(Yet another) Analysis of MLWE's performance impact on specific TLS Use-cases

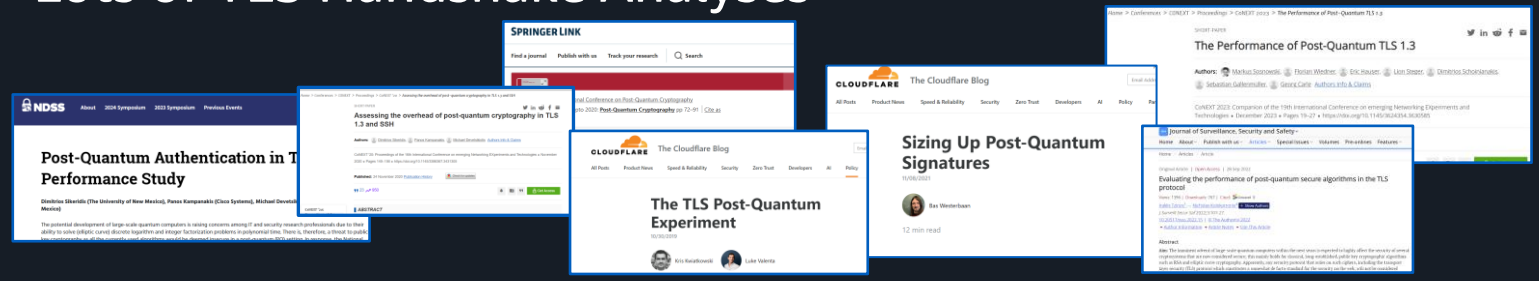
Panos Kampanakis

Principal Security Engineer

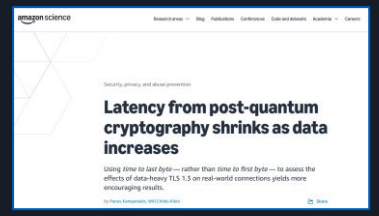
AWS

Previous Work

Lots of TLS Handshake Analyses



Time-To-Last-Byte Analysis



Web Analyses

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

This preso

Three AWS specific Examples

WebPage Experiments and Results

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The Performance Issue

MLWE in secure transport protocols means

ML-KEM: +1KB client ⟶ server
+1KB server ⟶ client
ML-DSA: +15 KB cert chain

Noticeable Application Performance Degradation ?

More data on the wire. ✓
Storage cost (e.g. Certificate Transparency immutable logs) ✓

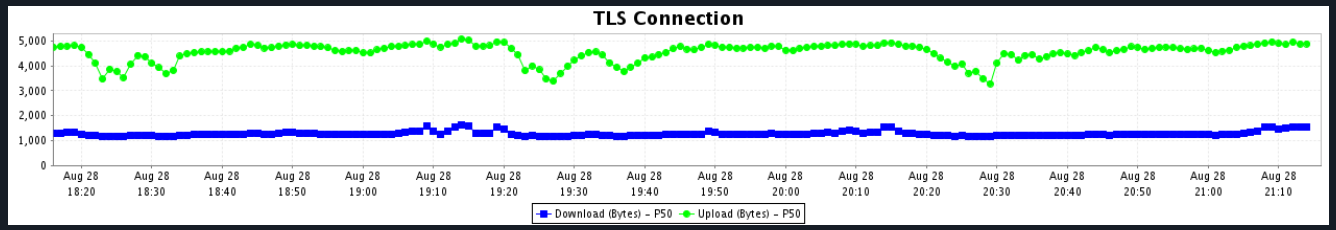
aws
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Three AWS specific Examples

