System Cloud Service Availability
Subsystem Operations
Component
Design Lead Adrian Cockcroft
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 11/11/2019
Page 1 of 1

											Action Results				
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	Actions Taken	ew Se	ew Oc	ew D	New RPN
Authentication	Montoring agent can't authenticate	Can't monitor application	5	Certificate timeout, version mismatch, account not setup, credential changed	3	Log and alert on authentication failures	3	45							0
	Montoring tool end user operator can't authenticate	Can't monitor system, increased MTTR	5	Certificate timeout, version mismatch, account not setup, credential changed	3	Log and alert on authentication failures	3	45							
	Slow or unreliable authentication	Errors and delays in observability and alerts	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
								0							0