DNS Flag Day 常見問題(FAQ)

1. 何謂「DNS Flag Day」？

為了提升並確保 DNS 通訊服務能夠符合 RFC 標準，並增強 DNS 安全性和支持新功能等必要性。因此包括 Google、Cloudflare、NLnet Labs（Unbound 開發組織）、ISC（BIND 開發組織）、Facebook、Quad9、PowerDNS、Cisco 及其它的 DNS 服務供應商決議於 2019 年 2 月 1 日為 DNS Flag Day，進行刪除 EDNS0 變通方法並推動 DNS 合規性。

1. 何謂「EDNS」？

EDNS 為 Extension mechanisms for DNS (DNS 擴展機制)的縮寫，是針對 DNS 網域名稱服務協議的參數所制定延伸的規範，由於過往 DNS 協議的封包長度受到限制(以傳統 UDP 的限制為 512 bytes)，因此於 1999 年由 IETF 組織制訂出 RFC 2671(也稱為 EDNS0)，將 DNS 訊息的長度由 512 Bytes 大幅擴展至 4096 Bytes，以便在同一個 DNS UDP 封包內攜帶更多的資料。之後包括 DNSSEC 等安全型態的執行也都會用到 EDNS。

2. 何謂 EDNS0 變通辦法

遞迴查詢主機先使用 EDNS0(長度 4096)對權威主機查詢網域名稱，當未收到回應時再使用 EDNS0(長度 512)對權威主機再次查詢網域名稱，如還是未收到回應時則使用標準 DNS(長度 512)對遞迴主機查詢網域名稱。

3. 何謂取消 EDNS0 變通辦法

遞迴查詢主機僅使用 EDNS0 對權威主機查詢網域名稱，當未收到回應時將直接將該權威主機標記為停用（treated as dead），不再嘗試使用標準 DNS 查詢，以增加 DNS 查詢速度。

4. 為何進行「DNS Flag Day」？

由於 EDNS 通訊在未受普遍的支援情況下，往往受限於資安設備或網路政策(如：路由器、防火牆、入侵偵測防禦等)的限制阻擋，主因傳統資安規則認為 DNS 通訊的長度為 512 bytes，因此拒絕並阻擋訊息更長的 DNS 封包。「DNS Flag Day」的推動，目的要求服務供應商將從其 DNS 解析器中取消 EDNS0 workaround 變通辦法，以便於（1）強制非 EDNS0 兼容的權威 DNS 服務器變得合規，以及（2）修正路由器、防火牆、及 DPI 封包深層檢測（e.g. 入侵偵測/防禦系統、狀態檢視防火牆）等設備中的網路裝置策略不支援 EDNS0 有效資料大小的狀況，進一步要求各 DNS 用戶端也必須遵循 EDNS 服務通訊規範。

5. 何時為「DNS Flag Day」？

2019 年 2 月 1 日。

6. 誰會受到影響 ？

ISP 及用戶單位使用不符合 EDNS 的 Authoritative DNS name servers(DNS 權威名稱服務器)。
路由器、防火牆、及 DPI 封包深層檢測（e.g. 入侵偵測/防禦系統、狀態檢視防火牆、負載平衡器）的規則不支持 EDNS0 payload sizes 大小的客戶。

7. Infoblox DNS 的客戶是否受影響？

Infoblox 權威 DNS 服務器符合 EDNS0 標準，需確認 Infoblox NIOS 版本為 v7.1 以上支援 EDNS，並且針對 EDNS 設定為 enable。遞歸 DNS 服務器則暫時保留了 EDNS 的變通方法。
Infoblox 的客戶只需要檢查他們的第三方權威 DNS 域名服務器是否支援 EDNS0，以及客戶端的路由器、防火牆、及 DPI 封包深層檢測（e.g. 入侵偵測/防禦系統、狀態檢視防火牆、負載平衡器）的規則支援並允許 EDNS ，以避免因為 EDNS0 而造成 DNS 封包被丟棄。

8. DNS 遞歸解析器(DNS recursive resolvers)是否受到影響 ？

Infoblox 遞歸 DNS 服務器將保留 EDNS0 的變通方法。 換句話說，他們暫時不會受到 DNS Flag Day 影響。 這意味著，查詢第三方非 EDNS 相容的權威 DNS 服務器將繼續工作。

對於已經停用 EDNS0 變通方法（如前述執行 DNS Flag Day 服務供應商）的遞歸 DNS 服務器，發送到第三方非 EDNS 標準的權威 DNS 服務器將不會嘗試重新使用標準 DNS 查詢，並且該權威 DNS 服務器會被視為停用（treated as dead）。 此外，如果第三方權威服務器支援 EDNS 規範，但所屬的網絡設備沒有支援的情況，則這些 DNS 服務器也將被視為停用。

9. 管理者對於 DNS Flag Day 的檢測確認方式 ？

- DNS Flag Day 檢測方式
- DNS Flag Day 專案官網: https://dnsflagday.net/
- ISC EDNS Compliance Tester: https://ednscomp.isc.org/ednscomp/
- 確認您的 Infoblox DNS 版本(NIOS v7.1 以上) 及設定 (EDNS 功能啟用)
- 確認並更新您的第三方權威 DNS 服務器支持 EDNS0。
- 修正您的相關網路設備及資安設備規則，需支援並允許 EDNS
- 重新測試

10. 如果一般 DNS 用戶什麼都不做怎麼辦 ？

遞歸名稱服務器可能會丟棄 DNS 數據包，並且網站將無法訪問。

11. Infoblox 是否為 DNS Flag Day 推動合規性的支援名單 ？

Infoblox 完全支持 DNS Flag Day 計劃，並且由於 Infoblox 為 ISC BIND 成員，因此列在 ISC 的支持者列表中。

參考資源:

- **DNS Flag Day: 2019 官網**

https://dnsflagday.net/

- **DNS Flag Day FAQ**

http://click.infoblox.com/q7KP000K5U0D4t01T08I00v

- **KB#9983: What is DNS Flag Day and is there an impact to Infoblox DNS services running in NIOS?**

https://support.infoblox.com/app/answers/detail/a_id/9983/kw/9983

- **KB#117: DNS packet sizes, TCP, and EDNS0**

https://support.infoblox.com/app/answers/detail/a_id/117/kw/117

- **Wiki: Extension mechanisms for DNS**

https://en.wikipedia.org/wiki/Extension_mechanisms_for_DNS