Azure status history

Product: All
Region: All
Date: Most recent

May 2018

5/17 Japan East - Service Management Operations Issues with Virtual Machines

Summary of impact: Between 23:06 UTC on 17 May 2018 and 01:30 UTC on 18 May 2018, a subset of customers using Virtual Machines in Japan East may have received failure notifications when performing service management operations - such as create, update, delete - for resources hosted in this region.

Preliminary root cause: Engineers determined that instances of a backend service (Azure Software Load balancer) responsible for processing service management requests became unhealthy, preventing requests from completing.

Mitigation: Engineers took the faulty Azure Software Load balancer out of rotation and rerouted network traffic to mitigate the issue.

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

5/15 Visual Studio App Center - Distribution Center

Summary of impact: Between 17:15 and 20:00 UTC on 15 May 2018, a subset of customers using Visual Studio App Center may have received error notifications when attempting to use the distribute feature in Distribution Center.

Mitigation: Engineers performed a manual restart of a backend service to mitigate the issue.

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

5/3 RCA - Multiple Services - West Central US

Summary of impact: Between 19:47 and 22:05 UTC on 03 May 2018, customers in West Central US may have experienced difficulties connecting to resources hosted in this region. The incident was caused by a configuration change deployed to update Management Access Control Lists (ACLs). The change was deployed to network switches in a subset of clusters in the West Central US Region. The configuration was rolled back to mitigate the incident.

Root cause and mitigation: Azure uses Management ACLs to limit access to the management plane of network switches to a small number of approved network management services and must occasionally update these ACLs. Management ACLs should normally have no effect on the flow of customer traffic through the router. In this incident, the Management ACLs were incorrectly applied in some network switches due to the differences in how ACLs are interpreted between different operating system versions for the network switches. In the impacted switches, this led to the blocking of critical routing Border Gateway Protocol (BGP) traffic, which led to the switches being unable to forward traffic into a subset of the storage clusters in this region. This loss of connectivity to a subset of storage accounts resulted in impact to VMs and services with a dependence on those storage accounts. Engineers responded to the alerts and mitigated the incident by rolling back the configuration changes.

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. Enhancing configuration deployment testing / validation processes and automation to account for variances in network switch operating systems - in progress
2. Reviewing and enhancing the deployment methods, procedures, and automation by incorporating additional network health signals - in progress
3. Monitoring and alerting improvements for Border Gateway Protocol (BGP) - in progress

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://survey.microsoft.com/721577

April 2018

4/26 RCA - App Service - Canada Central

Summary of impact: Between 02:45 to 3:28 UTC and 11:53 to 13:30 UTC on April 26, 2018, customers using App Service in Canada Central may have intermittently received HTTP 500-level response codes, experience timeouts or high latencies when accessing App Service deployments hosted in this region.

Root cause and mitigation: The root cause for the issue was that there was a significant increase in HTTP traffic to certain sites deployed to this region. The rate of requests was so much higher than usual that it exceeded the capacity of the load balancers in that region. Load balancer throttling rules were applied for mitigation initially. However, after a certain threshold, existing throttling rules were unable to keep up with the continued increase in request rate. A secondary mitigation was applied to load balancer instances to further throttle the incoming requests. This fully mitigated 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. In this case, this includes (but is not limited to):
1. Adding aggressive automated throttling to handle unusual increases in request rate
2. Adding network layer protection to prevent malicious spikes in traffic

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/722407

4/26 Traffic Manager - Connectivity Issues

Summary of impact: Between 12:46 and 18:01 UTC on 26 Apr 2018, a subset of customers using Traffic Manager may have encountered sub-optimal traffic routing or may have received alerts relating to degraded endpoints. Customers were provided a workaround during the incident.

Preliminary root cause: A configuration issue with a backend network route caused issues with Traffic Manager probes reaching customer endpoints while checking the endpoint health status which led to those endpoints being marked as unhealthy and traffic routed away from them.

Mitigation: Engineers made mapping updates to the network route which mitigated the issue.

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

4/19 Service Bus - West Europe

Summary of impact: Between approximately 12:00 and 14:44 UTC on 19 Apr 2018, a subset of customers using Service Bus in West Europe may have experienced intermittent timeouts or errors when connecting to Service Bus queues and topics in this region.

Preliminary root cause: This issue is related to a similar issue that occurred on the 18th of April in the same region. Engineers determined that the underlying root cause was a backend service that had become unhealthy on a single scale unit, causing intermittent accessibility issues to Service Bus resources.

