Azure status history

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

March 2017

3/27 Multiple Azure Services - Japan West - Mitigated

Summary of impact: Between 18:04 and 21:16 UTC on 27 Mar 2017, a subset of customers in Japan West may have experienced degraded performance, network drops or time outs when accessing their Azure resources hosted in this region.

Preliminary root cause: A storage scale unit being added to the Japan West region announced routes that blocked some network connectivity between two datacenters in the region. VMs and services dependent on that connectivity would have experienced restarts or failed connections. Unfortunately, automated recovery did not mitigate the issue. The manual health checks that are conducted around all new cluster additions were performed, but did not detect a problem. This led to a delay in correct root cause analysis and mitigation.

Mitigation: Engineers isolated the newly deployed scale unit, which mitigated the issue.

Next steps: Investigations are currently in progress to determine exactly how incorrect routing information was configured into the storage scale unit being added and how that incorrect information escaped the many layers of validations designed to prevent such issues. A full detailed Root Cause Analysis will be published approximately in 72 hours.

3/27 Multiple Azure Services Impacted by Underlying Network Infrastructure Issue - Japan West - Mitigated

Summary of impact: Between 18:04 and 21:16 UTC on 27 Mar 2017, a subset of customers in Japan West may have experienced degraded performance, network drops or time outs when accessing their Azure resources hosted in this region.

Preliminary root cause: A storage scale unit being added to the Japan West region announced routes that blocked some network connectivity between two datacenters in the region. VMs and services dependent on that connectivity would have experienced restarts or failed connections. Unfortunately, automated recovery did not mitigate the issue. The manual health checks that are conducted around all new cluster additions were performed, but did not detect a problem. This led to a delay in correct root cause analysis and mitigation.

Mitigation: Engineers isolated the newly deployed scale unit, which mitigated the issue.

Next steps: Investigations are currently in progress to determine exactly how incorrect routing information was configured into the storage scale unit being added and how that incorrect information escaped the many layers of validations designed to prevent such issues. A full detailed Root Cause Analysis will be published approximately in 72 hours.

3/27 Visual Studio Team Services

Summary of impact: Between 06:08 and 10:15 UTC on 27 Mar 2017, a subset of customers using Visual Studio Team Services in the Azure Management Portal (https://portal.azure.com) may have experienced difficulties connecting to the following services: VSTS Team Projects, Team Services, Load Testing, Team Service Accounts and Release Management - Continuous Delivery. This would have manifested in the form of continuous loading in the service blade. As a workaround, customers could continue to access these services via their Visual Studio accounts (https://accountname.visualstudio.com). More information is available at https://aka.ms/vstsblog .

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

Mitigation: Engineers rolled back the recent configuration change to mitigate the issue.

3/25 RCA - Intermittent Authentication Failures due to Underlying Azure Active Directory Issue

Summary of impact: Between 21:23 UTC on 24 Mar 2017 to 00:35 UTC on 25 Mar 2017, a subset of customers using Azure Active Directory (AAD) to authenticate to their Azure resources, or services with dependencies on AAD might have experienced failures. This included authentications using the Management Portal, PowerShell, Command-line interfaces (CLI) and other authentication providers. This incident started with high number of failing authentication requests across multiple regions. Failure rates were significantly higher in the US West and US South Central regions than other Azure regions. Engineering teams identified the issue to be a class of requests resulting in expensive backend queries (long running queries) causing timeouts and requests being dropped. Engineering teams worked on isolating the tenants causing this behavior to restore the service.

Customer impact: Customers using AAD, or services with dependencies on AAD authentication, such as Power BI Embedded, Visual Studio Team Services, Log Analytics, Azure Data Lake Analytics, Azure Data Lake Store, Azure Data Catalog, Application Insights, Stream Analytics, Key Vault, and Azure Automation would have seen login failures while accessing their resources.

