INTERNET ARCHIVE WaybackMachine https://azure.microsoft.com/en-us/status/history/ Go
28 captures
23 Dec 2016 – 27 May 2020
NOV JAN APR
2017 16 2019 2020
About this capture

Microsoft Azure
Contact Sales: 0800-627-1035 Search My account Portal Sign in
Overview Solutions Products Documentation Pricing Training Marketplace Partners Support Blog More Free account

Status / History

Azure status history

Product: All
Region: All
Date: Most recent

January 2019

1/10 Storage and Dependent Services - UK South

Summary of impact: Between 13:23 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.

Preliminary root cause: Engineers determined that a number of factors, initially related to a software error, caused several nodes on a single storage scale unit to become temporarily unreachable. This, along with the increase in load on the scale unit caused by the initial issue, resulted in impact to customers with Storage resources located on this scale unit. Due to 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.

Mitigation: To recover the nodes, the Azure team undertook a sequence of structured mitigation steps, including:

- performing a code update to mitigate a software error
- reducing background processes in the scale unit
- throttling and offloading traffic to allow the scale unit to gradually recover

Next steps: Engineers are continuing their investigations to establish the full root cause.

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

1/4 Log Analytics - East US

Summary of impact: Between 09:30 and 18:00 UTC on 04 Jan 2019, a subset of customers using Log Analytics in East US may have received intermittent failure notifications and/or experienced latency when attempting to ingest and/or access data. Tiles and blades may have failed to load and display data. Customers may have experienced issues creating queries, log alerts, or metric alerts on logs. Additionally, customers may have experienced false positive alerts or missed alerts.

Preliminary root cause: Engineers determined that a core backend Log Analytics service responsible for processing customer data became unhealthy when a database on which it is dependent became unresponsive. Initial investigation shows that this database experienced unexpectedly high CPU utilization.

Mitigation: Engineers made a configuration change to this database which allowed it to scale automatically. The database is now responsive and the core backend Log Analytics service is healthy.

Next steps: Engineers will continue to investigate the reason for the high CPU utilization to establish the full root cause. Looking to stay informed on service health? Set up custom alerts here: https://www.aka.ms/ash-alerts

December 2018

12/14 RCA - Networking - UK West

Summary of impact: Between 03:30 and 12:25 UTC on 14 Dec 2018, a subset of customers with resources in UK West may have intermittently experienced degraded performance, latency, network drops or time outs when accessing Azure resources hosted in this region. Customers with resources in UK West attempting to access resources outside of the region may have also experienced similar symptoms.

Root cause: Engineers determined that an external networking circuit experienced a hardware failure impacting a single fiber in this region. A single card on the optical system that services this fiber path had developed a fault, and this reduced the available network capacity, thus causing network issues for a subset of customers.

Mitigation: Azure Engineers initially re-directed internal Azure traffic to free up capacity for customer traffic, and this mitigated the issues being experienced by customers. Engineers subsequently performed a full hardware replacement which restored full connectivity across the fiber circuit, thus completely mitigating 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):

- Augmenting critical networking paths to UK West with 400Gb of additional capacity. 50% of this work is already now complete, and the remaining work is scheduled to be completed by end of February 2019.
- Updating our monitoring to ensure we are able to respond quicker to external networking issues, and thus reduce the impact time for customers.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/B7F1-JXZ

12/12 Azure Analysis Services - West Central US

Summary of impact: Between 21:55 UTC on 12 Dec 2018 and 09:55 UTC on 13 Dec 2018, a subset of customers using Azure Analysis Services in West Central US may have experienced issues accessing existing servers, provisioning new servers, resuming new servers, or performing SKU changes for active servers.

Preliminary root cause: Engineers determined that a recent update deployment task impacted a back-end Service Fabric instance which became unhealthy. This prevented requests to Azure Analysis servers from completing.

