Outage Prediction modelling in Cloud environment

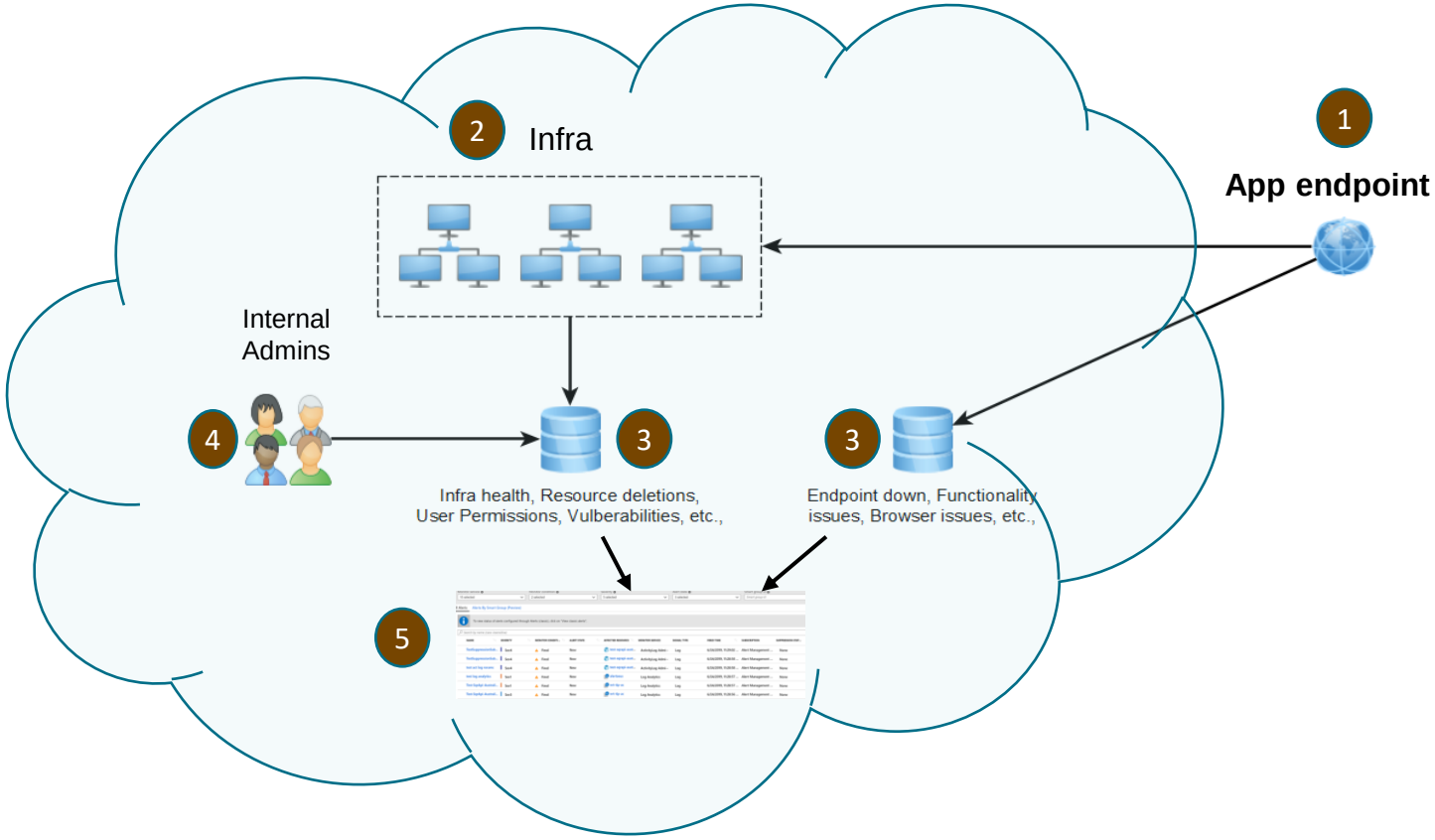
22-Jul-2021

HEXAGON

Agenda

- Cloud System overview
- Additional Notes
- Internal Monitoring system
- Problem Statement
- Symptom & incident relationship
- Relationship between counters
- Expected results
- Methodology – Initial thoughts
- Next Steps