Root cause and mitigation: Azure Active Directory (AAD) is a comprehensive identity and access management cloud solution. The security token service, which is a significant part of AAD, supports authentication for all modern authentication protocols. During the time of the incident, a specific behavior in the backend of the AAD Security Token Service (STS), resulted in high latency in which to process certain requests as it issued expensive queries to look up the database. This caused the backend of the STS to become overwhelmed and resulted in timeouts and requests being dropped. The Engineering team identified and blocked the requests that were causing these expensive queries. This resulted in full restoration of the service at 00:35 25 Mar 2017 UTC.

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):
- Improve telemetry mechanism for identifying the expensive queries to the AAD STS.
- Implement isolation mechanisms to identify and help stop processing expensive queries beyond a certain threshold.
- Enforce back end throttling based on various parameters (like CPU for example) to help protect against inefficient queries.
- Implement Fault isolation where a problem in one fault unit is prevented from spilling over beyond that fault unit.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/350475

3/23 RCA – Data Lake Analytics and Data Lake Store – East US 2

Summary of impact:

Between approximately March 22 15:02 UTC and March 22 17:25 UTC, a subset of customers experienced a number of intermittent failures when accessing Azure Data Lake Store (ADLS) in East US 2. This may have caused Azure Data Lake Analytics job and/or ADLS request failures. This incident was because of a misconfiguration which resulted in one of the ADLS microservices not serving the requests for the customers.

Azure Monitoring detected the event and an alert was triggered. Azure engineers engaged immediately and mitigated the issue by reverting the configuration that triggered the incident.

Customer impact: A subset of customers in East US 2 had intermittent failures when accessing their Azure Data Lake Service during the timeframe mentioned above.

Workaround:

Retry failed operation. If a customer uses Azure Data Lake Store Java SDK 2.1.4 to access the service, the SDK would have automatically retried and some of the requests may have succeeded with higher latencies.

Root cause and mitigation:

A misconfiguration in one of the microservices that ADLS depends on caused the ADLS microservices to not serve requests after they, or the instances they resided on restarted (which restart is part of regular maintenance process). As more instances were restarted, there were fewer instances of the affected ADLS microservice remaining to serve the requests, which resulted in high latencies and consequently requests failing. Azure engineers identified and reverted the configuration at fault. As the configuration fix was propagated as an expedited fix, and the services were restarted, the affected service instances started to serve requests again, which mitigated this issue. This resulted in intermittent Azure Data Lake Analytics job and ADLS request failures. The jobs that were submitted during the incident are expected to have been queued and ran after the incident, which would have resulted in delays for the start of the jobs.

Was the issue detected?
The issue was detected by our telemetry. An alert was raised, which prompted Azure engineers to investigate an Azure Data Lake Store issue and mitigate the issue.

To achieve quickest possible notification of Service Events to our customers, the Azure infrastructure has a framework that automates the stream from alert to Service Health Dashboard and/or Azure Portal Notifications. Unfortunately, this class of alert does not contain the needed correlation for automation now. We did surface this outage via the Resource Health feature with customer's ADLA and ADLS account(s) in this region. We will continue to implement notification automations as well as ensuring manual communications protocols are followed quickly as possible. In this incident, the issue was announced on Service Health Dashboard manually.

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 misconfiguration. [Completed]
• Improve testing by adding more validations for this sort of configuration error to prevent future occurrences. [Completed]
• Separate the defined configuration container such that it is limiting the impact of future occurrences to smaller slices of the service. [In progress]
• Improve the format of the configuration file to make the code review more efficient in the future. [In progress]
• Add alerts deeper in the stack such that there is earlier/redundant indications of a similar problem for faster debugging. [In progress]
• Rearchitect the initialization phase of the affected service to reduce the dependency on the service that was originally impacted. [Long term]

Provide feedback:

Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/346393

3/23 Azure Active Directory

Summary of impact: Between 22:00 UTC on 22 Mar 2017 and 00:30 UTC on 23 Mar 2017, Azure Active Directory encountered an issue that affected service to service authentication that impacted multiple Azure services. Azure Resource Manager, Logic Apps, Azure Monitor, Azure Data Lake Analytics, and Azure Data Lake Store customers may have experienced intermittent service management issues as downstream impact. AAD customers would not have seen impact.

