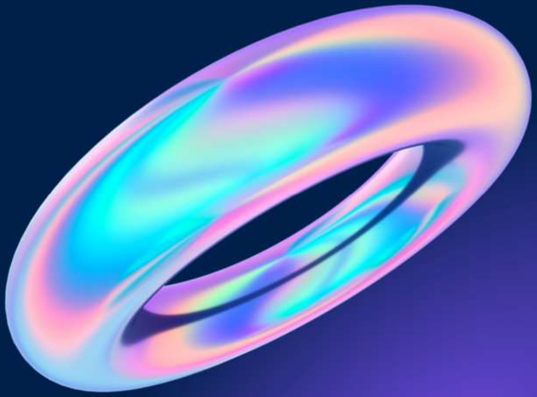
Digital Experience in an Opaque World

Observe Ability



Observe Ability

Your partner in Observability Architectures

Agenda

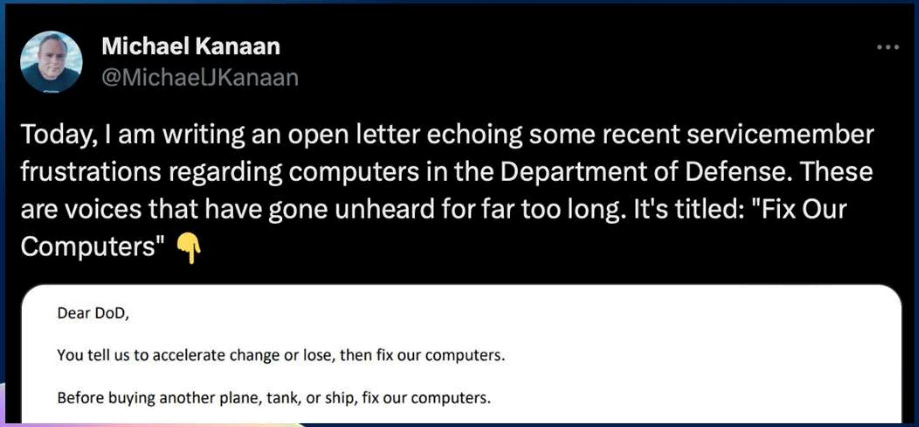
- Introduction
- An Open Letter
- How do we Observe
- Challenges
- Better Observability
- Wrap up

Digital Experience

"The way people interact digitally with your organization or service"

An Open Letter

An Open Letter



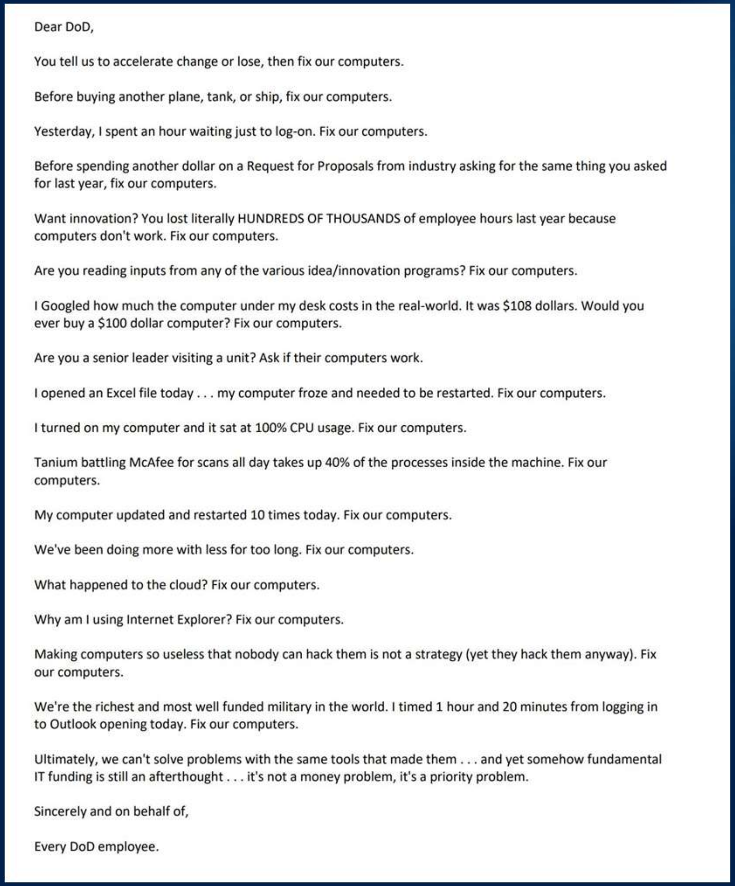
Michael Kanaan
@MichaelJKanaan

Today, I am writing an open letter echoing some recent servicemember frustrations regarding computers in the Department of Defense. These are voices that have gone unheard for far too long. It's titled: "Fix Our Computers" 👇

Dear DoD,

You tell us to accelerate change or lose, then fix our computers.

Before buying another plane, tank, or ship, fix our computers.



Dear DoD,

You tell us to accelerate change or lose, then fix our computers.

Before buying another plane, tank, or ship, fix our computers.

Yesterday, I spent an hour waiting just to log-on. Fix our computers.

Before spending another dollar on a Request for Proposals from industry asking for the same thing you asked for last year, fix our computers.

Want innovation? You lost literally HUNDREDS OF THOUSANDS of employee hours last year because computers don't work. Fix our computers.

Are you reading inputs from any of the various idea/innovation programs? Fix our computers.

I Googled how much the computer under my desk costs in the real-world. It was $108 dollars. Would you ever buy a $100 dollar computer? Fix our computers.

Are you a senior leader visiting a unit? Ask if their computers work.

I opened an Excel file today . . . my computer froze and needed to be restarted. Fix our computers.

I turned on my computer and it sat at 100% CPU usage. Fix our computers.

Tanium battling McAfee for scans all day takes up 40% of the processes inside the machine. Fix our computers.

My computer updated and restarted 10 times today. Fix our computers.

We've been doing more with less for too long. Fix our computers.

What happened to the cloud? Fix our computers.

Why am I using Internet Explorer? Fix our computers.

Making computers so useless that nobody can hack them is not a strategy (yet they hack them anyway). Fix our computers.

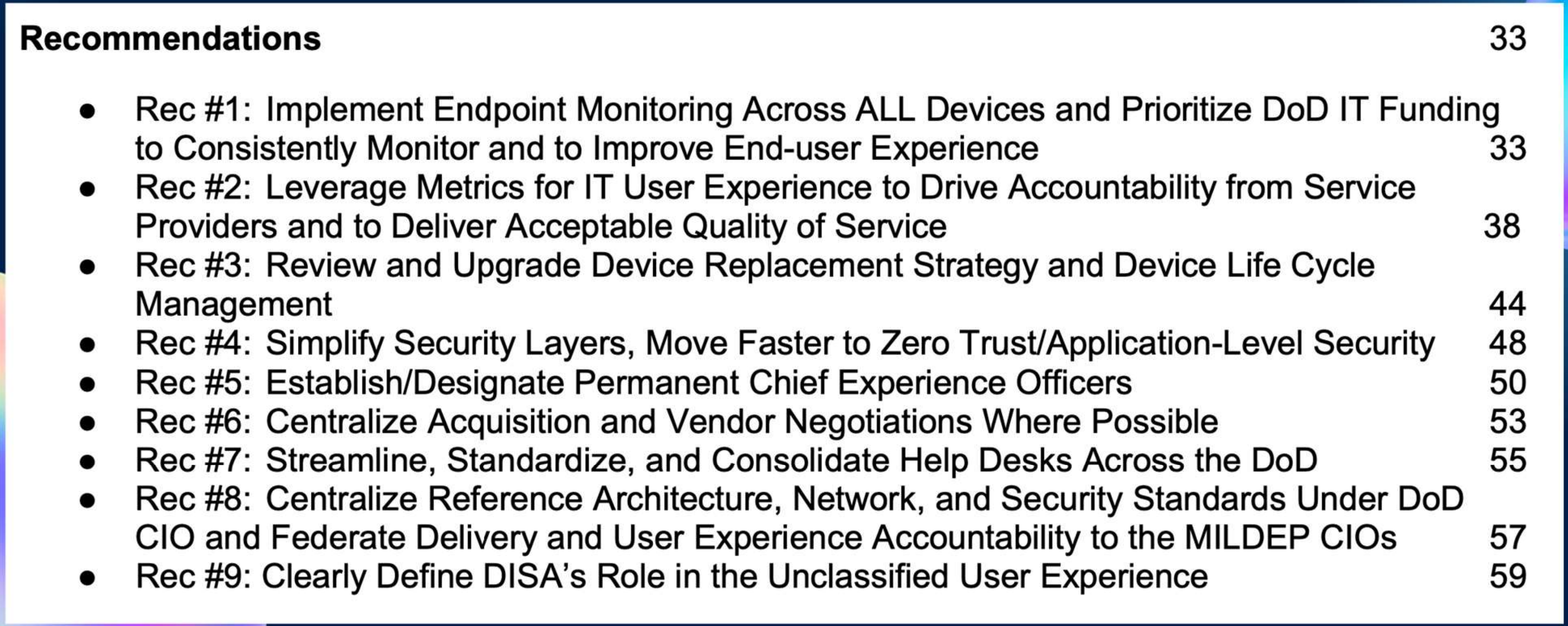
We're the richest and most well funded military in the world. I timed 1 hour and 20 minutes from logging in to Outlook opening today. Fix our computers.

Ultimately, we can't solve problems with the same tools that made them . . . and yet somehow fundamental IT funding is still an afterthought . . . it's not a money problem, it's a priority problem.

Sincerely and on behalf of,

Every DoD employee.

An Open Letter



“Fix our Computers”

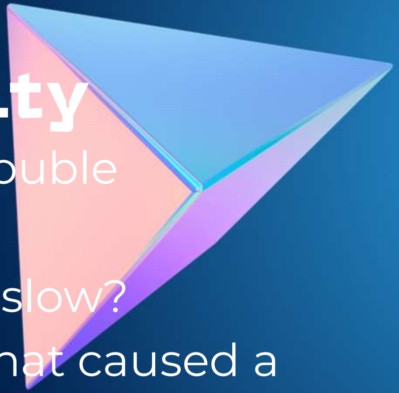
Why is this so hard?

1. Complexity of the environment
2. Administrative control
3. MTTI vs MTTR
4. Problems asking and answering the right questions
5. Improvements in cyber security posture
6. Lack of Observability and capability.

Monitoring & Observability

Monitoring

1. Is a service up or down?
2. What was the latency between X & Y?
3. What was the link utilization over the last 5 minutes?



Observability

1. Why did person X have trouble logging in?
2. Why was this transaction slow?
3. What was the DB query that caused a lock?
4. What path did this traffic take through the network?

How do we Observe?

How do we Observe?

