Are you being served: A Framework to manage Cloud outage repair times for Small Medium Enterprises.

Jonathan Dunne
Hamilton Institute
Maynooth University
Email: jonathan.dunne.2015@mumail.com

David Malone
Hamilton Institute
Maynooth University
Email: david.malone@nuim.ie

***Abstract*—Hosting software applications within a Cloud based infrastructure represents challenges for Small Medium Enterprises (SMEs), due to the variety of ways in which production outages can occur. We consider repair times for outage events in a framework where these downtimes are used to refocus Systems Operations resources. Using an enterprise dataset, we address the question of how outage events are distributed and what relationship these events have with different types of issues that can occur in a cloud data centre. The proposed framework can aid SMEs to maintain a highly available "On-Demand" service infrastructure, with limited resources.**

I. Introduction

SMEs have seen significant growth in recent years; a 71% increase in employment (excluding financial sector) was recorded in 2014. Moreover SMEs employed almost 90 million people [**?**] As the European economy continues to recover, both businesses and clients are looking for new avenues to drive growth across the EU as a whole.

One way to provide services with a high market reach is through Software as a service (SaaS) model. This cloud-based approach is seen as a shift away from highly complex bespoke solutions, to more focused and cost effective solutions [2]. As customers demand highly effective solutions to solve their business problems, a cloud platform model can help keep pace with these needs. A single delivery platform is used to host multiple software solutions and services.

However an SMEs will face a number of key challenges when embracing a cloud service model, especially in the area of availability and maintainability. Recent work as been conducted to outline these challenges, which include: outage frequency and duration. Almost all SMEs (93%) employ less than 10 people [3], therefore maintaining a reliable service represents their key priority.

In this paper we describe a framework, which the SME can use to best manage their limited pool of resources. The core idea of this framework is for cloud operations teams to focus areas with high outage times (typically areas with high human error) to reduce the overall time from outage to business as usual (BAU). This paper contains a study of software outage data from a large enterprise dataset. Through the study of this outage event data we show which types of outage events take the longest to resolve, why having standardised homogeneous data centres are key to reducing outage times, and how application types play a role in the duration of resolution of outages.

For Platform as a Service (PaaS) providers, where mutli-tennacy solutions are available, high-level outage data could be shared between organisations to triangulate cross application outage events.

The rest of the paper is structured in five Sections; Section II gives some description of study background and related works. Section III describes the enterprise dataset. Section IV discusses the analysis and method and it is followed by section V that explains the result. Finally, the conclusion and future work is described in Section VI.

II. Background and related research

A. *Software as a Service*

SaaS is defined as a delivery and licensing model in which software is used on a subscription basis (e.g. monthly, quarterly or yearly) and where applications or services are hosted centrally.

The key benefits for software vendors are the ability for software to be available on a continuous basis (on-demand) and for a single deployment pattern to be used. It?s this single deployment pattern that can great reduce times for code to be validated in pre-release testing. Additionally the centrally hosting also allows for rapid release of new features and updates through an automated deliver process [ref].

SaaS is now ubiquitous, while initially adopted by the large software vendors (e.g. Amazon, Apple, Google and Microsoft) many SMEs are now using the cloud as their delivery platform of choice [ref].

B. *Cloud Outages*

A cloud outage is the amount of time that a cloud service is unavailable to the customer. While the benefits of a cloud systems are well known, a key disadvantage is that when a cloud environment becomes unavailable in can take a significant amount of time to diagnose and resolve the problem.

TABLE I

Company	Outage Time	Outage Details
Verizon	40 hours	Scheduled maintenance to improve overall reliability.
Apple iCloud	12 hours	A DNS error meant that users were unable to make purchases.
Apple iCloud	7 hours	iCloud unavailable / poor performance affected 200 million users.
Windows Azure	2 hours	A network infrastructure outage resulted in loss of service for all central US users.
Starbucks	Unspecified	Scheduled maintenance resulted in the tilling system going off-line.

During this outage time the platform can be unavailable for all customers.

One of the first cloud outages to make the headlines in recent times was the Amazon outage in April 2011. In summary the amazon cloud experienced an outage that lasted 47 hours, the root cause of the issue was a configuration change as part of a network upgrade. While this issue would be damaging enough for Amazon alone, a number of consumers of Amazon's cloud platform (Reddit, Foresquare) also suffered the same downtime. [Ref]

While great improvements have been made in relation to redundancy, disaster recovery and the ring fencing of key critical services, the big players in cloud commuting not immune to some form of outage. As of mid 2015 a number of high profile outages were catalogued by CRN website. [Ref] A summary table is included below:

C. *Other related studies*

A number of studies have been conducted in relation to cloud outages and the time observed to resolve problems in repairable systems.

