Microsoft Windows DoH client

Explaining our announcement and what’s coming next

Overview

- Review Windows DoH design principles

- Explain Windows DoH first milestone

- See first milestone FAQs

- Look forward (and why we need a WG)

Windows DoH Design Principle 1

- **Windows DNS needs to be as private and functional as possible by default without the need for user or admin configuration**

- Private means not visible or modifiable by parties other than the stub (Windows) and the recursive resolver
  - Not addressing recursive to authoritative traffic

- Functional means no regression in existing “just works” nature of DNS
  - 99%+ users who know nothing about DNS or DoH should keep working
  - Power users can continue selecting their own DNS servers

Windows DoH Design Principle 2

- **Privacy-minded Windows users and administrators need to be guided to DNS settings even if they don't know what DNS is yet**
- Users who go looking for ways to limit their data being shared or gathered may not think to check DNS settings today
- DNS settings should be more clearly labeled and documented in the context of data sharing

Windows DoH Design Principle 3

- **Windows users and administrators need to be able to improve their DNS configuration with as few simple actions as possible**

- Users trying to use one DNS server everywhere they go shouldn’t have to set that DNS server for each new network they join

- Using encrypted DNS should be as simple as possible (such as on by default)

Windows DoH Design Principle 4

- **Windows users and administrators need to explicitly allow fallback from encrypted DNS once configured**

- This signal could be through UI, Group Policy, scripts, etc.

- In the absence of this signal, fallback will NOT occur
  - This prevents downgrade attacks via blocking HTTPS
  - This signal must be at the Windows level, as network-level indicators cannot be distinguished from network attacks

Windows DoH First Milestone

- Auto promotion of existing DNS servers to DoH
    - Windows will ship a list of configuration mappings (DNS IP -> DoH URI)
    - Any query destined to an address on that list will use DoH instead
    - Global on/off switch to enable/disable auto promotion

- No change to DNS server used
    - Continue to use network recommendation as default
    - Continue using DNS servers added in Control Panel and Settings app
    - Continue respecting NRPT rules
    - Continue respecting servers provided via APIs

Windows DoH First Milestone

- Pro: no change to existing server configurations (#1)
- Pro: no user input needed for improving connection integrity (#1)
- Pro: per-interface DNS servers will auto promote as well (#3)
- Pro: no fallback without device admin signal (#4)
- Pro: no app development needed to use system DoH

- Con: won’t benefit users using DoH-capable servers not on the list
  - Trade-off decision: wanting to have a slow ramp up to a future where encrypted DNS is a default path; this is the first step of many
- Con: Principle #2 is not addressed (educating users why DNS is important)
  - Trade-off decision: by waiting for a more complete encrypted DNS experience, this will be an easier conversation to have in UX

First milestone FAQs

- Why not do DoT first?
  - DoH is more compatible with scenarios such as Tommy Pauly’s Adaptive DNS
  - DoH allows us to reuse our HTTP stack
  - We’re open to DoT in future milestones based on industry feedback
- How do servers get on your DoH list?
  - Manual review for now. Please reach out to me at tojens@microsoft.com
- What’s your release timeline?
  - TBD. If you have a server you’d like us to test, please reach out!
  - Watch our blog for the latest updates: https://aka.ms/MSFTnetworkblog
- My customers use local network DNS that forwards queries to RRs…
  - We know our first milestone won’t help these customers get DoH
  - We look forward to new standards work to enable these scenarios (see next slide)

Looking forward (and why we need a WG)

- User Experience
  - Incorporate principle #2 and guide pro-privacy users to DNS UI
  - Allow DoH servers to be added like classic servers are today

- Discoverability
  - The list of URI mappings is a long-term stop gap until servers can advertise their own URIs for DoH use (or other protocols)
  - Hoping to work collaboratively on an industry-friendly way of getting DoH servers configured automatically

- Minimize parties with access to user data
  - Wide deployment of DoH and related technologies to avoid centralization
  - Intelligent approaches to server choices (Adaptive DNS and Oblivious DoH)

These should be driven by a WG or other industry-wide body to avoid one-off solutions!

Summary

- Windows is excited to bring DoH support to users
- Windows DoH auto-promotion won’t change which DNS servers you’re using
- We’re excited about creating cooperative standards that work for everyone to drive future milestone work

Please reach out with questions or follow up on DoH collaboration:

Tommy Jensen

tojens@microsoft.com

https://aka.ms/MSFTNetworkBlog