Metrics

- CPU Utilisation
- Disk Queue Length
- Packets per Second

Events

- Exceptions
- Alerts
- Creation of an object
- Traps

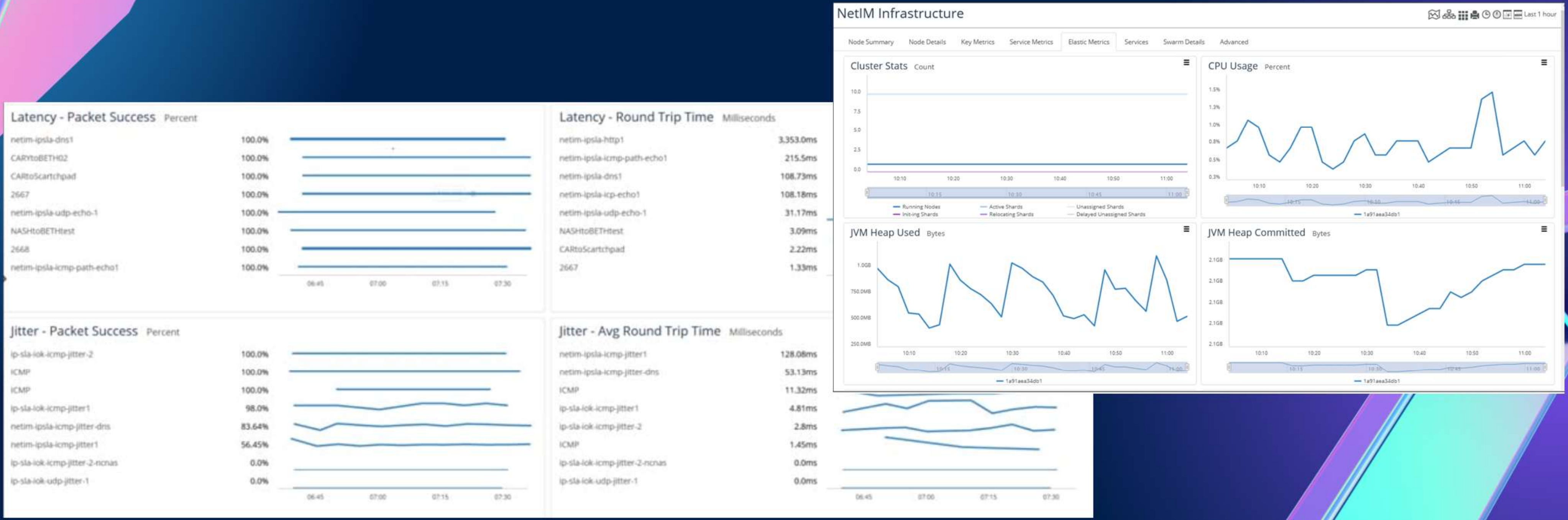
Logs

- Syslog
- Event Logs
- Application Logs
- Kernel logs

Traces

- Application Traces
- Packet traces
- Kernel tracing (eBPF)

Metrics



Latency - Packet Success Percent

netim-ipsla-dns1	100.0%
CARYtoBETH02	100.0%
CARtoScartchpad	100.0%
2667	100.0%
netim-ipsla-udp-echo-1	100.0%
NASHtoBETHtest	100.0%
2668	100.0%
netim-ipsla-icmp-path-echo1	100.0%

Latency - Round Trip Time Milliseconds

netim-ipsla-http1	3,353.0ms
netim-ipsla-icmp-path-echo1	215.5ms
netim-ipsla-dns1	108.73ms
netim-ipsla-icp-echo1	108.18ms
netim-ipsla-udp-echo-1	31.17ms
NASHtoBETHtest	3.09ms
CARtoScartchpad	2.22ms
2667	1.33ms

Jitter - Packet Success Percent

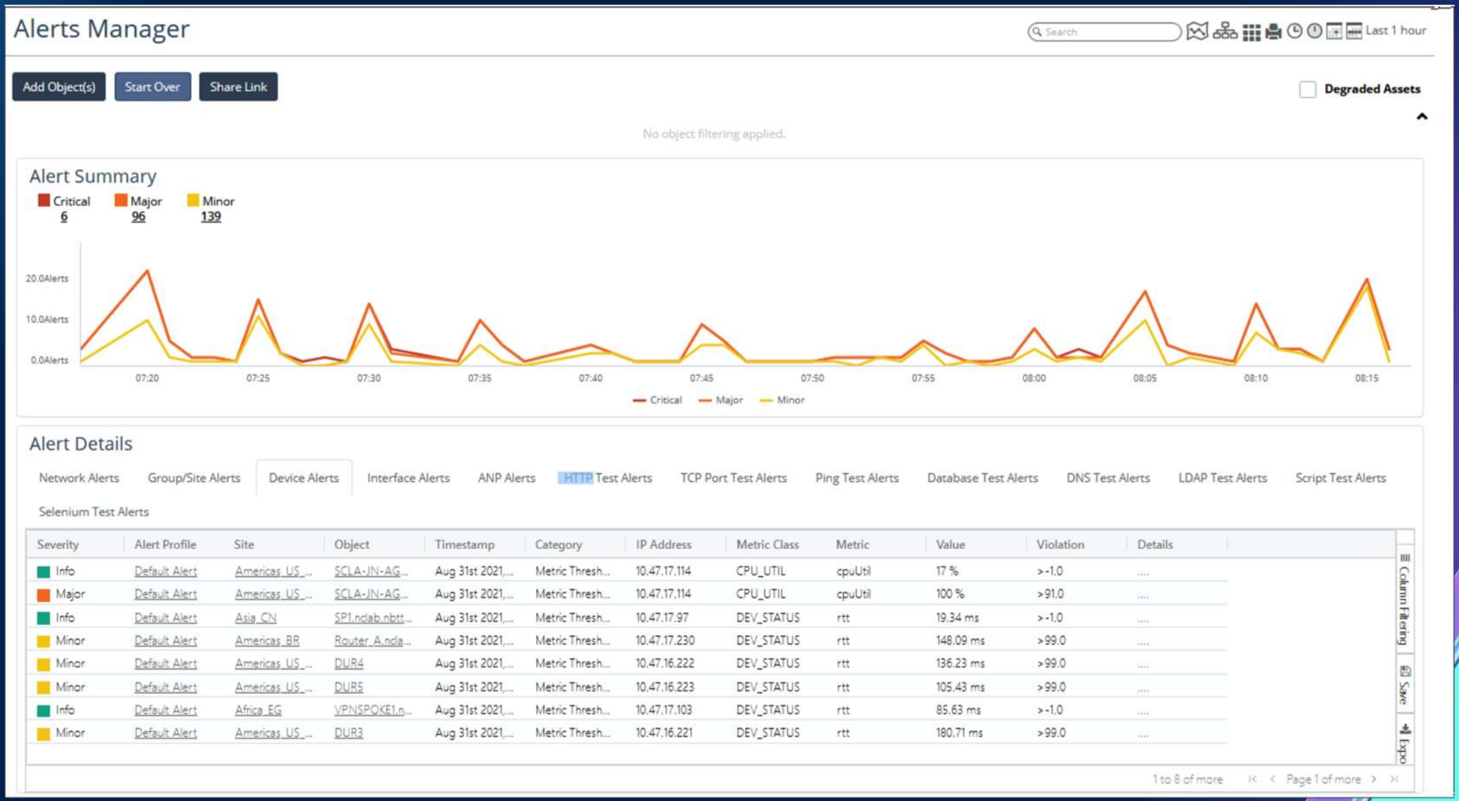
ip-sla-iok-icmp-jitter-2	100.0%
ICMP	100.0%
ICMP	100.0%
ip-sla-iok-icmp-jitter1	98.0%
netim-ipsla-icmp-jitter-dns	83.64%
netim-ipsla-icmp-jitter1	56.45%
ip-sla-iok-icmp-jitter-2-ncnas	0.0%
ip-sla-iok-udp-jitter-1	0.0%

Jitter - Avg Round Trip Time Milliseconds

netim-ipsla-icmp-jitter1	128.08ms
netim-ipsla-icmp-jitter-dns	53.13ms
ICMP	11.32ms
ip-sla-iok-icmp-jitter1	4.81ms
ip-sla-iok-icmp-jitter-2	2.8ms
ICMP	1.45ms
ip-sla-iok-icmp-jitter-2-ncnas	0.0ms
ip-sla-iok-udp-jitter-1	0.0ms

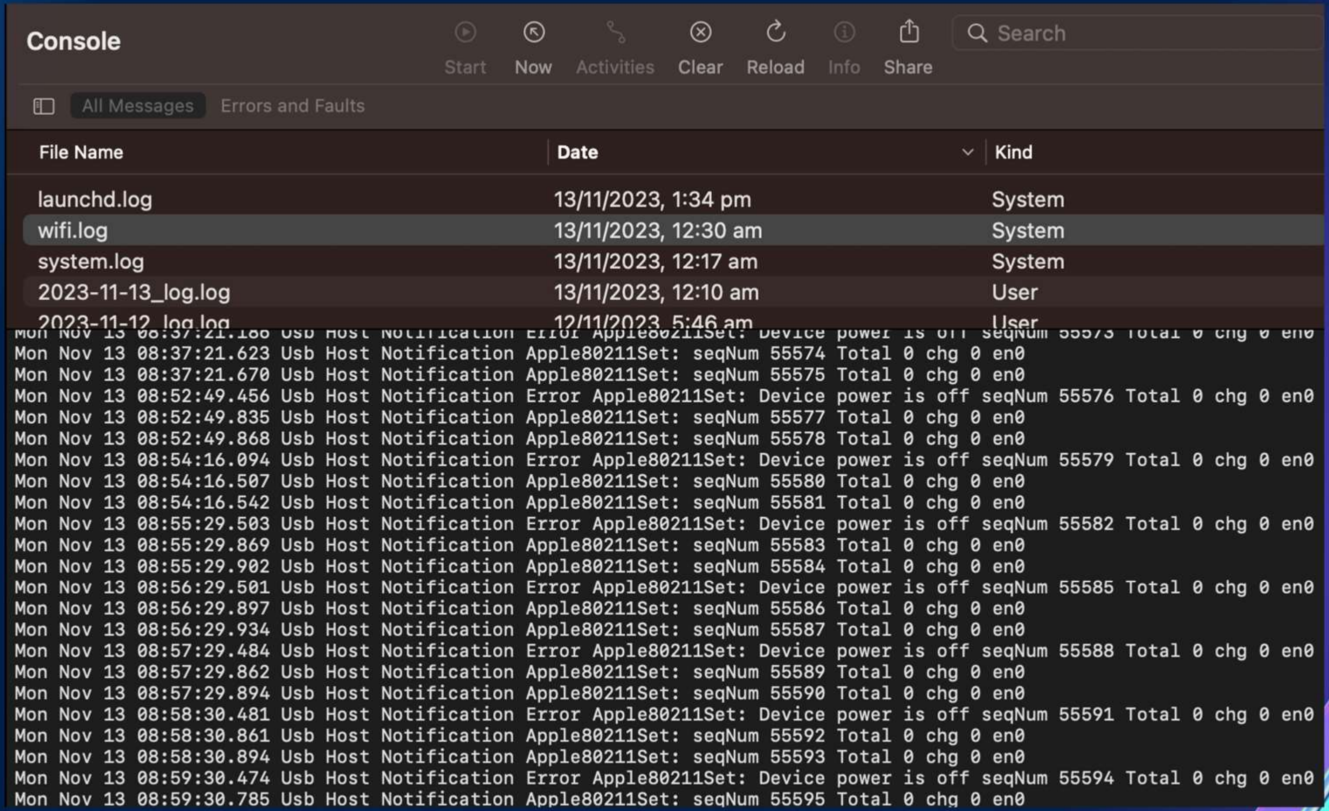
NetIM Infrastructure

Events



Severity	Alert Profile	Site	Object	Timestamp	Category	IP Address	Metric Class	Metric	Value	Violation	Details
🟩 Info	Default Alert	Americas_US_...	SCLA-JN-AG...	Aug 31st 2021,...	Metric Thresh...	10.47.17.114	CPU_UTIL	cpuUtil	17 %	>-1.0	....
🟧 Major	Default Alert	Americas_US_...	SCLA-JN-AG...	Aug 31st 2021,...	Metric Thresh...	10.47.17.114	CPU_UTIL	cpuUtil	100 %	>91.0	....
🟩 Info	Default Alert	Asia_CN	SP1.ndab.nbtt...	Aug 31st 2021,...	Metric Thresh...	10.47.17.97	DEV_STATUS	rtt	19.34 ms	>-1.0	....
🟨 Minor	Default Alert	Americas_BR	Router_A.nda...	Aug 31st 2021,...	Metric Thresh...	10.47.17.230	DEV_STATUS	rtt	148.09 ms	>99.0	....
🟨 Minor	Default Alert	Americas_US_...	DUR4	Aug 31st 2021,...	Metric Thresh...	10.47.16.222	DEV_STATUS	rtt	136.23 ms	>99.0	....
🟨 Minor	Default Alert	Americas_US_...	DUR5	Aug 31st 2021,...	Metric Thresh...	10.47.16.223	DEV_STATUS	rtt	105.43 ms	>99.0	....
🟩 Info	Default Alert	Africa_EG	VPNSPOKE1.n...	Aug 31st 2021,...	Metric Thresh...	10.47.17.103	DEV_STATUS	rtt	85.63 ms	>-1.0	....
🟨 Minor	Default Alert	Americas_US_...	DUR3	Aug 31st 2021,...	Metric Thresh...	10.47.16.221	DEV_STATUS	rtt	180.71 ms	>99.0	....

