# Azure status history

Product: All | Region: All | Date: Most recent

## December 2016

### 12/23 Azure Functions - Region Selection Issues in Portal | Recovered

**Summary of impact:** Between 00:35 UTC on 22 Dec 2016 to 02:30 UTC on 23 Dec 2016, customers using Azure Functions may not have been able to select regions in the Management Portal and the Functions dashboard when creating applications. Customers provisioning new App Service \ Web Apps in Visual Studio may also have experienced the inability to select regions.

**Preliminary root cause:** Engineers identified a software issue within a recent deployment as the potential root cause.

**Mitigation:** Engineers performed manual patches and rolled out a deployment update to mitigate .

**Next steps:** Engineers will continue to monitor and review deployment procedures to prevent future occurrences.

### 12/22 Visual Studio Team Services

**Summary of impact:** Between 23:55 UTC on 21 Dec 2016 to 01:15 UTC on 22 Dec 2016, you were identified as a customer using Visual Studio Team Services, Visual Studio Team Services \ Build & Deployment, and Visual Studio Team Services \ Load Testing who may have intermittently experienced degraded performance and slowness while accessing accounts or navigating through Visual Studio Online workspaces.

**Preliminary root cause:** Engineers identified a recent configuration change as the potential root cause.

**Mitigation:** Engineers reverted the configuration change to mitigate the issue.

**Next steps:** Engineers will continue to investigate to establish an underlying root cause and prevent future occurrences.

### 12/11 RCA for Network Infrastructure in West Europe

**Summary of impact:** Between 22:29 and 23:45 UTC on the 10 Dec 2016, customers in the West Europe region may have experienced intermittent periods of connectivity issues. This included elevated packet loss and latency to other Azure regions, and inbound/outbound Internet traffic. Network traffic within the region was unaffected during this time. The connectivity loss was a result of an issue in the traffic engineering software on our network routers that failed to route traffic around a fiber issue in the network. Approximately 10% of the traffic failed to reroute to the redundant fiber path.

**Customer impact:** The software bug caused 10% elevated packet drop and latency to traffic to other data centers and to the Internet for a subset of the customers in West Europe.

**Workaround:** There is no workaround for this network issue.

**Root cause and mitigation:** We encountered a software issue on our network routers that caused routing calculations to take longer than expected during a fiber issue in West Europe. The path computation slowdown caused traffic to be dropped instead of moving to the redundant fiber path. Our telemetry detected the issue and we were able to shift traffic to an unaffected path before the underlying fiber problem was resolved. During this impact period, traffic through the device in West Europe was impaired. To prevent a recurrence of this issue, we have added monitoring for the software issue to alert us before the constraint can impact traffic. In addition, there is continuous work towards installing a permanent software correction for the issue.

**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, and in this case it includes (but is not limited to): 1. Improve monitoring to more rapidly indicate when a router device is in this state. Monitoring did detect the traffic issue was occurring, but did not point to the impacted device. 2. Create and load a patch for the impacted routers for the software bug. Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/246853

### 12/10 HDInsight - North Central US

**Summary of impact:** Between 22:30 UTC on 09 Dec 2016 and 05:10 UTC on 10 Dec 2016, customers using HDInsight in North Central US may have received failure notifications when performing service management operations - such as create, update, delete - for resources hosted in this region. Existing clusters were not affected.

**Preliminary root cause:** Engineers identified a recent change in backend systems as a possible underlying cause.

**Mitigation:** Engineers rolled back the change to backend systems to mitigate the issue.

**Next steps:** Continue to investigate the underlying root cause and develop steps to mitigate future recurrences.

### 12/9 SQL Database - North Central US

**Summary of impact:** Between approximately 10:00 and 19:00 UTC on 09 Dec 2016, customers using SQL Database in North Central US may have experienced issues performing service management operations. Server and database create, drop, rename, and change edition or performance tier operations may have resulted in an error or timeout. Availability (connecting to and using existing databases) was not impacted.

**Preliminary root cause:** A backend ecosystem fell into an unhealthy state.

**Mitigation:** Engineers manually recovered the backend ecosystem, and have confirmed that the service is now in a healthy state.

**Next steps:** Engineers will further investigate the root cause for this issue to prevent recurrences.

### 12/9 Virtual Machines (v2) - South Central US

**Summary of impact:** Between approximately 20:00 UTC on 08 Dec 2016 and 00:47 UTC on 09 Dec 2016, customers using Virtual Machines (v2) in South Central US may have experienced failure notifications when attempting to perform networking-related update operations (such as network interfaces, NAT rules, or load balancing) to existing Virtual Machine (v2) configurations. This only affected networking-related operations on Virtual Machines (v2) as all other service management operations (such as Start, Stop, Create, Delete) on all Virtual Machines were fully functional.