Yuan et al. [?] performed a comprehensive study of distributed system failures. Their study found that almost all failures could be reproduced on reduced node architecture and that performing tests on the error handling code could have prevented the majority of failures. They conclude their study by discussing the efficacy of their own static code check as a way to easily check error-handling routines.

Hagen et al. [?] conducted a study into the root cause of the Amazon cloud outage on April 21st 2011. They found that an IT change to route traffic from one router to another while a network upgrade was conducted. The backup router did not have sufficient capacity to handle the required load. They developed a verification technique to detect change conflicts and safety constraints, within a network infrastructure prior to execution.

Li et al [?] conducted a systematic survey of public Cloud outage events. Their findings generated a lessons learned framework, which classified outage root causes. Of the seventy-eight outage events surveyed they found that the most common causes for outages included: System issues i.e. (human error, contention, software defects) and power outages being the primary root cause.

Kleyner and O'Connor [?] propose an important thesis regarding reliability engineering. While emphasis is placed on measuring reliability for both mechanical and electrical/electronic systems, the authors do broaden their scope to discuss reliability of computer software. One aspect of interest is their discussion of the log normal distribution and its application in modelling for system reliability with wear out characteristics and for modelling the repair times of a maintained systems.

Almog [?] analysed repair data from twenty maintainable electronic systems to validate whether either lognormal or exponential distribution would be a suitable candidate distribution to model repair times. His results showed that in 67% of datasets the log normal distribution was a suitable fit, while the exponential was unsuitable in 62% all of datasets.

Carcary et al. [?] conducted a study into Cloud Computing adoption by Irish SMEs. The key findings of the study were as follows: Almost half the ninety-five SMEs surveyed had not migrated their services to a cloud platform. Of those SME?s that had migrated they had not assessed their readiness to adopt cloud computing. Finally the study noted that the main constraints for SME Cloud computing adoption were: Security / compliance concerns, lack of IT skills and Data ownership and protection concerns.

III. Data set

Defect studies have been shown to provide an effective way to highlight customer usage patterns of software. Defect studies can also aid businesses align their test coverage more towards customer based use cases.

The study presented in this paper examines approximately 1400 field defects from a large enterprise, cloud based system. The data was collected over a 12-month period (Jan - Dec) and is comprised of four main components: E-mail, Collaboration, Social and Business Support System (BSS). The systems have been deployed within three data centres and are used by customers globally. The software is developed in Java and runs on Linux. Product development follows a CD model whereby small amounts of functionality are released to the public on a monthly basis. For each defect we have access to the full defect report, but we particularly focus on the defect impact, defect component, data centre location and defect type. The following terminology will now be defined to provide clear context. These definitions are given in the glossary of IEEE Standards Collection in Software Engineering [?].

IV. Data set

Cloud outage studies have been shown to provide an effective way to highlight the distribution of failure events. These studies can be leveraged by enterprises to pre-empt common failure patterns.

The study presented in this paper examines approximately 250 field outage events from a large cloud based system. The data was collected over a 12-month period (Jan - Dec) and is comprised of four main components: E-mail, Collaboration, Social and Business Support System (BSS). Additionally the failure events have been categorised into the following main categories: Configuration error, Hardware failure, Network and Software defect. The systems have been deployed within three data centres and are used by customers globally. The software is developed in Java and runs on Linux. Product development follows a Continuous delivery (CD) model whereby small amounts of functionality are released to the public on a monthly basis. For each outage event we have access to the full outage report, but we particularly focus on the time taken to resolve the outage with additional focus on the software component and the type of error, which was the root cause of the outage. The following terminology will now be defined to provide clear context. These definitions are given in the glossary of IEEE Standards Collection in Software Engineering [**?**].

- Outage Event:
- Maintenance window:
- Detection Time (DT):
- Resolution time (RT):

This study aims to answer a number of questions. First, How are the times of cloud outage events distributed? Second, does the distribution vary by component? Third, does the distribution differ by failure category? Fourth, does the relationship differ by data centre? Finally what is the relationship between time to detection and time to resolution? In order to answer these four questions, this study is broken down into the following attributes: outage distribution, outage component, outage failure category, data centre location and DT Vs RT.

A. Outage Distribution

Probability distributions are used in statistics to assign a probability or likelihood of an event-taking place. In the case of cloud outage events, by analysing the distribution of all events, it may be possible to fit a known distribution to our dataset. If a distribution can be fitted these distribution properties can be used to infer the most likely outcome of an outage event. For example a probability distribution could be used to infer the likelihood of an outage event taking a specific period of time to resolve. Outages distributions are plotted at an overall, component and type level.For validation of a suitable distribution type we used the R library ADGofTest [**?**]

B. Outage Component

Recognising the location of an outage event at a component level gives an understanding of a) which components are more likely to contribute to an outage event and b) the relative duration to detect and resolve an outage with respect to a component. For example operations teams may have various probes to determine if an event is likely to cause a failure. Development and test teams may have a suite of test cases to find a certain class of issue. Outage events can provide operations teams with an understanding of potential gaps in their probes and monitoring solutions. Likewise for development and test teams outage events can provide both teams with either weaknesses in feature implementation and gaps in test coverage. Depending on the nature of these test gaps and the size of the test organisation, they may be difficult to close. For this study we categorised our software components as follows: BSS, collaboration, e-mail and social.

