# Azure status history

This page contains all RCAs for incidents that occurred on November 20th, 2019 or later and will - from that date forward - provide a 5-year RCA history. RCAs prior to November 20th, 2019 are not available.

Product: All

Region: All

Date: All

## April 2020

### 4/22 RCA - Managed Database services - UK South (Tracking ID TS66-1C0)

**Summary of Impact:** Between 09:37 and 13:54 UTC on 22 Apr 2020, a subset of customers may have seen issues affecting service management operations for Azure SQL Database, Azure SQL Database Managed Instance, Azure Database for MariaDB, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Database for MySQL, and Azure Synapse Analytics services in UK South. Service management operations including create, rename, update and delete may have been impacted. Connectivity to database resources was not impacted.

**Root cause:** Engineers determined that a manual maintenance operation impacted instances of an internal cluster data service that is responsible for receiving and executing service management operations. The primary instance of the data service became unhealthy preventing some of the service management operations from completing.

**Mitigation:** Engineers paused the maintenance operation and initiated failover of the data service's primary to a healthy instance, thus mitigating the issue. Engineers monitored for an extended period post-mitigation to ensure there were no further occurrences. Engineers also worked to complete the maintenance operations offline and restore all instances to operational rotation.

**Next steps:** We sincerely apologize for the impact to the affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and to our processes to help ensure such incidents do not occur in the future.

- Engineers will continue to review the specific maintenance operation to understand the cause of the impact, and will ensure the operation is fully automated and covered by pre-deployment test cases.

**Provide Feedback**: Please help us improve the Azure customer communications experience by taking our survey: https://aka.ms/TS66-1C0

## March 2020

### 3/15 RCA - Service Availability Issue in West Central US (Tracking ID SMR4-D90)

**Summary of Impact:** Between approximately 20:30 UTC on 15 Mar 2020 and 00:30 UTC on 16 Mar 2020, a subset of customers in West Central US may have experienced issues connecting to resources hosted in this region.

**Root Cause:** At approximately 20:30 UTC on 15 Mar 2020, an ice storm in the region resulted in a loss of power to both primary and secondary utility power feeds in West Central US. This caused the datacenter to transition to generator power. Although largely successful, a subset of generators failed and UPS units supporting the downstream racks carried the load until their batteries drained. At that point, the affected racks lost power entirely. Any customer resources hosted on the affected racks became unavailable at the time.

**Mitigation:** Site engineers manually intervened to restore power to the affected infrastructure. Concurrently, impacted Azure services implemented their disaster recovery plans to work around the power failure. Subsequently, engineering worked to recover customer resources as affected infrastructure started to become available again.

**Next Steps:** We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future. In this case, this included (but was not limited to):

- Reviewing the sequence of operations and associated control systems to remediate identified single point failures
- Validating electrical hardware components to ensure proper functionality

**Provide Feedback:** Please help us improve the Azure customer communications experience by taking our survey: https://aka.ms/SMR4-D90.

### 3/5 RCA - Service Management/Authentication Errors - Azure China (Tracking ID SND4-L80)

**Summary of Impact:** Between 21:03 CST (UTC+8) on 05 Mar 2020 and 16:03 CST on 06 Mar 2020, a subset of customers in the Azure China regions may have encountered failures when performing service management operations on resources hosted in these regions. Customers may also have experienced authentication failures when attempting to access the Azure portal or other Azure resources in the Azure China regions.

**Root Cause:** When clients connect to an Azure service, they validate the Transport Layer Security (TLS) certificate of that Azure service. This validation requires access to an Online Certificate Status Protocol (OCSP) service and Certificate Revocation List (CRL).

Azure in China uses an external Certificate Authority (CA). This CA hosts the OCSP and CRL endpoints on remote locations. Those endpoints were not reachable from clients in China during the incident. This issue was in a telecom provider and it impacted both Azure and other customers of the CA. It caused clients to fail certificate validation, which in turn caused failure in connecting to Azure services.

These OCSP and CRL endpoints are mirrored in multiple locations via a Content Distribution Network (CDN).

**Mitigation:** To mitigate, engineers updated DNS records to re-route clients to alternate OCSP and CRL endpoints that were reachable. The troubleshooting took time as multiple companies were involved in the network path. Some Azure services were able to mitigate sooner by deploying the latest CRL to their servers out-of-band.