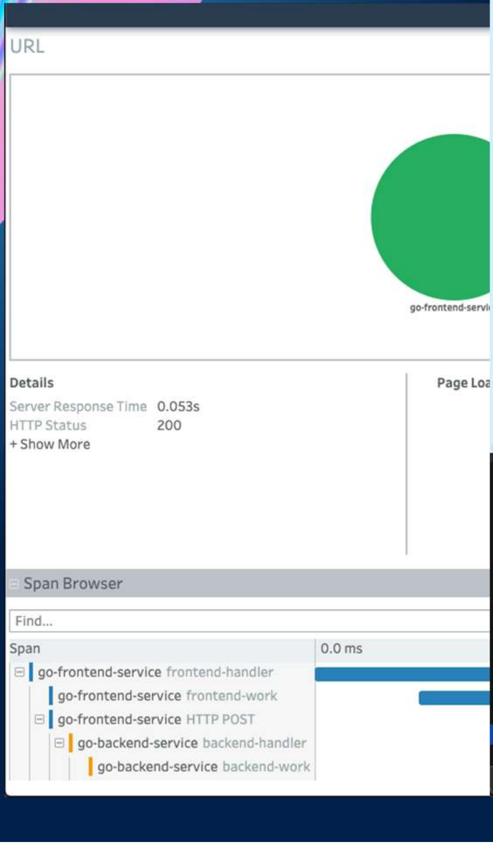
Logs



File Name	Date	Kind
launchd.log	13/11/2023, 1:34 pm	System
wifi.log	13/11/2023, 12:30 am	System
system.log	13/11/2023, 12:17 am	System
2023-11-13_log.log	13/11/2023, 12:10 am	User
2023-11-12_log.log	12/11/2023, 5:46 am	User

```
Mon Nov 13 08:37:21.188 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55573 Total 0 chg 0 en0
Mon Nov 13 08:37:21.623 Usb Host Notification Apple80211Set: seqNum 55574 Total 0 chg 0 en0
Mon Nov 13 08:37:21.670 Usb Host Notification Apple80211Set: seqNum 55575 Total 0 chg 0 en0
Mon Nov 13 08:52:49.456 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55576 Total 0 chg 0 en0
Mon Nov 13 08:52:49.835 Usb Host Notification Apple80211Set: seqNum 55577 Total 0 chg 0 en0
Mon Nov 13 08:52:49.868 Usb Host Notification Apple80211Set: seqNum 55578 Total 0 chg 0 en0
Mon Nov 13 08:54:16.094 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55579 Total 0 chg 0 en0
Mon Nov 13 08:54:16.507 Usb Host Notification Apple80211Set: seqNum 55580 Total 0 chg 0 en0
Mon Nov 13 08:54:16.542 Usb Host Notification Apple80211Set: seqNum 55581 Total 0 chg 0 en0
Mon Nov 13 08:55:29.503 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55582 Total 0 chg 0 en0
Mon Nov 13 08:55:29.869 Usb Host Notification Apple80211Set: seqNum 55583 Total 0 chg 0 en0
Mon Nov 13 08:55:29.902 Usb Host Notification Apple80211Set: seqNum 55584 Total 0 chg 0 en0
Mon Nov 13 08:56:29.501 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55585 Total 0 chg 0 en0
Mon Nov 13 08:56:29.897 Usb Host Notification Apple80211Set: seqNum 55586 Total 0 chg 0 en0
Mon Nov 13 08:56:29.934 Usb Host Notification Apple80211Set: seqNum 55587 Total 0 chg 0 en0
Mon Nov 13 08:57:29.484 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55588 Total 0 chg 0 en0
Mon Nov 13 08:57:29.862 Usb Host Notification Apple80211Set: seqNum 55589 Total 0 chg 0 en0
Mon Nov 13 08:57:29.894 Usb Host Notification Apple80211Set: seqNum 55590 Total 0 chg 0 en0
Mon Nov 13 08:58:30.481 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55591 Total 0 chg 0 en0
Mon Nov 13 08:58:30.861 Usb Host Notification Apple80211Set: seqNum 55592 Total 0 chg 0 en0
Mon Nov 13 08:58:30.894 Usb Host Notification Apple80211Set: seqNum 55593 Total 0 chg 0 en0
Mon Nov 13 08:59:30.474 Usb Host Notification Error Apple80211Set: Device power is off seqNum 55594 Total 0 chg 0 en0
Mon Nov 13 08:59:30.785 Usb Host Notification Apple80211Set: seqNum 55595 Total 0 chg 0 en0
```

Traces



URL

Details

Server Response Time 0.053s

HTTP Status 200

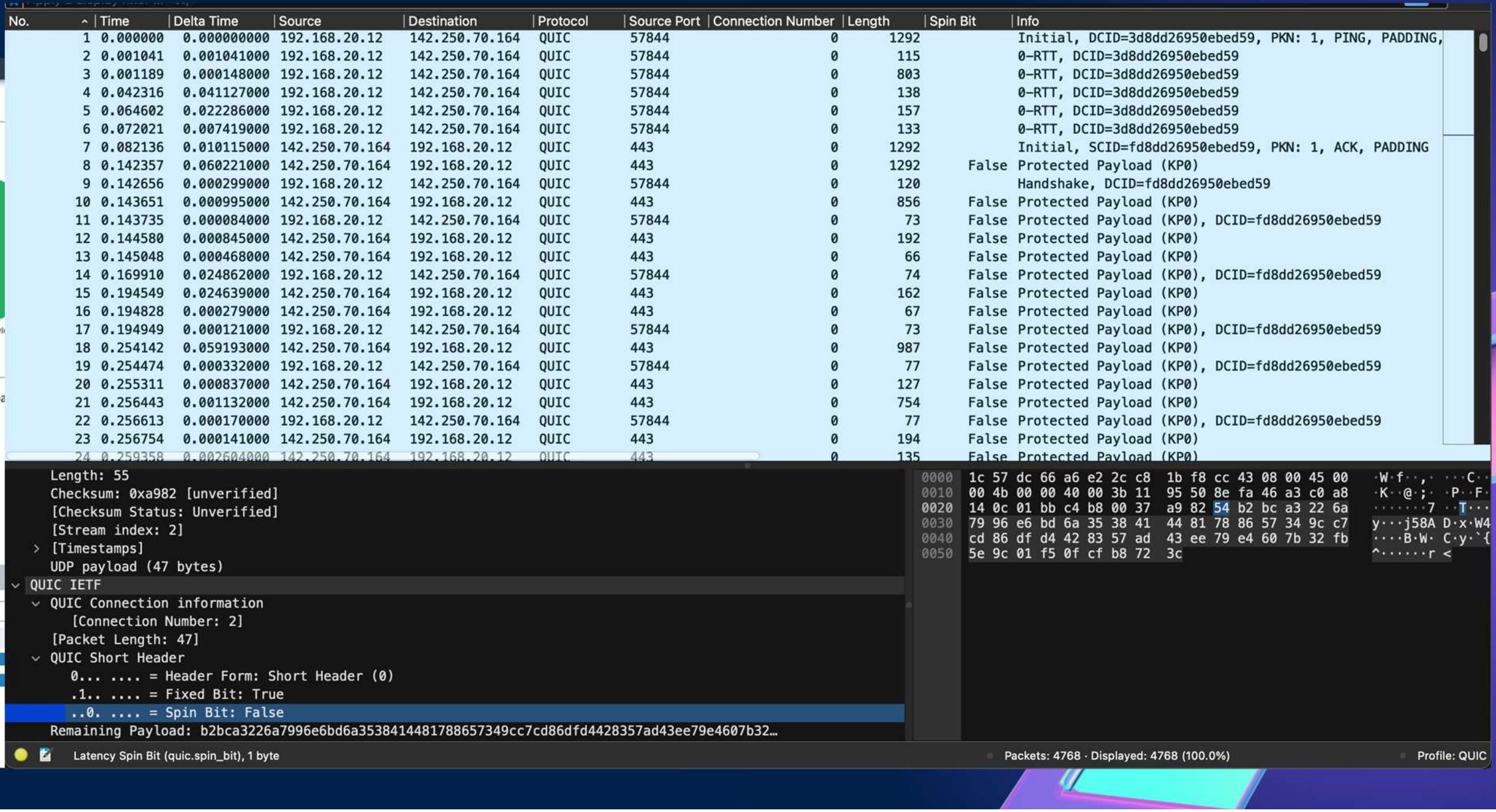
+ Show More

Page Loa

Span Browser

Find...

Span	0.0 ms
go-frontend-service frontend-handler	
go-frontend-service frontend-work	
go-frontend-service HTTP POST	
go-backend-service backend-handler	
go-backend-service backend-work	



```
No.     Time     Delta Time  Source        Destination    Protocol Source Port Connection Number Length Spin Bit Info
     1 0.000000 0.000000000 192.168.20.12 142.250.70.164 QUIC     57844                       0   1292          Initial, DCID=3d8dd26950ebed59, PKN: 1, PING, PADDING,
     2 0.001041 0.001041000 192.168.20.12 142.250.70.164 QUIC     57844                       0    115          0-RTT, DCID=3d8dd26950ebed59
     3 0.001189 0.000148000 192.168.20.12 142.250.70.164 QUIC     57844                       0    803          0-RTT, DCID=3d8dd26950ebed59
     4 0.042316 0.041127000 192.168.20.12 142.250.70.164 QUIC     57844                       0    138          0-RTT, DCID=3d8dd26950ebed59
     5 0.064602 0.022286000 192.168.20.12 142.250.70.164 QUIC     57844                       0    157          0-RTT, DCID=3d8dd26950ebed59
     6 0.072021 0.007419000 192.168.20.12 142.250.70.164 QUIC     57844                       0    133          0-RTT, DCID=3d8dd26950ebed59
     7 0.082136 0.010115000 142.250.70.164 192.168.20.12 QUIC     443                         0   1292          Initial, SCID=fd8dd26950ebed59, PKN: 1, ACK, PADDING
     8 0.142357 0.060221000 142.250.70.164 192.168.20.12 QUIC     443                         0   1292    False Protected Payload (KP0)
     9 0.142656 0.000299000 192.168.20.12 142.250.70.164 QUIC     57844                       0    120          Handshake, DCID=fd8dd26950ebed59
    10 0.143651 0.000995000 142.250.70.164 192.168.20.12 QUIC     443                         0    856    False Protected Payload (KP0)
    11 0.143735 0.000084000 192.168.20.12 142.250.70.164 QUIC     57844                       0     73    False Protected Payload (KP0), DCID=fd8dd26950ebed59
    12 0.144580 0.000845000 142.250.70.164 192.168.20.12 QUIC     443                         0    192    False Protected Payload (KP0)
    13 0.145048 0.000468000 142.250.70.164 192.168.20.12 QUIC     443                         0     66    False Protected Payload (KP0)
    14 0.169910 0.024862000 192.168.20.12 142.250.70.164 QUIC     57844                       0     74    False Protected Payload (KP0), DCID=fd8dd26950ebed59
    15 0.194549 0.024639000 142.250.70.164 192.168.20.12 QUIC     443                         0    162    False Protected Payload (KP0)
    16 0.194828 0.000279000 142.250.70.164 192.168.20.12 QUIC     443                         0     67    False Protected Payload (KP0)
    17 0.194949 0.000121000 192.168.20.12 142.250.70.164 QUIC     57844                       0     73    False Protected Payload (KP0), DCID=fd8dd26950ebed59
    18 0.254142 0.059193000 142.250.70.164 192.168.20.12 QUIC     443                         0    987    False Protected Payload (KP0)
    19 0.254474 0.000332000 192.168.20.12 142.250.70.164 QUIC     57844                       0     77    False Protected Payload (KP0), DCID=fd8dd26950ebed59
    20 0.255311 0.000837000 142.250.70.164 192.168.20.12 QUIC     443                         0    127    False Protected Payload (KP0)
    21 0.256443 0.001132000 142.250.70.164 192.168.20.12 QUIC     443                         0    754    False Protected Payload (KP0)
    22 0.256613 0.000170000 192.168.20.12 142.250.70.164 QUIC     57844                       0     77    False Protected Payload (KP0), DCID=fd8dd26950ebed59
    23 0.256754 0.000141000 142.250.70.164 192.168.20.12 QUIC     443                         0    194    False Protected Payload (KP0)
    24 0.259358 0.002604000 142.250.70.164 192.168.20.12 QUIC     443                         0    135    False Protected Payload (KP0)
```

```
    Length: 55
    Checksum: 0xa982 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (47 bytes)
v QUIC IETF
  v QUIC Connection information
      [Connection Number: 2]
    [Packet Length: 47]
  v QUIC Short Header
      0... .... = Header Form: Short Header (0)
      .1.. .... = Fixed Bit: True
      ..0. .... = Spin Bit: False
    Remaining Payload: b2bca3226a7996e6bd6a3538414481788657349cc7cd86dfd4428357ad43ee79e4607b32…
```

```
0000  1c 57 dc 66 a6 e2 2c c8  1b f8 cc 43 08 00 45 00   ·W·f··,·  ···C··
0010  00 4b 00 00 40 00 3b 11  95 50 8e fa 46 a3 c0 a8   ·K··@·;·  ·P··F·
0020  14 0c 01 bb c4 b8 00 37  a9 82 54 b2 bc a3 22 6a   ·······7  ··T···
0030  79 96 e6 bd 6a 35 38 41  44 81 78 86 57 34 9c c7   y···j58A D·x·W4
0040  cd 86 df d4 42 83 57 ad  43 ee 79 e4 60 7b 32 fb   ····B·W· C·y·`{
0050  5e 9c 01 f5 0f cf b8 72  3c                        ^······r <
```

Latency Spin Bit (quic.spin_bit), 1 byte

Packets: 4768 · Displayed: 4768 (100.0%)

Profile: QUIC

Where do we Observe?

