Azure status history

This page contains all RCAs for incidents that occurred on November 20th, 2019 or later and will - from that date forward - provide a 5-year RCA history. RCAs prior to November 20th, 2019 are not available.

Product: All

Region: All

Date: All

January 2020

1/30 RCA - Authentication issues for Microsoft Government Cloud resources (Tracking ID 0KYQ-PP8)

Summary of impact: Between 14:12 and 19:10 EST on 30 Jan 2020, approximately 6% of customers in US Government service regions experienced sign-in failures when attempting to access their resources for Azure Government & Office 365 Government services. Customers outside of US Government service regions were not impacted.

Root cause: Engineers made back end updates to the application collection representing Microsoft services in Azure Active Directory in production. The application settings of these services are routinely synchronized from Commercial Microsoft Services to their US Government equivalent. There was a code defect in the incremental/delta synchronization pipeline which left the applications in an incorrect state in US Government service regions. As a result, these applications failed to get a token from Azure Active Directory in the US Government service regions and sign-ins for users of those services failed.

Mitigation: Engineers performed a full synchronization of applications from the Commercial to US Government environment. After the full synchronization cycle was complete, the application state was fixed and the subsequent sign-in requests were successful. To prevent the manifestation of the bug in the US Government service regions, engineers disabled the task which synchronizes the applications from the Commercial to US Government environment. While the task is disabled, applications are kept in sync by making manual updates in both environments.

Next Steps: We sincerely apologize for the impact to the affected customers. We are continuously taking steps to improve the Microsoft Platform and to our processes to help ensure such incidents do not occur in the future. In this case, this included (but was not limited to):

- Engineers are working to fix the bug in the task before re-enabling the synchronization task.
- Improve telemetry to more quickly detect and mitigate bugs before they enter the production environment.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/0KYQ-PP8

1/25 RCA - SQL Database and dependent services - Service Availability Issues (Tracking ID 5TYQ-DC0)

Summary of Impact: Between 22:00 EST on 24 Jan 2020 and 08:15 EST on 25 Jan 2020, customers in the Azure Government regions may have experienced failures when trying to access Azure SQL Database and Data Warehouse resources or dependent services. Specifically, new connections to databases in these regions may have resulted in an error or timeout, but already established pooled connections continued to work. Some manageability operations such as failovers to geo-redundant regions were also impacted.

Root cause: Connections to Azure SQL Database and Azure Data Warehouse go through a set of load balanced front-end nodes called gateways. Engineers determined that a recent maintenance activity did not complete successfully which in-turn caused the gateways to hold an incorrect certificate configuration that effectively blocked connections to the associated SQL resources.

Mitigation: Engineers mitigated the incorrect configuration by deploying an update to the impacted regions. As the deployment progressed through the regions, partial recovery started at approx. 03:30 EST, followed by full recovery at 08:15 EST on 25 Jan 2020.

Next Steps: We sincerely apologize for the impact to the affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and to our processes to help ensure such incidents do not occur in the future. In this case, this includes (but is not limited to):

- Improve the alerting to help detect incorrect configurations quicker.
- Improve our preventative processes and resiliency of the Azure SQL Database and Azure SQL Data Warehouse to help avoid these types of service disruptions in the future.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/5TYQ-DC0

1/24 RCA - Cross-Region Connectivity Issue - North America (Tracking ID 4_YR-FC8)

Summary of Impact: Between 21:03 and 22:28 UTC on 24 Jan 2020, a programming error caused network congestion, dropping around 10% of traffic, and causing high latency for services traversing the network between data centers. A software update on the SWAN (Software enabled Wide Area Network)—Microsoft's backbone network that connects large data center regions together—caused the router forwarding tables to become mis-programmed.

Root Cause: From 21:03 UTC, the SWAN network was unable to generate and program a working Forwarding Information Base (FIB) into the SWAN routers due to a bad configuration push. Incompatible FIB pushes that caused failure on part of the routers resulted in FIB rollbacks. The incompatible FIB push caused all traffic engineering tunnels on the routers to go down, which made traffic go on the shortest path and resulted in congestion drops in the network of around 10% of traffic.

Mitigation: When the incompatible FIB was rolled back to the last known good state, Traffic Engineering worked again, and drops subsided. However, the non-working FIB continued to get generated, and its install/rollback kept causing drops until the configuration change was rolled back. Rollback of the configuration change was slow due to safeguards built into the system. The configuration problem was finally rolled back at 22:28 UTC, completely resolving the traffic drops.

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):

- A correction of the software defect that was introduced that prevented router programming
- Improving testing of SWAN software deployments with the router firmware
- Improving SWAN rollback procedures to make the process faster and less error-prone

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/4_YR-FC8

1/22 Service Management Failures for Application Gateway, Azure Bastion, and Azure Firewall (Tracking ID HT3R-990)

Summary of Impact: Between 05:55 UTC on 22 Jan and 00:56 UTC on 23 Jan 2020, a subset of customers using Application Gateway/WAF V2 SKU, Azure Firewall, and Azure Bastion services may have received failure notifications when performing service management operations—such as create/scale, update, and delete.

