Azure status history

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

October 2017

10/10 Visual Studio Team Services - Portal Access Issues

Summary of impact: Between 08:16 and 15:00 UTC on 10 Oct 2017, customers using Visual Studio Team Services may have experienced difficulties connecting to resources hosted by VisualStudio.com.

Preliminary root cause: Engineers suspected that a recent deployment increased the load on servers that handle requests to Shared Platform Services.

Mitigation: Engineers scaled out the number of web roles in the Shared Platform Service to mitigate the issue.

Next steps: Engineers will continue to investigate to establish the full root cause and prevent future occurrences. More information can be found on https://aka.ms/VSTS49171007

10/9 Backup and Site Recovery - UK South

Summary of impact: Starting at 06:10 UTC on 09 Oct 2017, engineers identified that a subset of customers using Backup and Site Recovery in UK South may have received failure notifications when performing service management operations via Powershell or the Azure Management Portal (https://portal.azure.com), for resources hosted in this region.

Preliminary root cause: Engineers at this time do not have a definitive root cause but suspect that a recent deployment task impacted instances of a backend service which became unhealthy, preventing requests from completing.

Mitigation: Engineers are exploring mitigation options.

Next steps: This message will be closed and impacted customers will receive further communications via their Portal. Engineers will continue to investigate to establish the full root cause and prevent future occurrences.

10/7 Infrastructure issue impacting multiple Azure services - Australia East

Summary of impact: Between 22:19 and 22:46 UTC on 6 October 2017, a subset of customer resources and services were impacted by network availability loss in a portion of the Australia East region. Facility engineers were quickly aware, took steps to remediate the issue, and network availability was restored by 22:39 UTC. Azure infrastructure and customer resources largely recovered in the few minutes following.

Customer impact: Because network connectivity was lost between some Virtual Machines and storage resources, VMs would have been shut down and then restarted once connectivity was restored. Additional impacted services include Cloud Services, Azure Search, Service Bus, Event Hub, DevTest Lab, Azure Site Recovery, Azure Key Vault, Visual Studio Team Services, and may have experienced latency or loss in availability to/from portions of the Australia East region.

Root cause and mitigation: During a planned facility power maintenance activity, power was removed from a single feed. No impact was expected from this planned activity, as there are redundant power feeds in the facility. Facility engineers were in the datacenter monitoring this planned activity, and detected unexpected breaker trips on the redundant feeds shortly after the start of maintenance. Engineers performed immediate investigation, and determined that the datacenter spine network devices in the portion of the facility impacted by the power maintenance had lost power. Engineers mitigated the loss of power to these devices by distributing load across additional circuits restoring network connectivity. A review of the datacenter spine network devices revealed that these devices were not power striped across feeds optimally to be resilient to loss of one of the two power feeds. The devices have been subsequently corrected in this facility, and Microsoft is reviewing design and implementation worldwide for these devices. All other devices, servers, and infrastructure maintained availability, as expected during the maintenance. The maintenance was completed without any further impact as originally expected. Azure networks are designed to be resilient to loss of individual or even multiple datacenter spine devices, however, due to the unexpected breaker trips, all devices in this physical facility were impacted, resulting in a loss of connectivity within the facility and with other segments in the Australia East region.

Next steps: We sincerely apologize for the impact to affected customers. We are continuously taking steps to improve the Microsoft Azure Platform and our processes to help ensure such incidents do not occur in the future. In this case, this includes (but is not limited to):
1) Remediate known vulnerability in Australia East facility [COMPLETE]
2) Facility team continuing to work with network engineering on design review to audit and remediate worldwide. [PENDING]

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/481145

10/4 Azure Cloud Shell - Authentication Issues

Summary of impact: Between 02:30 and 08:30 UTC on 04 Oct 2017, a subset of customers using Cloud Shell may have experienced the following authentication error when running Azure CLI command: "A Cloud Shell credential problem occurred. When you report the issue with the error below, please mention the hostname 'host-name'. Could not retrieve token from local cache."

Preliminary root cause: From initial investigations, engineers suspect that there was an issue with the cloud shell images used in the backend to provision this service, which were causing logins to take longer than normal.

Mitigation: Engineers redeployed the Cloud Shell images with a newer image, which was verified as not having the same symptoms, to mitigate the issue.

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

September 2017

9/29 RCA - Storage Related Incident - North Europe

Summary of impact: Between 13:27 and 20:15 UTC on 29 Sep 2017, a subset of customers in North Europe may have experienced difficulties connecting to or managing resources hosted in this region due to availability loss of a storage scale unit. Services that depend on the impacted storage resources in this region that may have seen impact are Virtual Machines, Cloud Services, Azure Backup, App Services\Web Apps, Azure Cache, Azure Monitor, Azure Functions, Time Series Insights, Stream Analytics, HDInsight, Data Factory and Azure Scheduler, Azure Site Recovery.

