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, Google Cloud DNS, Cloud Run, Cloud Spanner, Google Compute Engine, AI Platform Prediction

US-WEST1: Multiple cloud products experiencing network issues

Incident began at **2022-01-08 15:15** and ended at **2022-01-08 18:36** (all times are **US/Pacific**).

DATE	TIME	DESCRIPTION

✓ 21 Jan 2022	07:56 PST	**UPDATED INCIDENT REPORT**
		Summary
		On Saturday, 8 January 2022, multiple GCP products in us-west1-b experienced increased network latency for a duration of 3 hours and 22 minutes. To our affected customers in us-west1-b who were impacted during this outage, 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 leverages "Software-defined Networking" (SDN) to simplify and automate the growth and expansion of our data center networks. This allows us to dynamically scale up data center networks to meet customer demand. This outage began when a routine maintenance event was performed on one of the SDN components. This maintenance event triggered an application failover that prompted a newly active replica to perform reconciliation from a previous checkpoint. These events are expected to be seamless and cause no network disruption. However, the checkpoint data was incorrectly missing a particular piece of configuration information; this was propagated to ~15% of the network switches serving us-west1-b.
		Seconds after this event, the SDN automatically corrected the incomplete configuration. Reprogramming of the affected switches triggered a race condition within the switch firmware, eventually causing them to crash. Automatic repair and mitigation actions were invoked within 10 minutes of switches failing. However, the unexpectedly large number, and network proximity, of the failures prevented a fully automatic recovery. As such, the outage was not mitigated until on-call engineers manually recovered the affected switches. The corrupted checkpoint data was only present in a single location and therefore no other cloud zone was ever at risk.
		Remediation and Prevention
		The outage was detected by Google Engineers on Saturday, 8 January at 15:25 US/Pacific, who immediately started an investigation. At 16:03, engineers tried to migrate traffic away from the impacted switches in the switch fabric, but this did not resolve the issue. At 17:19, engineers ascertained that the impacted switches needed to have their services restarted, and at 17:37, they began to do so. The network issue was mitigated at 18:00, when enough switches had been restarted to successfully serve all network traffic. The issue was fully resolved by 18:36, when all services were marked as recovered.
		The conditions that caused this disruption existed only in a small subset of Google's network. The function responsible for causing it has been disabled and will not be reenabled until the steps below have been fully implemented.
		1. Avoiding the trigger:
		  - We have audited and disabled the SDN feature that triggered this incident.
		  - We have identified test coverage gaps in our SDN release process, which will be addressed to prevent a repeat of this and other similar issues.
		  - Our systems will be modified to validate SDN checkpoint data before it is persisted for later recovery.
		  - Our SDN maintenance workflow safety checks will be enhanced to automatically stop the workflow during an outage.
		2. Ensure changes are applied to the SDN more progressively:
		  - We will redistribute SDN services to limit the areas impacted by failed maintenance workflows.
		  - We will be developing new SDN safety components that validate potentially disruptive operations by applying them to network devices that are similarly configured, but not currently active, before deploying them further.
		3. Reduce time to resolution:
		  - We will improve network management tooling to simplify and expedite mass switch recovery.
		  - We will deploy monitoring improvements to more quickly identify broad network switch failures.
		Detailed Description of Impact
		On Saturday, 8 January from 15:15 to 18:36 US/Pacific:
		Cloud Router
		Affected Cloud Router customers would have experienced elevated packet loss from 40% to 100%.
		Cloud VPN
		Affected Cloud VPN customers would have experienced elevated packet loss from 40% to 100%.
		Cloud DNS
		Cloud DNS customers experienced increased latency and errors on DNS requests.
		Cloud AI
		Cloud AI customers experienced elevated latency on prediction requests.
		Cloud Run
		Cloud Run customers experienced network connectivity issues.
		Cloud Spanner
		Cloud Spanner Customers experienced elevated latency.
		Google Compute Engine
		Google Compute Engine customers experienced network latency, connectivity issues and slow input/output (I/O) operations on disks due to network latency, which may have manifested as unresponsive Compute Engine instances, including Google Kubernetes instances.
		Other Services
		Other services that require Google Cloud Networking in us-west1-b were also affected. Customers would experience latency, errors, and delays.