**Preliminary root cause:** A software error on a recent deployment was determined as the underlying root cause.

**Mitigation:** Engineers created a new software build and deployed the update to mitigate.

**Next steps:** Engineers will continue to monitor for operational stability and take steps to prevent future recurrences on deployments.

### 12/7 RCA for Storage in North Europe affecting Multiple Services

**Summary of impact:** Between 13:22 and 16:10 UTC on 07 December 2016, a subset of customers using Storage services in North Europe may have experienced difficulties whilst attempting to connect to their resources. In addition, customers using Virtual Machines (VMs) hosted in the affected region may have experienced VM restarts. App Service \ Web App and Azure Search customers that have a dependency on Storage services may also have experienced availability issues in this region. The issue was due to a software bug in an extent management process of Storage services that resulted in the inability to process requests in a scale unit. Azure engineering received VM failures alerts, identified the issue and applied a temporary mitigation by failing over the affected processes. This restored the system to a healthy state. A further subset of customers were identified who may have required additional steps to fully restore system health after VM reboots. Affected customers were notified via their management portal and were given instructions to follow the article https://aka.ms/vmrecovery to restore service health. We sincerely apologize for the extended impact to affected customers.

**Workaround:** During the impacted timeframe, retries may have succeeded for some customers.

**Root cause and mitigation:** The Azure Storage system writes data to extents in a three replica format to ensure high redundancy of the data. Each replica is stored on a separate node, in a separate rack to ensure isolation. The system is designed to ensure that no more than one replica is taken offline at a time for regular platform maintenance, such as software upgrades. Nodes in our datacenter typically have a low failure rate and the system is designed to maintain data availability in the event of unexpected failures. When a disk or node fails, the replication system recognizes it, and replicates the data elsewhere in order to maintain data durability. Though there is significant redundancy in the Storage service subsystem, there is active monitoring to detect impact across all three replicas. This monitoring is designed to trigger alerts that notify engineers to immediately initiate recovery methods on the unavailable replica. The system then enters into failsafe mode resulting in a pause of any data deletion actions on data tagged for deletion (Garbage Collection) until the replicas are again available, the system exits failsafe mode, and the service is fully recovered.

Additionally, the system has designed safeguards which control capacity of affected Storage scale unit if the system goes in extended failsafe mode operation by unpausing garbage collection. In this incident, a software bug in a storage unit reported a false positive for the above mentioned monitoring, in turn triggering the system to operate in failsafe mode. This software bug also suppressed the expected alerting from this monitoring, in turn not raising any warning to engineers to engage for recovery. Consequently, the system was operating in failsafe mode for an extended period. This should have automatically triggered the designed safeguard mechanism to free up space by a garbage collection process to maintain capacity. However due to the failsafe designed mechanism didn't start as expected, thus resulting in eventual running out of space in some of nodes.

Overall capacity in a scale unit was well below safeguard threshold although many individual nodes were almost full. We have a process that manages extents on each storage node that constantly communicates to a metadata server and signs up to take customer write requests based on available disk space. In a normal operation, a metadata server would have detected nodes with no available disk space and prevented accepting further write traffic. In this incident a software bug in an extent management process resulted in the incorrect reporting of available disk space and in turn, kept write traffic diverted to itself. Since these nodes didn't have enough disk space to serve write traffic, this eventually resulted an extent management process failure. Once the process recovered from a failure, receiving again incorrect report of available disk space, this resulted in getting more write traffic assigned to itself and failing to serve write operation then again experiencing a failure. This cycle kept repeating itself for a portion of write requests to this scale unit. As a result of this, a subset storage accounts data was temporary unavailable and in turn causing IaaS Virtual Machines to crash.

Failures of IaaS Virtual Machines raised alarms in our system and engineers were engaged for manual recovery of the system. As soon as engineers suppressed the false positive monitoring, the system exited failsafe mode and returned to normal operation. Normal garbage collection process was resumed as well. This freed up space on all of affected nodes and relieved the system from capacity pressure and in turn returning to normal operation where all write requests were successfully fulfilled.

**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):

1. Fix a software bug in the extent management process of Storage service. A fix has been rolled out to production – completed.
2. Review and assess data loss alerting and safe guard thresholds to cover similar scenarios.
3. Review recovery processes to be able to minimize the time to recovery and automate where it is possible.

