Azure status history

This page contains all root cause analyses (RCAs) for incidents that occurred on November 20, 2019 or later. Each RCA will be retained on this page for 5 years. RCAs before November 20, 2019 aren't available.

Product: All

Region: All

Date: All

December 2021

12/16 Mitigated - Microsoft Graph API (Tracking ID ZN7Y-5DG)

Summary of Impact: Between 14:00 UTC and 17:30 UTC on 16 December 2021, a subset of users in North America may have experienced performance issues and timeout errors with Microsoft Graph APIs.

Preliminary Root Cause: We determined that the scaling out process was affected by an internal infrastructure issue leading to high CPU usage. This resulted in the performance issues and timeout errors with Microsoft Graph APIs.

Mitigation: To mitigate the issue we redistributed traffic to other healthy regions in North America.

Next steps: We 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.

12/16 RCA - Azure Active Directory - Experiencing sign in issues when attempting to access Azure, Dynamics 365, and/or Microsoft 365 Services (Tracking ID S_3M-FZZ)

Summary of impact: Between 01:00 UTC and 02:25 UTC on 16 December 2021, Azure Active Directory (Azure AD) users may have experienced impact when accessing Microsoft 365, Dynamics 365 and Azure services.

Customers using desktop and mobile applications, such as Microsoft Teams, with their work or school accounts experienced minimal disruption as they were automatically routed to the Azure AD Backup Authentication service.

Some Azure AD B2C users may have experienced impact between 01:00 UTC and 02:25 UTC.

Some Microsoft Account users, using Outlook on iOS to access their email, may have experienced impact between 00:11 UTC and 02:25 UTC.

Root Cause: A regular operating system (OS) update was deployed to endpoints of a backend service in the Azure AD authentication stack, which interacted with the service in an unexpected way, making the service on the updated endpoints unresponsive. As the update rollout progressed, all redundant endpoints were impacted, at which point the service became unavailable, on 16 December 2021 at 00:11 UTC.

All changes, with this one included, follow the safe deployment process (SDP) with automated health monitoring in place meant to stop the rollout in the event of an issue. In this case, due to a gap in the backend service's health monitoring, the update rollout was not stopped until all redundant endpoints were impacted. As the backend service became unavailable, this issue started to manifest as sign-in failures for a subset of Microsoft Accounts (personal accounts).

The Azure AD authentication stack is designed with circuit-breakers that isolate failures in service dependencies , and in this case, limiting impact to Microsoft Accounts . However, due to a second latent issue in one of the circuit-breakers, requests that were queuing up as a result of sign-in failures were not limited by this circuit breaker, leading to sign-in failures for a subset of users of Azure AD and Azure AD B2C.

During this outage, we failed to communicate on the specific impact to Azure AD B2C, in particular marking it as impacted on the Azure Status Page, due to a coordination issue. In addition, our first notification to impacted customers was delayed.

Mitigation:

01:00 UTC – The backup authentication service was automatically activated and started taking traffic.

02:25 UTC – The backend service was restored .

04:34 UTC – Traffic to the backup authentication service was routed back to the primary authentication infrastructure.

05:44 UTC – The primary authentication infrastructure was monitored to ensure services stability. Further changes to the backend service were disabled and the incident was declared fully mitigated.

Next steps: We 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):

- Disable all infrastructure changes including OS updates to the active capacity of the backend service – Complete
- Perform changes to the backend service to help reduce time to detect and recover in similar scenarios – Complete
- Improve the communications process to help account for coverage of all impacted services and scenarios - Complete
- Deploy a change to the circuit breakers to fix the discovered latent issue and help minimize impact caused by this backend service – Complete
- Investigate and solidify a plan for additional process and tooling improvements to help reduce the notification time for impacted customers. - January 2022
- Continue to expand coverage of the Backup authentication service – July 2022

12/13 RCA - Azure Data Factory V2 - West Europe (Tracking ID B19M-T9G)

Summary of Impact: Between approximately 06:30 UTC and 12:30 UTC on 13 December 2021, you were identified as a customer that may have experienced intermittent errors accessing Azure Data Factory resources (ADF) in West Europe.