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

Next steps: Engineers will review deployment procedures to prevent future occurrences. To stay informed on any issues, maintenance events, or advisories, create service health alerts (https://www.aka.ms/ash-alerts) and you will be notified via your preferred communication channel(s): email, SMS, webhook, etc.

12/12 Log Analytics - East US

Summary of impact: Between 08:00 and 15:50 UTC on 12 Dec 2018, customers using Log Analytics in East US may have experienced delays in metrics data ingestion.

Preliminary root cause: Engineers determined that several service dependent web roles responsible for processing data became unhealthy, causing a data ingestion backlog.

Mitigation: Engineers manually rerouted data traffic to backup roles to mitigate the issue.

Next steps: Engineers will continue to investigate to establish the full root cause for why the service instances became unhealthy. To stay informed on any issues, maintenance events, or advisories, create service health alerts (https://www.aka.ms/ash-alerts) and you will be notified via your preferred communication channel(s): email, SMS, webhook, etc.

12/4 RCA - Networking - South Central US

Summary of impact: Between 02:48 UTC and 04:52 UTC on 04 Dec 2018, a subset of customers in South Central US may have experienced degraded performance, network drops, or timeouts 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 datacenters.

Root cause: Two network devices in the South Central US region received an incorrect configuration during an automated process to update their configuration and firmware. As a result of the incorrect configuration, these routers were unable to hold all of the forwarding information they were expected to carry and dropped traffic to some destinations. The Azure network fabric failed to automatically remove these devices from service and continued to drop a small percentage of the network traffic passed through these devices.

For the duration of the incident, approximately 7% of the available network links in and out of the impacted datacenter were partially impacted.

The configuration deployed to the network devices caused a problem as it contained one setting incompatible with the devices in the South Central US Region. The deployment process failed to detect that the setting should not be applied to the devices in that region.

Mitigation: The impacted devices were 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 issue (complete)
- Improvement in the system for validating the gold configuration file generated for each type of network device (in planning)
- Determine whether this class of conditions can be safely mitigated by automated configuration rollback, and if so add rollback to the error handling used by the configuration and firmware update service (in planning)

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/VXR4-7VZ

November 2018

11/29 Azure Data Lake Store/Data Lake Analytics - North Europe

Summary of impact: Between 08:00 and 13:39 UTC on 29 Nov 2018, a subset of customers using Azure Data Lake Store and/or Data Lake Analytics may have experienced difficulties accessing resources hosted in this region. Data ingress or egress operations may have also timed-out or failed. Azure Data Lake Analytics customers may have experienced job failures. In addition, customers using other services with dependencies upon Azure Data Lake Store resources in this region - such as Databricks, Data Catalog, HDInsight and Data Factory - may also have experienced downstream impact.

Preliminary root cause: A scheduled power maintenance in a datacenter in North Europe resulted in a small number of hardware instances becoming unhealthy. As result of this, Data Lake Store resources hosted on the impacted hardware became temporarily unavailable to customers.

Mitigation: The power maintenance task was cancelled and the impacted hardware was restarted. This returned the affected services hosted on this hardware to a healthy state, mitigating the impact for customers.

Next steps: Engineers will continue to investigate to establish the full root cause of why the power maintenance task failed and prevent future occurrences.

11/28 Storage - West US 2

Summary of impact: Between 04:20 and 12:30 UTC on 28 Nov 2018, a subset of Storage customers in West US 2 may have experienced difficulties connecting to resources hosted in this region. Customers using resources dependent on Storage may have also seen impact.

Preliminary root cause: Engineers determined that a recent deployment task introduced an incorrect backend authentication setting. As a result, some resources attempting to connect to storage endpoints in the region experienced failures.

Mitigation: Engineers developed an update designed to refresh the incorrect authentication setting. A staged deployment of this update was then applied to the impacted storage nodes to mitigate the issue. In a small number of cases, where application of the fix was not possible, impacted nodes were removed from active rotation for further examination.

