Azure status history

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

May 2017

5/18 RCA - Storage Latency - West Europe

Summary of impact: Between 02:45 and 15:59 UTC on 18 May 2017, with most impact occurring between 07:00 and 13:00 UTC, a subset of customers using Virtual Machines (VMs), Storage, HDInsight, or Azure Search in West Europe may have experienced high latency or degraded performance when accessing resources hosted in this region. A subset of customers using VMs in the region may have experienced unexpected restarts of their VM. Engineers investigated and determined that root cause was due to congested links in our network infrastructure resulting in reduced network capacity and subsequent impacts to downstream services.

Customer impact: A subset of customers using VMs instances may have experienced unavailability or connection errors due to Storage account accessibility issues. Customers could have seen VMs were either unavailable or having connectivity issues. After mitigation, Storage account access should have been restored.

Root cause and mitigation: Microsoft Azure has implemented an automated service, Lossy Link Monitor (LLM), to eliminate lossy links that monitors all our network interfaces and links for intermittent failures and automatically performs remediation when errors are detected. LLM operates by identifying links that appear to be dropping packets; determining that it would be safe to turn off the link; issuing commands to the switch to turn off the BGP (Border Gateway Protocol) session that directs traffic over the link; opening tickets with on-site staff to have the links repaired; and then restoring traffic to the links after they are repaired and verified working. LLM performs remediation within capacity and error rate thresholds. To increase capacity on aggregation routers, a routine maintenance was performed to deploy configuration updates. This resulted in increased link errors on adjacent downstream devices. LLM detected these link errors and shut down the links. Consequently, there was an unexpected reduction of network capacity for a single data center in the region, causing latency and increased packet-loss for up to 1/8th of flows into and out of the data center. The level of impact varied significantly during the incident period due to variation in the amount of traffic being carried in the data center and the progress of restoring capacity. While engineers worked towards mitigation, Microsoft owned-services reduced their offered traffic load to provide more headroom to Microsoft customer traffic. Engineers disabled the repair service and re-enabled all links that were verified to be carrying traffic correctly, eliminating network congestion and mitigating the issue. RECOMMENDATION (s): Customers may choose to leverage Availability Sets to provide additional redundancy for their application. To learn more about this and other best practices for application resiliency, please refer to the Resiliency checklist at the following link: https://aka.ms/d_nyzbkrl8. Azure Advisor also provides personalized IT recommendations to improve application availability. Please refer to the following link for additional information on Azure Advisor: https://aka.ms/x3aqmn

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. Update the automated monitoring and repair service to account for maintenance scenarios where higher than normal link errors are expected (in progress) 2. Improve alarming for reduced capacity workflows (in progress) 3. Improve telemetry to maintain and leverage accurate state of Networking devices (in progress)

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/365437

5/17 Service Bus - Multiple regions

Summary of impact: Between 21:30 and 23:35 UTC on 16 May 2017, a subset of customers using Service Bus may have experienced errors with SSL validations connecting to resources. This issue only impacted new connections to Service Bus, existing connections were not affected. We recommend customers to restart your processes to complete recovery of the service.

Preliminary root cause: One of the service's connection end points became unhealthy. At this stage engineers do not have a definitive root cause as to why this end point became unreachable.

Mitigation: The issue was self-healed by the Azure platform.

5/12 RCA - Network Infrastructure - East US

Summary of impact: Between 18:33 UTC and 19:08 UTC on 12 May 2017, a subset of customers may have experienced difficulties or received error notifications when connecting to resources hosted in East US. Azure Engineers detected a card failure on a backbone router servicing portions of East US. The router was removed from servicing the network. The backup device exceeded critical parameters due to previously undetected fiber damage on this device, and customers may have observed packet loss and increased latency.

Customer impact: Customers may have experienced 2-5% packet loss, which would have slowed throughput and increased latency to other Azure services and the Internet in portions of East US. Azure monitoring software immediately detected this condition, and Azure Engineers repaired the failed card and placed the first router back in service to correct the condition.

Root cause and mitigation: A failed line card on a network device combined with fiber damage to a second device caused customer impairment. Both issues were repaired and services were 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): 1. Auditing the network to ensure that fiber damage is not present in other locations. 2. Enhancing software capabilities so when line card failures occur, they are mitigated faster to avoid future a recurrence.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/364333

5/12 Virtual Machines - North Europe

Summary of impact: Between 09:07 UTC on 11 May 2017 and 03:02 UTC on 12 May 2017, a subset of customers in North Europe may have received intermittent allocation failure notifications when attempting to provision new D-series V2 Virtual Machines. Customers with existing D-Series V2 Virtual Machines may have also experienced failures when attempting to perform scaling or resizing operations. This issue did not impact the availability of existing Virtual Machines.

Preliminary root cause: Engineers identified a backend service which had reached an operational threshold.

Mitigation: Engineers repaired the unhealthy back end service and took extra steps to improve operational thresholds.

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

5/10 RCA - Intermittent Authentication Failures due to Underlying Azure Active Directory issues

Summary of impact: Between approximately 19:32 and 20:12 UTC on 10 May 2017, a subset of customers may have experienced difficulties or received failure notifications when attempting to authenticate into their resources that are dependent on Azure Active Directory Service. The issue was caused by a configuration change that was incorrectly deployed to Azure Active Directory production. The change was rolled back promptly, which mitigated the incident at 20:12 UTC.