Preliminary Root Cause: Engineers determined that a recent deployment task impacted service-to-service communication which resulted in failure of management requests.

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. Stay informed about Azure service issues by creating custom service health alerts: https://aka.ms/ash-videos for video tutorials and https://aka.ms/ash-alerts for how-to documentation.

1/20 RCA - Azure connectivity issues (Tracking ID 0TSQ-TT0)

Summary of impact: Between 15:01 and 16:30 UTC on 20 Jan 2020, a subset of customers in Sweden, Finland, Norway, and Russia may have experienced increased latency or difficulties connecting to Azure services. Impact to customers was based on the location of the customer. Customers in other geographic regions would have continued to be able to access resources during this time.

Root Cause: Microsoft has numerous "Edge Sites" on its network which greatly enhance the connectivity experience for Microsoft users in geographic regions where Edge sites exist. Starting at 15:01 UTC on 20th Jan 2020, a multiple fiber-cut event isolated the Stockholm and Helsinki Azure Edge sites, impacting internet traffic routing via these regions to the wider Microsoft network. For resiliency, these edge sites typically have 2 degrees of connectivity, but in this case, both paths went offline at the exact same time. Further investigation determined that the two diverse paths collapsed into the same conduit for a section outside Stockholm, and this is where the cut happened. Traffic to/from the internet towards Microsoft automatically shifted to other Edge sites in Europe, but the change in path and increase in traffic caused longer latency for some customers.

Mitigation: Microsoft properties in the impacted regions were asked to migrate to other locations to minimize impact. Once this migration completed, the impact to customers was mitigated. In addition, the Microsoft WAN team procured capacity from a different fiber path to bring the impacted sites back online. All sites were fully operational by 2020-01-21 21:18 UTC.

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. In this case, this includes (but is not limited to):

- Improve the speed at which traffic can be routed to other regions to mitigate the impact.
- Harden the fiber infrastructure in Stockholm and Helsinki to make it more resilient to multiple fiber cuts.
- Review of Edge Site connectivity architecture to ensure that there are no other circuit-convergences that inadvertently cause a single point of failure.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/0TSQ-TT0

December 2019

12/27 RCA - Unable to create new resources in Azure Portal (Tracking ID 4_6S-NC8)

Summary of Impact: Between 15:02 UTC and 16:22 UTC on 27 Dec 2019, customers using the Azure Portal may have received failure notifications or 404 errors when attempting to create new resources through the Azure Portal due to the Marketplace Blade not loading. Programmatic deployments, such as CLI, PowerShell, and template deployments would have been successful.

Root Cause: Customers were unable to create new resources in the Azure Portal due to a code change that was introduced which caused a key extension to fail, causing a null-reference within the Marketplace blade. The failure surfaced when a set of dependent static data became stale. Approximately 80% of the tenants issuing create calls through the portal were impacted during the incident. Post mitigation, less than 1% of tenants may have seen errors if the faulty extension was cached in their browser.

Mitigation: The incident was mitigated by rolling back the Marketplace extension to a previous build.

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):

- Code was checked to remove this specific error, and related code was vetted for similar errors.
- Extend tests to cover all extension flows.
- Refactor code to remove null return-values and references to static data.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/4_6S-NC8

12/12 RCA - Connectivity issue for Azure Resources in North America (Tracking ID HKZT-N88)

Summary of Impact: Between 09:45 and 16:26 UTC on 12 Dec 2019, a subset of customers in North America may have experienced degraded performance, network drops, or timeouts when accessing Azure resources. Customers may also have experienced downstream impact to dependent Azure services.

Root cause: Engineers identified a routing protocol metric change within an ISP backbone network, which resulted in network connectivity degradation for a limited subset of Azure customers. Instead of sending traffic to Microsoft to the closest interconnection point, the ISP was sending traffic from across US regions to an interconnection point in California, saturating some of the links in California.

Mitigation: Engineers brought down the affected peerings between Azure and the ISP and failed over network traffic in order to 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):

- Work with the ISP to streamline the engagement process for service incidents to help reduce the time to repair issues in the future.
- Fine tune Azure monitoring and telemetry to more quickly detect and mitigate events of this nature.
- Create automated remediation of interconnection points suffering from network congestion

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/HKZT-N88

12/11 RCA - Azure CDN and Azure Kubernetes Service - Service Availability Issue (Tracking ID LTPP-R98)

Summary of Impact: Between 17:24 and 18:48 UTC on 11 Dec 2019, clients of customers attempting to reach Azure CDN from Verizon endpoints would intermittently receive HTTP (5XX) errors or connection failures instead of expected content.