**Provide feedback:** Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/244454

## November 2016

### 11/30 Traffic Manager impacting Multiple Services

**Summary of impact:** Between 19:45 and 20:05 UTC on 30 Nov 2016, customers located primarily in the Asia-Pacific geographic region may have experienced failures attempting to connect to a subset of Azure customer resources and platform services. Alerts were received, and engineers were able to correlate failures to Azure Traffic Manager services. During this time, DNS resolution requests for domain records on the Azure Traffic Manager services in the Asia-Pacific region did not receive a response, resulting in timeouts. To mitigate the impact on customers and their services, engineers removed the Asia-Pacific Traffic Manager services from the Anycast advertisement. Traffic Manager services in other regions handled these requests until the Asia-Pacific regional services were fully restored.

**Customer impact:** Customers experienced failures or timeouts reaching resources, sites and services which relied on Traffic Manager DNS resolution.

**Workaround:** None

**Root cause and mitigation:** Maintenance was being completed on network devices in the Asia-Pacific region. Work to be completed increased resiliency and scalability of our network infrastructure. A misconfiguration resulted in inbound routing failure through one of the devices critical to the path of the Traffic Manager services. Telemetry used in monitoring this change in real-time was afterward determined to have been insufficient for this class of device. The engineers performing this maintenance activity received alerts for Traffic Manager, and withdrew the devices in the Asia-Pacific region mitigating the availability impact. Engineers identified the problem, reviewed the proposed fix, and implemented the fix, fully restoring Traffic Manager services in the region.

**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, and in this case it includes (but is not limited to): 1. Automated configuration validation pre and post change. 2.Device specific telemetry integration into change automation, to validate, pause or rollback based on real-time health signals, 3.Add geographic redundancy at the DNS name server level – Complete. Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/240331

### 11/26 Virtual Machines - Central US

**Summary of impact:** Between 05:15 and 05:53 on 26 Nov 2016, a subset of customers using Virtual Machines in Central US may have experienced connection failures when trying to access Virtual Machines as well as Storage availability hosted in this region. Queues, Tables, Blobs, Files, and Virtual Machines with VHDs backed by the impacted storage scale unit were unavailable for the duration of impact.

**Preliminary root cause:** Engineers identified an unhealthy storage component that impacted availability.

**Mitigation:** Systems self-healed by the Azure platform and engineers monitored metrics to ensure stability.

**Next steps:** Investigate the underlying cause and create mitigation steps to prevent future occurrences.

### 11/21 Microsoft Azure Portal – Errors using Azure Resource Manager to create Virtual Machines

**Summary of impact:** Between 16:15 UTC and 22:20 UTC on 21 Nov 2016, customers attempting to use Azure Resource Manager (ARM) to create Virtual Machines (VMs) from the Microsoft Azure portal may have been unable to create ARM VMs with errors. Customers who attempted using ARM to provision new Virtual Machine resources may have been successful by using PowerShell, Azure Command-Line Interface or REST APIs. Azure Engineering investigated this incident and identified an issue with recent changes to the underlying code. Engineers deployed a hotfix which resolved the issue and ensured that Virtual Machine deployment processes returned to a healthy state.

**Customer impact:** Customers attempting to use Azure Resource Manager (ARM) to create Virtual Machines (VMs) from the Microsoft Azure portal may have been unable to create ARM VMs with errors. Customers who attempted using ARM to provision new Virtual Machine resources may have been successful by using PowerShell, Azure Command-Line Interface or REST APIs. Customers would have been able to use ARM within the Microsoft Azure portal to deploy other ARM enabled resources. Some customers may have experienced issues after the mitigation of this incident and mitigated by using a private browsing session to access the Microsoft Azure portal, which cleared the browser caches.

**Workaround:** ARM VM creation by using PowerShell, Azure Command-Line Interface or REST APIs could be used as a workaround during this incident.

**Root cause and mitigation:** An issue with recent changes to the underlying code. Unfortunately the change had a side effect and caused a failure while validating the location of VM at a creation. This was not detected during the testing phase due to an issue with the testing framework that didn't catch this error scenario. We will review the testing framework to be able to catch this sort of failures in future.

**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): 1. Fix the validation failure of locations while creating ARM VM – Completed. 2. Review and improve the testing framework to help ensure detecting this sort of failures in future. 3. Improve deployment methods for the portal changes to be able to apply a hotfix much faster. 4. Improve telemetry by adding more alerting around failures on key scenarios.

**Provide feedback:** Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/153975