A Hardware failure relates to a class of problem, which causes a piece of hardware to fail. These failures relate to a malfunction within the electronic circuits or electromechanical components (disks, tapes) of a computer system. Recovery from a hardware failure requires repair or replacement of the offending part.

A network error relates to a class of failure outside of misconfiguration or a hardware failure within the network infrastructure. Network failures can typically present themselves as intermittent temporal network outages, high latency / packet loss conditions or congestion based on overloading of available bandwidth. As cloud data centres contain a number of distributed systems, having a reliable network infrastructure is highly desirable.

A software defect refers to a class of issue, which is triggered through normal operations on the underlying server component code by the customer. These issues are triggered due to the inability of the code to handle either concurrent or parallel usage. Software defects may include issues related to contention under load (e.g. memory leaks, high Disk I/O, CPU usage), concurrency (e.g. deadlocks) or miscellaneous error conditions.

C. Data Centre Location

Understanding the measure of outage events at a data centre level can highlight whether a specific data centre is a factor in the duration and distribution of outage events raised. There are three data centres in our dataset: data centre A (High usage), data centre B (Low usage) and data centre C (Medium usage). Having a correlation between outage duration can be a useful data point for cloud operations teams.

D. Detection time Vs Resolution time

Examining the ratio between the times taken to detect an outage compared to the time taken to resolve an outage is important. Studying detection times can highlight whether firstly an operations team has sufficient monitoring capabilities and/or whether the server side components produces sufficient error events to service the problem. Additionally studying resolution times can provide insight into whether staffing and/or crisis operations processes are sufficient in the case of multiple concurrent outage events.

E. Limitations of dataset

The Dataset has a number of practical limitations, which are now discussed. While the outage event tracking system allows for a granular categorisation system, whereby outages can be mapped to a subcomponent, there are a number of outages, which due to their severe nature can affect more

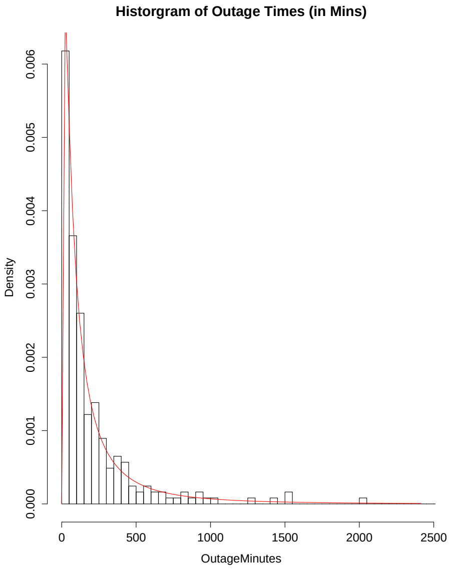

Fig. 1. Histogram of Outage Times (In Minutes) with fitted Log Normal Curve

TABLE II

Statistic	Value
Samples	246
Mean	314.14
Std Dev	1414.43
Median	105
Skew	13.80
Distribution	Log Normal
AD GoF Test (p)	0.95

than one component and subsystem. The authors reviewed the functional location of each defect to ensure precision across the analysis of the dataset.

The outage events that form part of this study are from an enterprise cloud system. The outage events are applicable to the software domain of BSS, Collaboration, Email and Social. Additionally the outage events are applicable to the field of hardware failure, software defect, Network errors and misconfiguration of server components.

V. Results

We now explore the attributes of field defects observed.

A. Outage Distribution

Fig. 1 shows a probability density function curve for all 246 outage events with a fitted Log Normal curve. TABLE II lists the summary statistics of the dataset. The mean time is approximately 314 minutes in duration. The dataset has a high degree of skew with 13.80. An Anderson-Darling Goodness of fit test was also computed to determine which distribution was most appropriate. Using the R library ”ADGofTest” [ref], a log normal distribution was the best fit with an Anderson-Darling p-value of 0.95.

