How to achieve “100%” availability
Problem statement

We want to be able to explain in a simple, but effective way, that “100% availability” is **not** what we need nor want.
When Life Gives you Lemons, make a LaaS – Lemonade as a Service

• I know everybody craves lemonade all the time!
• So let’s think big and offer it as a service
• Apply some principles of Cloud Services to it
• Skip some of the boring Business plan items and get to the core!
Mini Market Analysis

Competition
- As of today, nobody offers a 24/7 lemonade stand service
- We are creating a new demand and the market to satisfy this craving

Our studies show that 100% of the time:
- Customers want to have 100% organic fresh lemons
- Customers want to have their lemonade served in <60 seconds
- Customers want Lemonade with a temperature between 4° C and 5° C
- Customers want to buy Lemonade at any time and in any day
- Customers want a 0.4l serving size
- Customers are willing to pay up to € 2.50 for a cup of lemonade
Secret Lemonade Recipe (2.5 l)

- Juice of 1 kg organic lemons
- 250 g cane sugar
- 2 l water
- Ice cubes

<table>
<thead>
<tr>
<th>Costs per Serving</th>
<th>Price per unit</th>
<th>Unit</th>
<th>2500ml juice</th>
<th>400 ml</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lemons</td>
<td>4.16</td>
<td>1</td>
<td>4.16</td>
<td>€ 0.67</td>
</tr>
<tr>
<td>Sugar</td>
<td>0.2</td>
<td>0.25</td>
<td>0.05</td>
<td>€ 0.01</td>
</tr>
<tr>
<td>Water</td>
<td>0.02</td>
<td>2</td>
<td>0.04</td>
<td>€ 0.01</td>
</tr>
<tr>
<td>Cups</td>
<td>0.1</td>
<td>1</td>
<td>-</td>
<td>€ 0.10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td><strong>4.25</strong></td>
<td><strong>€ 0.79</strong></td>
</tr>
</tbody>
</table>
### Other Costs

<table>
<thead>
<tr>
<th>Item</th>
<th>cost per unit</th>
<th>Unit</th>
<th>cost per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electricity</td>
<td>250</td>
<td>1</td>
<td>€250.00</td>
</tr>
<tr>
<td>Permit</td>
<td>50</td>
<td>1</td>
<td>€50.00</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td><strong>€300.00</strong></td>
</tr>
</tbody>
</table>

### Monthly Costs

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost per Unit</th>
<th>lifetime</th>
<th>cost per month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juicing Machine</td>
<td>100</td>
<td>36</td>
<td>€2.78</td>
</tr>
<tr>
<td>Nice Stand</td>
<td>1000</td>
<td>36</td>
<td>€27.78</td>
</tr>
<tr>
<td>Ice Cube Machine</td>
<td>350</td>
<td>36</td>
<td>€9.72</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1450</td>
<td></td>
<td><strong>€40.28</strong></td>
</tr>
</tbody>
</table>
Break-even points

- Stand can sell 1000 lemonades per day

<table>
<thead>
<tr>
<th>Fix costs per month</th>
<th>Variable costs</th>
<th>1000</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>€ 340.28</td>
<td>€ 1,130.28</td>
<td>€ 1.13</td>
</tr>
</tbody>
</table>

- We sell for € 2.50, and our monthly profits are € 1,369.72!
We need to hire people!

- An employee makes €10 per hour.
- We need to hire multiple shifts to cover 24/7.
- This adds $24 \times €10 = €240$ (€7200 per month).
- Our break-even point moves up to €8.33.
- But customers won’t pay that much… We are now making losses.
We start our business!

- There is a huge demand!
- People are forming lines at peak times to get our lemonade!!!!!
- But we are losing money!
Is huge demand a good problem to have?

- We are missing our “Time to get Lemonade” target of < 60 secs at peak times
- We are hitting our stand capacity
Elastic-like scaling!

- To reach capacity we need to operate:
  - 3 stands at peak times (6 hours)
  - 2 stands at normal times (6 hours)
  - 1 stand for low times (12 hours)
Rise of the Machines

- A fully automatic lemonade machine costs $25k and can serve up to 3000 servings per day
- We don’t need a stand
- We don’t need people to sell lemonade

HAL 3000
(Herman, the Automaton for Lemonades)
Machines break!

