

SSH 隧道與代理

```
% GIT_TRACE=1 GIT_CURL_VERBOSE=1 git push
21:32:14.216308 exec-cmd.c:139          trace: 解析可執行路徑從 Darwin 堆疊: /Applications/Xcode.app/Contents/D
21:32:14.216594 exec-cmd.c:238          trace: 解析可執行目錄: /Applications/Xcode.app/Contents/Developer/usr/b
21:32:14.216949 git.c:460              trace: 內建: git push
21:32:14.218655 run-command.c:655        trace: run_command: unset GIT_PREFIX; ssh git@github.com 'git-receive-
一切正常
```

我在 `git push` 操作中遇到了延遲，特別是在 `ssh git@github.com` 阶段。為了解決這個問題，我配置了 SSH 使用代理。

要使用 `corkscrew` 進行 SSH 隧道，首先需要安裝它。在 macOS 上，可以使用 Homebrew 並使用以下命令: `brew install corkscrew`

`~/.ssh/config` :

```
```bash
Host *
 UseKeychain yes
 AddKeysToAgent yes
 IdentityFile ~/.ssh/id_rsa
 ProxyCommand corkscrew localhost 7890 %h %p
```

日誌：

“ ‘bash % ssh root@138.201.174.0 -vvv ┌ 檢測到代理設置: - HTTP\_PROXY: http://127.0.0.1:7890 - HTTPS\_PROXY:
http://127.0.0.1:7890

OpenSSH\_9.8p1, LibreSSL 3.3.6 debug1: 讀取配置數據 /Users/lzwjava/.ssh/config debug1: /Users/lzwjava/.ssh/config  
1 行: 適用於 \* 的選項 debug1: 讀取配置數據 /etc/ssh/ssh\_config debug1: /etc/ssh/ssh\_config 21 行: 匹配的文  
件 include /etc/ssh/ssh\_config.d/\* 不匹配 debug1: /etc/ssh/ssh\_config 54 行: 適用於 \* 的選項 debug2: re-  
solve\_canonicalize: 主機名 138.201.174.0 是地址 debug3: 覆蓋 UserKnownHostsFile ‘~/.ssh/known\_hosts’ ->  
‘/Users/lzwjava/.ssh/known\_hosts’ debug3: 覆蓋 UserKnownHostsFile ‘~/.ssh/known\_hosts2’ -> ‘/Users/lzwjava/.ssh/known\_’  
debug1: Authenticator provider \$SSH\_SK\_PROVIDER 未解析; 禁用 debug3: channel\_clear\_timeouts: 清除 debug1:  
執行代理命令: exec corkscrew localhost 7890 138.201.174.0 22 debug1: 身份文件 /Users/lzwjava/.ssh/id\_rsa  
類型 0 debug1: 身份文件 /Users/lzwjava/.ssh/id\_rsa-cert 類型 -1 debug1: 本地版本字符串 SSH-2.0-  
OpenSSH\_9.8 debug1: 遠程協議版本 2.0, 遠程軟體版本 OpenSSH\_9.6p1 Ubuntu-3ubuntu13.5 debug1:  
compat\_banner: 匹配: OpenSSH\_9.6p1 Ubuntu-3ubuntu13.5 正則表達式 OpenSSH\* 兼容 0x04000000 de-  
bug2: fd 5 設置 O\_NONBLOCK debug2: fd 4 設置 O\_NONBLOCK debug1: 認證到 138.201.174.0:22 作為 ‘root’  
debug3: record\_hostkey: 在文件 /Users/lzwjava/.ssh/known\_hosts:164 中找到密鑰類型 ED25519 debug3:  
record\_hostkey: 在文件 /Users/lzwjava/.ssh/known\_hosts:165 中找到密鑰類型 RSA debug3: record\_hostkey: 在文  
件 /Users/lzwjava/.ssh/known\_hosts:166 中找到密鑰類型 ECDSA debug3: load\_hostkeys\_file: 從 138.201.174.0 載入  
3 個密鑰 debug1: load\_hostkeys: fopen /Users/lzwjava/.ssh/known\_hosts2: 沒有這個文件 debug1: load\_hostkeys:

fopen /etc/ssh/ssh\_known\_hosts: 沒有這個文件 debug1: load\_hostkeys: fopen /etc/ssh/ssh\_known\_hosts2: 沒有這個文件 debug3: order\_hostkeyalgs: 有匹配的最優密鑰類型 ssh-ed25519-cert-v01@openssh.com, 使用 HostkeyAlgorithms 原始 debug3: send packet: 類型 20 debug1: SSH2\_MSG\_KEXINIT 發送 debug3: receive packet: 類型 20 debug1: SSH2\_MSG\_KEXINIT 收到 debug2: 本地客戶端 KEXINIT 提議 debug2: KEX 算法: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com debug2: 主機密鑰算法: ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256 