Infrastructure

- Hypervisor
- Server Infrastructure
- Routers
- Switches
- Firewalls
- Load Balancers

Applications

- Application
- Application Server
- Container
- Platform

Network

- Routers
- Switches
- vSwitches
- Firewalls
- Endpoints

Endpoints

- Mobile
- Laptop
- Desktop

Challenges

Challenges

Perspective

Silod Operations

Need to Know

SRE Mindset

Evolution

Software Lifecycle

Technology Evolution

Scaling

Cyber

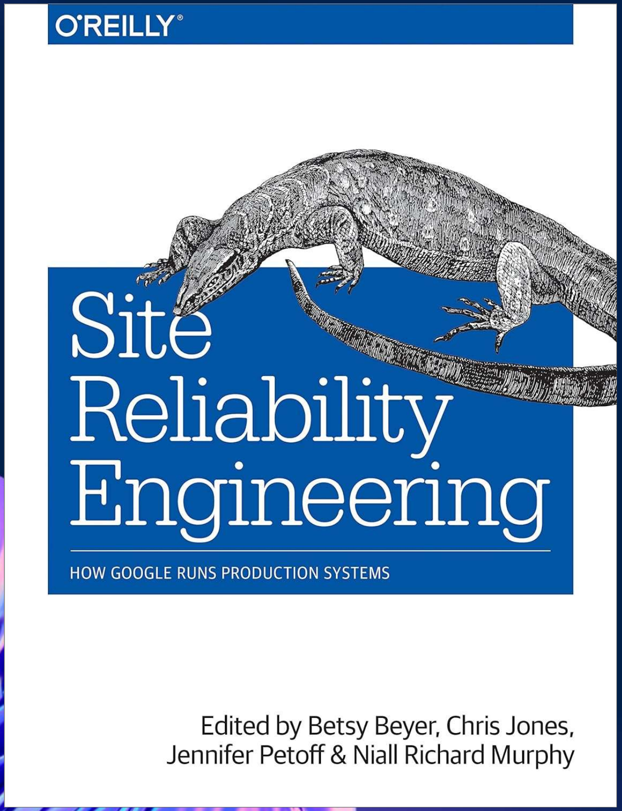
Very Necessary

Cannot Secure What we Cannot See

Passive Monitoring Becoming Hard

Perspective — Silos

Perspective — SRE Mindset

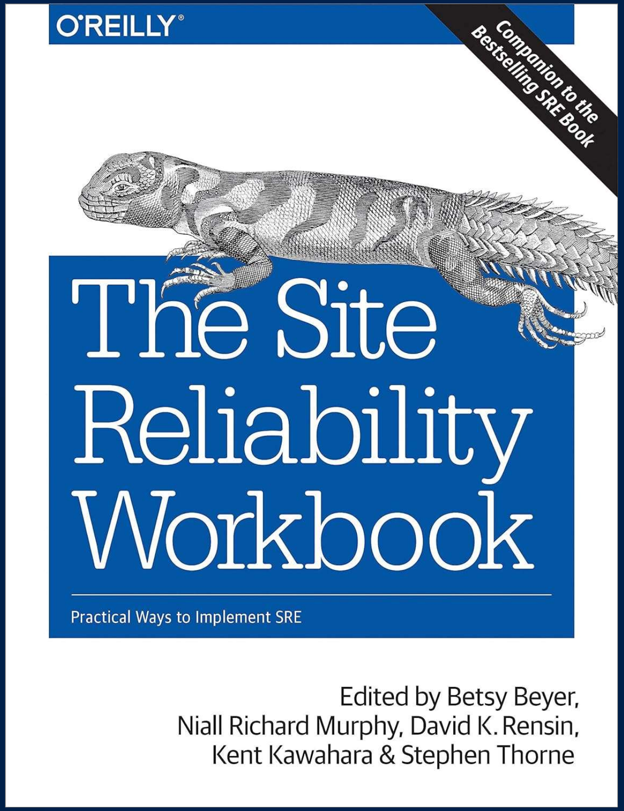


O'REILLY®

Site Reliability Engineering

HOW GOOGLE RUNS PRODUCTION SYSTEMS

Edited by Betsy Beyer, Chris Jones, Jennifer Petoff & Niall Richard Murphy



O'REILLY®

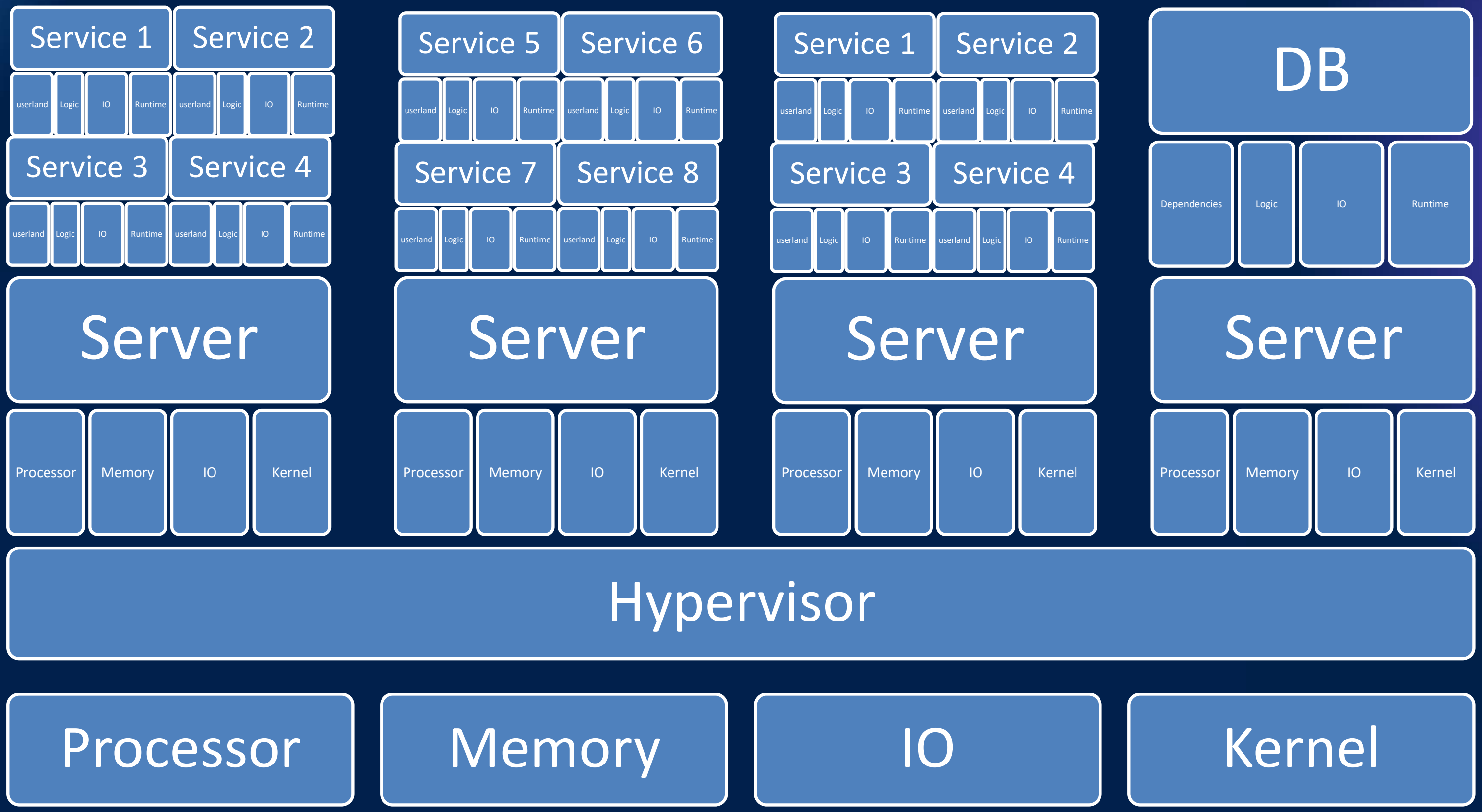
Companion to the Bestselling SRE Book

The Site Reliability Workbook

Practical Ways to Implement SRE

Edited by Betsy Beyer, Niall Richard Murphy, David K. Rensin, Kent Kawahara & Stephen Thorne

Evolution – Scaling



Service 1 Service 2
userland Logic IO Runtime userland Logic IO Runtime
Service 3 Service 4
userland Logic IO Runtime userland Logic IO Runtime
Server
Processor Memory IO Kernel

Service 5 Service 6
userland Logic IO Runtime userland Logic IO Runtime
Service 7 Service 8
userland Logic IO Runtime userland Logic IO Runtime
Server
Processor Memory IO Kernel

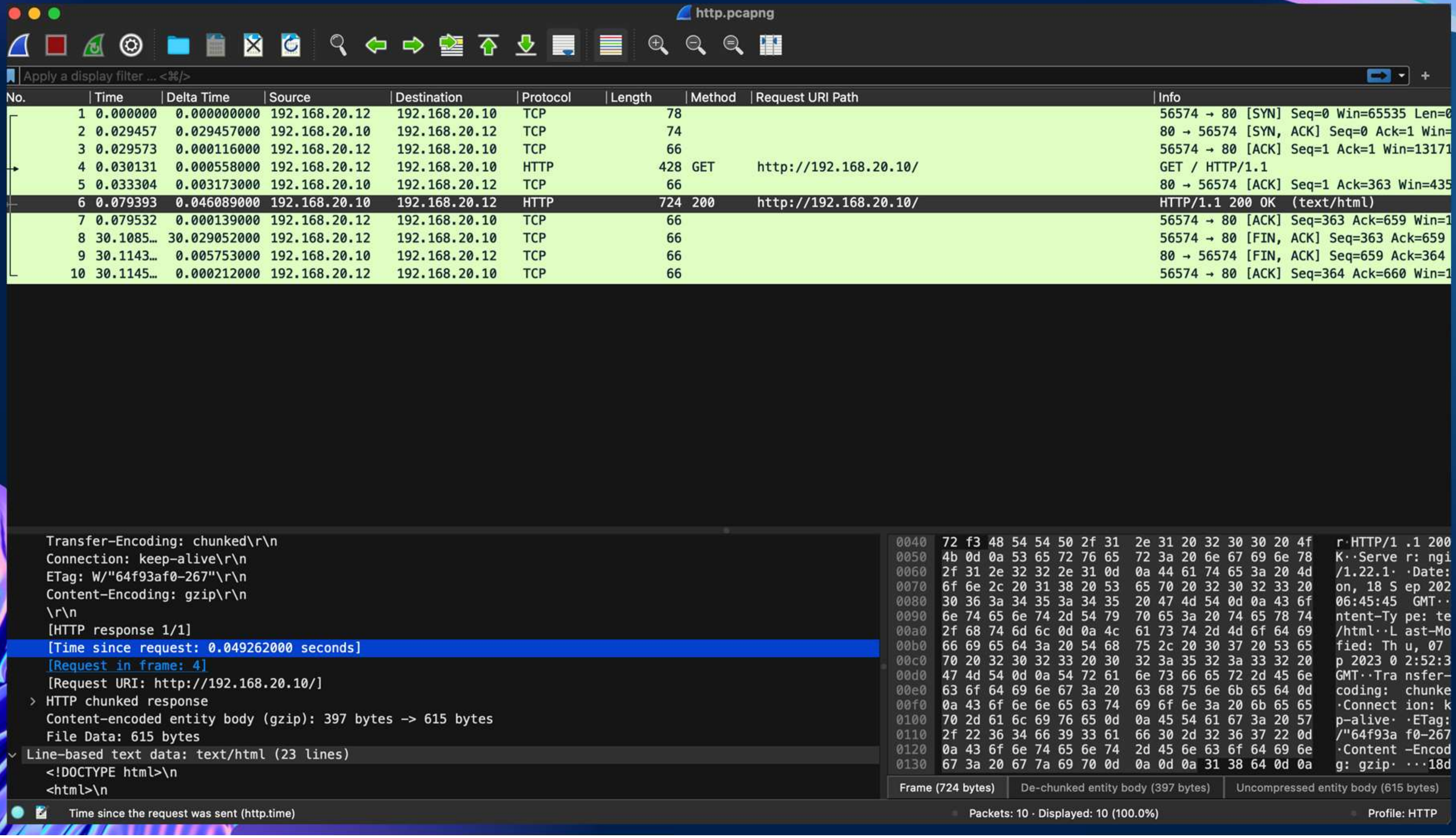
Service 1 Service 2
userland Logic IO Runtime userland Logic IO Runtime
Service 3 Service 4
userland Logic IO Runtime userland Logic IO Runtime
Server
Processor Memory IO Kernel