- HAL offers a no-headaches maintenance plan for “just” €500 per month, but we also need to overcome the downtime
- We need a spare HAL 3000 + maintenance plan
- We also need to account for when one machine is broken and one needs to be refilled with ingredients
- We go for n+2!
• Brrr! It is getting cold: HAL is frozen

• Operation temperatures for HAL are just between 5°C and 30°C

• We need something like a garden shed that is warm in the winter and cool in the summer

• Costs €2000 (lifespan = 10 years)
Blizzard!!!

- Huge Power Outage
- Add a generator for up to 4 hours outage!
- What about a week? Or longer?
- Adding some solar panels and batteries to our shed
Floods from the melting snow!

- Due to the floods public water is unsuitable for consumption 😞
- We need a water purification system for €2500 (1Y depreciation)
After the rain comes the sun again!

- There is a drought! No water is coming out of the tap!
- We need an alternative water supply
  - Mineral water shipments (€ 0.30 per liter) → € 2.51
  - Building well (€5000, 15 year depreciation) → € 2.45
• The droughts are leading to fires and it is killing the lemon trees!
• Kg price went up to € 20 → € 4.98
What’s the next disaster?

· Volcanos? Tornados? Earthquakes?

· How much more do we want to spend to sell lemonades for € 2.50?
How much availability/reliability do we need?

- As much as customers are willing to pay for
- As much as it makes sense without making the costs explode
Lightning Talks

SREcon19 Dublin
Understanding vicious cycles with Causal Loop Diagrams

Laura Nolan, Slack Technologies
My Little Distributed Filesystem

replicaChecker()

while true {

    for each block in filesystem.GetAllBlocks() {

        if block.replicasHeartbeatedOK() < minReplicas {

            block.StartCopyNewReplica()

        }

    }

}
My Little Distributed Filesystem

for each block in filesystem.GetAllBlocks() {
    if block.replicasHeartbeatedOK() < minReplicas {
        block.StartCopyNewReplica()
    }
}
REREPPLICATING ALL YOUR UNDER-REPLICATED BLOCKS

OH, YOU STILL WANTED TO BE ABLE TO CONNECT TO THOSE MACHINES?
That’s an example of a vicious cycle.
Enter the causal loop diagram.
Replication

Failed heartbeats

System load
Replication

Failed heartbeats

System load

+ + + +
Replication System load

Failed heartbeats

Write load

Replicas per block

Hardware and power failure

System load

Read load

DELAY
- **Replication**
  - **System load**
  - **Replicas per block**
  - **Write load**
  - **Read load**
  - **Failed heartbeats**
  - **Hardware and power failure**

- **REPRESENTATIONS**
  - **DELAY**

- **CONNECTORS**
  - **R**
Replication

System load

Failed heartbeats

Write load

Replicas per block

Hardware and power failure

Delay

Read load

System load

Delay
So, you want to be a wizard?
Figure 1-3  Causal-loop diagram of several important feedback loops in World3
@lauralifts on Twitter.

Slack is hiring!
Find me in the hallway.
Lightning Talks

SREcon19 Dublin
Flame Graphs
A meeting point between developers and SRE

Doron Sekler & Amir Langer
I’m a developer

And as such I know my code. I also test it.
So before it reaches production I am pretty certain it is perfect.
I’m an SRE

I am responsible for reliability, availability and performance of production services. I triage performance problems and can see that we have a performance issue.
But

Look at the results of my performance tests. I can prove to you that whatever you're seeing is not my service.

Have you checked the network latency?
My metrics

Suggest it is not the network latency. It's your service that can't cope in production for whatever reason.
Sigh...

At eBay we have various production metrics that developers never encounter in their environments. They also approach us SREs with a production issue but do not know (or reveal) why it is happening.
To solve performance issues both SREs and developers need to see the same view. This view needs to be both global and also be able to drill down to the single line of code that’s at the heart of the problem.
Flamegraphs

Are a visualization of profiled software, allowing the most frequent code-paths to be identified quickly and accurately.