✓ 19 Jan 2022	07:39 PST	INCIDENT REPORT **Summary** On Saturday, 8 January 2022, multiple GCP products in us-west1-b experienced increased network latency for a duration of 3 hours and 22 minutes. To our affected customers in us-west1-b who were impacted during this outage, 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 leverages "Software-defined Networking" (SDN) to simplify and automate the growth and expansion of our data center networks. This allows us to dynamically scale up data center networks to meet customer demand. This outage began when a routine maintenance event was performed on one of the SDN components. This maintenance event triggered an application failover that prompted a newly active replica to perform reconciliation from a previous checkpoint. These events are expected to be seamless and cause no network disruption. However, the checkpoint data was incorrectly missing a particular piece of configuration information; this was propagated to ~15% of the network switches serving us-west1-b. Seconds after this event, the SDN automatically corrected the incomplete configuration. Reprogramming of the affected switches triggered a race condition within the switch firmware, eventually causing them to crash. Automatic repair and mitigation actions were invoked within 10 minutes of switches failing. However, the unexpectedly large number, and network proximity, of the failures prevented a fully automatic recovery. As such, the outage was not mitigated until on-call engineers manually recovered the affected switches. The corrupted checkpoint data was only present in a single location and therefore no other cloud zone was ever at risk. **Remediation and Prevention** The outage was detected by Google Engineers on Saturday, 8 January at 15:25 US/Pacific, who immediately started an investigation. At 16:03, engineers tried to migrate traffic away from the impacted switches in the switch fabric, but this did not resolve the issue. At 17:19 engineers ascertained that the impacted switches needed to have their services restarted, and at 17:37 they began to do so. The network issue was mitigated at 18:00 when enough switches had been restarted to successfully serve all network traffic. The issue was fully resolved by 18:36 when all services were marked as recovered. We are still working on the details of steps to avert further issues of this type, which in line with Google's standard practice, are being designed to ensure the following: - Prevention of a reoccurrence of an outage of this nature. - Detection and mitigation of similar, future outages more quickly. The conditions that caused this disruption existed only in a small part of the network. The function responsible for causing it has been disabled and will not be re-enabled until the steps above have been fully implemented. **Detailed Description of Impact** On Saturday, 8 January from 15:15 to 18:36 US/Pacific: **Cloud Router** Affected Cloud Router customers would have experienced elevated packet loss from 40% to 100%. **Cloud VPN** Affected Cloud VPN customers would have experienced elevated packet loss from 40% to 100%. **Cloud DNS** Cloud DNS customers experienced increased latency and errors on DNS requests. **Cloud AI** Cloud AI customers experienced elevated latency on prediction requests. **Cloud Run** Cloud Run customers experienced network connectivity issues. **Cloud Spanner** Cloud Spanner Customers experienced elevated latency. **Google Compute Engine** Google Compute Engine customers experienced network latency, connectivity issues and slow input/output (I/O) operations on disks due to network latency, which may have manifested as unresponsive Compute Engine instances, including Google Kubernetes instances. **Other Services** Other services that require Google Cloud Networking in us-west1-b were also affected. Customers would experience latency, errors, and delays.
✓ 10 Jan 2022	18:34 PST	Mini Incident Report (Full Incident Report To Follow) We apologize for the inconvenience this service disruption/outage 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 January 2022 15:14 **Incident End:** 08 January 2022 18:36 **Duration:** 3 hours, 22 minutes **Affected Services and Features:** - Cloud Router - Cloud VPN - Cloud DNS - Cloud AI - Cloud Run - Cloud Spanner - Persistent Disk **Regions/Zones:** us-west1-b **Description:** Multiple GCP products experienced network issues in the us-west1 region for 3 hours and 22 minutes. From preliminary analysis, the root cause of the issue is related to an unexpected port/switch configuration and we are continuing investigations. **Customer Impact:** - Cloud Router - Customers may experience elevated packet loss. - Cloud DNS - Increased latency and/or errors reaching out to Cloud DNS - Cloud AI - Elevated prediction latencies - Cloud Run - Network connectivity issues - Cloud Spanner - Elevated network latencies - Persistent Disk - Short period of slow I/O operations on disks, which may have manifested as unresponsive -Compute Engine instances.
✓ 8 Jan 2022	18:42 PST	The issue with Cloud Networking has been resolved for all affected projects as of Saturday, 2022-01-08 18:36 US/Pacific. We will publish an analysis of this incident once we have completed our internal investigation. We thank you for your patience while we worked on resolving the issue.
✕ 8 Jan 2022	18:02 PST	Summary: US-WEST1: Multiple cloud products experiencing network issues Description: We are experiencing network issues in us-west1. Below is the list of affected products: - Cloud Router - Customers may experience elevated packet loss. - Cloud DNS - Increased latency and/or errors reaching out to Cloud DNS - Cloud AI - Elevated prediction latencies - Cloud Run - Network connectivity issues - Cloud Spanner - Elevated network latencies Mitigation work is currently underway by our engineering team. We do not have an ETA for mitigation at this point. We will provide more information by Saturday, 2022-01-08 18:53 US/Pacific. Diagnosis: Affected customer will see packet loss. Workaround: None at this time.
✕ 8 Jan 2022	17:49 PST	Summary: US-WEST1: Multiple cloud products experiencing network issues Description: We are experiencing network issues in us-west1. Below is the list of affected products: - Cloud Router - Customers may experience elevated packet loss. - Cloud DNS - Increased latency and/or errors reaching out to Cloud DNS - Cloud AI - Elevated prediction latencies - Cloud Run - Network connectivity issues Mitigation work is currently underway by our engineering team. We do not have an ETA for mitigation at this point. We will provide more information by Saturday, 2022-01-08 18:53 US/Pacific. Diagnosis: Affected customer will see packet loss. Workaround: None at this time.
! 8 Jan 2022	16:54 PST	Summary: Multiple cloud connectivity products experiencing packet loss in US-WEST1 Description: Mitigation work is currently underway by our engineering team. We do not have an ETA for mitigation at this point. We will provide more information by Saturday, 2022-01-08 17:53 US/Pacific. Diagnosis: Affected customer will see packet loss. Workaround: None at this time.