DB
Dependencies Logic IO Runtime
Server
Processor Memory IO Kernel

Hypervisor

Processor Memory IO Kernel

Evolution – HTTP



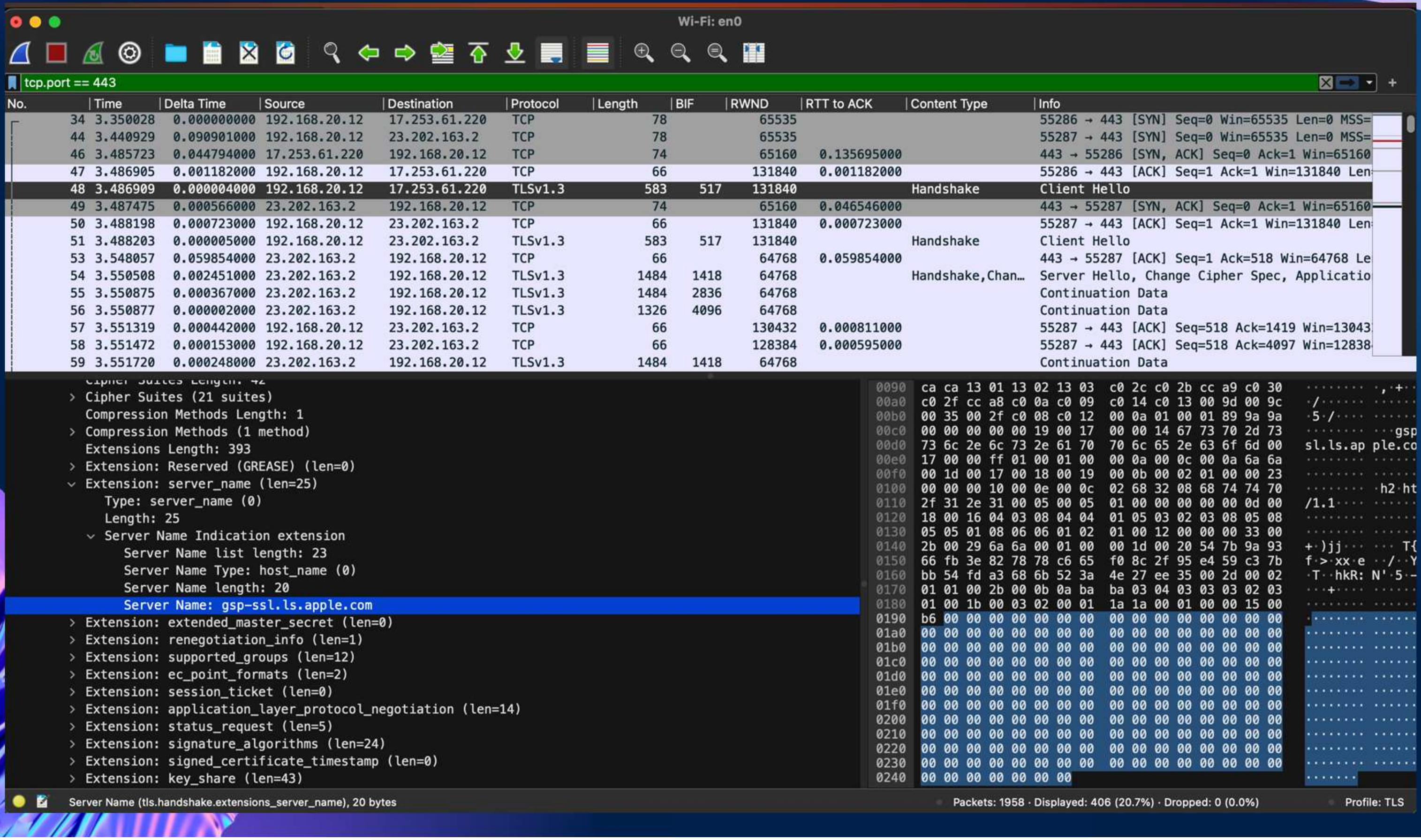
```
No.   Time       Delta Time   Source          Destination     Protocol  Length  Method  Request URI Path           Info
  1   0.000000   0.000000000  192.168.20.12   192.168.20.10   TCP           78                                     56574 → 80 [SYN] Seq=0 Win=65535 Len=0
  2   0.029457   0.029457000  192.168.20.10   192.168.20.12   TCP           74                                     80 → 56574 [SYN, ACK] Seq=0 Ack=1 Win=
  3   0.029573   0.000116000  192.168.20.12   192.168.20.10   TCP           66                                     56574 → 80 [ACK] Seq=1 Ack=1 Win=13171
  4   0.030131   0.000558000  192.168.20.12   192.168.20.10   HTTP         428  GET     http://192.168.20.10/      GET / HTTP/1.1
  5   0.033304   0.003173000  192.168.20.10   192.168.20.12   TCP           66                                     80 → 56574 [ACK] Seq=1 Ack=363 Win=435
  6   0.079393   0.046089000  192.168.20.10   192.168.20.12   HTTP         724  200     http://192.168.20.10/      HTTP/1.1 200 OK  (text/html)
  7   0.079532   0.000139000  192.168.20.12   192.168.20.10   TCP           66                                     56574 → 80 [ACK] Seq=363 Ack=659 Win=1
  8   30.1085…   30.029052000 192.168.20.12   192.168.20.10   TCP           66                                     56574 → 80 [FIN, ACK] Seq=363 Ack=659
  9   30.1143…   0.005753000  192.168.20.10   192.168.20.12   TCP           66                                     80 → 56574 [FIN, ACK] Seq=659 Ack=364
 10   30.1145…   0.000212000  192.168.20.12   192.168.20.10   TCP           66                                     56574 → 80 [ACK] Seq=364 Ack=660 Win=1
```

```
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
    ETag: W/"64f93af0-267"\r\n
    Content-Encoding: gzip\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.049262000 seconds]
    [Request in frame: 4]
    [Request URI: http://192.168.20.10/]
  > HTTP chunked response
    Content-encoded entity body (gzip): 397 bytes -> 615 bytes
    File Data: 615 bytes
v Line-based text data: text/html (23 lines)
    <!DOCTYPE html>\n
    <html>\n
```

```
0040  72 f3 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   r·HTTP/1 .1 200
0050  4b 0d 0a 53 65 72 76 65  72 3a 20 6e 67 69 6e 78   K··Serve r: ngi
0060  2f 31 2e 32 32 2e 31 0d  0a 44 61 74 65 3a 20 4d   /1.22.1· ·Date:
0070  6f 6e 2c 20 31 38 20 53  65 70 20 32 30 32 33 20   on, 18 S ep 202
0080  30 36 3a 34 35 3a 34 35  20 47 4d 54 0d 0a 43 6f   06:45:45  GMT··
0090  6e 74 65 6e 74 2d 54 79  70 65 3a 20 74 65 78 74   ntent-Ty pe: te
00a0  2f 68 74 6d 6c 0d 0a 4c  61 73 74 2d 4d 6f 64 69   /html··L ast-Mo
00b0  66 69 65 64 3a 20 54 68  75 2c 20 30 37 20 53 65   fied: Th u, 07
00c0  70 20 32 30 32 33 20 30  32 3a 35 32 3a 33 32 20   p 2023 0 2:52:3
00d0  47 4d 54 0d 0a 54 72 61  6e 73 66 65 72 2d 45 6e   GMT··Tra nsfer-
00e0  63 6f 64 69 6e 67 3a 20  63 68 75 6e 6b 65 64 0d   coding:  chunke
00f0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: k
0100  70 2d 61 6c 69 76 65 0d  0a 45 54 61 67 3a 20 57   p-alive· ·ETag:
0110  2f 22 36 34 66 39 33 61  66 30 2d 32 36 37 22 0d   /"64f93a f0-267
0120  0a 43 6f 6e 74 65 6e 74  2d 45 6e 63 6f 64 69 6e   ·Content -Encod
0130  67 3a 20 67 7a 69 70 0d  0a 0d 0a 31 38 64 0d 0a   g: gzip· ···18d
```

Frame (724 bytes)
De-chunked entity body (397 bytes)
Uncompressed entity body (615 bytes)
Time since the request was sent (http.time)
Packets: 10 · Displayed: 10 (100.0%)
Profile: HTTP

Evolution – HTTPS



Wi-Fi: en0

tcp.port == 443

```
No.  |Time     |Delta Time  |Source        |Destination   |Protocol |Length |BIF  |RWND   |RTT to ACK  |Content Type     |Info
  34 3.350028  0.000000000  192.168.20.12  17.253.61.220  TCP           78          65535                                55286 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=
  44 3.440929  0.090901000  192.168.20.12  23.202.163.2   TCP           78          65535                                55287 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=
  46 3.485723  0.044794000  17.253.61.220  192.168.20.12  TCP           74          65160  0.135695000                   443 → 55286 [SYN, ACK] Seq=0 Ack=1 Win=65160
  47 3.486905  0.001182000  192.168.20.12  17.253.61.220  TCP           66         131840  0.001182000                   55286 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len
  48 3.486909  0.000004000  192.168.20.12  17.253.61.220  TLSv1.3      583    517  131840               Handshake         Client Hello
  49 3.487475  0.000566000  23.202.163.2   192.168.20.12  TCP           74          65160  0.046546000                   443 → 55287 [SYN, ACK] Seq=0 Ack=1 Win=65160
  50 3.488198  0.000723000  192.168.20.12  23.202.163.2   TCP           66         131840  0.000723000                   55287 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len
  51 3.488203  0.000005000  192.168.20.12  23.202.163.2   TLSv1.3      583    517  131840               Handshake         Client Hello
  53 3.548057  0.059854000  23.202.163.2   192.168.20.12  TCP           66          64768  0.059854000                   443 → 55287 [ACK] Seq=1 Ack=518 Win=64768 Le
  54 3.550508  0.002451000  23.202.163.2   192.168.20.12  TLSv1.3     1484   1418   64768               Handshake,Chan…   Server Hello, Change Cipher Spec, Applicatio
  55 3.550875  0.000367000  23.202.163.2   192.168.20.12  TLSv1.3     1484   2836   64768                                 Continuation Data
  56 3.550877  0.000002000  23.202.163.2   192.168.20.12  TLSv1.3     1326   4096   64768                                 Continuation Data
  57 3.551319  0.000442000  192.168.20.12  23.202.163.2   TCP           66         130432  0.000811000                   55287 → 443 [ACK] Seq=518 Ack=1419 Win=13043
  58 3.551472  0.000153000  192.168.20.12  23.202.163.2   TCP           66         128384  0.000595000                   55287 → 443 [ACK] Seq=518 Ack=4097 Win=12838
  59 3.551720  0.000248000  23.202.163.2   192.168.20.12  TLSv1.3     1484   1418   64768                                 Continuation Data
```

```
    Cipher Suites Length: 42
  > Cipher Suites (21 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 393
  > Extension: Reserved (GREASE) (len=0)
  ⌄ Extension: server_name (len=25)
      Type: server_name (0)
      Length: 25
    ⌄ Server Name Indication extension
        Server Name list length: 23
        Server Name Type: host_name (0)
        Server Name length: 20
        Server Name: gsp-ssl.ls.apple.com
  > Extension: extended_master_secret (len=0)
  > Extension: renegotiation_info (len=1)
  > Extension: supported_groups (len=12)
  > Extension: ec_point_formats (len=2)
  > Extension: session_ticket (len=0)
  > Extension: application_layer_protocol_negotiation (len=14)
  > Extension: status_request (len=5)
  > Extension: signature_algorithms (len=24)
  > Extension: signed_certificate_timestamp (len=0)
  > Extension: key_share (len=43)
```