Mitigation: While the original incident self-healed, engineers have additionally performed a change to the service configuration to reroute traffic from the affected scale unit to mitigate the issue. In addition, a manual backend scale out was performed.

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

4/17 Content Delivery Network Connectivity

Summary of impact: Between approximately 18:30 and 20:50 UTC on 17 Apr 2018, a subset of customers using Verizon CDN may have experienced difficulties connecting to resources within the European region. Additional Azure services, utilizing Azure CDN, may have seen downstream impact.

Preliminary root cause: Engineers determined that a network configuration change was made to Verizon CDN, causing resource connectivity issues.

Mitigation: Verizon engineers mitigated the issue by rerouting traffic to another IP.

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

4/15 RCA - Issues Performing Service Management Operations - Australia East/Southeast

Summary of impact: Between 21:00 UTC on 15 Apr 2018 and 03:20 UTC on 16 Apr 2018, customers in Australia Southeast may have been unable to view resources managed by Azure Resource Manager (ARM) via the Azure Portal or programmatically and may have been unable to perform service management operations. After further investigation, customers using ARM in Australia East were not impacted by this issue. Service availability for those resources was not affected.

Customer impact: Customers ability to view their existing resources was impacted.

Root cause and mitigation: Customers in Australia Southeast were not able to view the resources managed by Azure Resource Manager (ARM) either through the Azure Portal or programmatically due to a bug in the storage account which only impacted ARM service availability. A storage infrastructure configuration change as part of a new deployment resulted in an authentication failure. ARM system did not recognize the failed calls to the storage account and therefore automatic failover was not executed. Engineers rolled back the configuration change in the deployment to restore successful request processing. This action negated the need for manual failover of the ARM 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 includes (but is not limited to):
1. Apply the mitigation steps to all the scale units [completed]
2. Release the fix to address the storage bug [completed]
3. Update alerts and processes to detect failed storage accounts [pending]

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://survey.microsoft.com/711121

4/9 Azure Active Directory B2C - Multiple Regions

Summary of impact: Between 19:57 and 22:05 UTC on 09 Apr 2018, customers using Azure Active Directory B2C in multiple regions may have experienced client side authorization request failures when connecting to resources. Customers attempting to access services may have received a client side error - "HTTP Error 503. The service is unavailable" - when attempting to login.

Preliminary root cause: Engineers have identified a recent configuration update as the preliminary root cause for the issue.

Mitigation: Engineers rolled back the recent configuration update to mitigate the issue. Some service instances had become unresponsive, and were manually rebooted so that they could pick up the change and the issue could be fully mitigated.

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

4/6 RCA - Azure Active Directory - Authentication Errors

Summary: Between 08:18 and 11:25 UTC on 06 Apr 2018, a subset of customers may have experienced difficulties when attempting to authenticate into resources with Azure Active Directory (AAD) dependencies, the primary impact being experienced for resources located in Asia, Oceania, and European regions. This stemmed from incorrect data mappings in two scale units which caused degraded authentication service for impacted customers, impacting approximately 2.5% of tenants. Downstream impact was reported by some Azure services during the impact period. Customers may have experienced for the following services:

Backup: Failures for the registration of new containers and backup/restore operations
StorSimple: New device registration failures and StorSimple management/communication failures
Azure Bot Service: Bots reporting as unresponsive
Visual Studio Team Services: Higher execution times and failures while getting AAD tokens in multiple regions
Media Services: Authentication failures
Azure Site Recovery: New registrations and VM replications may also have failed
Virtual Machines: Failures when starting VMs. Existing VMs were not impacted
We are aware that other Microsoft services, outside of Azure, were impacted. Those services will communicate to customers via their appropriate channels.

Root cause and mitigation: Due to a regression introduced in a recent update in our data storage service that was applied to a subset of our replicated data stores, data objects were moved to an incorrect location in a single replicated data store in each of the two impacted scale units. These changes were then replicated to all the replicas in each of the two scale units. After the changes replicated, Azure AD frontend services were no longer able to access the moved objects, causing authentication and provisioning requests to fail. Only a subset of Azure AD scale units were impacted due to the nature of the defect and the phased update rollout of the data storage service. During the impact period, authentication and provisioning failures were contained to the impacted scale units. As a result, approximately 2.5% of tenants will have experienced authentication failures.