Root Cause: We determined a backend service, responsible for processing API requests became unhealthy. Retry logic from ADF, coupled with this unhealthy service, resulted in a rare combination of transient conditions and lead to additional errors. This resulted in intermittent API failing calls for Azure Data factory resources.

Mitigation: We restarted the backend service which mitigated the issue.

Next Steps: We 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):

- Implement an early alert system to notify failures at this level
- Create a repair item and work with the backend service team to create a solution to help prevent future occurrences

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

12/9 RCA - Errors connecting to SCM App Service and/or Azure Functions deployments (Tracking ID SNCJ-9ZG)

Summary of Impact: Between approximately 21:00 UTC on 09 Dec 2021 and 00:23 UTC on 10 Dec 2021, a subset of customers using App Service and/or Azure Functions may have encountered issues with deployments using web deploy, managing WebJobs, connecting to Web SSH console, executing certain Diagnostic Tools using Azure portal or while accessing SCM endpoint. App Service resources utilizing other deployment methods were not affected. Standard App Service control plane operations and runtime were not impacted.

Root Cause: As part of introducing certain resiliency measure, a configuration change was implemented to create a redundant Domain Name Resolution zone for App Service SCM endpoints. However, due to a misconfiguration, this change incorrectly affected the name resolution for App Service SCM endpoint, which resulted in a subset of our customers not being able to connect to the SCM endpoints of the service. This misconfiguration was limited in scope to the SCM endpoint and no other data plane or control plane operations experienced any failures.

Mitigation: Engineering was engaged upon receiving reports of failure. In order to mitigate the issue, the misconfigured state of the zone was corrected and persisted for SCM endpoints. Most customers observed resolution within 20 - 40 minutes from when the mitigation was applied. Resolution times varied for customers depending on the Time To Live (TTL) setting of the various networking devices in their traffic pipelines.

Next Steps: We 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):

- Adding automated detection for SCM endpoint related failures.
- Adding improved validation for zone configuration updates.
- Enhancing review measures for critical network configurations.

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

November 2021

11/16 RCA - Azure Active Directory - Issues when attempting to authenticate (Tracking ID SVT2-VCZ)

Summary of Impact: Between 20:20 UTC on 16 Nov 2021 and 05:00 UTC on 17 Nov 2021, a subset of customers using Azure Active Directory B2C in the Australia region may have encountered failures while attempting to authenticate. These attempts may have succeeded on retry.

Root Cause: The engineering team has determined that an underlying code defect triggered some service nodes to experience a shortage of outbound ports to complete network tasks. This in turn caused an increase in service latency and timeouts.

Mitigation: As an immediate mitigation, traffic was migrated away from the affected nodes into healthy nodes in a different environment. The engineering team also proactively increased capacity in this environment.

Next Steps: We sincerely apologize for the impact to affected customers. We are currently conducting an internal review to take additional steps to continuously improve the Microsoft Azure platform and our processes to ensure such issues do not occur in the future. In this case, this includes (but is not limited to):

• Enhancement of service capacity and automatic scaling rules to include additional dependencies such as outbound port connections

• Improvement of detection logic for cases where long-running network calls affect customer-facing performance

• An overall service capacity review in the affected region, and worldwide

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

11/12 Microsoft Graph - Intermittent 400-level errors accessing Graph APIs - Mitigated (Tracking ID PLT7-RTZ)

Summary of Impact: Between 02:00 UTC on 12 Nov 2021 and 17:00 UTC on 15 Nov 2021, a subset of customers primarily located in the North America and APAC geographies may have encountered intermittent 400-level errors when attempting to access Microsoft Graph APIs.

Preliminary Root Cause: We determined that a recent update to improve the underlying Microsoft Graph API infrastructure created a configuration issue between the Microsoft Graph API interface and its underlying Internet Information Services driver. This configuration issue prevented calls to various APIs from completing as expected.

Mitigation: We failed-over our service to a previously-known healthy state and rolled back the update to mitigate impact.

Next steps: We sincerely apologize for the impact to affected customers. We 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.