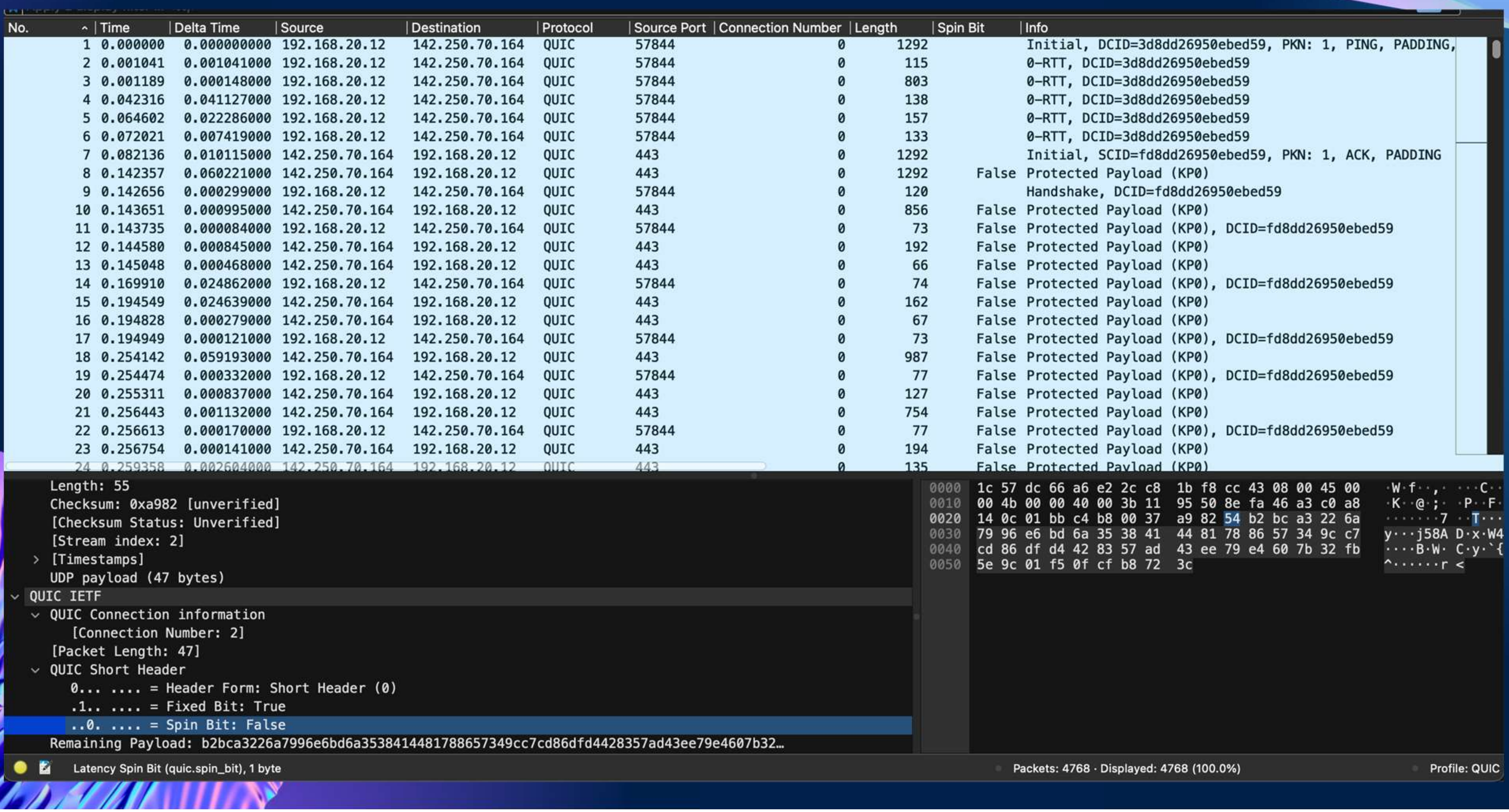
```
0090  ca ca 13 01 13 02 13 03  c0 2c c0 2b cc a9 c0 30   ········ ·,·+···
00a0  c0 2f cc a8 c0 0a c0 09  c0 14 c0 13 00 9d 00 9c   ·/······ ·······
00b0  00 35 00 2f c0 08 c0 12  00 0a 01 00 01 89 9a 9a   ·5·/···· ·······
00c0  00 00 00 00 00 19 00 17  00 00 14 67 73 70 2d 73   ········ ···gsp
00d0  73 6c 2e 6c 73 2e 61 70  70 6c 65 2e 63 6f 6d 00   sl.ls.ap ple.co
00e0  17 00 00 ff 01 00 01 00  00 0a 00 0c 00 0a 6a 6a   ········ ·······
00f0  00 1d 00 17 00 18 00 19  00 0b 00 02 01 00 00 23   ········ ·······
0100  00 00 00 10 00 0e 00 0c  02 68 32 08 68 74 74 70   ········ ·h2·ht
0110  2f 31 2e 31 00 05 00 05  01 00 00 00 00 00 0d 00   /1.1···· ·······
0120  18 00 16 04 03 08 04 04  01 05 03 02 03 08 05 08   ········ ·······
0130  05 05 01 08 06 06 01 02  01 00 12 00 00 00 33 00   ········ ·······
0140  2b 00 29 6a 6a 00 01 00  00 1d 00 20 54 7b 9a 93   +·)jj··· ··· T{
0150  66 fb 3e 82 78 78 c6 65  f0 8c 2f 95 e4 59 c3 7b   f·>·xx·e ··/··Y
0160  bb 54 fd a3 68 6b 52 3a  4e 27 ee 35 00 2d 00 02   ·T··hkR: N'·5·-
0170  01 01 00 2b 00 0b 0a ba  ba 03 04 03 03 03 02 03   ···+···· ·······
0180  01 00 1b 00 03 02 00 01  1a 1a 00 01 00 00 15 00   ········ ·······
0190  b6 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
01a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
01b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
01c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
01d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
01e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
01f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
0200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
0210  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
0220  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
0230  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ·······
0240  00 00 00 00 00 00 00                               ·······
```

Server Name (tls.handshake.extensions_server_name), 20 bytes

Packets: 1958 · Displayed: 406 (20.7%) · Dropped: 0 (0.0%)

Profile: TLS

Evolution Cyber – QUIC



```
No.      Time     Delta Time   Source          Destination     Protocol  Source Port  Connection Number  Length  Spin Bit  Info
      1 0.000000  0.000000000 192.168.20.12   142.250.70.164  QUIC      57844                        0   1292            Initial, DCID=3d8dd26950ebed59, PKN: 1, PING, PADDING,
      2 0.001041  0.001041000 192.168.20.12   142.250.70.164  QUIC      57844                        0    115            0-RTT, DCID=3d8dd26950ebed59
      3 0.001189  0.000148000 192.168.20.12   142.250.70.164  QUIC      57844                        0    803            0-RTT, DCID=3d8dd26950ebed59
      4 0.042316  0.041127000 192.168.20.12   142.250.70.164  QUIC      57844                        0    138            0-RTT, DCID=3d8dd26950ebed59
      5 0.064602  0.022286000 192.168.20.12   142.250.70.164  QUIC      57844                        0    157            0-RTT, DCID=3d8dd26950ebed59
      6 0.072021  0.007419000 192.168.20.12   142.250.70.164  QUIC      57844                        0    133            0-RTT, DCID=3d8dd26950ebed59
      7 0.082136  0.010115000 142.250.70.164  192.168.20.12   QUIC      443                          0   1292            Initial, SCID=fd8dd26950ebed59, PKN: 1, ACK, PADDING
      8 0.142357  0.060221000 142.250.70.164  192.168.20.12   QUIC      443                          0   1292     False  Protected Payload (KP0)
      9 0.142656  0.000299000 192.168.20.12   142.250.70.164  QUIC      57844                        0    120            Handshake, DCID=fd8dd26950ebed59
     10 0.143651  0.000995000 142.250.70.164  192.168.20.12   QUIC      443                          0    856     False  Protected Payload (KP0)
     11 0.143735  0.000084000 192.168.20.12   142.250.70.164  QUIC      57844                        0     73     False  Protected Payload (KP0), DCID=fd8dd26950ebed59
     12 0.144580  0.000845000 142.250.70.164  192.168.20.12   QUIC      443                          0    192     False  Protected Payload (KP0)
     13 0.145048  0.000468000 142.250.70.164  192.168.20.12   QUIC      443                          0     66     False  Protected Payload (KP0)
     14 0.169910  0.024862000 192.168.20.12   142.250.70.164  QUIC      57844                        0     74     False  Protected Payload (KP0), DCID=fd8dd26950ebed59
     15 0.194549  0.024639000 142.250.70.164  192.168.20.12   QUIC      443                          0    162     False  Protected Payload (KP0)
     16 0.194828  0.000279000 142.250.70.164  192.168.20.12   QUIC      443                          0     67     False  Protected Payload (KP0)
     17 0.194949  0.000121000 192.168.20.12   142.250.70.164  QUIC      57844                        0     73     False  Protected Payload (KP0), DCID=fd8dd26950ebed59
     18 0.254142  0.059193000 142.250.70.164  192.168.20.12   QUIC      443                          0    987     False  Protected Payload (KP0)
     19 0.254474  0.000332000 192.168.20.12   142.250.70.164  QUIC      57844                        0     77     False  Protected Payload (KP0), DCID=fd8dd26950ebed59
     20 0.255311  0.000837000 142.250.70.164  192.168.20.12   QUIC      443                          0    127     False  Protected Payload (KP0)
     21 0.256443  0.001132000 142.250.70.164  192.168.20.12   QUIC      443                          0    754     False  Protected Payload (KP0)
     22 0.256613  0.000170000 192.168.20.12   142.250.70.164  QUIC      57844                        0     77     False  Protected Payload (KP0), DCID=fd8dd26950ebed59
     23 0.256754  0.000141000 142.250.70.164  192.168.20.12   QUIC      443                          0    194     False  Protected Payload (KP0)
     24 0.259358  0.002604000 142.250.70.164  192.168.20.12   QUIC      443                          0    135     False  Protected Payload (KP0)
```

```
    Length: 55
    Checksum: 0xa982 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
    UDP payload (47 bytes)
v QUIC IETF
  v QUIC Connection information
      [Connection Number: 2]
    [Packet Length: 47]
  v QUIC Short Header
      0... .... = Header Form: Short Header (0)
      .1.. .... = Fixed Bit: True
      ..0. .... = Spin Bit: False
    Remaining Payload: b2bca3226a7996e6bd6a35384144817886573 49cc7cd86dfd4428357ad43ee79e4607b32…
```

```
0000  1c 57 dc 66 a6 e2 2c c8  1b f8 cc 43 08 00 45 00   ·W·f··,·  ···C··E·
0010  00 4b 00 00 40 00 3b 11  95 50 8e fa 46 a3 c0 a8   ·K··@·;·  ·P··F···
0020  14 0c 01 bb c4 b8 00 37  a9 82 54 b2 bc a3 22 6a   ·······7  ··T···"j
0030  79 96 e6 bd 6a 35 38 41  44 81 78 86 57 34 9c c7   y···j58A  D·x·W4··
0040  cd 86 df d4 42 83 57 ad  43 ee 79 e4 60 7b 32 fb   ····B·W·  C·y·`{2·
0050  5e 9c 01 f5 0f cf b8 72  3c                        ^······r  <
```

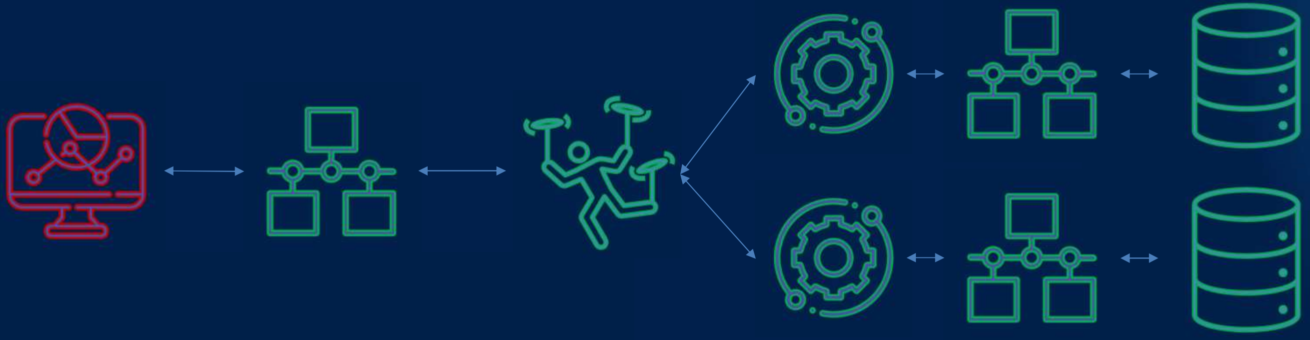
Latency Spin Bit (quic.spin_bit), 1 byte

