跨來源資源共用 CROS（Cross-Origin Resource Sharing）

跨來源資源共用是一種使用額外 HTTP 標頭令目前瀏覽網站的使用者代理取得存取其他來源伺服器特定資源權限的機制。當使用者代理請求一個不是目前文件來源，而是來自於不同網域、通訊協定或通訊埠的資源時，會建立一個跨來源 HTTP 請求。

因為安全性的考量，瀏覽器預設都會限制網頁做跨網域的連線，基本上都會被同源政策阻擋，但如果要提供資料存取的服務給其它人使用，這代表網路應用程式所使用的 API 必須使用 CORS 標頭，否則只能請求與應用程式相同網域的 HTTP 資源。CORS 機制提供了網頁伺服器跨網域的存取控制，增加跨網域資料傳輸的安全性。現代瀏覽器支援在 API 容器，如 XMLHttpRequest 或 Fetch 中使用 CORS 以降低跨來源 HTTP 請求的風險。

跨來源資源共用標準的運作方式是藉由加入新的 HTTP 標頭讓伺服器能夠描述來源資訊以提供予瀏覽器讀取。另外，針對會造成副作用的 HTTP 請求方法，特別是 GET 以外的 HTTP 方法，或搭配某些 MIME types 的 POST 方法，規範要求瀏覽器必須要請求傳送「預檢」請求，以 HTTP 的 OPTIONS 方法之請求從伺服器取得其支援的方法。當伺服器許可後，再傳送 HTTP 請求方法送出實際的請求，伺服器也可以通知客戶端是否要連同安全性資料（包括 Cookies 和 HTTP 認證資料）一併隨請求送出。

當一個網頁送出一個 request，瀏覽器會在 request 中 XMLHttpRequest 的 header 塞入 Origin 這個資料，這個資料就是代表這個網頁的來源。Origin 通常就是這個網頁對應網址的網域，也就是網頁發出的 request 必須與原本的網頁要有相同的來源。當一個 request 的 Origin 網域與 request 的目標伺服器不同就是所謂的跨網域連線。

當一個支援 CORS 瀏覽器在網頁送出一個 request 時，瀏覽器根據送出 request 的 HTTP verb 與 heade，判斷這個 request 是一個簡單請求或是非簡單

請求。如果是一個簡單請求，則直接送出 request；如果是一個非簡單請求的 request，則進行 CORS preflight。

先對伺服器送出一個 verb 為 OPTION 的 preflight request，它會帶有特定的 header 告訴伺服器接下來的 request 需要哪些跨網域連線的權限。當伺服器收到 preflight 後，就會回傳帶有特定 header 的 response 給瀏覽器，告訴它有哪些權限是允許的。瀏覽器取得伺服器的 response 後，如果符合連線權限，就會送出真正的 request。如果發現權限不符，就會出現錯誤訊息而中斷送出 request 的步驟。