Cloud System Overview



1. SaaS application runs in the cloud and accessible through a web interface.
2. In SaaS model – servers, databases and code that makes up an application are hosted in cloud environment.
3. Monitoring data is collected from a variety of sources viz., Application, Virtual Machines, Database, etc., and stored in a database.
4. User role permission changes are also monitored.
5. Critical conditions are identified in the monitoring data collected and notified through alerts for further investigation.

HEXAGON

Additional Notes

- Cloud system is a system of systems.
- Failures can happen due to frequent updates of components, changes in environments, malware, etc.,
- Failures can degrade system availability and lead to bad user experience.
- Each component has continuously monitoring system.
- Monitoring data across the whole cloud system is collected and should be utilized to diagnose and predict outages.
- To diagnose where outages come from and investigate dependency relationships between signals and outages.
- Find the relationship between signals and outages for outage prediction.

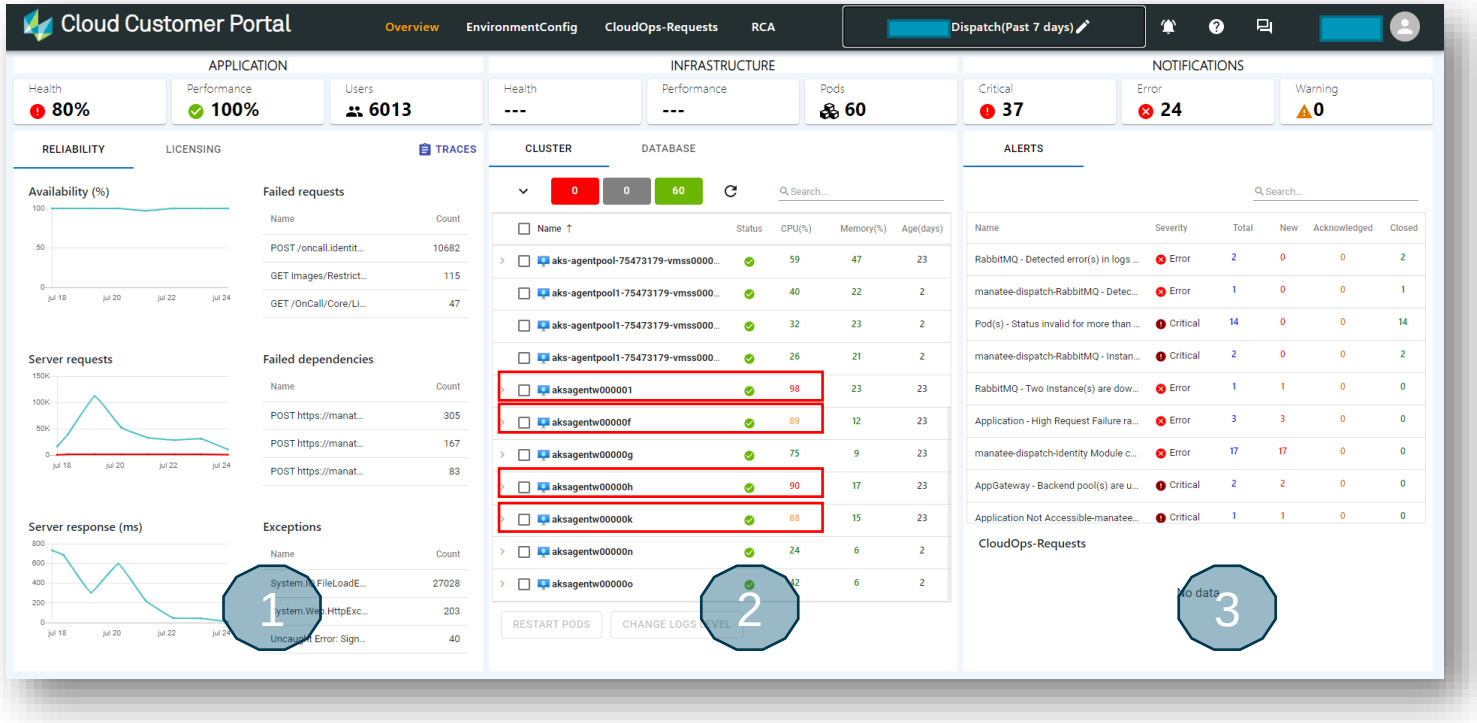
Internal Monitoring system

An internal monitoring dashboard is used for application, infra and alerts monitoring.

1. Application metrics such as Availability, Server requests, Server responses, failed requests, exceptions are monitored.

2. Infra metrics such as cluster details, node/pod status, cpu utilization, memory utilization, etc., are monitored.

3. Alerts fired and its details such as severity, state, etc., are monitored.



HEXAGON

Problem Statement

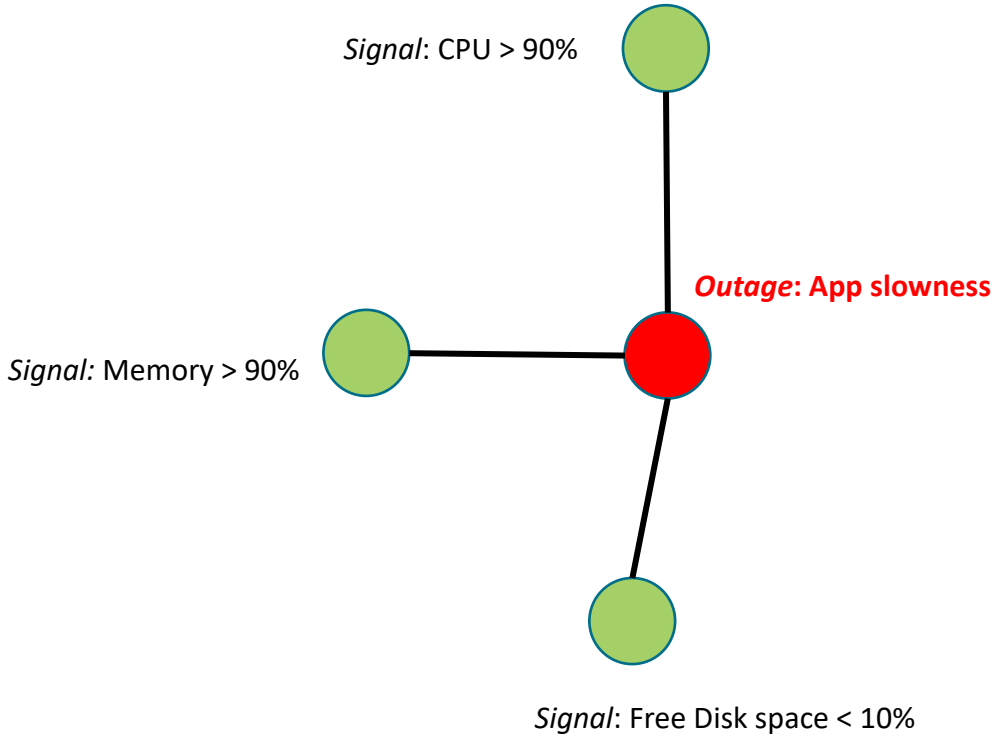
- Outages in cloud environment are very critical and could dramatically degrade system availability and impact user experience.
- Outages can happen due to one or combination of below components:
  - Infra
  - Application
  - Network
  - Security
  - Service
- Appropriate Alert mechanism in place to monitor the state and health of above components.
- Repeated occurrence of such alerts may lead to eventual outages at service/component level.
- Alerts are correlated and there exists a relationship.