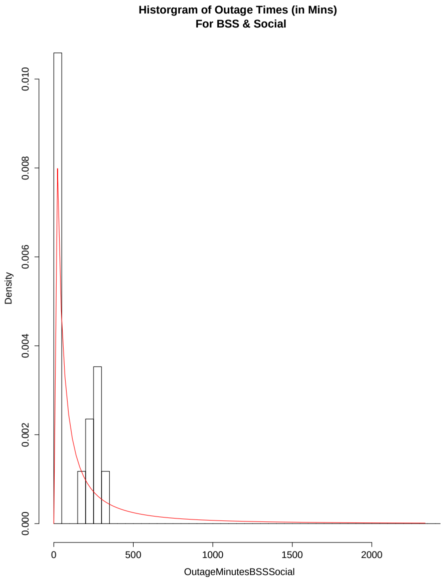

Fig. 2. Histogram of BSS-Social Times (In Minutes) with fitted Log Normal Curve

TABLE III

Statistic	BSS-Social	Collaboration	Email	Mixed
Samples	16	34	152	43
% Samples	(7)	(14)	(62)	(17)
Mean	274.23	189	258.10	626.95
Std Dev	639.44	379.33	423.27	3260.78
Median	45	61.5	126.5	85
Skew	3.56	3.83	5.45	6.30
Distribution	Log Normal	Log Normal	Log Normal	Log Normal
AD GoF (p)	0.69	0.62	0.99	0.64

B. Outage Component

Fig. 2, 3 & 4 and show the probability density function curves for outage events by component with a fitted Log Normal curve. These four categories total the full 246 outages. Due to the low number of samples (17) for the BSS & Social category, the goodness of fit value should be treated with caution.

In each of the component categories, there is a degree of variability in relation to the mean outage times. Table III lists the summary statistics of outage events broken down by Component. E-Mail recorded the highest number of outages with 62% of all outages, while Mixed, Collaboration and BSS-Social recorded 17%, 14% and 7% respectively.

C. Outage Type

Fig. 6 - 10 and show the probability density function curves for outage events by type with a fitted Log Normal curve. These five categories total the full 246-outage events. Due to the low number of samples (23) for the Hardware-Other category, the goodness of fit value should be treated with caution.

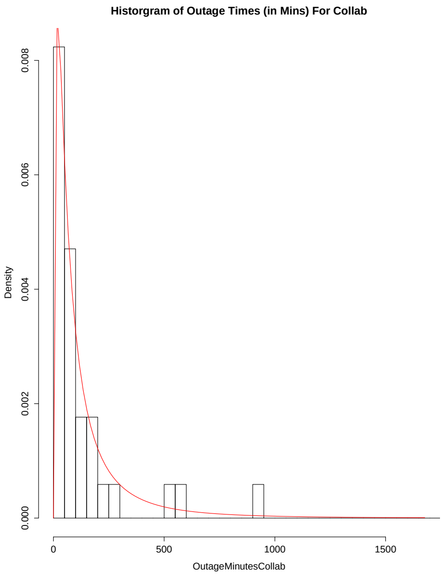

Fig. 3. Histogram of Collaboration Times (In Minutes) with fitted Log Normal Curve

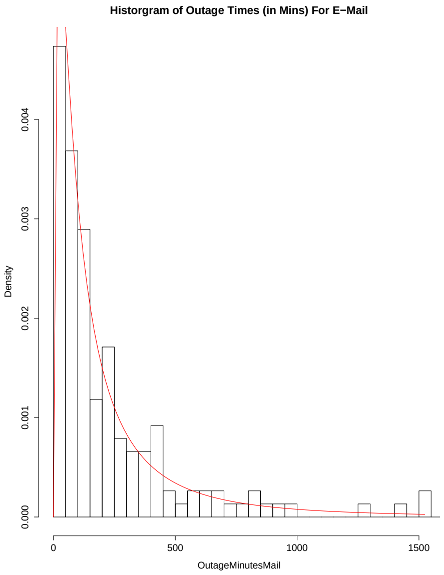

Fig. 4. Histogram of E-Mail Outage Times (In Minutes) with fitted Log Normal Curve

In each of the type categories, there is a degree of variability in the mean outage times. Table IV lists the summary statistics of outage events broken down by type. Configuration-Manual and Contention-Concurrency recorded the highest number of outages with 30% and 26% respectively. Network, Disaster Recovery and Hardware-Other categories recorded 20%, 15% and 9% respectively.

D. Data Centre Location

Fig. 12, 13 and 14 show the probability density function curves for outage events by data centre with a fitted Log

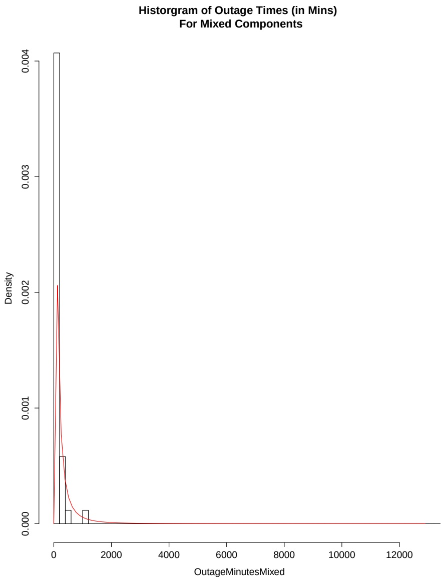

Fig. 5. Histogram of Mixed Outage Times (In Minutes) with fitted Log Normal Curve

