System: Cloud Service Availability
Subsystem: Application Layer
Component: Code created by the application dev team
Design Lead:
Core Team:

Potential Failure Modes and Effects

Key Date: N/A

FMEA Number: 1
Prepared By: Adrian Cockcroft
FMEA Date: 12/5/2018
Revision Date: 11/10/2019
Page: 1 of 1

Item / Function	Potential Failure Mode(s)	Potential Effect(s) of Failure	Sev	Potential Cause(s)/ Mechanism(s) of Failure	Prob	Current Design Controls	Det	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Action Results: Actions Taken	New Sev	New Occ	New Det	New RPN
Authentication	Client can't authenticate	Can't connect application	5	Certificate timeout, version mismatch, account not setup, credential changed	3	Log and alert on authentication failures	3	45							0
	Slow or unreliable authentication	Slow start for application	4	Auth service overloaded, high error and retry rate	3	Log and alert on high authentication latency and errors	4	48							
								0							0
Client Request to API Endpoint	Service unknown, address un-resolvable	Delay while discovery or DNS times out, slow fallback response	5	DNS configuration error, denial of service attack, or provider failure	1	Customer eventually complains via call center	10	50	Dual redundant DNS, fallback to local cache, hardcoded IP addresses. Endpoint monitoring and alerts						0
	Service unreachable, request undeliverable	Fast fail, no response	4	Network route down or no service instances running	1	Autoscaler maintains a number of healthy instances	1	4	Endpoint monitoring and alerts						0
	Service reachable, request undeliverable	Connect timeout, slow fail, no response	4	Service frozen/not accepting connection	1	Retry request on different instance. Healthcheck failure instances removed.	2	8							0
	Request delivered, no response - stall	Application request timeout, slow fail, no response	4	Broken service code, overloaded CPU or slow dependencies	1	Retry request on different instance. Healthcheck failure instances removed.	2	8							0
	Response undeliverable	Application request timeout, slow fail, no response	4	Network return route failure, dropped packets	1	Retry request on different instance. Healthcheck failure instances removed.	2	8							0
	Response received in time but empty or unintelligible	Fast fail, no response	3	Version mismatch or exception in service code	2	Retry request on different instance. Healthcheck failure instances removed.	2	12							0
	Request delivered, response delayed beyond spec	Degraded response arrives too late, slow fallback response	6	Service overloaded or GC hit, dependent services responding slowly	2	Retry request on different instance. Healthcheck failure instances removed. Log and alert.	2	24							0
	Request delivered, degraded response delivered in time	Degraded timely response	2	Service overloaded or GC hit, dependent services responding slowly	2	Log and alert on high service latency and errors	2	8							0
Time Bombs	Internal application counter wraparound								Test long running operations of code base						
	Memory leak								Monitor process sizes and garbage collection intervals over time						0
Date Bombs	Leap year, leap second, epoch wrap around, "Y2K"								Test across date boundaries						
Content Bombs	Incoming data that crashes the app								Fuzz the input with generated random and structured data to show it doesn't crash.						
Configuration Errors	Configuration file syntax errors or incorrect values								Canary test deployments incrementally. Chaos testing.						0
Versioning Errors	Incompatible interface versions								Canary test deployments incrementally						0
Retry Storms	Too many retries, too large timeout values								Chaos testing applications under stress						
Excessive Logging	Cascading overload								Chaos testing applications under stress						0