It shows the results of sampling profiling, on CPU, memory allocation... any data that has a code path associated with it.
In a single image

We can see all the code paths as flames. The total time of each frame is its width.
The self time is the delta between the frames (a.k.a. its edge).
We can see how we arrived to the frame and where do we go from it.
Colour

scheme shows us the type of code in that frame. In this example green is java code, yellow is JVM C++ code, orange is kernel code, red is the rest of JVM code. Other types of processes have their own colour schemes.
Our experience shows that using flamegraphs is a good common ground that allows both SRE and developers to cooperate, reason about and solve production performance problems.

Flame Graph
Real life examples

In this Java process it only took a quick look to deduce we have a serious GC problem. Unlike other visualizations, Flamegraph can show everything that happens on the CPU in this process and it is obvious half of the CPU time is spent on garbage collection.
Real life examples

And after JVM GC tuning we can see the difference.
Real life examples

Here we could prove to developers that production data meant the process worked much harder than anticipated on queries to an embedded Solr index.

You can dig into the code paths by searching a regex and the results are painted here in purple.
Real life examples

In this service we noticed that most CPU time was spent doing Unsafe.park i.e. parking the thread. It came from an open source ring buffer library (Disruptor). This behaviour indicated that the internal ring buffer was full most of the time and the publisher had to wait for it to drain.
Real life examples

Flamegraphs also tells us a lot about how the code runs even if we’re not familiar with it beforehand.

Here’s a picture of recursion.
Real life examples

We can also see the effects of the JIT compiler on a service startup by seeing how much CPU is used by the JVM compiler threads.
Automation and Streamlining

We built a project that allows everyone, SRE and developers to generate on-demand Flamegraphs from any production host.

We’re currently working on
- having a constant stream of flamegraphs (and their visualization).
- Proactive, alert based profiling

We’re also in the process of open-sourcing this tool.
Automation and Streamlining

All snapshots are stored, aggregated and can be searched / browsed by both developers and SREs and can be used as the starting point to analysis / discussion.
Thank you

Amir Langer | Doron Sekler
alanger@ebay.com | dsekl@ebay.com

http://www.brendangregg.com/flamegraphs.html

That's all we have time for. Come grab us afterwards and let's chat some more...
Lightning Talks

SREcon19 Dublin
Smart and Effective Way to Reduce Distributed Tracing Overhead
SMART?
EFFECTIVE?
EH !?
Is tracing already not present in any form?
Is tracing already not present in any form?
Why is this of importance to SRE based teams or any team as a matter of fact?
Why is this of importance to SRE based teams or any team as a matter of fact?
Present day solutions
Present day solutions
Drawbacks
Drawbacks
Or as they say, every failure is a success in making.. :)

Comic courtesy - Dilbert.com
Problems ?? Solution..

● Overview
Problems ?? Solution..

● Overview
Problems ?? Solution..

- Smartness of the solution
Problems ?? Solution..

- Smartness of the solution
Problems ?? Solution..

- Effectiveness
Problems ?? Solution..

- Effectiveness
TECHNOLOGY ACHIEVEMENT UNLOCKED!
THANK YOU!
For discussing more please reach out to me,

@ susobhitpanigrahi@gmail.com
Lightning Talks

SREcon19 Dublin
In Recent News...

Supermicro Bug Could Let 'Virtual USBs' Take Over Corporate Servers

A newly disclosed vulnerability in Supermicro hardware brings the threat of malicious USBs to corporate servers.
Your solution: do a firmware update
Your hardware is still mostly software

Handling Firmwares in your fleet

Yannick Brosseau
You are deploying fast and frequently already...
... but have you thought of firmwares?
You need actual hardware
Motherboard and CPU
Storage elements
And many more!
(Network switches, Back up devices, Power supply, UPS, etc)
Why should you care?
Security issues
Stability and performance
New features
How do we handle firmware?
Packaging
One format for all
Versions database
Deployment
Open source firmware
Lightning Talks

SREcon19 Dublin
Issuance controls for SSL/TLS certificates

James Renken
(he/him)
SRE @ Let’s Encrypt
Let's Encrypt is a free, automated, and open Certificate Authority.

You can request certificates using the Automated Certificate Management Environment (ACME) protocol, RFC 8555.
Why control certificate issuance?

Operations & policy

Ensure that private keys are stored only in approved, secure ways.

Track certificate inventory for renewal, revocation, etc.

Meet compliance and audit requirements.
Why control certificate issuance?

Operations & policy

Ensure that private keys are stored only in approved, secure ways.