Next steps: Engineers will review deployment procedures to prevent future occurrences and a full root cause analysis will be completed. To stay informed on any issues, maintenance events, or advisories, create service health alerts (https://www.aka.ms/ash-alerts) and you will be notified via your preferred communication channel(s): email, SMS, webhook, etc.

11/27 RCA - Multi-Factor Authentication

Summary of impact:
At 14:20 UTC on November 27th, the Azure Multi-Factor Authentication (MFA) service experienced an outage that impacted cloud-based MFA customers worldwide. Service was partially restored at 14:40 UTC and fully restored at 17:39 UTC. Login scenarios requiring MFA using SMS, voice, phone app, or OATH tokens-based logins were blocked during that time. Password-based and Windows Hello-based logins were not impacted, nor were valid unexpired MFA sessions.

From 14:20 to 14:40 UTC, any user required to perform MFA using cloud-based Azure MFA was unable to complete the MFA process and so could not sign-in. These users were shown a browser page or client app that contained an error ID.

From 14:40 to 17:39 UTC, the problem was resolved for some users but continued for the majority. This subset of users continued to experience difficulties in authenticating via MFA. When experienced, the user would appear to begin the MFA authentication but never receive a code from the service.

This affected all Azure MFA methods (e.g. SMS, Phone, or Authenticator) and occurred whether MFA was triggered by Conditional Access policy or per-user MFA. Conditional access policies not requiring MFA were not impacted. Windows Hello authentication was not impacted.

Root cause and mitigation:
This outage was caused by a Domain Name System (DNS) failure which made the MFA service temporarily undiscoverable and a subsequent traffic surge resulting from the restoration of DNS service. Microsoft detected the DNS outage when it began at 14:20 UTC when engineers were notified by monitoring alerts.
We sincerely apologize to our customers whose business depends on Azure Multi-Factor Authentication and were impacted by these two recent MFA incidents. Immediate and medium-term remediation steps are being taken to improve performance and significantly reduce the likelihood of future occurrence to customers across Azure, O365 and Dynamics.

As described above, there were two stages to the outage, related but with separate root causes.

- The first root cause was an operational error that caused an entry to expire in the DNS system used internally in the MFA service. This expiration occurred at 14:20 UTC, and in turn caused our MFA front-end servers to be unable to communicate with the MFA back-end.
- Once the DNS outage was resolved at 14:40 UTC, the resultant traffic patterns that were built up from the aforementioned issue caused contention and exhaustion of a resource in the MFA back-end that took an extended time to identify and mitigate. This second root cause was a previously unknown bug in the same component as the MFA incident that occurred on 19 of Nov 2018. This bug would cause the servers to freeze as they were processing the backlogged traffic.
- To prevent this bug causing servers to freeze while a sustainable mitigation was being applied, engineers recycled servers.
- Engineering teams continued add capacity to the MFA service to assist in alleviating the backlog.
- Draining the resultant traffic back to normal levels took until 17:39 UTC at which point the incident was mitigated.

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):

- Implementing the code fix to the MFA backend service to stop servers from freezing when processing high rate of backlogged requests. [COMPLETE]
- During the last incident we increased capacity in the Europe region, capacity is now being scaled out to all regions for MFA. [COMPLETE]
- Deploy improved throttling management system to manage traffic spikes. [COMPLETE]
- All DNS changes will be moved to an automated system [IN PROGRESS]

Provide feedback:
Please help us improve the Azure customer communications experience by taking our survey - https://aka.ms/AA3dtmc

11/26 RCA - Virtual Network - UK South and UK West

Summary of impact: Between 11:19 and 16:56 UTC on 26 Nov 2018, a subset of customers using Virtual Networks in UK South and UK West may have experienced difficulties connecting to resources hosted in these regions. Some customers using Global VNET peering or replication between these regions may have experienced latency or connectivity issues. This issue may have also impacted connections to other Azure services.