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

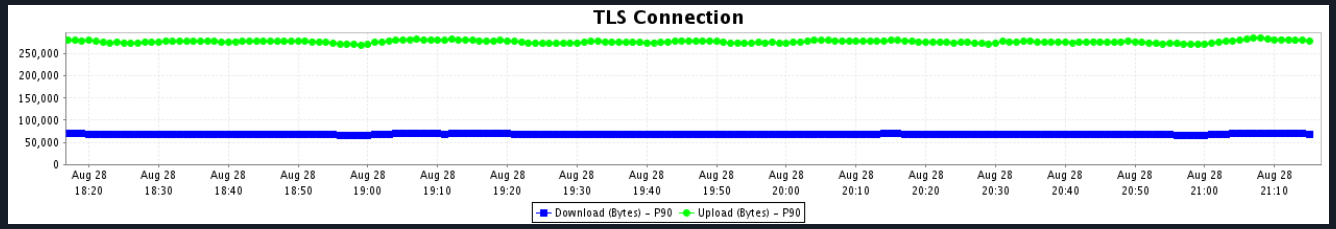
Example – AWS “Service1” (some region)

Download, Upload Conn Sizes - 50th percentile



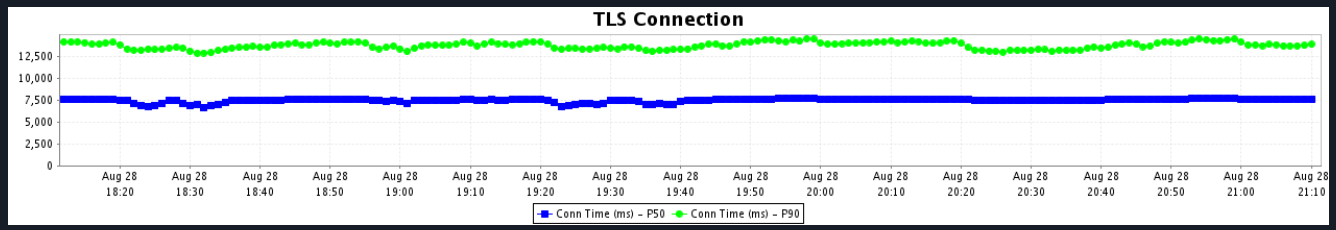
4-5KB / conn up
1KB / conn down
4-5ms / handshake

Download, Upload Conn Sizes – 90th percentile



275KB / conn up
75KB / conn down
12ms / handshake
100 reqs / conn

Total Conn Time (50th, 90th percentile)

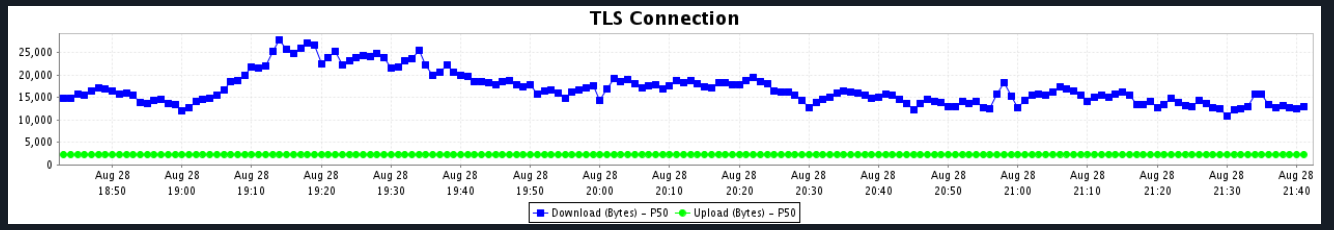


7.5s @ 50th
12.5s @ 90th

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

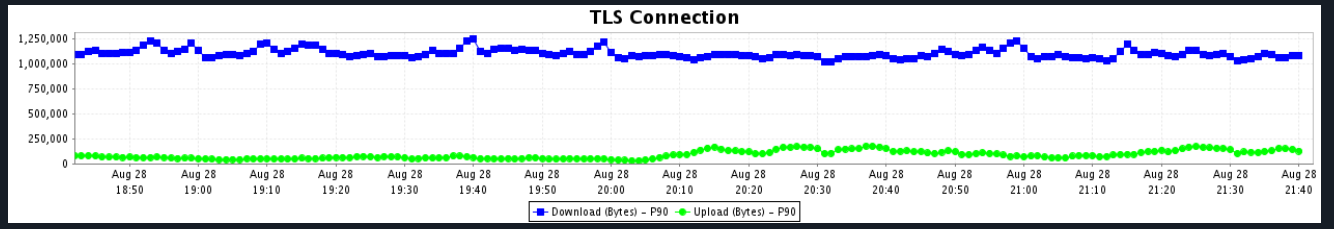
Example – AWS “Service2” (some region)