Root Cause: Azure CDN providers use staged deployment processes to deploy configuration changes across their global infrastructure Points of Presence (PoPs). A recent change to Verizon's deployment pipeline introduced a latent bug that caused some deployment service health notifications to provide incorrect health status. While Verizon was performing maintenance to resolve a delay in a separate configuration deployment, an improperly encoded configuration file was deployed to production. Due to the aforementioned bug which caused latency in their service health notifications, the regular safety features in their deployment process did not trigger, and allowed the improper configuration to reach global PoPs. This configuration caused service instability across the their global PoPs and resulted in customers receiving HTTP errors (5XX) or connection errors when attempting to reach Azure CDN from Verizon endpoints. Verizon's monitoring caught this issue immediately however, and teams were engaged to resolve the issue. Upon Verizon mitigating the issue, Microsoft services were restored to a healthy state.

Mitigation: After determining the root cause to be the improperly encoded configuration file, a new hotfix was developed and deployed globally. After which, the Verizon's global infrastructure began recovering.

Next Steps: We sincerely apologize for the impact to affected customers. We are continuously taking steps with our partners 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 all service change management processes and practices to ensure that all health check mechanisms are monitored and interact correctly with deployment staging.
- Add additional validation to maintenance and deployment practices to ensure all configuration deployment paths result in valid configuration.
- Review all CDN monitoring and alerting services to ensure that all CDN infrastructure availability alerting escalates quickly to Microsoft engineering teams.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/LTPP-R98

November 2019

11/20 RCA - Multiple Services - Downstream impact from Azure Front Door (Tracking ID HLMF-R88)

Summary of Impact: Between 00:56 and 03:40 UTC on 20 Nov 2019, multiple services across Microsoft including Azure, Microsoft 365 and Microsoft Power Platform leveraging the Azure Front Door (AFD) service experienced availability issues resulting from high request failure rates. During this event, some impacted services were able to divert traffic away from the AFD service to mitigate impact for them.

One of the impacted services was the Azure Status Page at https://status.azure.com. Engineering executed the failover plan to the secondary hosting location, but this resulted in a delay in status communication changes. Communications were successfully delivered via Azure Service Health, available within the Azure management portal.

Root Cause: Azure Front Door services provide network edge caching and web acceleration services to many of Microsoft's SaaS services, in addition to the optimization offering direct to Azure customers. A routine, periodic deployment was released through our validation pipeline that, when combined with specific traffic patterns, caused service-wide, intermittent HTTP request failures for all services utilizing the AFD service.

Investigation into the faulting behavior revealed that the combination of a sequenced code deployment, a configuration deployment and specific traffic patterns triggered a dormant code bug that instigated the platform to crash. These deployed changes were tested before being shipped to the broader cloud; however, the specific traffic pattern was not observed during test and pilot phases.

Azure Front Door deploys to over one hundred points of presence (PoPs) around the globe and deploys customer configuration globally to each of these PoPs, enabling customers to quickly make changes to their service. This is done to ensure customers are able to promptly remove regional components out of specification and update configuration for network security services to mitigate attacks. Through a staged deployment, these changes passed validation and service health-checks. Having passed these validations, propagation to global PoPs was quick, by design, to meet the aforementioned service objectives. After propagation, the fault triggering behavior was instigated only by specific traffic patterns, that occurred after the deployment had completed.

This resulted in impacted customers experiencing a high, but intermittent, rate of web request failures globally while accessing shared services across the Azure and Office platforms.

Mitigation: Global monitoring detected the issue and engaged engineers at 01:04 UTC. Engineers confirmed the multiple sources of the issue to be primarily triggered by the configuration deployment and identified a fix for the issue by 01:27 UTC. Engineers immediately initiated deployment rollback procedures to return the service to a healthy state; this rolled out quickly, progressively and completely to all global platforms by 02:40 UTC. Many of the Microsoft SaaS impacted services were able to initiate failover away from the AFD service, providing mitigation to customers while the underlying AFD mitigation was deployed.

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):

- Verify that the fix deployed globally to AFD, during mitigation, is a stable release and will remain in place until all internal reviews of this issue have been completed.
- Review all service change management processes and practices to help ensure appropriate deployment methods are used.
- Review the change validation process to identify components and implement changes, required to increase test traffic diversity, improving the scope of trigger and test code paths.
- Prioritize deployment of a component independent automated recovery process so impacted deployments, like that experienced during this incident, are automatically returned to the last-known-good (LKG) state at a component layer, quickly and without manual intervention, to help reduce time to mitigate and scope of impact.
- Investigate and remediate the delay experienced with publishing communications to the Azure Status Page during the impact window.

Provide Feedback: Please help us improve the Azure customer communications experience by taking our survey https://aka.ms/HLMF-R88