Root cause and mitigation: A 16 minute hardware failure on a WAN router caused a large amount of traffic to failover from the primary path out of the region to the backup path, causing increased congestion on the backup path. Once the hardware failure was resolved, a firmware issue with our WAN traffic engineering solution prevented traffic from returning to the primary path, causing the congestion issue to persist. Engineers manually rerouted network traffic back to the primary path to reduce the congestion and mitigate 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):

- Fix the firmware issue that prevented traffic from rerouting back to the primary path (completed)
- Create alerts to detect similar issues with our traffic engineering solution in the future (completed)
- Assess possible design changes to the WAN Traffic Engineering solution to maximize performance in extreme congestion scenarios (in progress)
- Create alerts and monitoring process to detect large traffic flows that can be throttled to reduce congestion in this type of situation (completed)
- Increase capacity in the region to avoid the potential for congestion (completed)

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/F7M1-9QG

11/19 RCA - Multi-Factor Authentication

Summary of impact:
Between 04:39 UTC and 18:38 UTC on 19 November 2018, Microsoft Azure AD Multi-Factor Authentication (MFA) services experienced an outage. Users of Azure Active Directory authentication services - including users of Office 365, Azure, Dynamics and other services which use Azure Active Directory for authentication – were unable to log in if MFA was required as determined by their organization's policy. The event was mitigated on Monday, 19 November 2018 at 18:38 UTC. Furthermore, engineers kept the event open and confirmed through extensive monitoring thatthe root causes identified were correct, incorporated immediate telemetry and processed changes to close the incidentonWednesday, 21 November 2018 at 03:00 UTC.

Root cause:
There were three independent root causes discovered. In addition, gaps in telemetry and monitoring for the MFA services delayed the identification and understanding of these root causes which caused an extended mitigation time.

The first two root causes were identified as issues on the MFA frontend server, both introduced in a roll-out of a code update that began in some datacenters (DCs) on Tuesday, 13 November 2018 and completed in all DCs by Friday, 16 November 2018. The issues were later determined to be activated once a certain traffic threshold was exceeded which occurred for the first time early Monday (UTC) in the Azure West Europe (EU) DCs. Morning peak traffic characteristics in the West EU DCs were the first to cross the threshold that triggered the bug. The third root cause was not introduced in this rollout and was found as part of the investigation into this event.

- The first root cause manifested as latency issue in the MFA frontend's communication to its cache services. This issue began under high load once a certain traffic threshold was reached. Once the MFA services experienced this first issue, they became more likely to trigger second root cause.
- The second root cause is a race condition in processing responses from the MFA backend server that led to recycles of the MFA frontend server processes which can trigger additional latency and the third root cause (below) on the MFA backend.
- The third identified root cause, was previously undetected issue in the backend MFA server that was triggered by the second root cause. This issue causes accumulation of processes on the MFA backend leading to resource exhaustion on the backend at which point it was unable to process any further requests from the MFA frontend while otherwise appearing healthy in our monitoring.

Mitigation:
There were three main phases of this event:

Phase 1: Impact to EMEA and APAC customers - 04:39 UTC to 07:50 UTC on 19 Nov 2018:
To enhance reliability and performance, caching services are used throughout Azure Active Directory. The MFA team recently deployed a change to more effectively manage connections to the caching services. Unfortunately, this change introduced more latency and a race-condition in the new connection management code, under heavy load. This caused the MFA service to slow down processing of requests, initially impacting the West EU DCs (which services APAC and EMEA traffic). During this time, multiple mitigations were applied - including changes in the traffic patterns in the EU DCs, disablement of auto-mitigation systems to reduce traffic volumes and eventually traffic which was rerouted to East US DC. Our expectation was that a healthy cache service in the East US DC would mitigate the latency issues and allow the engineers to focus on other mitigations in the West EU DCs. However, the additional traffic to the East US DC caused the MFA frontend servers to experience the same issue as West EU, and eventually requests started to timeout. Engineers therefore rerouted traffic back to the West EU DCs and continued with the investigation.