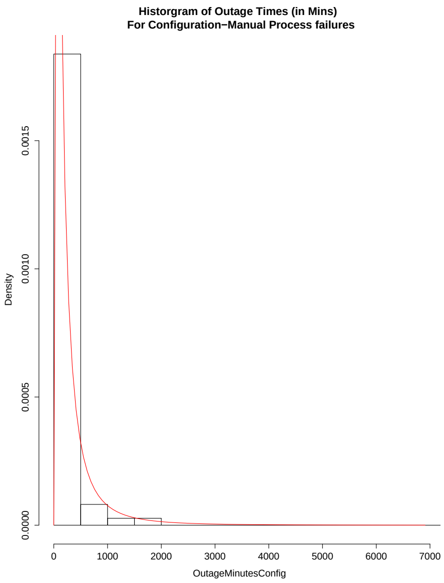

Fig. 6. Histogram of Configuration-Manual Outage Times (In Minutes) with fitted Log Normal Curve

TABLE IV

Statistic	Configuration -Manual	Contention -Concurrency	Disaster Recovery	Network	Hardw -Othe
# Samples	74	64	36	49	23
% Samples	30	26	15	20	9
Mean	488.61	238.78	134.03	314.59	243.4
Std Dev	2488.21	468.62	160.72	590.74	357.5
Median	114.5	86	72	145	91
Skew	8.28	3.69	2.33	5.30	2.11
Distribution	Log Normal	Log Normal	Log Normal	Log Normal	Log No
AD GoF (p)	0.91	0.97	0.94	0.75	0.96

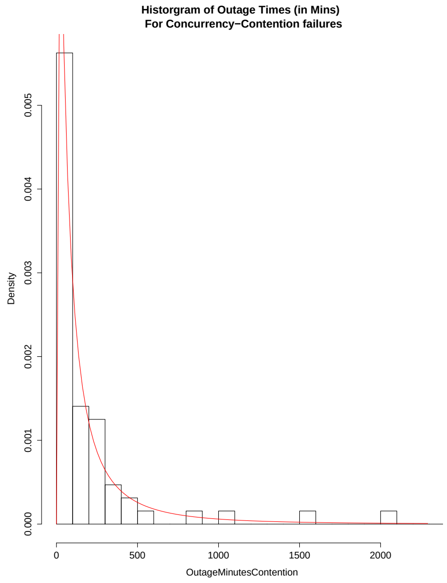

Fig. 7. Histogram of Contention-Concurrency Outage Times (In Minutes) with fitted Log Normal Curve

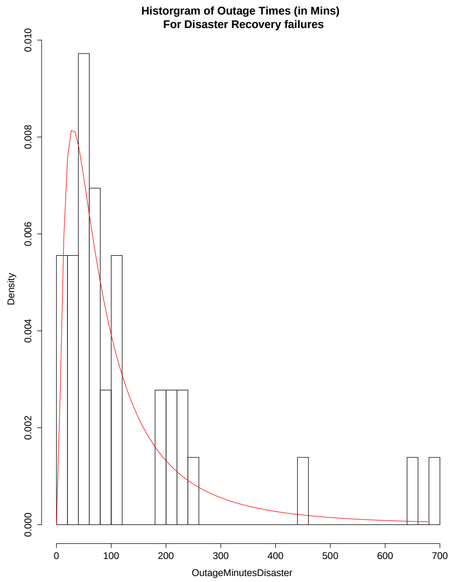

Fig. 8. Histogram of Disaster Recovery Outage Times (In Minutes) with fitted Log Normal Curve

Normal curve. These three categories total 238 events. A further 8 outages were found in all three data centres, however due to the low number of samples detailed analysis was not performed. Furthermore the researches felt it in was inappropriate to merge these eight samples into one of the existing data centre pools.

In each data centre there is variability in the mean outage times. Previously it was noted that Data Centre A, B and C are high, medium and low use respectively. Given the level of outage events in each data centre, the logical concept that higher usage results in more outages. However from the data set below this is the case for Data centre A, however Data centre C had more than double the outages than Data Centre B.

