Azure status history

Product: All
Region: All
Date: Most recent

March 2019

3/29 RCA - SQL Database

Summary of impact: Between 16:45 and 22:05 UTC on 29 Mar 2019, a subset of customers may have experienced the following:

- Difficulties connecting to SQL Database resources in the East US, UK South, and West US 2 regions
- Difficulties connecting to Service Bus and Event Hubs resources in the East US and UK South regions
- Failures when attempting service management operations for App Service resources in the UK South and East US regions
- Failures when attempting service management operations for Azure IoT Hub resources

Root cause: Azure SQL DB supports VNET service endpoints for connecting specific databases to specific VNETs. A component used in this functionality, called the virtual network plugin, runs on each VM used by Azure SQL DB, and is invoked at VM restart or reboot. A deployment of the virtual network plugin was rolling out worldwide. Deployments in Azure follow the Safe Deployment Practice (SDP), which aims to ensure deployment related incidents do not occur in many regions at the same time. SDP achieves this in part by limiting the rate of deployment for any one change. Prior to the start of the incident this particular deployment had already successfully occurred across multiple regions and for multiple days such that the deployment had reached the later stages of SDP, where changes are deployed to several regions at once. This deployment was using a VM restart capability, which occurs without impact to running workloads on those VMs.

On 5 capacity units across 3 regions, an error in the plugin load process caused the VM to fail to restart. The virtual network plugin is configured as 'required to start', as absence of it prevents key VNET service endpoint functionality from being used on that VM. The error led to repeated restart attempts causing the VMs to continuously cycle. This occurred on enough VMs across those 5 capacity units that there were not enough resources available to provide placement for all databases in those units causing those databases became unavailable. The plugin error was specific to the hardware types and configurations on the impacted capacity units.

The 5 capacity units affected included some of the databases used by Service Bus, Event Hub and App Services in those regions which led to the impact to those services. An impacted database in East US was the global service management state for Azure IoT Hub, hence the broad impact to that service.

Mitigation: Impacted databases using the Azure SQL DB AutoDR capability were failed over to resources in other regions. Some impacted databases were moved to healthy capacity within the region. Full recovery occurred when sufficient affected VMs were manually rebooted on the impacted capacity units. This brought enough healthy capacity online for all databases to become available.

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):

- Fix the error in deployment, which led to continuous recycling on the specific hardware types and configurations [in progress].
- Repair deployment block system - it stopped the deployment in each capacity unit before the entire unit became unhealthy, but not soon enough [in progress].
- Improve detection mechanism - it detected correlated impact at region level, but would have detected faster if each capacity unit was treated separately [in progress].
- Improve service resiliency for IoT Hub [in progress].

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/F4SN-7VZ

3/28 RCA - Data Lake Storage / Data Lake Analytics

Summary of impact: Between 22:10 on 28 Mar 2019 and 03:23 UTC on 29 Mar 2019, a subset of customers using Data Lake Storage and/or Data Lake Analytics may have experienced impact in three regions:

- East US 2 experienced impact from 23:40 UTC on 28 Mar to 03:23 UTC on 29 Mar 2019.
- West Europe and Japan East experienced impact from 22:10 to 23:50 UTC on 28 Mar 2019.

Impact symptoms would have been the same for all regions:

- Customers using Azure Data Lake Storage may have experienced difficulties accessing Data Lake Storage accounts hosted in the region. In addition, data ingress or egress operations may have timed out or failed.
- Customers using Azure Data Lake Analytics may have seen U-SQL job failures.

Root cause:

Background: ADLS Gen1 uses a microservice to manage the metadata related to placement of data. This is a partitioned microservice where each partition serves a subset of the metadata. Each partition is served by a fault tolerant group of servers. Load across various partitions is managed by an XML config file called partition.config – this a master file which has information about all instances of the microservice; a per region file is generated by a tool. (This tool is applied to all config files, not just partition.config.) Load balancing actions are done in response to the overall load in the region and load on specific partitions. Frequency of load balancing actions is dependent on the overall load in the region. Currently, these load-balancing actions are not automated.