Customer impact: Impacted services for this issue included Azure Management Portal, Visual Studio Team Services, Azure Log analytics, App Service (Web Apps), Azure Machine Learning, Application Insights, Azure Stream Analytics, and Azure Scheduler.

Root cause and mitigation: We have a stringent process in place for all deployments to help ensure that the impact is minimal when bad configurations are introduced. Unfortunately, this process was not closely followed resulting in an unintentional configuration change being rolled out to the Azure Active Directory production services. This issue was detected promptly by our monitoring systems alerting our on-call engineers on a large drop in successful user authentication. The configuration change was rolled back immediately to resolve the incident.

Next steps: We sincerely apologize to our customers impacted by this incident. We have already taken, and are continuing to take measures to address the learnings in this incident. In this case, this includes (but is not limited to): 1. Continue to automate all stages of the Azure Active Directory release management and deployment process. [In progress] 2. Continue to adopt safe deployment principle of progressive rollout for configurations integrated with quality of service and health monitoring as controlling gates. This has been completed for regular code deployments, and work is in progress for configuration updates. 3. Identify early signals to trigger notification processes to reduce time to notify customers [In progress].

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/363702

5/9 Virtual Machines and Storage -West US 2

Summary of impact: Between 21:49 and 22:01 UTC on 08 May 2017, a subset of customers in West US 2 using Virtual Machines may have experienced Virtual Machine reboots as well as Storage customers may have lost connectivity to their premium storage resources.

Preliminary root cause: Engineers determined that a power handling configuration issue was identified as the underlying root cause

Mitigation: The issue was self-healed by the Azure platform.

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

5/4 RCA - Virtual Machines - Japan East

Summary of impact: Between 20:55 and 21:35 UTC on 04 May 2017, a subset of customers using Virtual Machines in Japan East may have experienced intermittent connection failures when trying to access Virtual Machines in the region. Some Virtual Machines may have also restarted unexpectedly. Engineers detected alerts and engaged promptly. The issue was self-healed by the Azure platform self-heal mechanism, Engineers continued to investigate to establish the full root cause and implemented preventive measures to avoid future occurrences.

Customer impact: A subset of customers using Virtual Machines in Japan East may have experienced intermittent connection failures when trying to access Virtual Machines in the region. Some Virtual Machines may have also restarted unexpectedly. A subset of customers using Backup in Japan East may have received timeout error notifications when performing backup and restore operations.

Root cause and mitigation: The Azure Storage system writes data to extents in a 3 replica format to ensure high availability and durability of the data. Each replica is stored on a separate node, in a separate rack. Care is taken to ensure that no more than one replica is taken offline at a time for regular platform maintenance such as software upgrades or hardware repairs. 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. During the incident window, this storage cluster had an abnormally high percentage of nodes out for HW repairs, and was undergoing a software update deployment. The storage system is designed to handle some storage nodes being down for repairs and maintenance without any impact on data availability or customer experience. Unfortunately in this incident the combination of the above and a higher than normal request load on the cluster, exposed a rare software bug which resulted in the failure of storage roles on several additional nodes. This resulted in some data extents becoming temporarily unavailable to clients, including VMs relying on those extents. The VM failures raised alerts in our system and engineers were engaged. The failed storage roles recovered automatically, but engineers took additional action to reduce the overall load on the cluster. Storage returned to normal operation and VMs were recovered.

Next steps: We sincerely apologize for the impact to the 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. Adjustments are being made to the deployment pipeline to further increase the existing safety margin requirement for deployments
2. A fix for the rare software bug is being engineered and will roll out as soon as possible while observing safe deployment process.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/361159

5/3 Backup - Failure notifications when performing Backup operations

Summary of impact: Between 10:00 and 19:55 UTC on 03 May 2017, customers using Backup in North Europe and South Central US may have experienced difficulties when creating new and running scheduled Virtual Machine backup jobs in the region. Customers attempting to access these resources may have encountered the following error message: "VM Agent is unable to communicate with the Azure Backup Service.

Preliminary root cause: Engineers identified a recent deployment task as the potential root cause.

Mitigation: Engineers deployed a platform hotfix to mitigate the issue.

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

5/3 Backup - Failure notifications when performing Backup operations

At 10:00 UTC on 02 May 2017, engineers received a monitoring alert for Backup in West Europe. As engineers continued their underlying cause investigation they concluded that West Europe was not impacted and confirmed that all services are healthy, and a service incident did not occur.

April 2017

4/11 IoT Suite - Failures Provisioning New Solutions - Germany

Summary of impact: Between 07:15 on 08 Apr 2017 and 04:00 UTC on 11 Apr 2017, customers using Azure IoT Suite may have been unable to provision solutions. Engineers recommended deploying from an MSbuild prompt using code at https://aka.ms/rms_git. Existing resources were not impacted.

Preliminary root cause: Engineers identified a recent change to backend systems as the preliminary root cause.

Mitigation: Engineers deployed a platform hotfix to mitigate the issue.

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

4/11 IoT Suite - Failures Provisioning New Solutions

Summary of impact: Between 07:15 on 08 Apr 2017 and 00:00 UTC on 11 Apr 2017, customers using Azure IoT Suite may have been unable to provision solutions. Engineers recommended deploying from an MSbuild prompt using code at https://aka.ms/rms_git. Existing resources were not impacted.

Preliminary root cause: Engineers identified a recent change to backend systems as the preliminary root cause.

Mitigation: Engineers deployed a platform hotfix to mitigate the issue.

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