Track certificate inventory for renewal, revocation, etc.

Meet compliance and audit requirements.

Transport security

An attacker with a valid certificate could intercept traffic, and impersonate your service, with a Monster in the Middle attack.

This would defeat the purpose of Transport Layer Security.
Let’s Encrypt issues only **Domain Validated (DV)** certificates:

- **CN / SAN** = enigma.gchq.dev
- **O** = Government Digital Service
- **L** = London
- **ST** = Greater London
- **C** = GB

**Certificate types**
Domain validation methods

“Confirming the Applicant's control over the FQDN by confirming...via HTTP/HTTPS over an Authorized Port...[t]he presence of the Request Token or Random Value contained in the content of a file.”

“Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record...”

(CA/Browser Forum Baseline Requirements, v1.6.6, §§ 3.2.2.4.6-7)
Certificate Authority Authorization (CAA)

RFC 6844

$ORIGIN gchq.dev.
.
  IN  CAA   0  issue  "letsencrypt.org"
You now have a Certificate Management agreement with us. We won’t sign any certificate for gchq.dev until your registered contacts have approved the request.”
CAA Record Extensions

RFC-to-be 8647

$ORIGIN gchq.dev.

. IN CAA 0 issue "letsencrypt.org; accounturi=https://acme-v02.api.letsencrypt.org/acme/acct/42056462"
CAA Record Extensions

RFC-to-be 8647

$ORIGIN gchq.dev.

. IN CAA 0 issue "letsencrypt.org; validationmethods=dns-01"
You now have a Certificate Management agreement with us a CAA record in DNS.”
CAA records’ control is only as good as DNS’ integrity.

DNS responses usually aren’t authenticated.
BGP hijacking

Paths to Bob:

CA → Alice → Charlie → Max → Bob
CA → Alice → Mallory → “Bob”

Shortest path wins!
Improving DNS’ integrity

Network presence & ops

Use authoritative DNS servers that are:

- Well-connected worldwide
- Announced as small prefixes (/24)
- Protected with RPKI
- Actively monitored and defended
Improving DNS' integrity

Network presence & ops
Use authoritative DNS servers that are:
- Well-connected worldwide
- Announced as small prefixes (/24)
- Protected with RPKI
- Actively monitored and defended

Authenticated responses
Use DNSSEC.
When properly deployed, DNSSEC authenticates the presence/lack and content of DNS records.
It is a lovely morning on the Internet, and DNSSEC is a horrible goose.
Both prevention & monitoring

CAA record controls are great, they’re getting better, and you can improve their integrity—but not perfect it.

Monitor the Internet for unexpected certificates.
RFC 6962

There are public, verifiable logs of most SSL/TLS certificates.

Google Chrome does not trust unlogged certificates, so the vast majority of CAs submit their certs.

Your SSL/TLS clients can do the same by validating Signed Certificate Timestamps (SCTs).

Certificate Transparency
CT monitoring resources

- Facebook for Developers
- Hardenize
- Report URI
- SSLMate Cert Spotter

Or build your own with resources from certificate-transparency.org.
Thanks!
Lightning Talks

SREcon19 Dublin
Copilot
Application and Network Service Mesh
Brennen Smith
SPEEDTEST®

Copilot
Application and Network Service Mesh
Brennen Smith
Amazon Load Balancer

Request 1

Request 2

Elastic Load Balancer
Amazon Load Balancer

Request 1: Az A to Service A
Request 2: Az C to Service B

Elastic Load Balancer

Copilot
Application and Network Service Mesh
Brennen Smith
Amazon Load Balancer

Request 1

Request 2

Elastic Load Balancer

Copilot
Application and Network Service Mesh
Brennen Smith
Amazon Load Balancer

Request 1
Request 2

Elastic Load Balancer

Service A
Service B

AZ A
AZ B
AZ C

Copilot
Application and Network Service Mesh
Brennen Smith
Copilot Service Mesh

Cartographer

Service A

Service B

AZ A

AZ B

AZ C

Copilot
Application and Network Service Mesh
Brennen Smith
Copilot Service Mesh

Cartographer

Service A

Service B

AZ A

AZ B

AZ C

Copilot
Application and Network Service Mesh
Brennen Smith
Copilot Service Mesh

Copilot
Application and Network Service Mesh
Brennen Smith
**Avg. Global Timings:** Frontdoor Service → STNET Servers API