Customer impact: A portion of storage resources were unavailable resulting in dependent Virtual Machines shutting down to ensure data durability. Some Azure Backup vaults were not available for the duration resulting in backup and restore operation failures. Azure Site Recovery may not be able to failover to latest recovery points or replicate VMs. HDInsight, Azure Scheduler and Functions may have experienced service management and job failure where resources were dependent on the impacted storage scale unit. Azure Monitor and Data Factory may have seen latency and errors in pipelines that have dependencies in this scale unit. Azure Stream Analytics jobs stopped processing input and/or producing output for several minutes. Azure Media Services saw failures & latency for streaming requests, uploads, and encoding.

Workaround: Implementation of Virtual Machines in Availability Sets with Managed Disks would have provided resiliency against significant service impact for VM based workloads.

Root cause and mitigation: During a routine periodic fire suppression system maintenance, an unexpected release of inert fire suppression agent occurred. When suppression was triggered, it initiated the automatic shutdown of Air Handler Units (AHU) as designed for containment and safety. While conditions in the data center were being reaffirmed and AHUs were being restarted, the ambient temperature in isolated areas of the impacted suppression zone rose above normal operational parameters. Some systems in the impacted zone performed auto shutdowns or reboots triggered by internal thermal health monitoring to prevent overheating of those systems. The triggering of inert fire suppression was immediately known, and in the following 35 minutes, all AHUs were recovered and ambient temperatures had returned to normal operational levels. Facility power was not impacted during the event. All systems have been restored to full operational conditions and further system maintenance has been suspended pending investigation of the unexpected agent release. Due to the nature of the above event and variance in thermal conditions in isolated areas of the impacted suppression zone, some servers and storage resources did not shutdown in a controlled manner. As a result, additional time was required to troubleshoot and recover the impacted resources. Once the scale unit reached the required number of operational nodes, customers would have seen gradual, but consistent improvement until fully mitigated at 20:15 UTC when storage and dependent services were able to fully recover.

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): Suppression system maintenance analysis continues with facility engineers to identify the cause of the unexpected agent release, and to mitigate risk of recurrence. Engineering continues to investigate the failure conditions and recovery time improvements for storage resources in this scenario. As important investigation and analysis are ongoing, an additional update to this RCA will be provided before Friday, 10/13.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey: https://survey.microsoft.com/476163

9/24 App Service - South Central US

Summary of impact: Between 23:18 and 23:37 UTC on 23 Sep 2017, a subset of customers using App Service in South Central US may have experienced intermittent latency, timeouts, or HTTP 500-level response codes while performing service management operations such as site create, delete, and move resources on their App Service applications.

Preliminary root cause: Engineers determined preliminary root cause as a backend networking connectivity issue.

Mitigation: Engineers determined that the issue was self-healed by the Azure platform.

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

9/22 App Service \ Web Apps - North Europe

Summary of impact: Between 10:00 and 12:09 UTC on 22 Sep 2017, a subset of customers using App Service \ Web Apps in North Europe may have received HTTP 500-level response codes, or experienced timeouts or high latency when accessing Web Apps deployments hosted in this region.

Preliminary root cause: At this stage engineers do not have a definitive root cause.

Mitigation: Engineers determined that the issue was self-healed by the Azure platform.

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

9/21 Unable to Access Azure Management Portal

Between approximately 12:45 and 16:15 UTC on 21 Sep 2017, a subset of customers may have received intermittent HTTP 503 errors or seen a blue error screen when loading the Azure Management Portal page (https://portal.azure.com).

Preliminary root cause: At this stage engineers do not have a definitive root cause.

Mitigation: Engineers determined that the issue was self-healed by the Azure platform.

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

9/15 App Service - North Europe

Summary of impact: Between 19:30 and 20:15 UTC on 15 Sep 2017, a subset of customers using App Service in North Europe may have received HTTP 500-level response codes, have experienced timeouts or high latency when accessing App Service deployments hosted in this region.

Preliminary root cause: At this stage engineers do not have a definitive root cause.

Mitigation: Engineers determined that the issue was self-healed by the Azure platform.

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

9/4 RCA - ExpressRoute \ ExpressRoute Circuits - Washington DC

Summary of impact: Between approximately 09:07 and 14:56 UTC on 04 Sep 2017, a subset of customers using ExpressRoute Services with circuits terminating in the Washington DC region may have experienced difficulties connecting to Microsoft Azure resources, Dynamics 365 services or Office 365 services. Customers with backup Express Route Service circuits in other regions or with internet failover paths should not have been impacted. Customers using Azure Virtual Network services were not impacted during this time.

Customer impact: Connectivity between customer sites and Microsoft Express Route Service Endpoints was interrupted in the Washington DC region.

Workaround: Customers with a failover path would not have been impacted. More information can be found here: aka.ms/s3w930

Root cause and mitigation: A routine maintenance was being conducted on the Microsoft Network in the Washington DC area. As part of the change, a legacy configuration was applied that did not include required routing policy statements. As a result, multiple routes in the Washington DC location were withdrawn, which resulted in the connectivity failures.

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): Standard Operational Procedures (SOP) updated for this class of change world-wide including health validation signals at time of change; Additional rigor applied to SOP reviews and changes; and ExpressRoute Engineering will be adding monitoring to generate alerts on all routes that are withdrawn.

Provide feedback: Please help us improve the Azure customer communications experience by taking our survey https://survey.microsoft.com/462133