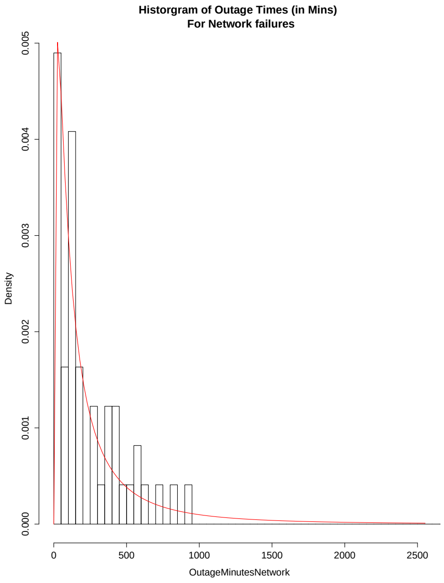

Fig. 9. Histogram of Network Outage Times (In Minutes) with fitted Log Normal Curve

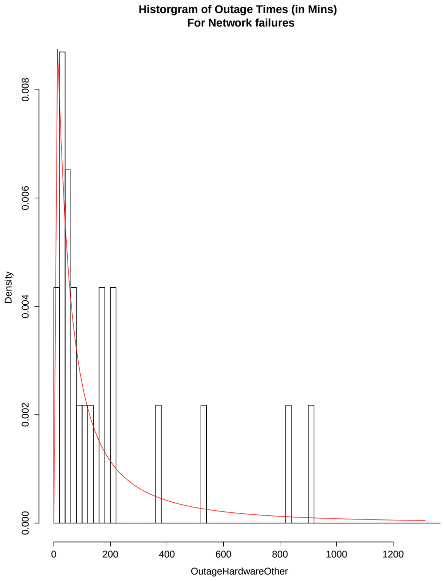

Fig. 10. Histogram of Hardware-Other Outage Times (In Minutes) with fitted Log Normal Curve

Table V lists the summary statistics of outage events broken down by data centre. Data Centre A recorded the highest number of outages with 65% of all outages, while Data centre B and C recording 10% and 22% respectively. The remaining 3% were from outages found in all thee data centres.

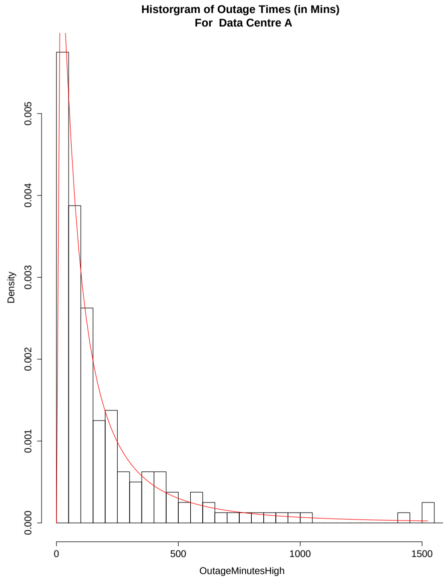

Fig. 11. Histogram of Data Centre A Outage Times (In Minutes) with fitted Log Normal Curve

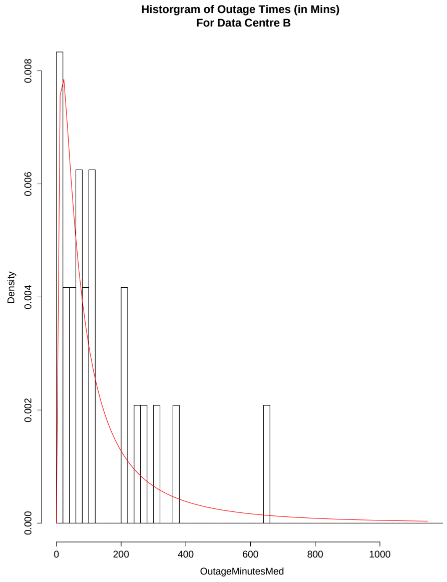

Fig. 12. Histogram of Data Centre B Outage Times (In Minutes) with fitted Log Normal Curve

TABLE V

Statistic	Data Centre A	Data Centre B	Data Centre C
Samples	160	24	54
% Samples	65	10	22
Mean	224.43	187.67	645.39
Std Dev	312.83	279.97	2961.09
Median	113.5	89.5	79.5
Skew	2.93	2.89	6.67
Distribution	Log Normal	Log Normal	Log Normal
AD GoF (p)	0.99	0.99	0.31

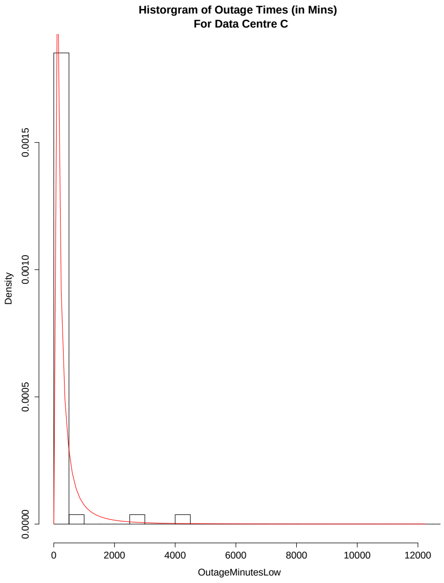

Fig. 13. Histogram of Data Centre C Outage Times (In Minutes) with fitted Log Normal Curve

VI. Discussion

Section IV provided an outline of outage events that were studied as part of our overall dataset, including distribution, component, type, data centre location and a comparison between detection time and resolution time. The following section provides deeper analysis of the results. In each section references will be made to each research question asked in section III.

