

ECH Update

Dennis Jackson

Ongoing ECH Experiments

- Firefox Nightly since 104
- Chrome Canary since 105
- Cloudflare on a subset of domains since Dec '21

Telemetry from Firefox Nightly and Beta is public at telemetry.mozilla.org

Public Data and Tools



Firefox Public Data Report

See the activity, behavior, and hardware configuration of Firefox users.



Mozilla Public Datasets

An endpoint listing all the public datasets published by Mozilla.



Network Outages Datasets

Signals about network outages based on existing telemetry from Mozilla products.



Graphics Telemetry

Aggregated breakdowns for Firefox graphics features.



Histogram Simulator

Simulate histogram bucket widths.



Measurement Dashboard

View the legacy measure distributions and evolutions over time.



Dashboard Generator

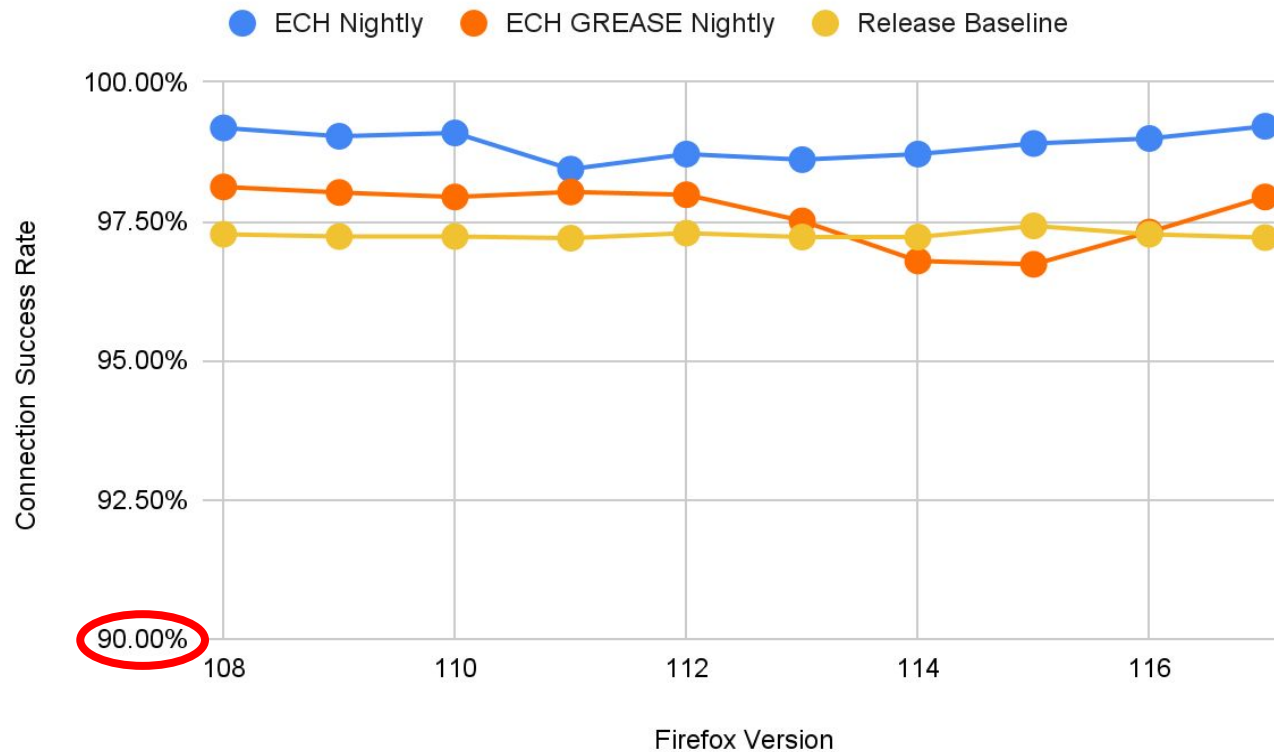
Hand-craft your own dashboard with the push of a few buttons.