Phase 2: Broad customer impact - 07:50 UTC to 18:38 UTC on 19 Nov 2018:
A previously undetected issue in the Azure MFA backend, triggered by the race condition in the front end, and caused an accumulation of processes. Azure MFA backend resource limits were exhausted, preventing the delivery of MFA messages to customers. During this time, the West EU DCs were still experiencing timeouts in serving requests and in the absence of signals/telemetry to indicate other issues, the engineering team's continued focus was on mitigating the latency issue in the MFA frontend servers. In order to restore the health of these datacenters, engineers rolled back the recent deployment, added capacity, increased throttling limits, recycled MFA cache servers and frontend servers and applied a hotfix to the frontend servers to bypass the cache. This mitigated the latency issue, but customers (inclusive of US Gov and China) were still reporting issues with MFA, therefore engineers increased their focus in looking for root causes other than the MFA frontend latency issue.
After investigating and identifying issues in the MFA backend servers, engineers cycled the MFA backend servers to fully restore service health. The initial diagnosis of these issues was difficult because the various events impacting the service were overlapping and did not manifest as separate issues. This was made more acute by the gaps in telemetry that would identify the backend server issue. Once these issues were determined and fully mitigated across all DCs, the team continued to monitor events and customer reported issues for the following 48 hours.

Phase 3: Post recovery - RCA, Monitoring and analysis of customer reported issues - 18:38 UTC on 19 Nov 2018 to 03:00 UTC on 21 Nov 2018:
Engineers kept the incident open for a period of approximately 48 hours to monitor and fully investigate any further customer reported cases and confirm that the issues were fully mitigated. We also wanted to increase our confidence that the root causes identified were, in fact, the source of the failures. On Wednesday, 21 November 2018 at 03:00 UTC, the incident was closed.

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):

- Review our update deployment procedures to better identify similar issues during our development and testing cycles (completion by Dec 2018)
- Review the monitoring services to identify ways to reduce detection time and quickly restore service (completion by Dec 2018)
- Review our containment process to avoid propagating an issue to other datacenters (completion by Jan 2019)
- Update communications process to the Service Health Dashboard and monitoring tools to detect publishing issues immediately during incidents (completed)

We always encourage customers to stay informed on any issues, maintenance events, or advisories. They should visit:https://www.aka.ms/ash-alertsand configure notifications via their preferred communication channel(s): email, SMS, webhook, etc. In this incident communications were not promptly sent to the Service Health blade in the management portal for all impacted customers. This was an error from the Azure team, for which we apologize.

Provide feedback:
Please help us improve the Azure customer communications experience by taking our survey - https://aka.ms/R4S4-RWG

11/14 Azure DevTest Labs - Mitigated

Summary of impact: Between 20:29 and 22:28 UTC on 14 Nov 2018, a subset of customers using Azure DevTest Labs may have received failure notifications when attempting to access their Labs via the Azure Portal.

Preliminary root cause: Engineers determined that a recent deployment task contained an update which caused calls to an internal API to fail.

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.

11/13 App Service and Function Apps

Summary of impact: Between 11:10 and 12:25 UTC on 13 Nov 2018, you were identified as a customer using App Service and/or Function Apps who may have received intermittent HTTP 500-level response codes, have experienced timeouts or high latency when accessing App Service (Web, Mobile and API Apps) deployments hosted in these regions. Impacted customers may have also seen issues with their Azure App Service Scaling settings.

Preliminary root cause: Engineers determined that unhealthy instances of a backend application caused a subset of servers to become unstable, preventing requests from completing.

Mitigation: Engineers performed a hotfix to patch these servers, in order to mitigate the issue.