Timeline:
08:18 UTC - Authentication failures when authenticating to Azure Active Directory detected across a subset of tenants in Asia-Pacific and Oceania.
08:38 UTC - Automated alerts notified Engineers about the incident in APAC and Oceania regions.
09:11 UTC - Authentication failures when authenticating to Azure Active Directory detected across a subset of tenants in Europe.
09:22 UTC - Automated alerts notified engineers about the incident in Europe. As part of the earlier alerts, Engineers already investigating.
10:45 UTC - Underlying issue was identified and engineers started evaluating mitigation steps.
11:21 UTC - Mitigation steps applied to impacted scale units.
11:25 UTC - Mitigation and service recovery confirmed.

Next steps: We understand the impact this has caused to our customers, we apologize for this and are committed to making the necessary improvements to 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. Isolate and deprecate replicas running the updated version of the data store service [Complete]
2. A fix to eliminate the regression is being developed and will be deployed soon [In Progress]
3. Improve telemetry to detect unexpected data movement of data objects to incorrect location [In Progress]
4. Improve resiliency by updating data storage service to prevent impact should similar changes occur in the data object location [In Progress]

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/698785

March 2018

3/20 RCA - App Service and App Service Linux - Multiple Regions

Summary of impact: Between 10:32 UTC and 13:30 UTC on 21 March, customers may have experienced HTTP 5xx errors, latencies and timeouts when performing service management requests - such as create, update, delete - for their App Service (Web, Mobile and API Apps) and App Service(Linux) applications. Retries of these operations during the impact window may have succeeded. Autoscaling and loading site metrics may have also been impacted. App Service runtime operations were not impacted during this incident.

Root cause and mitigation: The root cause of the issue was a software bug introduced in a specific API call during a recent platform update. Due to this bug, any call to this API endpoint resulted in a query against an infrastructure table. Due to high volume of requests in the table, the infrastructure database became overloaded and experienced a CPU spike. This spike was automatically detected and mitigations were applied by the engineering team. Additional fixes were applied to mitigate the bug in production and restore normal CPU levels.

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. Additional monitoring added for detecting rise in CPU consumption for infrastructure database -completed
2. Root cause issue causing the CPU spike fixed and deployed to PROD - completed
3. Additional resiliency measures being investigated for future recurrences - in progress

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/671810

3/19 RCA - SQL Database - West Europe

Summary of impact: Between 11:00 UTC on 19 Mar 2018 and 10:30 UTC on 20 Mar 2018, a subset of customers using SQL Database in West Europe may have experienced difficulties connecting to databases hosted in this region. Service management operations such as scaling Database performance tier were also impacted. During the impact period, some customers using API Management in the region may have also experienced service degradation.

Root cause and mitigation: As part of continuous improvements to support high performance levels, a code deployment was rolled out starting at 02:45 UTC 19 Mar 2018, each backend node downloads the new image from storage. During the regular scheduled code deployment, a set of heavily loaded nodes in the region experienced contention with the image download process. While deployment proceeded as expected across other regions, in West Europe we experienced tensile point which dramatically increased the rate and caused nodes to become unhealthy. The specific point was due to a combination of factors & heavy load on the region, a bug causing an increase in the size of the image being downloaded, and a pre-existing configuration mismatch on a small set of scale units in the region. In addition, our monitoring system had an unrelated issue during part of the incident time window, delaying our detection and impacting our ability to quickly diagnose the issues. Our health monitoring eventually caught up and a rollback was triggered, however the detection threshold allowed too much impact prior to rollback, and the rollback itself took much longer than expected, due to the same tensile point. Once the rollback of the deployment completed, SQL engineers confirmed full mitigation and normal operations were restored by 10:30 UTC 20 Mar 2018.

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. Roll out fix to resolve the bug impacting image download contentions and configuration mismatch in a subset of scale units with urgent priority. [In progress]
2. Enhance dial tone alerting to provide more reliable telemetry for monitoring system failover. [In progress]
3. Improve the configuration for health thresholds at the node level to trigger auto rollbacks. [In progress]
4. Refine drift monitoring to detect specific configuration mismatch to prevent future occurrence. [In progress]
5. Add further tensile tests to our validation pipeline to detect such issues prior rolling to production. [in progress]

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/664182

3/13 Automation - West Europe

Summary of impact: Between 07:00 and 13:39 UTC on 13 Mar 2018, a subset of customers using Automation in West Europe may have observed delays when running new or scheduled jobs in the region. Customers utilizing the update management solution may also have experienced impact.

Preliminary root cause: Engineers determined that instances of a backend service responsible for processing service management and scheduled jobs requests had reached an operational threshold, preventing requests from completing.