A. Outage Distribution

To answer the question how are the times of cloud outage events distributed, Fig. 1 and TABLE II clearly show that the distribution type is Log Normal. Of interest is the quality of the fit. An Anderson Darling goodness of fit test was conducted and a p value was found to be 0.947 with a test statistic of 0.287. In this case the hypothesis of whether the outage times are Log normally distributed cannot be rejected given the overwhelming evidence to the contrary.

It is also worth noting that the mean outage time is approximately 314 minutes, which indicates that resolution of an outage in complex system architecture is a non-trivial task. Additionally with a standard deviation found to be approximately 1414 minutes and a skew value of 13.80, clearly indicated that there is a high level of dispersion within the dataset.

Given the nature of cloud computing new code updates and configuration changes are made on a regular basis. It is not uncommon for an enterprise to introduce changes or a monthly or bi-weekly basis. Therefore with this high level of system activity it is not unsurprising that outages can occur when least expected. If a state of the art outage tracking system were introduced, it would be interesting to determine as overall both process improvements were made coupled with underlying code stability to observe the overall affect on both the distribution type and shape. This would provide a concrete answer to questions such as: what impact do specific process improvements make to overall outage times? As a business where do resources need to be deployed to improve platform stability - Development, Operations or Quality Assurance?

B. Outage Component

Examining outages by component can given insight as to which component are likely to exhibit outages and whether these times vary by component.

Fig. 2 to 5 and TABLE III highlight that there is indeed variability in mean outages times across the components measured. Mixed components had the highest mean time with 626.95 minutes, followed by BSS-Social, Mail with 274.23 & 258.10 respectively and finally Collaboration with 189 minutes. Indeed Mixed components also had the highest standard deviation and skew. This indicated firstly that mixed component outages take longer to resolve than single component issues, which makes sense given the level of remediation required. However in terms of overall outages the level of mixed component outages was 17% of the overall total. It is also worth noting the number of outages in the e-mail category with 59% is by far the highest contributor by component, yet the expected outage time is 258.10 minutes. From closer inspection, the mean outage times for mixed component are due to a number of outages with high durations.

In all cases, each component class had a good fit to a Log Normal distribution, with the e-mail category fitting best with a p value of 0.995. However with a low sample count the goodness of fit values for the BSS-Social category should be treated with some caution.

Based on these results there are two areas of focus: first the quantities of outages related to the e-mail component and second the outage times to the mixed component outages. Tiger teams [ref] could be engaged to understand the root cause of both sets of issues. With knowledge gained through investigative techniques process improvements can be introduced which will allow deployment of crisis situation teams to other parts of the infrastructure.

C. Outage Type

Examining outages by type gives and deeper understanding of what types of problems are likely to cause an outage within a cloud infrastructure. Fig 6 ? 10 and TABLE IV provide this insight.

Configuration-Manual and Contention-Concurrency had the highest proportion of outages found with 30% and 36% respectively. While Network, Disaster Recovery and Hardware other had 20%, 15% and 9% respectively. Significantly Configuration-Manual had the highest expected outage time with 488.61 minutes, with Network next highest with 314.59 minutes. Contention-Concurrency, Hardware and Disaster recovery had expected outages times of 238.78, 243.44 and 134.03 respectively. Finally the outage times of each category were fitted with a Log Normal distribution. In each case the hypothesis of whether a Log Normal distribution was a suitable distribution could not be rejected. However one caveat is that the Hardware-Other category had a low number of samples, so this result must be treated with caution.

Based on the above findings it is clear that issues related to Configuration-Manual contribute most to the overall number of outages but also take the longest to resolve. Given the relative complexity of the overall cloud architecture it is apparent that a system of managed configuration changes is require. Firstly to ensure there is an audit trail of all changes made but secondly to ensure a level of pre-validation is done to ensure that harmful (extreme) values are rejected. Additionally tiger teams should also implement a system, which can monitor real-time configuration changes across the plurality of data centres.

With any distributed system the network health plays an important role in system stability, while a data. Our network issues fell into two main categories: network congestion and temporal network outages. For congestion issues, business and operations teams need to define clear bandwidth capacity requirements to ensure that their infrastructure had the bandwidth to meet the demands of the existing user base and future subscription signings. Finally the underlying application and middleware stack should have additional resiliency added to ensure that temporal outages do not cause cascade failures, which can cause a single or multiple components to become unavailable once the network path has been restored.