**Next Steps:** We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future. In this case, this includes (but is not limited to):

- Work with our telecom partner in China to address the root cause of why the primary CRL and OCSP endpoints were not reachable.
- Improve the resiliency of our certificate infrastructure, including hosting the CRL and OCSP endpoints closer to Azure servers.

**Provide feedback:** Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/SND4-L80

### 3/4 Intermittent latency in US Government Cloud - Mitigated (Tracking ID DLS5-TZ0)

**Summary of impact:** Between 14:00 and 17:15 EST on 04 Mar 2020, a limited subset of customers in US Gov Texas and US Gov Arizona may have experienced intermittent issues or latency connecting to resources hosted in these regions. A smaller subset of customers in other US Gov regions may have also experienced issues connecting to resources.

**Preliminary root cause:** After a preliminary investigation, engineers determined that a recent maintenance event on network infrastructure in the US Gov Texas region led to a shift in network traffic, causing a single network device to become congested. As this network device was responsible for routing some network traffic for other US Gov regions, some customers outside of US Gov Texas may have encountered brief periods of high latency, though most of the impact would have been to a limited number of customers with resources in US Gov Texas.

**Mitigation:** Engineers isolated the impacted network device and rerouted network traffic to mitigate the issue.

**Next steps:** We apologize for the impact to affected customers. Engineers will continue to investigate to establish the full root cause and prevent future occurrences.

### 3/3 RCA- Issues connecting to resources in East US (Tracking ID 9SS0-VT8)

**Summary of Impact:** Between 15:30 and 22:00 UTC on 03 March 2020, a subset of customers in East US may have experienced issues connecting to resources in this region.

**Root Cause:** A malfunction in building automation control caused temperatures in multiple rooms of a data center in the East US region to spike impacting Storage, Compute, Networking and other dependent services. Although the cooling system has N+1 redundancy, the automation failure resulted in a significant reduction in cooling air flow. This caused a cascade of events which caused network devices to become unresponsive, VMs to shutdown, and some storage hardware to go offline.

**Mitigation:** The malfunction in the building automation control was fixed by resetting the controllers for the cooling system. Due to the nature of the automation failure, each cooling unit had to be manually reset. By 16:00 UTC the cooling controller was back online and ambient temperatures and air flow had returned to normal ranges. Engineers then power cycled and restored failed server hardware in groups to restore services in the region. After recovery of the building and network infrastructure, engineers recovered storage hardware and compute VMs that did not recover automatically. By 22:00 UTC, 99.999% of affected VMs were back up and running. Availability of all storage data was restored.

**Next steps:** We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future. In this case, this includes (but is not limited to):

- Review of the building automation control system responsible for this incident, mitigation of any issues if found, and application of the mitigation to other data centers with the same control system
- Review of mechanical cooling system, mitigation of any issues if found, and application of the mitigation to other data centers with the same cooling system.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/9SS0-VT8

## February 2020

### 2/28 RCA - Networking Issue in South Central US (Tracking ID DMP0-HT8)

**Summary of Impact:** Between 12:48 and 19:10 UTC on 28 Feb 2020, a subset of customers in South Central US may have encountered failure notifications when performing service management operations on resources hosted in this region. Additionally, some customers using Azure Data Factory V2 may have seen errors when running pipelines and job executions for dataflow activities as well as seeing errors when attempting to provision SQL Server Integration Services (SSIS) and Integration Runtime for Azure Data Factory SSIS packages.

**Root Cause:** During a scale-up operation of the service that manages customer network resources, a new capacity configuration was deployed. This configuration triggered a conflict with an existing backend service configuration and caused an increase in the failure rate of requests to the service used for service discovery. The increased failure rate exceeded the Azure platform's capability for retry logic to avoid customer impact.

**Mitigation:** Resources deployed during the scale-up operation performed with the incompatible configuration were removed from rotation, allowing the automatic recovery of the backend service.

**Next Steps:** We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future. In this case, this included (but was not limited to):

- Improving deployment testing and detection to avoid configuration conflicts
- Implementing last known good configuration fall back in the event of resource deployment errors, instead of the requirement to deploy new configuration

**Provide Feedback:** Please help us improve the Azure customer communications experience by taking our survey: https://aka.ms/DMP0-HT8.