11/9 RCA - Intermittent Failures When Accessing or Using Access Panel (Tracking ID DK83-BDZ)

Summary of Impact: Between 14:03 UTC and 19:28 UTC on Nov 9 2021, customers using Azure Active Directory's Access Panel whose traffic was routed through West Central US and Central US may have experienced issues when attempting to access or use Access Panel functionality. Users may have experienced intermittent failures when attempting the following operations:

• Launching Single Sign on (SSO) applications from My Apps or when using direct sign-on links

• Registering for Multi-Factor authentication (MFA)

• Self-Service Password Reset

• Performing self-service management of groups

• Accepting terms of use agreements

This incident had no impact on authentication and MFA scenarios outside of MFA registration, authentication for applications that were not launched through My Apps or through direct sign-on links.

Root Cause: On 09 Nov 2021 between 03:00 and 05:30 UTC, a code change to Access Panel was deployed and introduced an unrelated bug impacting a small subset of customers. After we failed to detect this bug through testing, it was discovered during telemetry validation in the first deployment stage in West Central US, at which point we failed-over traffic from West Central US to Central US at 07:00 UTC to prevent customers from experiencing this discovered bug. Based on the information available at the time, failing-over traffic was deemed to be the safest and fastest recovery alternative until a fix could be safely deployed the following morning.

Failing-over is a standard operating procedure exercised on at least a monthly basis, however in this case we made the decision to keep the service in a failed-over state, while working on a fix to be deployed the following morning. Since this procedure is regularly tested and is an order of magnitude faster than rolling back the change, we had determined this path as the best course of action, and did not expect any issues. The difference in this instance was that the failover happened during off-business hours and persisted into business hours. This meant that at the point of failover the Central US datacenter was scaled to handle the low amounts of off-business hours traffic.

As we reached business hours for the region, at 14:03 UTC on 09 Nov 2021, we started seeing traffic rising quickly for the Access Panel service in Central US, at a pace which exceeded what the auto-scaling configuration, which our service relies on for reacting to traffic fluctuations, could handle. Our auto-scaling configuration was not equipped to provision capacity at the pace required to keep up with the rate of traffic increase related to both the failover and incoming morning peak traffic combined. That resulted in customer requests to the service timing out and failing.

The issue was detected by automation at 14:09 UTC on 09 Nov 2021 and engineers were engaged at 14:14 UTC. While investigating and validating the scope of impact, communications were delayed, with first notification being sent at 15:25 UTC.

While the incident was ongoing, we inaccurately scoped the customer impact in our communications to only applications launched through the My Apps portal, without calling out direct sign-on links used outside of My Apps. Upon further investigation, we have also found that a workaround could have been possible for a subset of impacted scenarios, where, for applications using sign-on methods other than SAML, customers could have accessed the application's site directly.

Mitigation: Impact was mitigated by rebalancing traffic and manually scaling out the service in the impacted regions, West Central US and Central US. Since the Access Panel service in West Central US was previously auto-scaled down, due to no incoming traffic following the service failover, the scaling out operation took a more significant amount of time. The scale out operations completed at 18:40 UTC on 09 Nov 2021 and mitigated impact for the vast majority of customers. Complete mitigation was accomplished when deployment rollback completed at 19:28 UTC.

Next steps: We 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):

- Adjust provisioned capacity and autoscaling configuration for the Access Panel service in all regions to support failover scenarios during peak hours. (To be completed in November 2021)
- Update Access Panel standard operating procedures to include rapidly increasing capacity during scale-out operations to help shorten mitigation times for similar scenarios. (To be completed in November 2021)
- Update test cases to include missing scenarios as surfaced in this incident. (To be completed in November 2021)
- Improve Access Panel tooling and processes to enable rapid rollbacks of configuration changes. (To be completed in December 2021)
- Improve standard operating procedures for notifying customers to drive down time to notify for this class of incident. (To be completed in March 2022)
- Plan to onboard the Access Panel service to automated communication to help drive down time to notify for this class of incidents. (To be completed in March 2022)
- Adjust standard operating procedures to help improve the quality of communications, including details around scope of impact and potential workarounds. (To be completed in March 2022)

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

October 2021

10/27 SMS MFA not being received by multiple tenants (Tracking ID ZKP4-NSG)

Starting at 10:03 UTC, a subset of customers using SMS for Multi-Factor Authentication in United States are experiencing difficulties signing into Azure resources, such as Azure Active Directory, when Multi-Factor Authentication is required by policy.