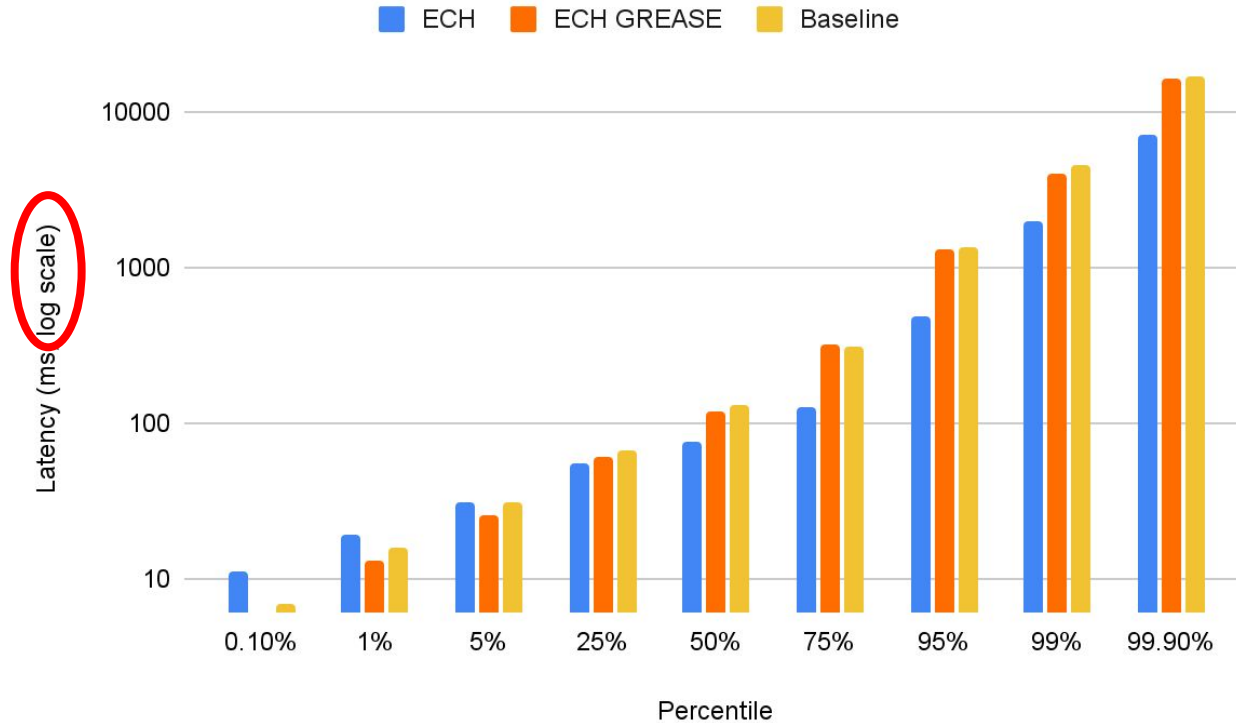
Use Counters

View usage of web features relative to page loads.

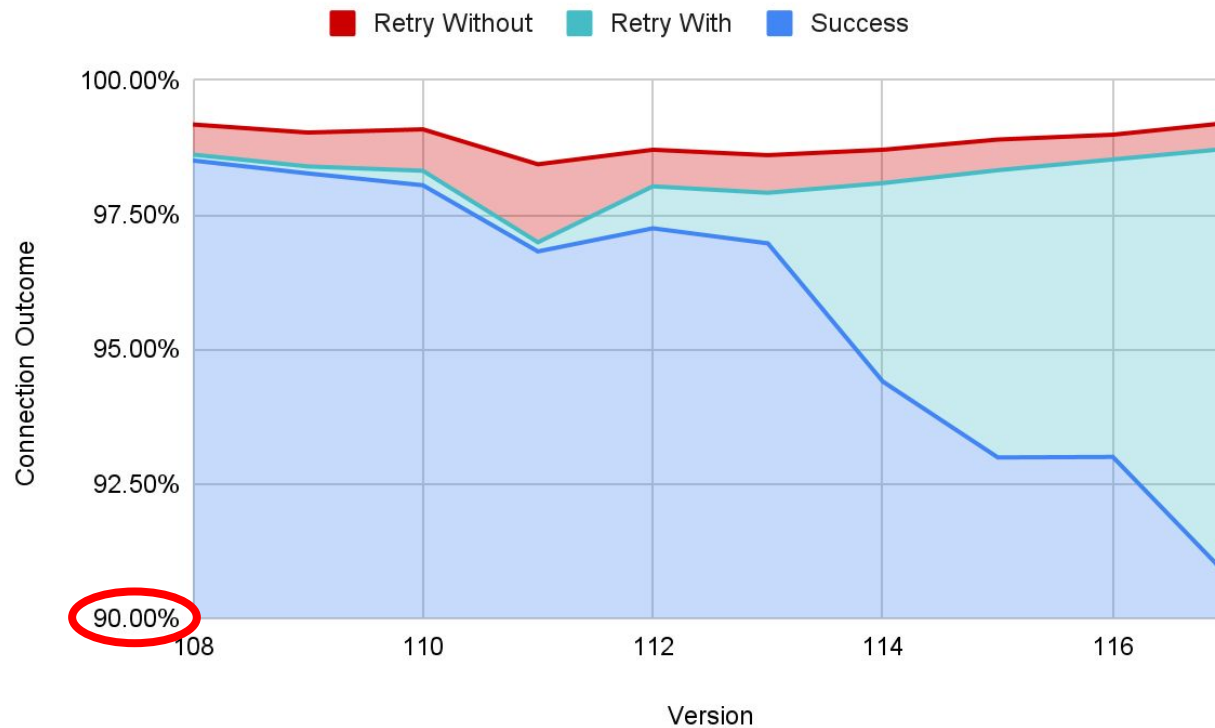
Connection Success Rate by Type



Connection Latency by Type



ECH Retry Rate



Site Incompatibility

- In April we switched Firefox Nightly into hard-fail mode.
- We are aware of 2 sites, operated by the same entity, in the Tranco top 50k which reject connections with ECH GREASE Xtns.
- Testing confirms they fail with **any** unrecognized extension due to a faulty TLS 1.2 implementation. **Not ECH specific.**
- Operator has committed to fixing issue and rolling out TLS 1.3 by September

Next Steps

- Investigating the ECH Retry issue
- Small-scale release experiments
 - Chrome announced a 1% trial between now and December
 - Firefox will be starting a 1% trial next week

FIN