### 2/24 503 errors accessing the Azure Portal - Mitigated (Tracking ID 8_K4-TD0)

**Summary of impact:** Between approximately 19:45 and 22:15 UTC on 24 Feb 2020, a limited subset of customers may have encountered HTTP 503 error codes when attempting to access the Azure Portal. The availability of individual resources (Virtual Machines, Web Apps, databases, etc.) was not impacted.

**Preliminary root cause:** After a preliminary investigation, engineers determined that an internal automation workflow was generating a high volume of requests to a backend CosmosDB partition on which the Azure Portal relies. As the volume of incoming requests grew, an automated throttling process began on the impacted partition, preventing requests from completing.

**Mitigation:** Engineers manually stopped the internal automation workflow, allowing the volume of requests to return below normal thresholds and the partition throttling to stop.

**Next steps:** We apologize for the impact to affected customers. Engineers will continue to investigate the underlying cause and take steps to prevent future occurrences.

### 2/22 RCA - MSA Login Failures (Tracking ID CT05-PC0)

**Summary of impact:** Between 00:00 UTC and 04:41 UTC on Feb 22, 2020, a subset of our customers may have been unable to sign in with their Microsoft Service accounts (MSA) to access their Azure resources. Users signing in with non-Microsoft accounts would have been unaffected. Users may also have been unable to create new Microsoft accounts.

**Root Cause:** Engineers determined that a server authentication component reached an operational threshold which resulted in increased failures and the unavailability of the service metadata required for successful user sign-in. The issue occurred during planned server maintenance and was detected by internal monitoring.

**Mitigation:** Engineers added additional resources to address the server authentication component hitting a threshold but complete service restoration required a full recovery of the domain controllers followed by service metadata store restarts which extended the duration of the issue. Service was monitored using telemetry to verify the issue was fully mitigated.

**Next Steps:** We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future. In this case, this includes (but not limited to):

- Adding additional capacity and resiliency features for this component to prevent future occurrences.
- Updating datacenter decommission and capacity planning documentation.
- Updating internal monitoring to quickly flag capacity issues when they arise.

**Provide feedback:** Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/CT05-PC0

### 2/21 RCA - Networking - Intermittent Connectivity (Tracking ID CTH0-HZ8)

**Summary of Impact:** Between 22:17 UTC on 21 Feb 2020 and 00:53 UTC on 22 Feb 2020 Azure customers may have experienced network connection failures for IPv4 traffic. During this time:

- Network connections that originated from or were destined to West Europe (Amsterdam) or Southeast Asia (Singapore) regions may have resulted in a connection failure. Two-thirds of the new connection attempts would have been impacted; previously established connections between these two regions were unaffected.
- Any traffic going to or from the Internet was not impacted. IPv6 traffic was not impacted.

**Root Cause:** The incident was caused by a configuration error pushed to routers in Microsoft Wide Area Network (WAN), in Singapore and Amsterdam. The configuration change sent all SYN packets (used to initiate a connection) to the router CPU for inspection, which caused the router's built-in denial of service protection to drop a subset of packets to protect the router CPU.

**Mitigation:** Engineers mitigated the incorrect configuration by deploying an update to the configuration changes of the two impacted network routers. As the deployment progressed through the routers, partial recovery started at approximately 20:40 UTC, followed by full recovery at 00:53 UTC on 22 Feb 2020.

**Next Steps:** We sincerely apologize for the impact to the affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and to our processes to help ensure such incidents do not occur in the future. In this case, this included (but was not limited to):

- Improving the network router configuration testing process in the lab for its efficacy at large traffic scales.
- Improving the alerting to more quickly detect configuration errors.

**Provide Feedback:** Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/CTH0-HZ8

### 2/5 Connectivity errors with Azure Portal - Mitigated (Tracking ID LN_-JC0)

**Summary of impact:** Between 20:25 and 22:10 UTC on 05 Feb 2020, a subset of customers may have experienced difficulties connecting to the Azure Portal.

**Preliminary root cause:** Engineers will continue to investigate to establish the full root cause and prevent future occurrences.

**Mitigation:** Engineers successfully rerouted traffic to another region, allowing connectivity to the Azure Portal to resume, mitigating the issue.

**Next Steps:** We sincerely apologize for the impact to the affected customers. Stay informed about Azure service issues by creating custom service health alerts: https://aka.ms/ash-videos for video tutorials and https://aka.ms/ash-alerts for how-to documentation.