Title:	Mitigated - Storage - Timeout errors in USGov Texas
Tracking ID:	CS55-LR0
Event Type:	Service Issue
Status:	Resolved
Service(s):	Storage
Region(s):	USGov Texas
Start time:	2024-11-01T16:24:54.217Z
Resolve time:	2024-11-01T19:53:45.000Z
Last update time:	2024-11-01T22:10:59.663Z
Impacted subscriptions:	f1b079b4-2e4e-40f6-9f79-c7d2d04f80a9, dbc97370-ba60-40bf-8f44-f7652eb5afd3, 668034d3-759f-4ca0-b335-b69e62f339da, 137c0b71-bd77-4d72-bdcc-a3619fa47602

Last update:

What happened?

Between 12:11 EDT and 15:02 EDT on 1 November 2024, a single storage scale unit became unavailable leading to customer impact in USGov Texas region. Customers using Virtual Machines (VMs), databases and other Azure services may have seen timeout errors or their VMs being unavailable.

Since the incident was due to an outage in a storage cluster any services hosted in or communicating with that cluster were also impacted including VMs, Cosmos DB, Azure Kubernetes Service (AKS), SQL Database, Service Bus, Azure B2B Invitation Manager, Log Analytics, Application Insights and Microsoft Sentinel.

What do we know so far?

For this issue, we identified that an inadvertent power event occurred. This impacted physical infrastructure which included the network devices in that cluster which degraded connectivity to the storage infrastructure.

How did we respond?

12:11 EDT - Impact began
12:24 EDT - Teams were alerted and engaged once connectivity was disrupted to the storage infrastructure.
14:35 EDT - Infrastructure team confirms power event as the primary cause.
14:41 EDT - To mitigate, we reenergized restoring power to critical network devices.
15:02 EDT - No further errors were observed, issue declared mitigated.

What happens next?

Our team will be completing an internal retrospective to understand the incident in more detail. Once that is completed, generally within 14 days, we will publish a Post Incident Review (PIR) to all impacted customers. To get notified when that happens, and/or to stay informed about future Azure service issues, make sure that you configure and maintain Azure Service Health alerts – these can trigger emails, SMS, push notifications, webhooks, and more: https://aka.ms/ash-alerts. For more information on Post Incident Reviews, refer to https://aka.ms/AzurePIRs. The impact times above represent the full incident duration, so are not specific to any individual customer. Actual impact to service availability may vary between customers and resources – for guidance on implementing monitoring to understand granular impact: https://aka.ms/AzPIR/Monitoring. Finally, for broader guidance on preparing for cloud incidents, refer to https://aka.ms/incidentreadiness.

Update history:

Fri Nov 01 2024 17:10:59 GMT-0500 (Central Daylight Time)
What happened?

Between 12:11 EDT and 15:02 EDT on 1 November 2024, a single storage scale unit became unavailable leading to customer impact in USGov Texas region. Customers using Virtual Machines (VMs), databases and other Azure services may have seen timeout errors or their VMs being unavailable.

Since the incident was due to an outage in a storage cluster any services hosted in or communicating with that cluster were also impacted including VMs, Cosmos DB, Azure Kubernetes Service (AKS), SQL Database, Service Bus, Azure B2B Invitation Manager, Log Analytics, Application Insights and Microsoft Sentinel.

What do we know so far?

For this issue, we identified that an inadvertent power event occurred. This impacted physical infrastructure which included the network devices in that cluster which degraded connectivity to the storage infrastructure.

How did we respond?

12:11 EDT - Impact began
12:24 EDT - Teams were alerted and engaged once connectivity was disrupted to the storage infrastructure.
14:35 EDT - Infrastructure team confirms power event as the primary cause.
14:41 EDT - To mitigate, we reenergized restoring power to critical network devices.
15:02 EDT - No further errors were observed, issue declared mitigated.

What happens next?

Our team will be completing an internal retrospective to understand the incident in more detail. Once that is completed, generally within 14 days, we will publish a Post Incident Review (PIR) to all impacted customers. To get notified when that happens, and/or to stay informed about future Azure service issues, make sure that you configure and maintain Azure Service Health alerts – these can trigger emails, SMS, push notifications, webhooks, and more: https://aka.ms/ash-alerts. For more information on Post Incident Reviews, refer to https://aka.ms/AzurePIRs. The impact times above represent the full incident duration, so are not specific to any individual customer. Actual impact to service availability may vary between customers and resources – for guidance on implementing monitoring to understand granular impact: https://aka.ms/AzPIR/Monitoring. Finally, for broader guidance on preparing for cloud incidents, refer to https://aka.ms/incidentreadiness.