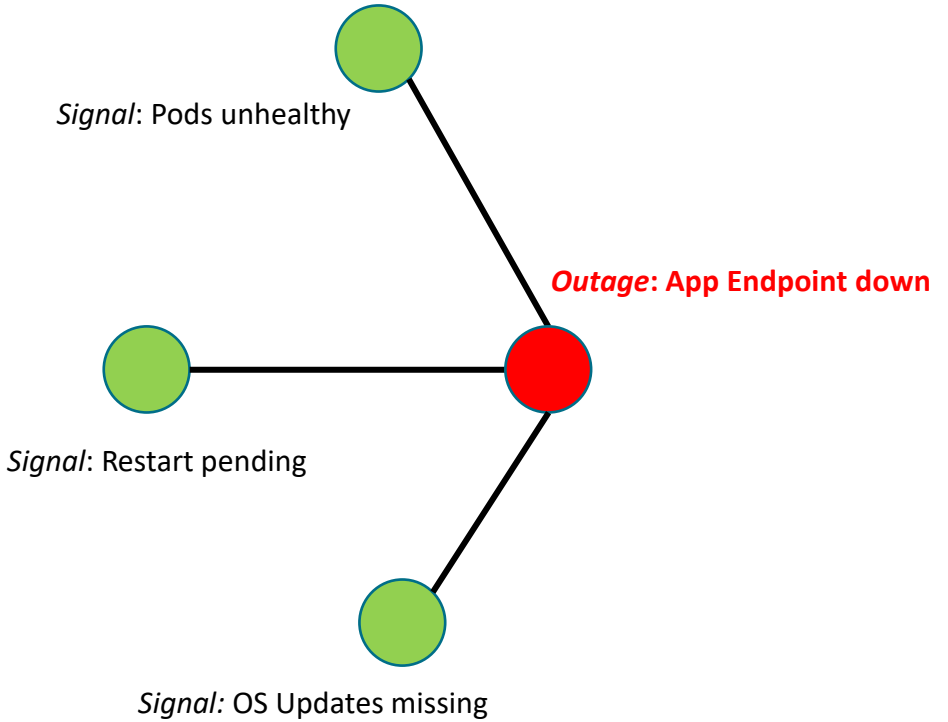
Symptom & Incident relationship

Time	CPU	Memory	Free Disk space	Missing Security & OS Updates	Restart Pending	Pods State	App Health	Type of Outage
D1	> 90%	< 90%	< 10%	Yes	No	Healthy	Good	APP NOT RESPONDING
D2	< 90%	> 90%	> 10%	No	No	UnHealthy	Bad	ENDPOINT NOT AVAILABLE
D3	< 90%	> 90%	> 10%	No	No	UnHealthy	Bad	EVENTS CREATED NOT SAVING TO DATABASE
D4	> 90%	> 90%	> 10%	Yes	No	Healthy	Good	USER NOT ABLE TO LOGIN
D5	> 90%	< 90%	> 10%	No	No	UnHealthy	Good	SLOWNESS
D6	< 90%	> 90%	> 10%	Yes	No	UnHealthy	Good	WAIT CURSOR
D7	> 90%	< 90%	> 10%	Yes	Yes	UnHealthy	Bad	SECURITY COMPROMISED

* Approx. ~20 parameters

Relationship between counters





HEXAGON

Expected Results

- An AI/ML model for anomaly detection and outage prediction.
- Predict whether a component or service will have an outage in near future.

Methodology – Initial thoughts

- Multi-variate Time series problem
- Essentially a classification problem
- Build multiple models using classical ML and DL techniques and compare them

Next Steps

- Conduct a session to students on use cases – Hexagon
- Literature survey – Hexagon/Students
- Provide test data – Hexagon
- Students to perform data exploration – Students
- Start positioning the viable approaches – Hexagon/Students

Thank You

HEXAGON