All (code and config) microservice deployments are staged and controlled such that deployment goes to a few machines in a region then to all the machines in a region before moving to the next region. A software component called watchdogs is responsible for testing the service continually and raising errors, which will stop a deployment after the first scale unit or two and revert the bad deployment. The watchdogs can also raise alerts that result in engineers being paged. Moving to next region requires success of deployment in the current region AND approval of the engineer.

What happened: Some of the microservice instances across different regions needed balancing of load to continue to provide best experience and availability. An engineer made changes to the global partition.config file for the identified regions and triggered deployment using the process described above. After observing success in a canary region, the engineer approved deployment in all remaining regions. After deployment completed successfully, the engineer received alerts in two regions: East Japan and West Europe.

Investigation revealed a syntax error in the partition.config. The tool which generates this per region config file, deleted the previous version of the region specific partition.config file and failed to generate a new region specific partition.config file. This did not cause any problem for the metadata service and the deployments succeeded. But later, when for unrelated reasons a new metadata service Front End (FE) process would start, the missing partition.config would cause FE to crash. The deployment in the canary region and other regions succeeded because there were no FE starts so the errors were not seen.

Mitigation: The engineer reverted the bad syntax error in the partition.config file. This new version of partition.config fixed the syntax error, mitigating those two regions as FEs stopped crashing. But this revealed a logic error specific to US East2 region in the partition.config which now caused failures in that region until the engineer fixed that error as well restoring the service availability.

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):

- Mandatory test run automatically at submit time, that sanity-checks partition.config. This test would catch both the syntax error and the logic error.
- Hardening the config deployment mechanism, so that it has built-in delay between regions instead of manual approvals.
- Enhance the watchdogs so that they catch more errors and cause deployments to fail automatically and revert.
- Enhance microservice logic to deal more gracefully with errors in partition.config.
- Fix the tool that generates per region config file for the issue that caused it to delete the output file; instead have it raise an error to fail the deployment.
- Move partition.config to a data folder with separate file for each region, so that an error in one region doesn't affect other regions.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/WFTJ-3XG

3/27 RCA - Service Management Failures - West Europe

Summary of impact: Between approximately 15:20 UTC on 27 Mar 2019 and 17:30 UTC on 28 Mar 2019, a subset of customers may have received failure notifications when performing service management operations such as create, update, deploy, scale, and delete for resources hosted in the West Europe region.

Root cause and mitigation:

Root Cause: Regional Network Manager (RNM) is a core component of the network control plane in Azure. RNM is an infrastructure service that works with another component called the Network Service provider (NRP) to orchestrate the network control plane and drive the networking goal state on host machines. Days leading up to the incident, peak load in RNM's partition manager sub-component had been increasing steadily due to organic growth and load spikes. In anticipation of this, the engineering team had prepared a code improvement to the lock acquisition logic to enhance the efficiency of queue draining and improve performance. On the day of the incident, before the change could be deployed, the load increased sharply, concentrating on a few subscriptions. This pushed RNM to a tipping point. The load caused operations to time out, resulting in failures. Most of the load was concentrated on a few subscriptions, leading to lock contentions where one thread was waiting on the other, causing a slow drain of operations. The gateway component in RNM started to aggressively add the failures back in to the queue as retries, leading to a rapid snowball effect. Higher layers in the stack such as ARM and Compute Resource Provider (CRP) further aggravated load with retries.

Mitigation: To mitigate the situation and restore RNM to its standard operating levels, the reties had to be stopped. A hotfix to stop the gateway component in RNM from adding retry jobs to the queue was successfully applied. In addition, the few subscriptions that were generating peak load were blocked from sending control plane requests to West Europe. Timeout value to obtain locks was extended to help operations succeed. As a result, RNM recovered steadily and the load returned to operating levels. Finally the originally planned code change was rolled out to all replicas of the RNM, bringing RNM back to its standard operating levels and providing it the ability to take higher loads and improving its performance.