Download, Upload Conn Sizes – 50th percentile



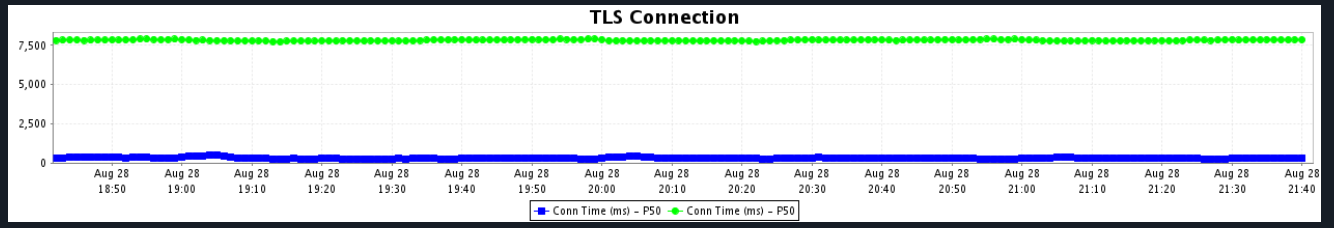
2KB / conn up
15KB / conn down
5ms / handshake

Download, Upload Conn Sizes – 90th percentile



100KB / conn up
1MB / conn down
3-4 reqs / conn
22ms / handshake

Total Conn Time (50th, 90th percentile)

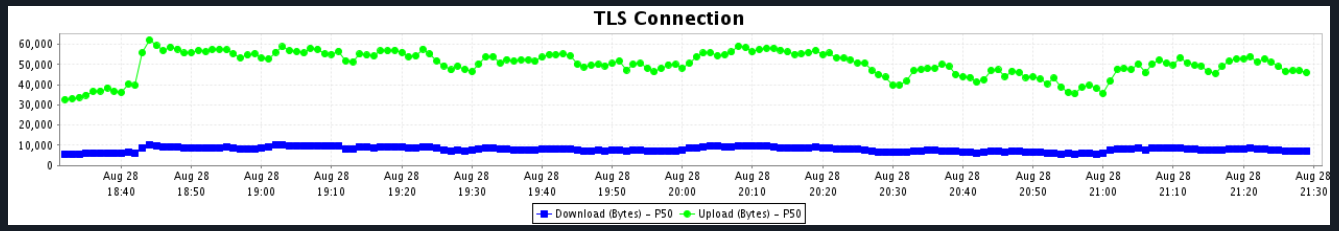


300ms @ 50th
7.5s @ 90th

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

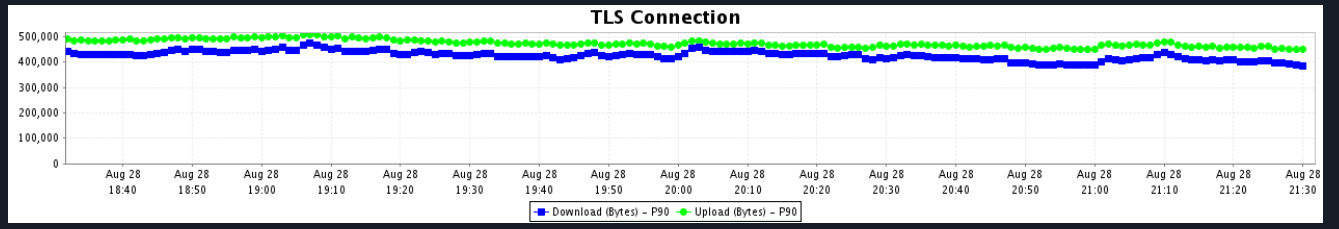
Example – AWS “Service3” (some region)