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

11/11 Storage - West US

Summary of impact: Between 07:12 and 17:19 UTC on 11 Nov 2018, you were identified as a customer using Storage in West US who may have experienced difficulties reading from a subset of blob storage accounts hosted in this region.

Root cause: Engineers received monitoring alerts for degraded storage accessibility. Upon investigation, they determined that a single storage scale unit was unreachable from internet. It started when a route configuration at one of the regional internet service providers caused traffic to get re-routed incorrectly and drop. Traffic inside the Microsoft network for the storage scale unit was not affected by this issue.

Mitigation: Engineers worked with the internet service provider to correct the route configuration and removed the incorrect route advertisement.

Next steps: Microsoft monitors all its route advertisement on the internet to validate the origins of the route. Since this incident, Microsoft has hardened the check for its routes on the internet. Microsoft is also working with large service providers to not accept Microsoft routes from any other service provider.

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.

11/9 App Service and Azure Functions

Summary of impact: Between 22:48 UTC on 08 Nov 2018 and 13:30 UTC on 09 Nov 2018, a subset of customers using App Services may have experienced errors when accessing the Azure Functions blade, or experienced issues when accessing App settings in the Azure portal (https://portal.azure.com)

Preliminary root cause: Engineers identified a recent deployment to a specific regional instance of the Functions portal as the 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.

11/2 Azure Portal Timeouts and Latency

Summary of impact: Between 23:05 UTC on 02 Nov 2018 and 00:21 UTC on 03 Nov 2018, some customers may have experienced high latency or timeouts when viewing resources or loading blades through the Azure Portal (https://portal.azure.com).

Preliminary root cause: Engineers determined that a recent deployment task introduced an updated DNS record that caused the backend service hosting portal blades to become unhealthy, preventing requests from completing.

Mitigation: Engineers performed a configuration change to revert the impacting update.

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

October 2018

10/27 Virtual Machines/VM Scale Sets - West US 2

Summary of impact: Between 02:50 and 10:37 UTC on 27 Oct 2018, a subset of customers using Virtual Machines and/or Virtual Machine Scale Sets in West US 2 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 some instances of a backend service responsible for interservice communication became unhealthy which in turn, caused requests between Storage and dependent resources to fail.

Mitigation: Engineers performed a change to the backend service to achieve mitigation. Platform telemetry was then observed and service team engineers from affected services confirmed all requests completed successfully.

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

10/24 RCA - Networking in West US

Summary of impact: Between 22:40 UTC on 24 Oct 2018 and 00:03 UTC on 25 Oct 2018, a subset of customers may have experienced degraded network performance and/or difficulties connecting to resources in the West US region.

Root cause: A network device connecting a datacenter in the West US region experienced a fault during routine fiber maintenance. Azure Networking lost a subset of capacity between the affected data center and other facilities in the West US region. The failed network device also began silently dropping a portion of the flows that traversed it.

Mitigation: The incident was mitigated by rebalancing traffic across the remaining links. The incident was resolved via restoration of the fiber and the optical system.

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. Steps specific to this incident include:

Evaluate faster link level bidirectional failure detection [in progress]
Evaluate escalated timeline for higher capacity links for this data center [in progress]
Expand existing black hole detection scenarios [in progress]
Review process and validations after fiber plant maintenance [in progress]

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/BRH3-JT0

Go Social
Facebook
Twitter
YouTube
LinkedIn
Rss
Newsletter

Microsoft Azure
Solutions
Products
Regions
Case Studies
Pricing
Member Offers
Calculator
Documentation
Downloads
Samples
Marketplace
Datacenters

Community
Blog
Azure Updates
Tech Community
Events
Careers
Education
Students
Startups

Support
Forums
Azure Status Dashboard
Support

Account
Subscriptions
Profile
Preview Features
Microsoft Azure portal
Privacy data management

Trust Center
Security
Privacy
Compliance

Hello from Seattle. English (US) US Dollar ($) Contact Us Feedback Trademarks Privacy & Cookies Microsoft