Packets: 4768 · Displayed: 4768 (100.0%)

Profile: QUIC

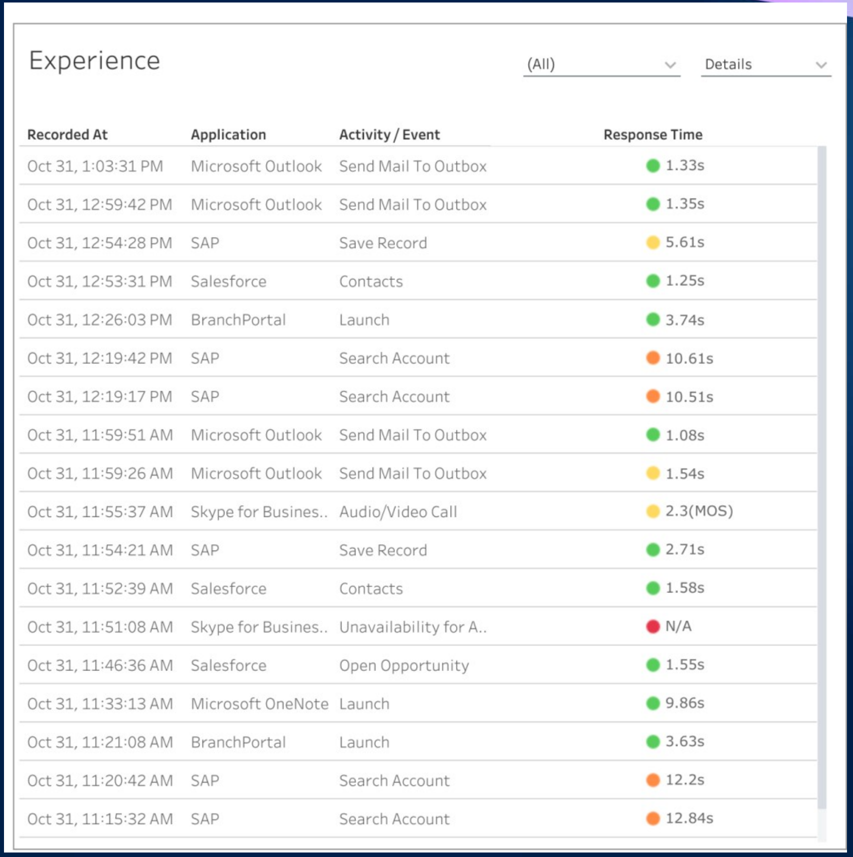
Better Observability

The Point of Consumption



The Point of Consumption

1. Endpoint Agents
2. JavaScript Injection
3. Twitter

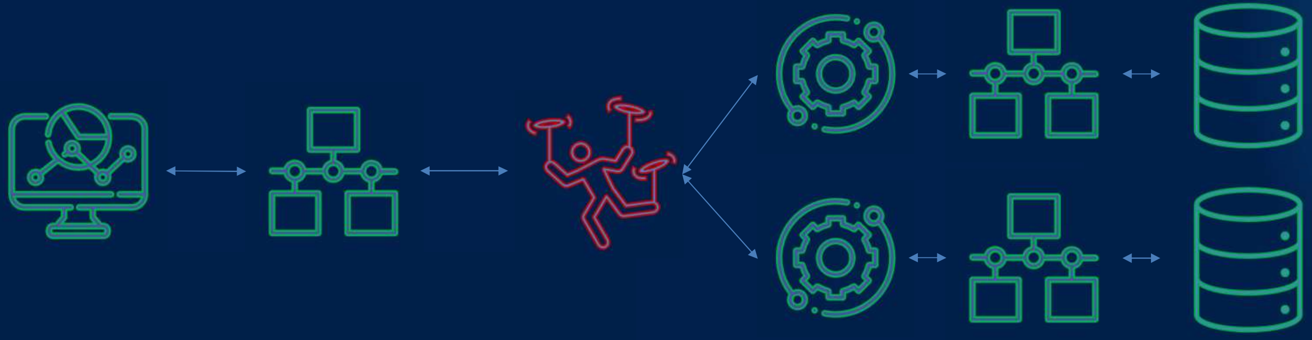


Experience

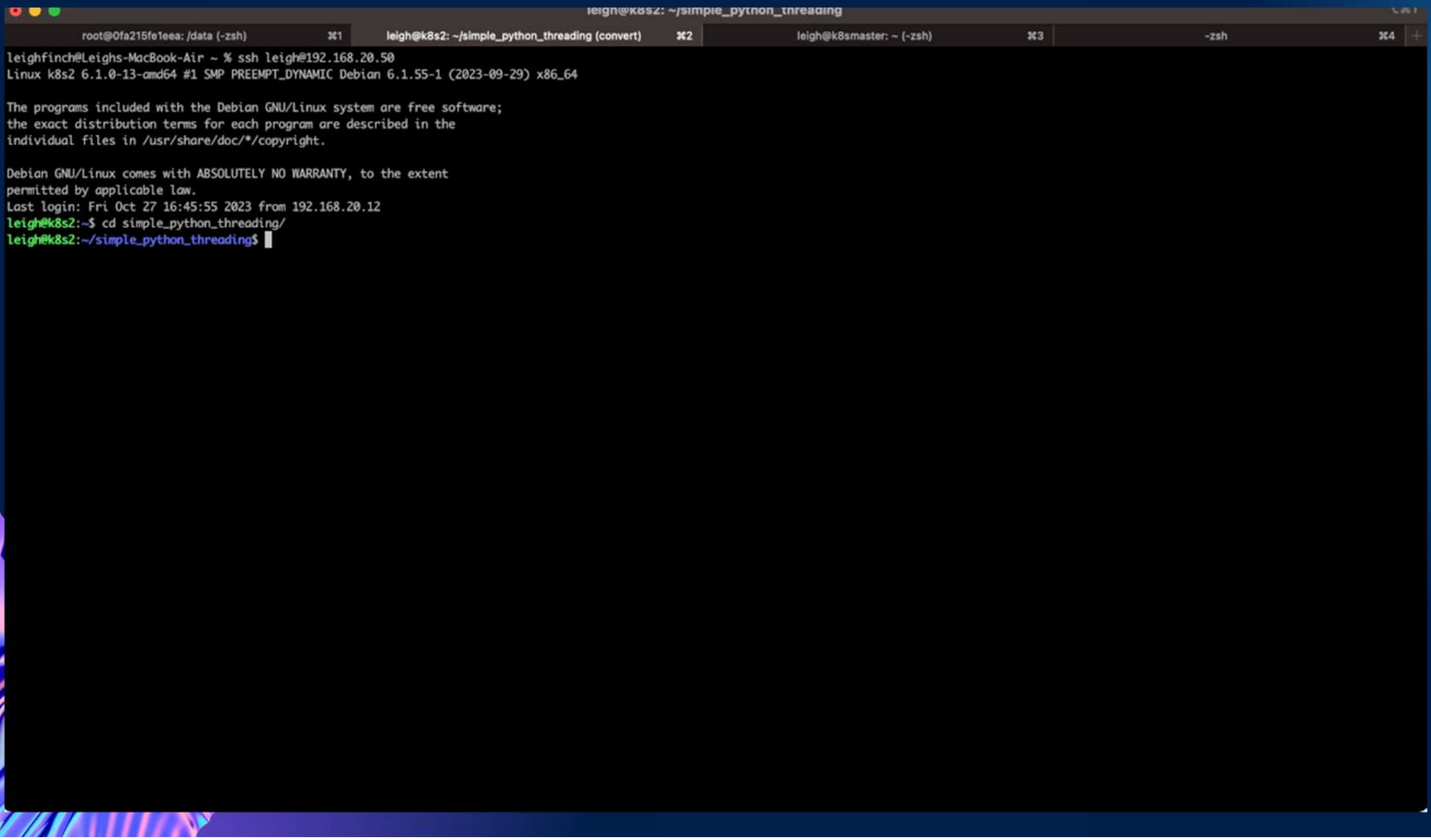
(All) ⌄ Details ⌄

Recorded At	Application	Activity / Event	Response Time
Oct 31, 1:03:31 PM	Microsoft Outlook	Send Mail To Outbox	🟢 1.33s
Oct 31, 12:59:42 PM	Microsoft Outlook	Send Mail To Outbox	🟢 1.35s
Oct 31, 12:54:28 PM	SAP	Save Record	🟡 5.61s
Oct 31, 12:53:31 PM	Salesforce	Contacts	🟢 1.25s
Oct 31, 12:26:03 PM	BranchPortal	Launch	🟢 3.74s
Oct 31, 12:19:42 PM	SAP	Search Account	🟠 10.61s
Oct 31, 12:19:17 PM	SAP	Search Account	🟠 10.51s
Oct 31, 11:59:51 AM	Microsoft Outlook	Send Mail To Outbox	🟢 1.08s
Oct 31, 11:59:26 AM	Microsoft Outlook	Send Mail To Outbox	🟡 1.54s
Oct 31, 11:55:37 AM	Skype for Busines..	Audio/Video Call	🟡 2.3(MOS)
Oct 31, 11:54:21 AM	SAP	Save Record	🟢 2.71s
Oct 31, 11:52:39 AM	Salesforce	Contacts	🟢 1.58s
Oct 31, 11:51:08 AM	Skype for Busines..	Unavailability for A..	🔴 N/A
Oct 31, 11:46:36 AM	Salesforce	Open Opportunity	🟢 1.55s
Oct 31, 11:33:13 AM	Microsoft OneNote	Launch	🟢 9.86s
Oct 31, 11:21:08 AM	BranchPortal	Launch	🟢 3.63s
Oct 31, 11:20:42 AM	SAP	Search Account	🟠 12.2s
Oct 31, 11:15:32 AM	SAP	Search Account	🟠 12.84s

The Point of Distribution

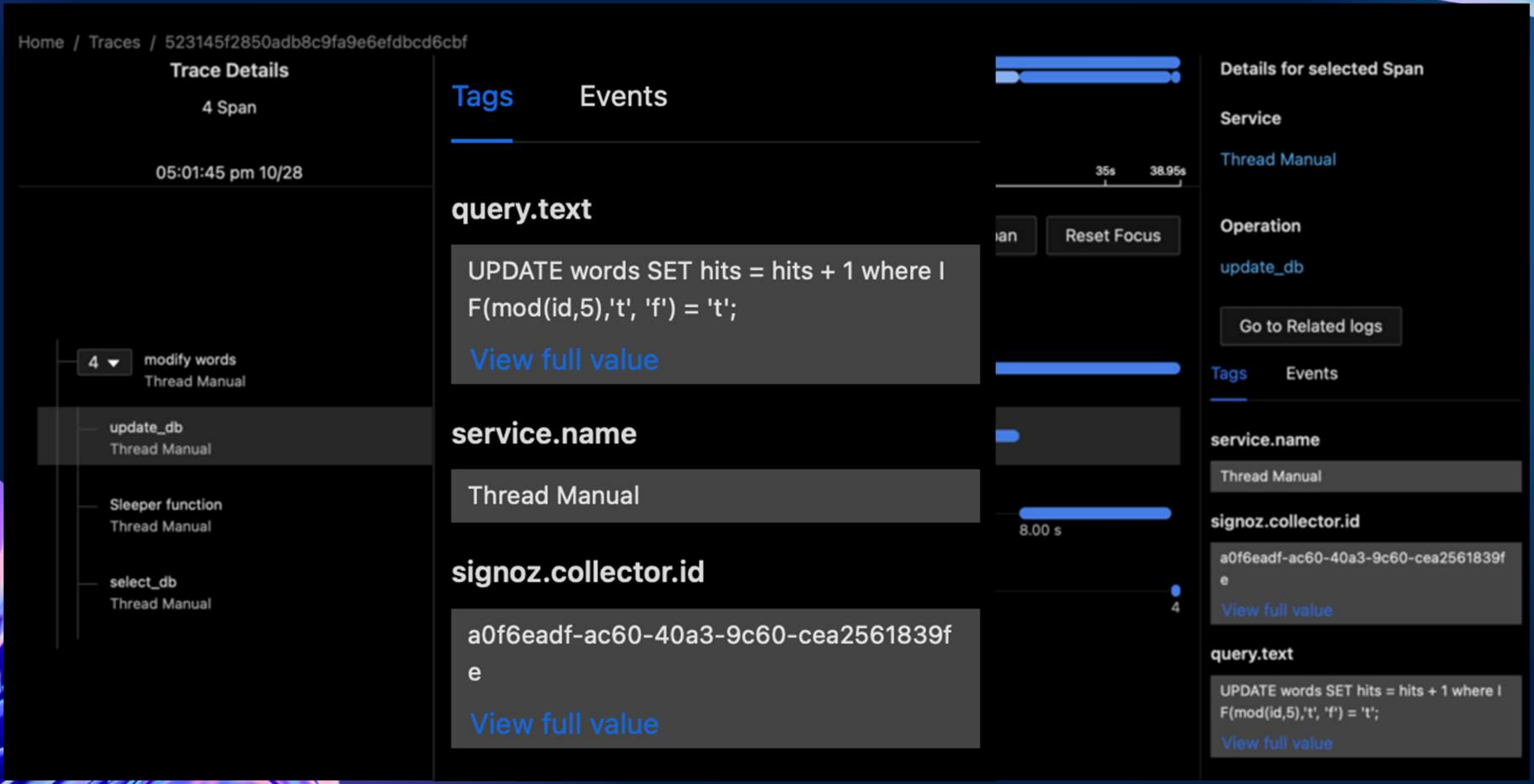


Logs and Traces


leigh@k8s2: ~/simple_python_threading
root@0fa215fe1eea: /data (-zsh) ⌘1
leigh@k8s2: ~/simple_python_threading (convert) ⌘2
leigh@k8smaster: ~ (-zsh) ⌘3
-zsh ⌘4

```
leighfinch@Leighs-MacBook-Air ~ % ssh leigh@192.168.20.50
Linux k8s2 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct 27 16:45:55 2023 from 192.168.20.12
leigh@k8s2:~$ cd simple_python_threading/
leigh@k8s2:~/simple_python_threading$ 
```