Download, Upload Conn Sizes – 50th percentile



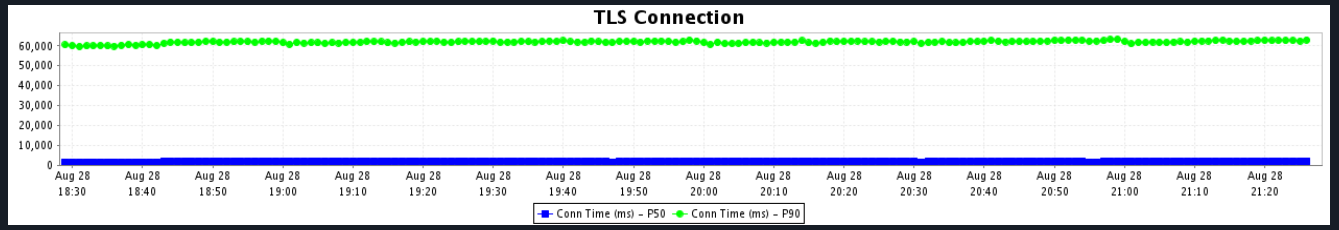
50KB / conn up
10KB / conn down
75 reqs / conn
3ms / handshake

Download, Upload Conn Sizes – 90th percentile



500KB / conn up
400KB / conn down
80 reqs / conn
10ms / handshake

Total Conn Time (50th, 90th percentile)