- 30ms
- 20ms
- 10ms


---

**Copilot**  
*Application and Network Service Mesh*  
Brennen Smith
Avg. Global Timings: Frontdoor Service → STNET Servers API

AWS Application Load Balancer

Copilot

Application and Network Service Mesh
Brennen Smith
Avg. Global Timings: Frontdoor Service → STNET Servers API

30ms

20ms

10ms

AWS Application Load Balancer

Copilot

Copilot

Application and Network Service Mesh
Brennen Smith
{ "next_steps": { "open_source": "Soon!", "learn_more": "Reach Out!" },
"global_team": "ookla.com/jobs",
"questions": [ "Brennen Smith",
"brennen@ookla.com",
"linkedin.com/in/brennensmith" ] }
}
{
    "next_steps": {
        "open_source": "Soon!",
        "learn_more": "Reach Out!"
    },
    "global_team": "ookla.com/jobs",
    "questions": [
        "Brennen Smith",
        "brennen@ookla.com",
        "linkedin.com/in/brennensmith"
    ]
}
Lightning Talks

SREcon19 Dublin
How Shopify Launched the Welcome Back Returnship Program

Jane Maguire, Engineering Recruitment Lead
@jane_maguire
We’re not just an ecommerce software, Shopify is the best ecommerce platform that has everything you need to sell online, on social media or in person.
For ENTREPRENEURS
We’re halfway through! 😂😂
Lightning Talks

SREcon19 Dublin
Managing On-Call Atrophy

Version 1
September 2019
What is On-Call Atrophy

When you don’t exercise your On-Call muscles
What is On-Call Atrophy

When you don’t exercise your On-Call muscles

- Low call out rate - Google call this Operational Underload
What is On-Call Atrophy

When you don’t exercise your On-Call muscles

- Low call out rate - Google call this Operational Underload
- Wide product base\legacy product base
What is On-Call Atrophy

When you don’t exercise your On-Call muscles

- Low call out rate - Google call this Operational Underload
- Wide product base\legacy product base
- Infrequent rotations - loss of touch
Wait, What!!

You’re saying “It’s bad NOT being paged”
Wait, What!!

You’re saying “It’s bad NOT being paged”

- No system ever is 100% reliable and probably shouldn’t be
Wait, What!!

You’re saying “It’s bad NOT being paged”

- No system ever is 100% reliable and probably shouldn’t be

99.9%
Wait, What!!

You’re saying “It’s bad NOT being paged”

- No system ever is 100% reliable and probably shouldn’t be
- Emotional safety and comfort
Wait, What!!

You’re saying “It’s bad NOT being paged”

- No system ever is 100% reliable and probably shouldn’t be
- Emotional safety and comfort
- Be prepared for now
Wait, What!!

You’re saying “It’s bad NOT being paged”

- No system ever is 100% reliable and probably shouldn’t be
- Emotional safety and comfort
- Be prepared for now
You did WHAT!!

Don’t tell me you did something Dumb like paging On-Call at Random?
You did WHAT!!

Don’t tell me you did something Dumb like paging On-Call at Random?

- Opt in approach and strict rules
You did WHAT!!

Don’t tell me you did something Dumb like paging On-Call at Random?

- Opt in approach and strict rules
- Set of comprehensive drills
You did WHAT!!

Don’t tell me you did something Dumb like paging On-Call at Random?

- Opt in approach and strict rules
- Set of comprehensive drills
You did WHAT!!

Don’t tell me you did something Dumb like paging On-Call at Random?

- Opt in approach and strict rules
- Set of comprehensive drills
- What have we found out
  - Out of date software
  - Ipv6 and Google firewalls
  - People like it! (People are strange!)
Obligatory War Story

So this one time at band camp.........
Obligatory War Story

So this one time at band camp........
Who the hell was that?

So I am....

- James Wynne
- Pivotal CloudOps R&D
- You can drop me a mail at jwynne@pivotal.io
- Or come up to me afterwards and ask me anything (within a very narrow scope!)

0:30
Transforming How The World Builds, Operates Software
Slide Karaoke

for the brave and fearless
Lightning Talks
SREcon19 Dublin