D. Data Centre Location

Fig. 11 - 13 and TABLE V give insight into the outages by data centre. Discussed previously in section III, user concurrency varies by data centre. Data centre A (High Usage) had the highest number of outages with 65% while Data centre B (Medium Usage) and Data centre C (Low Usage) had 10% and 22% respectively. A remaining 3% of issues affected two or more data centres. Data Centre C had the highest mean outage time with 645.39 minutes, while data centre A & B had mean outages times of 224.43 and 187.67 respectively. All three data centre outage times were modelled with a Log Normal distribution and both data centre A & B were excellent fits with p values of 0.995 and 0.986 respectively. Data centre C faired worst in terms of fit with a p value of 0.316. Even with this value the hypothesis of whether a log normal distribution is a suitable fit cannot be rejected.

In some ways the above results are expected, it seems reasonably logical that a high use data centre would have the most outages logged due to the high level of activity, however even with all these outages the mean outage time is 224.43 minutes, which is approximately 90 minutes less than the overall mean. What appears somewhat counter intuitive is that data centre c has the second highest number of outages and the highest mean outage time. From closer inspection the mean outage times of data centre c are due to a number of outages with high durations.

In the context of software delivery to multiple data centres, the same code is release to each system. Clearly customers are impacted in different ways depending on which data centre is used. With this knowledge tiger teams can investigate in two areas. Firstly does the underlying customer use case of each data centre vary? Secondly a root and branch investigation of each data centre configuration should be conducted and compared for discrepancies, with specific focus on the e-mail component configuration.

E. Detection time Vs Resolution time

We outlined in section III that the overall outage time is divided further into two discrete units: The detection and resolution time. We discussed previously that a number of entries were removed from our analysis due to the having a value of 0. In the case of a 0 minute detection time, upon closer inspection these failures were flagged by internal operations teams, which in effect meant the time between first failure and resolution work, was immediate. In the case of a 0 minute resolution time, against these relate to issues that were raised internally. Operations times were working in parallel to upgrade a piece of infrastructure to prevent an failure, therefore when the failure event was flagged the new piece of infrastructure was in place to remediate the original issue when mean an immediate resolution due to the pre-emptive work.

Comparing the measures of location of both sets of untransformed data is readily apparent that it takes over twice as long for operations teams to become aware of a failure event than it does to resolve the problem once the failure is known. Additionally the dispersion within the detection times is high, a skew of 13.57 was computed. This may point to the quality of real-time monitoring solutions to detect failure events not only in the application and middle stack but also in the underlying data centre configuration and underlying network. Enhancing real-time anomaly detection may help reduce the detection time. We noted previously that e-mail, configuration-manual, and data centre a outages scored highest in each category. It is logical to assume that the operations and critical situation teams are engaged in resolving these issues over other types. By triangulation of outages on these three axes we now have a targets model for tiger teams to reduce repair time outcomes.

Finally it is worth commenting on the distribution type for both units. Fig. 14 and 15 show the distribution curves for both. In the case of resolution time a lognormal curve was fitted and goodness of fit was value was computed to be 0.5. In this case the assumption of log normal distribution for resolution times cannot be rejected. This finding complements existing work related to the usefulness of the log normal distribution to model repair times of maintainable systems. In the case of detection time a lognormal curve was fitted however a goodness of fit test was conducted and a p-value of 0.01 was computed. In this case there was moderate evidence against the use of log normal to model detection times. Given the level of skew within the detection time data a log transformation was applied. Subsequently a log normal distributed was fitted and a goodness of fit test conducted. A p-value was calculated to be 0.46. . In this case the assumption of log normal distribution for log transformed detection times cannot be rejected. While detection times are a function of the overall outage time, this finding suggests that detection times themselves have wider spread of values than resolution times and should be treated a special case in itself.

VII. Conclusion

Previous studies have shown that shown that Cloud Outages are an infrequent occurrence. Additionally that the Log normal distribution is a useful tool for modelling repair times in mechanical and electronic maintainable systems.

The purpose of this study was to examine the duration of outage events within a Cloud based application platform. It was found that the log normal distribution is a useful model for modelling repair times for SaaS applications. The findings of this study support previous studies particularly in the area of system reliability and repair times.

This work provides a more comprehensive study in relation to how outage times can vary between the types of outage, the component involved and the data centre in use at the time of outage.

In future SMEs can assess their outage data to understand the core issues that effect their underlying service platform. A specific operations framework can then be developed to allow the SME to focus on specific parts of their architecture or business process, which impede high value growth. Likewise usage of framework on an iterative basis can be used to by SMEs to set achieve realistic remediation targets.

In future work we shall assess our framework in conjunction with the time between outage events to understand how best operations teams can be deployed where parallel outage events occur.