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. This includes (but is not limited to):

- Improve lock contention in RNM
- Improve RNM performance and scale out capacity with enough headroom
- Mechanisms to throttle workload before RNM service hits tipping point

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey at https://aka.ms/Q6DN-3BG

February 2019

2/27 RCA - USGov Virginia - Service Availability

Summary of impact: Between 07:38 and 09:50 EST on 27 Feb 2019, a subset of customers may have experienced degraded performance or timeouts while accessing Azure resources.

Root cause: During routine electrical equipment maintenance at a datacenter, the equipment responsible for load transfer to our redundant power source failed, causing temporary power loss to a subset of racks and devices within the US Virginia data center. This resulted in cascading impact to dependent Azure services.

During this event, a STS (static transfer switch) failed during a load transfer causing the load to rapidly shift back to its primary source, tripping a circuit breaker to prevent damage to the equipment. The dual failure resulted in a drop in power to both feeds powering the server equipment in part of the data center.

Mitigation: Site engineers were able to bring up the redundant power system and restore power to the affected racks and devices while repairs were made to the defective component, which was then brought back online. Recovery to dependent services was done so manually, and engineers subsequently confirmed mitigation once connectivity was fully restored. Engineers actively monitored the restoration process, and full service restoration was confirmed at 09:50 EST, although most services would have recovered before this time.

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. This includes, but is not limited to:

- Review the pre-checks and validation used on electrical equipment prior to any maintenance and add steps to validate the equipment functionality [in progress]

Provide feedback: Please help us improve Azure customer communications experience by taking our survey https://aka.ms/W59G-LRG

2/22 RCA - Virtual Machines (Classic)

Summary of impact: Between 7:18 UTC and 10:50 UTC on 22 Feb 2019 a subset of customers using Virtual Machines (Classic) or Cloud Services (Classic) may have experienced failures or high latency when attempting service management operations. Retries would have been successful for customers.

Some customers may also have experienced downstream impact to API Management and Backup.

Root cause and mitigation: The Azure Service Management layer (ASM), that manages Classic VMs and Classic Cloud Services, is composed of multiple services and components. During this event, ASM Front ends were running low on available resources, causing some incoming requests to timeout. Engineers established that a platform service update introduced this regression that surfaced only at high incoming traffic volume. The ASM update went through the standard extensive testing and the fault did not manifest itself when the update transited through first, the pre-production environments, and later through the first Production slice where it baked for multiple days. There was no indication of such a failure in those environments during this time.

As a mitigation, the Front Ends were scaled out which restored the service health.

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):

- Refine validation and service upgrade processes to prevent future occurrences with customer impact [complete].
- Enhance telemetry for detecting machine-level resource exhaustion to prevent impact to customer functionality [complete].

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

2/20 RCA - SQL Services - West Europe

Summary of impact: Between 09:40 UTC and 17:15 UTC on 20 Feb 2019 a subset of customers using SQL Services (inclusive of Azure DB for MariaDB, MySQL, and PostgreSQL, SQL DB, and SQL Data Warehouse) in West Europe experienced issues performing service management operations and/or experienced service availability issues following scaling operations. Symptoms may have included but were not limited to:
• Service management operations returning failure notifications
• Server and database create, drop & scale operations may result in "deployment failed" errors
• Failures when creating databases through SQL Script
• Databases may become unavailable after performing scaling operations.

Note: This issue was impacting all types of SQL service deployments (e.g. Elastic Pool, Single and Managed Instances).

Root cause and mitigation: Engineers observed that the SQL Control Plane reached an operational threshold, causing service management for dependent services and service availability failures for scale operations. Logic that selects a ring, a unit of capacity within a region, to place a service instance during creation or SLO change could incorrectly pick the same overloaded ring for incoming placement operations. It would correctly recognize rings close to full capacity and initiate the placement retry. However it would forget prior selection, restart the whole process from the beginning and reconsider a prior rejected ring again. Engineers manually offloaded a backlog of operations, which allowed traffic to resume and mitigated the issue. The mitigation involved removing rings close to full capacity from the selection list first manually and eventually through automation.