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

Mitigation: Engineers rolled back the configuration change to mitigate the issue.

3/22 RCA - Increased latency accessing Azure resources

Summary of impact: Between 23:52 UTC on 21 Mar 2017 and 01:14 UTC on 22 Mar 2017, a subset of customers around the South East US may have seen latency and failures accessing Microsoft services including Azure resources. This was due to an infrastructure event impacted by a facilities issue at a 3rd party regional routing site located in South East US. Azure Engineering teams executed standard procedures to redirect traffic and isolate the impacted facility restoring expected routing availability.

Customer impact: A small subset of customers would have observed increased latency or network timeouts while accessing their services on Azure. For a brief period of time, certain customers had significant packet loss that prevented them from reaching Azure sites in the Eastern United States.

Root cause and mitigation: Azure East US Datacenters are connected to the network backbone through a 3rd party network peering site. Due to severe weather in the Atlanta, Georgia, one of the 3rd party peering sites experienced an infrastructure event resulting in loss of cooling. The network equipment in this site started to have increased temperature, and was shutdown to prevent failure. The automated peering load and fail out to a secondary region did not work as expected. This resulted in partial network interruption between Azure Data centers and the Internet, resulting in increased latency and timeouts for customers. Azure Engineering teams worked on manually shifting the traffic to alternate peering sites in East US to resolve the issue. Mitigation of congestion was achieved on 22 Mar 2017 at 01:14 UTC. Cooling was restored to the site, and the routers were recovered to normal operation, after which full peering capacity was restored to the Networking site.

Next steps: 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. Fix and improve the automated peer offloading and balancing logic between sites which prevented safe failover.
2. Investigate and fix the infrastructure issues through vendor co-ordination.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/349643

3/21 Microsoft Accounts Experiencing Login Failures

Summary of impact: Between 17:30 and 18:55 UTC on 21 Mar 2017, a subset of Azure customers may have experienced intermittent login failures while authenticating with their Microsoft Accounts. This would have impacted the ability for customers to authenticate to their Azure management portal (https://portal.azure.com). PowerShell, or other workflows requiring Microsoft Account authentication. Customers authenticating with Azure Active Directory or organizational accounts were unaffected. Customers who had an active session already authenticated with a Microsoft Account before the impact started would also have been unaffected.

Preliminary root cause: Engineers are investigating the full root cause.

Mitigation: Engineers deployed a fix to mitigate the issue. Users may need to exit or refresh their browsers in order to successfully sign in.

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

3/21 RCA - Storage and Virtual Machines - West Europe

Summary of impact: A line card failure on an Azure Networking optical system caused a loss of network capacity to the West Europe Region. During this event, customers experienced increased latency accessing their services and also sporadic packet loss. Azure Networking Engineers replaced the failed optical card to restore service.

Customer impact: Virtual Machines in the West Europe Region saw increased latency and sporadic packet loss during this event.

Root cause and mitigation: Due to the failure of an optical line card, network operational thresholds were reduced in West Europe. Traffic was rerouted to a redundant line card that used a different data path leading to latency across services. The faulty line card was replaced with a spare to restore full services.

Next steps: 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. Operational threshold increases in the Western Europe region. 2. A redesign of the redundancy capabilities in West Europe region to reduce the probability of future occurrences.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/349653

3/18 Log Analytics - East US

Summary of impact: Between 02:47 and 13:15 UTC on 18 Mar 2017, a subset of customers using Log Analytics in East US may have received intermittent failure notifications - such as internal server errors, or tile or blade not loading - when performing log search operations.

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

Mitigation: Engineers cleared out the service management request queues and restarted the backend service to mitigate the issue.

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