Mitigation: Engineers performed a temporary change to the service configuration to downscale a back-end micro-service which mitigated the issue. All jobs are now processing, some may experience a delayed start (max. 6 hours).

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

3/5 Virtual Machines Creation Failure via Azure Portal

Summary of impact: Between 17:40 and 20:20 UTC on 05 Mar 2018, a subset of customers in all regions may have received failure notifications when performing Virtual Machine create job via Microsoft Azure Portal. Virtual Machines creation using PowerShell was not affected during this time.

Preliminary root cause: Engineers determined that a recent Marketplace deployment was preventing requests from completing.

Mitigation: Engineers rolled back the recent deployment task to mitigate the issue.

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

3/2 Log Analytics - Data Processing in East US

Summary of impact: Between approximately 08:00 and 19:00 UTC on 02 Mar 2018, customers using Log Analytics in East US may have been unable to view recently uploaded analytics data. Data has processed slower than expected due to a data ingestion queue backlog.

Preliminary root cause: Engineers determined that some backend instances became unhealthy, preventing analytics data from processing and creating a backlog.

Mitigation: Engineers made a configuration change and restarted backend instances to mitigate the issue.

Next steps: Engineers continue to monitor the backlog which is currently decreasing. Customers who continue to be impacted with this ingestion delay will be communicated to within the Azure Portal.

3/1 RCA - Microsoft Azure Portal

Summary of impact: Between approximately 08:00 and 15:20 UTC on 01 Mar 2018, a subset of customers in West Europe and North Europe may have experienced degraded performance when navigating the Azure Management Portal and attempting to manage their resources. Some portal blades may have been slow to load. Customers may also have experienced slow execution times when running PowerShell commands using Azure Resource Manager templates. Retries may have succeeded.

Root cause and mitigation: The Azure Management Portal has a dependency on a back end service called Azure Resource Manager (ARM). This dependency is called when attempting to view the properties deployed under ARM. ARM front end servers are distributed in regions close to the resources so they can manage incoming requests efficiently. During the impact window of this incident, a subset of front end servers in the UK South region intermittently experienced higher than expected CPU usage. This high usage introduced latency when processing incoming requests which degraded the overall portal experience and PowerShell command execution. Engineers determined that the UK South front end servers received increased traffic as a front end servers in the West Europe region were taken out of rotation for testing on February 28th. The increase in traffic was unexpected as steps had been taken to scale out front end servers in other regions - mainly North Europe - to load balance the traffic. Upon investigation, engineers determined that the scale out operation in North Europe did not complete successfully due to ongoing deployment in that region. The issue was mitigated once additional instances were scaled out across proximity regions.

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. Improve our monitoring, detection and alerting of latency conditions.
2. Scale out to all Europe related regions when taking front end servers out of rotation in one of the Europe regions.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://survey.microsoft.com/638079

February 2018

2/20 RCA - Multiple Services - UK South

Summary of impact: Between 20:48 UTC on 20 February 2018 and 00:02 UTC on 21 February 2018, a subset of customers in UK South may have experienced difficulties connecting to resources hosted in the region. Impacted services during this time included Azure Search, Virtual Machines, Storage, Azure Site Recovery, and Backup. Some virtual machines may have experienced unexpected reboots.

Root cause and mitigation: On 20 February 2018, engineers were performing Datacenter build-out operations in the UK South Datacenter. This type of operation is managed on a regular basis with no impact to customers. During the operation, the additional nodes that were being added to the Datacenter encountered an issue and needed manual input in order to power cycle before continuing the automated build-out process. The engineer responsible for executing the manual step had previously been engaged in investigating an unrelated issue on a production scale unit and had acquired access to this scale unit through standard just-in-time procedures. While using an internal dev-ops tool, the engineer executed the manual power cycle on the scale unit that was already in production instead of the one in build-out. The nodes power cycled as expected and customers services returned to health once this power cycle had completed. During initial investigation, this issue showed signs of a Datacenter hardware power issue. After the detailed investigation, engineers confirmed that the Datacenter power hardware operated as expected, without any unexpected gap in power supply, as this issue was initiated by the commands executed during build-out.

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):
- Temporarily removing bulk power cycle capabilities from the operations tool.
- Broadly reviewing all bulk operation tooling.
- Instituting stricter controls by throttling the operations and requiring additional approvals.
- We will also improve logging so that we can quickly distinguish between power events and power cycles.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://survey.microsoft.com/618897