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):
• Introduce alerts for this type of the issue
• Fix logic to avoid in order ring traversal
• Introduce stochastic scheme to pick up next available ring for placement
• Create tensile tests simulating the situation to verify the solution and avoid regressions going forward

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

2/18 RCA - Erroneous Browser Warning - Azure Germany Portal

Summary of impact: Between 14:10 and 17:20 UTC on 18 Feb 2019, customers attempting to login to the Azure Germany portal (portal.microsoftazure.de via login.microsoftonline.de) may have received erroneous warnings stating "Deceptive site ahead." This message was erroneous and the site and user credentials were fully secure. The URLs were accidentally marked as malicious in a high-usage URL reputation feed.

Root cause: The URL login.microsoftonline.de was incorrectly classified as an unsafe site due to an operational error, resulting in impact.

Mitigation: Azure engineers worked with the third party provider to mitigate the issue and addressed the root cause of the erroneous classification.

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):
Engineers will continue to investigate alongside the third party provider involved to determine how this incorrect classification occurred to prevent future occurrences.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/V6HG-RQZ

2/11 RCA - Azure Kubernetes Service - East US

Summary of impact: Between 15:00 and 22:05 UTC on 11 Feb 2019, a subset of customers using Azure Kubernetes Service (AKS) in East US may have experienced the following symptoms:

- Intermittent failures with cluster service management operations - such as create, update, delete, and scaling.
- Issues performing workload management operations.
- Brief cluster downtime.

During this time, cluster etcd state may have been rolled back and restored from the previous backup (AKS makes these backups automatically every 30 minutes). Additionally, between 15:00 and 17:45 UTC, new clusters could not be created in this region.

Root cause: Engineers determined that during a recent deployment of new capacity to the backend services responsible for managing deployments and maintenance on customer clusters encountered an error. Specifically, the state store in the East US region was unintentionally modified during troubleshooting of a capacity expansion and caused the system to think that previous deployments of the service did not exist. When the engineers ran automation for adding capacity to the region, it used the modified state store and tried to create additional resources over the top of existing ones. This led to the backend configuration and networking infrastructure needed for Kubernetes to function properly to be recreated. Because of this, the various reconciliation loops that keep customer clusters in sync became stuck when trying to fetch their configuration and it had changed. This caused outages for customers as the backend services were in a stuck state and not reconciling data as needed.

Mitigation: Engineers removed the unhealthy resources from rotation so no new customer resources would be created on the affected clusters. Backend data was rolled back to its previous state and the reconciliation loops for all the resources were restarted as we began to see customer resources recover. Due to the number of changes in the backend data and restarts in the reconciliation loops caused by these changes, several customer resources were stuck with the incorrect state. Engineers restarted customer resources which cleared out stale data and allowed resources to recover.

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):

- An additional validation step before new capacity is rolled out by our automation tools **[COMPLETED]**
- Segmentation of previous capacity expansions in the state store to avoid unintentional modification when adding new capacity **[IN PROGRESS]**

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://aka.ms/4SK-1WG

2/8 RCA - Azure IoT Hub

Summary of impact: Between 08:16 and 14:12 UTC on 08 Feb 2019, a subset of customers using Azure IoT Hub may have received failure notifications or high latency when performing service management operations via the Azure Portal or other programmatic methods.

Workaround: Retrying the operation might have succeeded.

Root cause and mitigation: Engineers found that one of the SQL queries automatically started using a bad query plan causing the SQL DB to start consuming a significantly large percentage of database transaction units (DTUs). This resulted in the client-side connection pools to max out on the concurrent connections to the SQL DB. As a result, any new connections that were being attempted were failing. The operations which were in progress were also taking a long time to finish causing higher end to end latency. The first mitigation step performed was to increase the connection pool size on the clients. This was followed by scaling up the SQL Azure DB and almost doubling the DTUs. The scale up resulted in the bad query plan to get evicted and the good plan to get cached. All incoming calls started passing after this.

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):

- Investigate and drop the offending query plan [in progress].
- Investigate feasibility of auto scale up of SQL DB in use [in progress].
- Implement administrative command to evict a bad query plan [in progress].
- Add troubleshooting guides so the on-call personnel are better equipped to deal with this in future and can mitigate this much more quickly [in progress].