Workaround: Customers are recommended to use voice calls or non-telecom authentication methods to complete Multi-Factor Authentication.

Current status: The issue is mitigated as of 13:20 UTC. This issue was due to a 3rd party cellular provider in United States which was experiencing issues, impacting Azure MFA users.

10/13 RCA - Virtual Machines (Tracking ID 0NC_-L9G)

Summary of Impact: Between 06:27 UTC and 12:42 UTC on 13 Oct 2021, a subset of customers using Windows-based Virtual Machines (Windows VMs) may have received failure notifications when performing service management operations – such as start, create, update, delete. Deployments of new VMs and any updates to extensions may have failed. Management operations on Availability Set, Virtual Machine Scale Set were also impacted.

Non-Windows Virtual Machines were unaffected, however services with dependencies on Windows VMs may have also experienced similar failures when creating resources.

Root Cause: Windows-based Virtual Machines utilize the Windows Virtual Machine Agent (VM Agent) extension, which is used to manage interactions between the Virtual Machine and the Azure Fabric.

When creating and updating Windows VMs, the Compute Resource Provider (CRP) has a dependency upon the Platform Image Repository to retrieve download locations for the latest version of the VM Agent package. Using this information, the VM Agent will update itself to the latest version in the VM.

As part of the journey to move all classic resources to Azure Resource Manager (ARM), we are migrating the image and extension publishers to the regional ARM publishing pipeline. Approximately 20% of all extensions have been successfully migrated.

At approximately 06:27 UTC, tooling provided an ARM template for use in performing these migrations. This tooling did not consider an edge case and as an unintended consequence marked the Windows VM Agent extension as visible in the publishing subscription only in the ARM regional service after migration. As the result, VM management operations started to fail after receiving zero results from the regional Platform Image Repositories.

The outcome of this was that service management operations (start, stop, create, delete, etc.) on customers Windows VM were unable to locate the Windows VMAgent extension, and thus unable to complete successfully.

Part of our change management process is to leverage the Safe Deployment Practice (SDP) framework (https://azure.microsoft.com/en-us/blog/advancing-safe-deployment-practices/). In this case, some of the functionality of our classic infrastructure is incompatible with the SDP framework. This incompatibility underscores the importance in which we are treating the complete migration to ARM. Once the migration is complete, it will allow us to make all changes using the SDP framework without using bespoke tools that support classic resources only.

Mitigation: Determining the root cause took an extended period due to multiple releases for Azure components being in flight simultaneously on the platform, each of which had to be investigated. Additionally, involving subject matter experts (SMEs) for each of the involved components added to this time as we needed to eliminate multiple possible scenarios to ensure we could triage the underlying cause.

Once we determined the issue, and reviewed multiple mitigation options, we mitigated impact by making the extension public in one region at first and validating the results, ensuring no further impact would be caused by a surge in requests for Virtual Machines. Once validated, we started rolling out the change to the new pipeline region-by-region, mitigating the issue. Engineers monitored the platform success rate for operations after the changes were completed.

Next Steps: We 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):

- The migration of remaining packages in this category (including the Linux version of the VM Agent) is on hold until all repairs are in place
- Additional pre-check and post-checks are being developed and implemented
- VM operation resilience to failures when VM agent cannot be found
- Engineering is also evaluating other safeguards to flight each extension type and prevent any potential negative impact with the remainder of migration.

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

September 2021

9/3 Microsoft Azure Portal - Issues while trying to create an application - Mitigated (Tracking ID 4M8X-VTZ)

Summary of Impact: Between 15:00 UTC on 03 Sep 2021 and 01:24 UTC on 09 Sep 2021, customers may have experienced issues while trying to create an application on the Azure portal when signed-in with their Microsoft Account (MSA). This issue had no impact on users who have Azure AD tenants.

Preliminary Root Cause: We determined that this issue was caused due to insufficient capacity to handle requests.

Mitigation: We scaled up the capacity to mitigate the issue.

Next Steps: We 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.