgrades or deployments.
Feb 12, 2021	17:06	Description: Mitigation work is currently underway by our engineering team and we are starting to see recovery. We do not have an ETA for mitigation at this point. Current known impacted products: Compute Engine Cloud SQL Dataproc Memorystore App Engine Flex Cloud Composer Kubernetes Engine We will provide more information by Friday, 2021-02-12 17:45 US/Pacific. Diagnosis: Customers using Cloud VPN, creating new Network Load Balancer VIPs, and new VM Instances with external IPs may not be able to achieve external connectivity. Existing configurations should be unaffected. This issue would impact services that rely on instances to function, dataproc cluster creation, new dataflow jobs, and App Engine Flex deployments may also be impacted. Workaround: No workaround at this time. However, to reduce the likelihood of impact customers should pause autoscalers and other systems which may cause changes such as upgrades or deployments.
Feb 12, 2021	16:45	Description: We are experiencing an issue with network configuration propagation for Cloud Networking VPN, Network Load Balancer VIPs, and VM Instance Public IPs in us-central1 with some impact in: us-east1, europe-west4, europe-west1, asia-east1, asia-northeast1, beginning at Friday, 2021-02-12 14:50 US/Pacific. Connectivity for existing configurations should not be impacted. Current known impacted products: Compute Engine Cloud SQL Dataproc Memorystore App Engine Flex Cloud Composer Our engineering team continues to investigate the issue. We will provide an update by Friday, 2021-02-12 17:15 US/Pacific with current details. We apologize to all who are affected by the disruption. Diagnosis: Customers using Cloud VPN, creating new Network Load Balancer VIPs, and new VM Instances with external IPs may not be able to achieve external connectivity. Existing configurations should be unaffected. This issue would impact services that rely on instances to function, dataproc cluster creation, new dataflow jobs, and App Engine Flex deployments may also be impacted. Workaround: No workaround at this time. However, to reduce the likelihood of impact customers should pause autoscalers and other systems which may cause changes such as upgrades or deployments.
Feb 12, 2021	16:10	Description: We are experiencing an issue with Cloud Networking VPN, Network Load Balancer VIPs, and VM Instance Public IPs in us-east1, us-central1, europe-west4, europe-west1, asia-east1, asia-northeast1, beginning at Friday, 2021-02-12 14:50 US/Pacific. Our engineering team continues to investigate the issue. We will provide an update by Friday, 2021-02-12 17:00 US/Pacific with current details. We apologize to all who are affected by the disruption. Diagnosis: Customers using Cloud VPN, creating new Network Load Balancer VIPs, and new VM Instances with external IPs may not be able to achieve external connectivity. Existing configurations should be unaffected. Workaround: None at this time.