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/XC4G-D_Z

January 2019

1/30 RCA - Intermittent Network Related Timeouts - West US

Summary of impact: Between 00:53 UTC and 03:33 UTC on 30 Jan 2019, a subset of customers in West US may have experienced degraded performance, network drops or time outs when accessing Azure resources hosted in this region. Applications and resources that retried connections or requests may have succeeded due to multiple redundant network devices and routes available within Azure data centers.

Workaround: Retries likely to succeed via alternate network device and routes. Services in other availability zones unaffected.

Root cause: A network device in the US West region experienced a FIB/Linecard problem during a routine firmware update. As a result of the invalid programming, this device was unable to forward all dataplane traffic it was expected to carry, and dropped traffic to some destinations. The Azure network fabric failed to automatically remove this device from service and the device dropped a subset of the outbound network traffic passed through this device. For the duration of the incident, approximately 6% of the available network links in and out of the impacted datacenter were partially impacted. The network device encountered a previously unknown software issue, and was unable to fully program all linecards on it. This led to the device advertising prefixes that were not reachable.

Mitigation: The impacted device was identified and manually removed from service by Azure engineers, the network automatically recovered utilizing alternate network devices. The automated process for updating configuration and firmware detected that the devices had become unhealthy after the update and ceased updating any additional devices.

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):

- Additional monitoring to detect repeats of this device issue *(complete)*
- Improvement in the system for validating device health after changes to validate fib/rib status. *(In Progress)*
- Alerting to detect traffic imbalances on upstream traffic *(complete)*
- Process updates to add manual checks for this impacting scenario *(complete)*

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://aka.ms/QCF2-PXZ

1/29 RCA - Network Infrastructure Event

Summary of impact: Between 21:00 UTC on 29 Jan 2019 and 00:10 UTC on 30 Jan 2019, customers may have experienced issues accessing Microsoft Cloud resources, as well as intermittent authentication issues across multiple Azure services affecting the Azure Cloud, US Government Cloud, and German Cloud. This issue was mitigated for the Azure Cloud at 23:05 UTC on 29 Jan 2019. Residual impact to the Azure Government Cloud was mitigated at 00:00 UTC on 30 Jan 2019 and to the German Cloud at 00:10 UTC on 30 Jan 2019.

Azure AD authentication in the Azure Cloud was impacted between 21:07 - 21:48 UTC, and MFA was impacted between 21:07 - 22:25 UTC.

Customers using a subset of other Azure services including: Microsoft Azure portal, Azure Data Lake Store, Azure Data Lake Analytics, Application Insights, Azure Log Analytics, Azure DevOps, Azure Resource Graph, Azure Container Registries, and Azure Machine Learning may have experienced intermittent inability to access service resources during the incident. A limited subset of customers using SQL transparent data encryption with bring your own key support may have had their SQL database dropped after Azure Key Vault was not reachable. The SQL service restored all databases.

For customers using Azure Monitor, there was a period of time where alerts, including Service Health alerts, did not fire. Azure internal communications tooling was also affected by the external DNS incident. As a result, we were delayed in publishing communications to the Service health status on the Azure Status Dashboard. Customers may have also been unable to log into their Azure Management Portal to view portal communications.

Root cause and mitigation:

Root Cause: An external DNS service provider experienced a global outage after rolling out a software update which exposed a data corruption issue in their primary servers and affected their secondary servers, impacting network traffic. A subset of Azure services, including Azure Active Directory were leveraging the external DNS provider at the time of the incident and subsequently experienced a downstream service impact as a result of the external DNS provider incident. Azure services that leverage Azure DNS were not impacted, however, customers may have been unable to access these services because of an inability to authenticate through Azure Active Directory. An extremely limited subset of SQL databases using "bring your own key support" were dropped after losing connectivity to Azure Key Vault. As a result of losing connectivity to Azure Key Vault, the key is revoked, and the SQL database dropped.

