# 改用 OIDC 之後，別忘了驗收日誌真的送達

2026-11-29 · 8plus

GitHub 於 2026 年 11 月 19 日宣布，具資料落地選項的 GitHub Enterprise Cloud（GHE.com）可透過 OIDC 將企業稽核日誌串流至 Amazon S3，不必在 GitHub 儲存長期 AWS 憑證。本文採近三十日官方消息，並從交付角度延伸，不是部署實測。

## 連線成功，只回答了第一個問題

少管理一組長期憑證，有助於簡化憑證的生命週期；但認證方式改變，不會自動證明資料完整抵達。設定頁顯示成功、儲存空間出現物件、查詢端找得到預期事件，是三個不同的驗收問題。

先把交付範圍寫清楚：哪個企業、哪個目的地、誰負責接收、誰使用資料，以及預期多久能查到。具體權限與 OIDC 信任設定依官方文件核對，不從其他環境直接複製，也不為了讓測試通過而擴大到不必要的存取範圍。

## 用一個可辨識事件走完整條路

在有授權的測試範圍內，選擇可逆、低影響且會記錄在稽核中的操作，記下時間與可用的識別資訊。確認來源有紀錄，再查目的地是否收到，最後用實際分析流程找到它。不要只看檔案總數，也不要假設所有操作都會產生相同的事件。

這是一種驗收方法，並非 GitHub 對所有事件延遲的保證。團隊應依實際需求定義等待窗口；超出窗口時標記待查，而不是把沒找到解讀成沒有發生。時區、查詢條件及資料轉換，也可能影響查找結果。

## 接收端的正常，要有持續證據

交付紀錄可以保留最近成功接收的時間、測試事件的受控參照，以及負責處理中斷的人。若環境本來就很少事件，單純一段時間沒有新檔案不能證明故障；監控需要結合來源活動與接收端狀態判讀。

同時測試資料能否被需要的人查詢。物件已寫入，但下游解析失敗或權限不符，對使用者而言仍是不可用。把接收與查詢分成兩個檢查，較容易定位問題，也避免把所有異常都歸因於 OIDC。

## 切換完成，要留下可接手的紀錄

在確認新路徑可用後，再依既有流程處理舊設定與憑證。記下切換時間、驗證範圍、尚未確認的項目與復原方式；不在報告附上完整日誌或身分資訊。稽核資料應留在有適當權限與保存政策的地方，不能拿來當公開示例或網站分析資料。

好的交付不是「我們改用 OIDC 了」這一句話，而是能讓接手的人回答：資料從哪裡來、到哪裡去、如何證明它到了，以及沒有到時要找誰。

## 來源

官方公告

延伸閱讀