Logs and Traces



Home / Traces / 523145f2850adb8c9fa9e6efdbcd6cbf

Trace Details

4 Span

05:01:45 pm 10/28

query.text

UPDATE words SET hits = hits + 1 where I F(mod(id,5),'t', 'f') = 't';

service.name

Thread Manual

signoz.collector.id

a0f6eadf-ac60-40a3-9c60-cea2561839f e

Details for selected Span

Service

Thread Manual

Operation

update_db

service.name

Thread Manual

signoz.collector.id

a0f6eadf-ac60-40a3-9c60-cea2561839f e

query.text

UPDATE words SET hits = hits + 1 where I F(mod(id,5),'t', 'f') = 't';

Metrics, Logs, and Traces

Layer	Examples
Application	Tracing, logs, OpenTelemetry
Presentation	eBPF trace, logs
Session	eBPF trace, ETL tracing
Transport	eBPF trace, tcpdump
Network	eBPF trace, tcpdump, netflow
Data-Link	Logs MAC flip, SNMP
Physical	Logs link flaps, SNMP

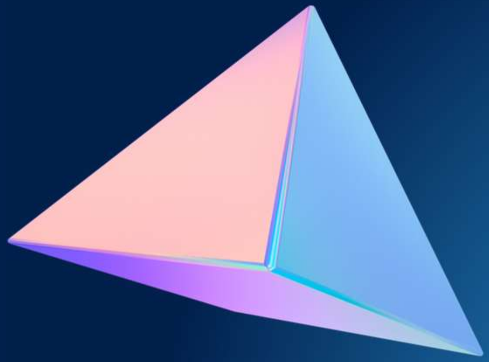
Next Generation Observability

Next Generation Observability

eBPF

OpenTelemetry

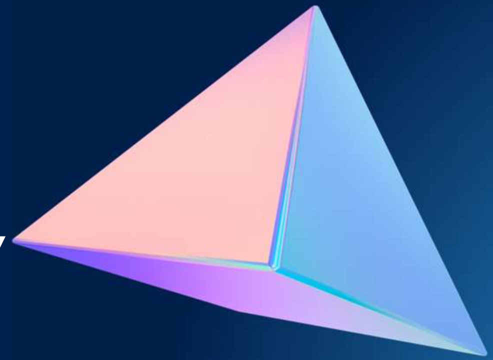
Streaming
Telemetry



eBPF

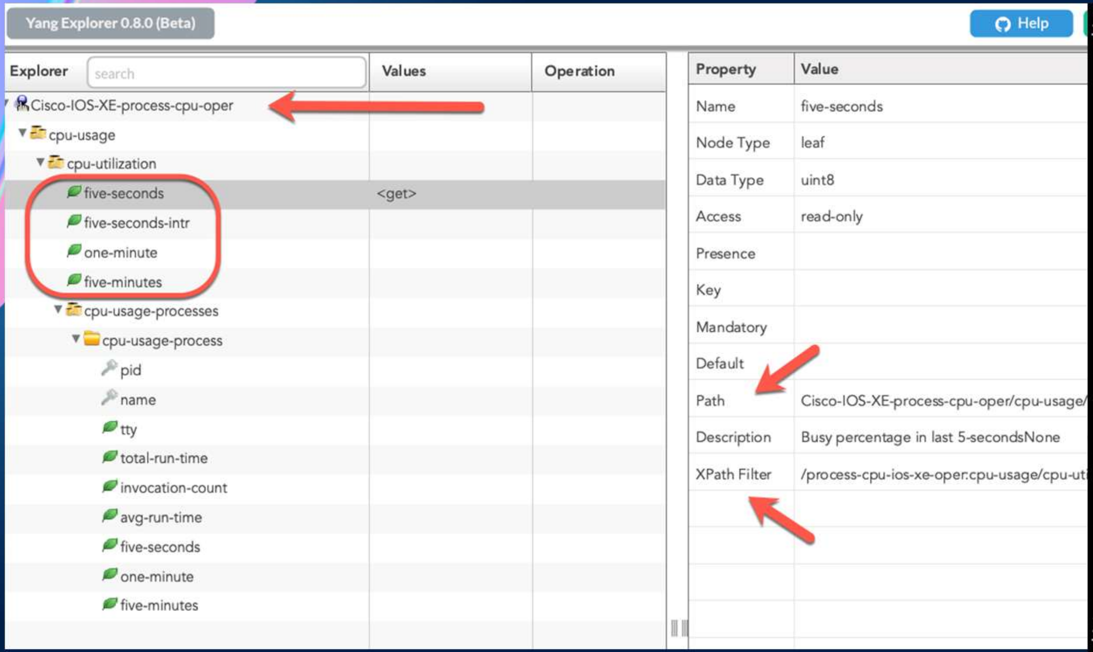
- Ability to run user code within the kernel
- Ability to intercept and modify traffic
- Trace system calls
- Ability to observe anything in the kernel

OpenTelemetry



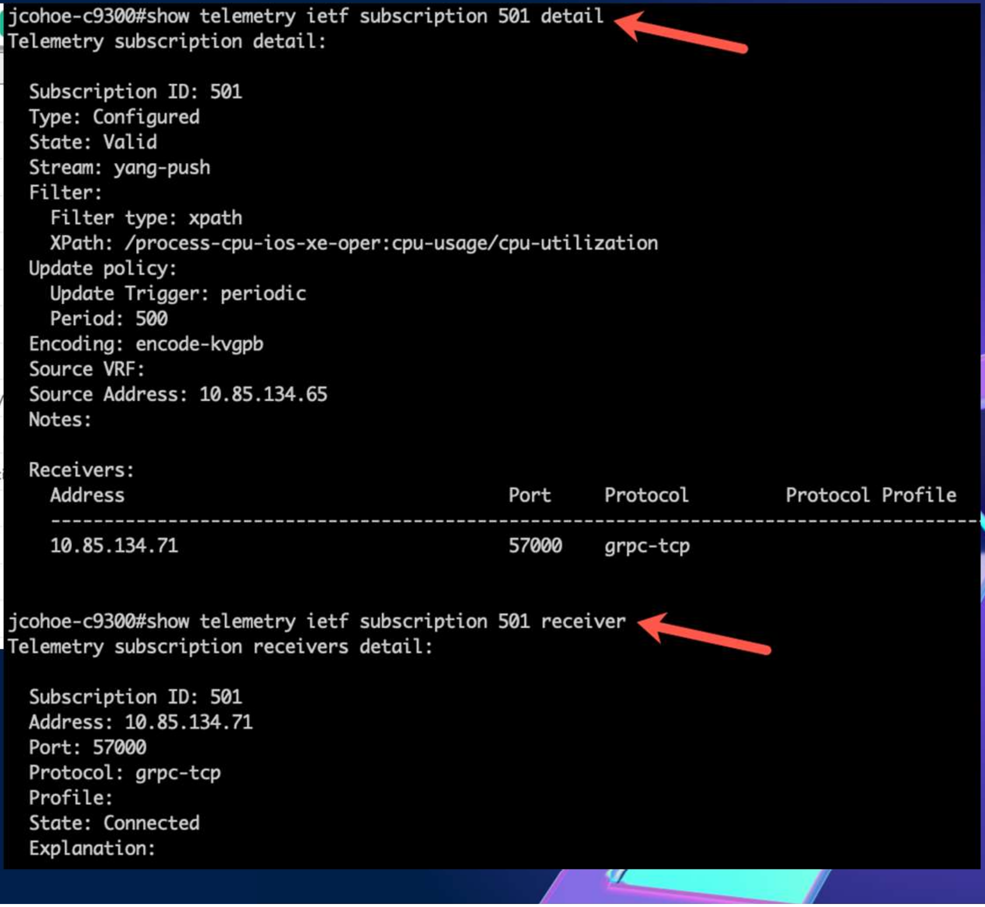
- Open standard for APM
- Defines the protocols for MLT
- Includes working code to consume telemetry

Streaming Telemetry

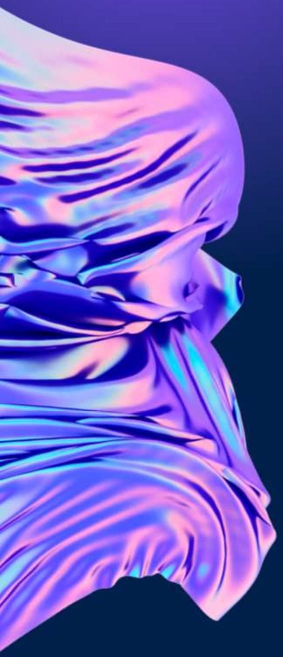


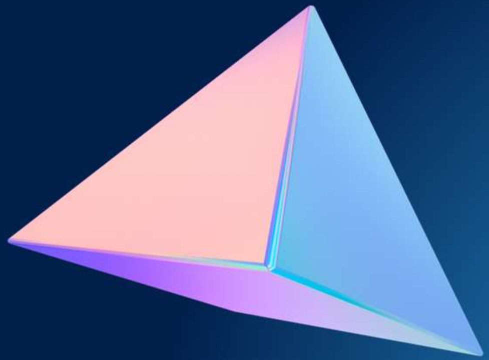
- Cisco-IOS-XE-process-cpu-oper
  - cpu-usage
    - cpu-utilization
      - five-seconds <get>
      - five-seconds-intr
      - one-minute
      - five-minutes
    - cpu-usage-processes
      - cpu-usage-process
        - pid
        - name
        - tty
        - total-run-time
        - invocation-count
        - avg-run-time
        - five-seconds
        - one-minute
        - five-minutes

Property	Value
Name	five-seconds
Node Type	leaf
Data Type	uint8
Access	read-only
Presence	
Key	
Mandatory	
Default	
Path	Cisco-IOS-XE-process-cpu-oper/cpu-usage/
Description	Busy percentage in last 5-secondsNone
XPath Filter	/process-cpu-ios-xe-oper:cpu-usage/cpu-ut



```
jcohoe-c9300#show telemetry ietf subscription 501 detail
Telemetry subscription detail:

  Subscription ID: 501
  Type: Configured
  State: Valid
  Stream: yang-push
  Filter:
    Filter type: xpath
    XPath: /process-cpu-ios-xe-oper:cpu-usage/cpu-utilization
  Update policy:
    Update Trigger: periodic
    Period: 500
  Encoding: encode-kvgpb
  Source VRF:
  Source Address: 10.85.134.65
  Notes:

  Receivers:
    Address                                   Port     Protocol         Protocol Profile
    ------------------------------------------------------------------------------------
    10.85.134.71                              57000    grpc-tcp


jcohoe-c9300#show telemetry ietf subscription 501 receiver
Telemetry subscription receivers detail:

  Subscription ID: 501
  Address: 10.85.134.71
  Port: 57000
  Protocol: grpc-tcp
  Profile:
  State: Connected
  Explanation:
```





Summary

- An Open Letter
- How do we Observe
- Challenges
- Better Observability
- Next Generation Observability

Thank You

@Leighfinch1

Leigh.finch@observeability.com.au

www.observeability.com.au

riverbed

UTS

Defense Business Board Report