Mitigation: DNS services were failed over to an alternative DNS provider which mitigated the issue. This issue was mitigated for the Azure Cloud at 23:05 UTC on 29 Jan 2019. Residual impact to the Azure Government Cloud was mitigated at 00:00 UTC on 30 Jan 2019 and to the German Cloud at 00:10 UTC on 30 Jan 2019. Authentication requests which occurred prior to the routing changes may have failed if the request was routed using the impacted DNS provider. While Azure Active Directory (AAD) leverages multiple DNS providers, manual intervention was required to route a portion of AAD traffic to a secondary provider.

The external DNS service provider has resolved the root cause issue by addressing the data corruption issue on their primary servers. They have also added filters to catch this class of issue in the future, lowering the risk of reoccurrence.

Azure SQL engineers restored all SQL databases that were dropped as a result of this incident.

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):

• Azure Active Directory and other Azure service that currently leverage an external DNS provider are working to ensure that impacted services are on-boarded to our fully redundant, native to Azure, DNS hosting solution and exercising best practices around DNS usage. This will help to protect against a similar recurrence [in progress].
• Azure SQL DB has deployed code that will prevent SQL DB from being dropped when Azure Key Vault is not accessible [complete]
• Azure SQL DB code is under development to correctly distinguish between Azure Key Vault being unreachable from a key revoked [in progress]
• Azure SQL DB code is under development to introduce a database inaccessible state that will move a SQL DB into an inaccessible state instead of dropping in the event of a key revocation [in progress]
• Azure Communications tooling infrastructure resiliency improvements have been deployed to production which will help ensure an expedited fail over in the event internal communications tooling infrastructure experiences a service interruption [complete]

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/Q7N7-VWG_V4B3-HBG

1/10 RCA - Storage and Dependent Services - UK South

Summary of impact: Between 13:19 UTC on 10 Jan 2019 and approximately 05:30 UTC on 11 Jan 2019, a subset of customers leveraging Storage in UK South may have experienced intermittent service availability issues. Other resources with dependencies on the affected Storage scale unit may have also experienced impact related to this event.

Root cause and mitigation: At 13:15 UTC on 10 Jan 2019, a backend storage node crashed because of a hardware error. Over the next several minutes, the system attempted to balance this load to other servers. This triggered a rare race condition error in the process that served Azure Table traffic. The system then attempted to heal by shifting the Azure Table load to other servers, but the additional load on those servers caused a few more Azure Table servers to hit the rare race condition error. This in turn lead to more automatic load balancing and more occurrences of the race condition. By 13:19 UTC, most of the nodes serving the Azure Table traffic in the scale unit were recovering from the bug, and the additional load on the remaining servers began to impact other services, including disk, blob, and queue traffic.

Unfortunately in this incident, the unique nature of the problem, combined with the number of subsystems affected and the interactions between them, led to a longer than usual time to root cause and mitigate.

To recover the scale unit, the Azure team undertook a sequence of structured mitigation steps, including:

- Removing the faulty hardware node from the impacted scale unit
- Performing a configuration change to mitigate a software error
- Reducing internal background processes in the scale unit to reduce load
- Throttling and offloading traffic to allow the scale unit to gradually recover

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):

- Fix for the race condition which is already deploying across all storage scale units (in progress)
- Improve existing throttling mechanism to detect impact of load transfer on other nodes and rebalance to ensure overall stamp health (in progress)

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://aka.ms/Q5Z2-NWG

1/8 Azure DevTest Labs - Virtual Machine Error Message

Summary of impact: Between 16:30 UTC on 08 Jan 2019 and 00:52 UTC on 10 Jan 2019, a subset of customers using Azure DevTest Labs may have experienced issues creating Virtual Machines from Formulas in lab. Impacted customers may have also experienced incorrect error messages when connecting to Virtual Machines.
Root cause: Engineers determined that an issue within a recent Azure Portal UI deployment task caused impact to customer resource error messaging and operations.
Mitigation: Engineers deployed a platform hotfix in order to mitigate the issue for the majority of impacted customers. Remaining impacted customers will continue to receive communication updates via their Azure Management Portal: https://aka.ms/azserviceissues