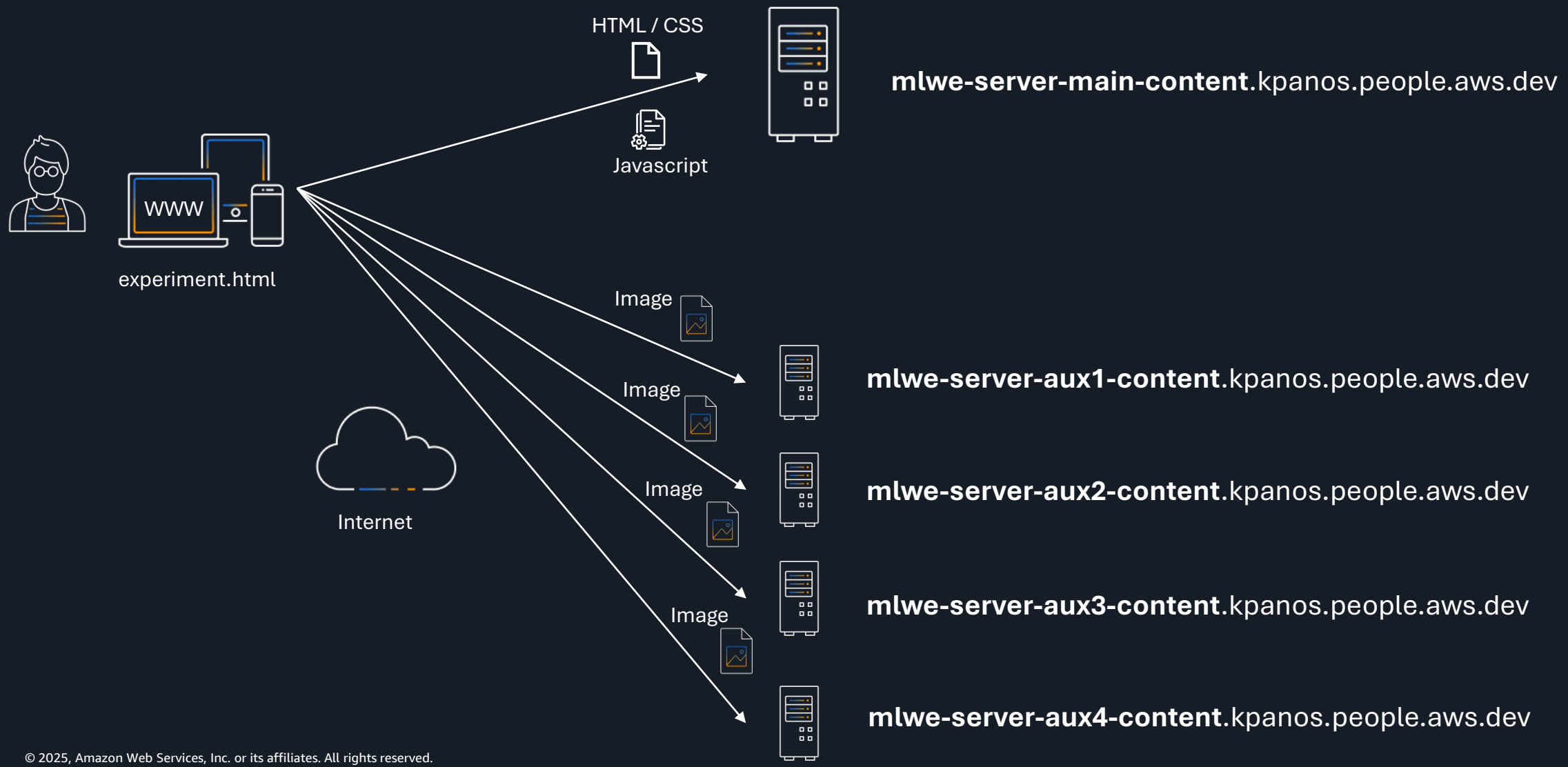
1s @ 50th
60s @ 90th

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

And now the Web

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Experimental Setup



aws
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The (pessimistic) Experimental Webpage

https://mlwe-server-main-content.kpanos.people.aws.dev/nocache/experiment.html

clock.js
Javascript

25 or 50 KB

loadcontent.js
Javascript

3 KB

HTML
CSS

25 or 50 KB

(fetched from different server)

5 or 25 KB

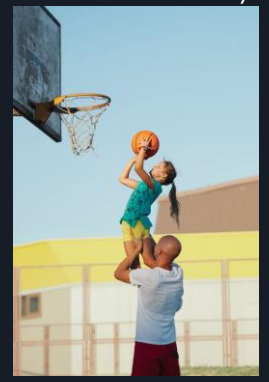
(fetched from different server)

5 or 25 KB

favicon.ico

1KB

(fetched from different server)



25 or 45 KB

(fetched from different server)

5 or 25 KB

Omitted if the browser has them cached.

Uncached

Total KB: 221 (large) or 91 (small)

Total Conn #: 6 (large) or 5 (small)

Cached

Total KB: 100 (large) or 51 (small)

Total Conn #: 2 (large) or 1 (small)

aws

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

(X25519 + RSA) vs (X25519MLKEM768 + MLDSA65)

(Pessimistic scenario, no “cert chain trimming”)

Web Metrics Measured

by webpagetest.org
(100 page loads)

- Main server TLS handshake (200 page loads)
- Time-To-First-Byte (TTFB)
- Largest (and First) Contentful Paint (LCP)
- Load time
- Fully loaded time
- CLS

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Performance (pessimistic) Results – "Cable"

5/1 Mbps, 28ms RTT

Multiple Parallel Conns

Parallel Conns

	TLS handshake		TTFB		LCP		Load Time		Fully Loaded Time		CLS	
	50th	90th	50th	90th	50th	90th	50th	90th	50th	90th	50th	90th
Small Page: 51 KB – 1 conn – caching	+47%	+42%	+13%	+5.9%	+2.4% (11ms)	+0.9% (+4ms)	+6.3% (+26ms)	+6.3% (+29ms)	+6.3% (+26ms)	+6.3% (+29ms)	0%	+114%
Small Page: 91 KB – 5 conns (2 lazy loaded)			+11%	+9%	+5.7% (+21ms)	+0.9% (+4ms)	+11% (+69ms)	+8.2% (+58ms)	+12% (+103ms)	+9.6% (+90ms)	0%	0%
Large Page: 100 KB – 2 conns – caching	+49%	+76%	+14%	+8.1%	+0.3% (+1ms)	+2.2% (+9ms)	+5.4% (+27ms)	+6.8% (+37ms)	+5.4% (+27ms)	+6.8% (+37ms)	0%	0%
Large Page: 221 KB – 6 conns (2 lazy loaded)			+16%	+4.5%	+8% (+29ms)	+2.7% (+12ms)	+7.0% (+54ms)	+6.0% (+50ms)	+8.6% (+88ms)	+5.5% (+61ms)	0%	0%

Sequential Conns

82nd: +58%
95th: +30%

+29ms on 363ms
(<2500ms is GOOD)

+69ms on 634ms

CLS went from 0.81 to 0.173
(>100ms is NEEDS IMPROVEMENT)

+103ms on 944ms

© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Performance (pessimistic) Results – "4G"

9/9 Mbps, 170 ms RTT

Multiple Parallel Conns

Parallel Conns

Small Page

Large Page

Sequential Conns

	TLS handshake		TTFB		LCP		Load Time		Fully Loaded Time		CLS	
	50th	90th	50th	90th	50th	90th	50th	90th	50th	90th	50th	90th
51 KB – 1 conn – caching	+8.8%	+12%	+2.3%	+2.6%	+2% (18ms)	+0.6%	+1.6%	+0.9%	+1.6%	+0.9%	0%	0%
91 KB – 5 conns (2 lazy loaded)			+1.7%	-5.7%	+0.6%	-2.9%	+1.4%	+3.7% (+76ms)	+2.8% (+75ms)	+4.5% (+128ms)	0%	0%
100 KB – 2 conns – caching	+8.8%	+10%	+2.1%	+1.9%	+2.3% (+21ms)	+1.5% (+14ms)	+1.7%	+1.4%	+1.7%	+1.4%	0%	0%
221 KB – 6 conns (2 lazy loaded)			+2.1%	-13%	+0.4%	-4.7%	+0.6%	-2.6%	+0.4%	-1.6%	0%	0%

86th : +1%
98th : + 0%

74nd: 0%
98th: -8%

74th : +0.4%
97th : +4.9%

72nd: 0%
98th: +2%

+76ms on 1298ms

+128ms on 2811ms

aws

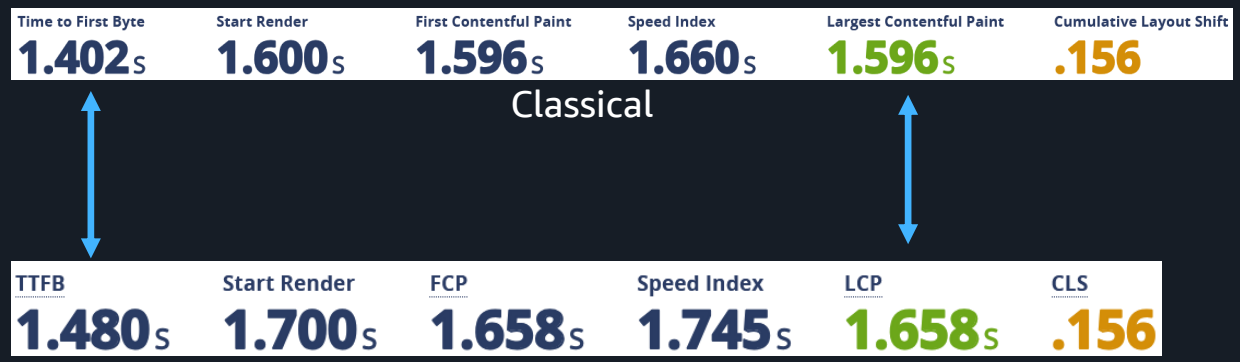
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

(Qualitative) Performance Results – “2G”, “3G”

Small cached webpage (51KB, 1 conn)

2G - 280/256 Kbps, 800ms RTT

3G - 1600/768 Kbps, 300ms RTT



© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Takeaways

MLWE puts more data on the wire;
trimming it is beneficial,
session resumption is great!

Not all use-cases are web use-cases and
could use MLWE fine.

MLWE impact on web performance metrics may be overestimated;
web clients spend little time on TLS handshaking;
the Internet is “unstable”;
longer RTTs amortize MLWE’s cost;
parallel fetching alleviates MLWE’s cost per conn;
performance under slow conditions is already bad;
chubby pages won’t be hurt by MLWE.

aws
© 2025, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you

Panos Kampanakis

kpanos@amazon.com