debug2: 密碼 ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: 密碼 stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,u128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 國際化 ctos: none,zlib@openssh.com,zlib debug2: 國際化 stoc: none,zlib@openssh.com,zlib debug2: 語言 ctos: debug2: 語言 stoc: debug2: first\_kex\_follows 0 debug2: 保留 0 debug2: 遠程服務器 KEXINIT 提議 debug2: KEX 算法: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-s,kex-strict-s-v00@openssh.com debug2: 主機密鑰算法: rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp256,ssh-ed25519 debug2: 密碼 ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: 密碼 stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 國際化 ctos: none,zlib@openssh.com,zlib debug2: 國際化 stoc: none,zlib@openssh.com,zlib debug2: 語言 ctos: debug2: 語言 stoc: debug2: first\_kex\_follows 0 debug2: 保留 0 debug3: kex\_choose\_conf: 將使用嚴格 KEX 排序 debug1: kex: 算法: sntrup761x25519-sha512@openssh.com debug1: kex: 主機密鑰算法: ssh-ed25519 debug1: kex: 服務器->客戶端密碼: chacha20-poly1305@openssh.com MAC: 國際化: none debug1: kex: 客戶端->服務器密碼: chacha20-poly1305@openssh.com MAC: 國際化: none debug3: send packet: 類型 30 debug1: 期待 SSH2\_MSG\_KEX\_ECDH\_REPLY debug3: receive packet: 類型 31 debug1: SSH2\_MSG\_KEX\_ECDH\_REPLY 收到 debug1: 服務器主機密鑰: ssh-ed25519 SHA256:+5SaMkJXG9yZrsYjXgxFfRZpvb6qjc/arFG2Nk4Vv48 debug3: record\_hostkey: 在文件 /Users/lzwjava/.ssh/known\_hosts:164 中找到密鑰類型 ED25519 debug3: record\_hostkey: 在文件 /Users/lzwjava/.ssh/known\_hosts:165 中找到密鑰類型 RSA debug3: record\_hostkey:

在文件 /Users/lzwjava/.ssh/known\_hosts:166 中找到密鑰類型 ECDSA debug3: load\_hostkeys\_file: 從 138.201.174.0 載入 3 個密鑰 debug1: load\_hostkeys: fopen /Users/lzwjava/.ssh/known\_hosts2: 沒有這個文件 debug1: load\_hostkeys: fopen /etc/ssh/ssh\_known\_hosts: 沒有這個文件 debug1: load\_hostkeys: fopen /etc/ssh/ssh\_known\_hosts2: 沒有這個文件 debug1: 主機 ‘138.201.174.0’ 已知並匹配 ED25519 主機密鑰。debug1: 在 /Users/lzwjava/.ssh/known\_hosts:164 中找到密鑰 debug3: send packet: 類型 21 debug1: ssh\_packet\_send2\_wrapped: 重置發送 seqnr 3 debug2: ssh\_set\_newkeys: 模式 1 debug1: 重新密鑰後 134217728 塊 debug1: SSH2\_MSG\_NEWKEYS 發送 debug1: 發送 SSH2\_MSG\_EXT\_INFO debug3: send packet: 類型 7 debug1: 期待 SSH2\_MSG\_NEWKEYS debug3: receive packet: 類型 21 debug1: ssh\_packet\_read\_poll2: 重置讀取 seqnr 3 debug1: SSH2\_MSG\_NEWKEYS 收到 debug2: ssh\_set\_newkeys: 模式 0 debug1: 重新密鑰入 134217728 塊 debug2: KEX 算法: sntrup761x25519-sha512@openssh.com,curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256,ext-info-c,kex-strict-c-v00@openssh.com debug2: 主機密鑰算法: ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256 debug2: 密碼 ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: 密碼 stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,u128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 圧縮 ctos: none,zlib@openssh.com,zlib debug2: 圧縮 stoc: none,zlib@openssh.com,zlib debug2: 語言 ctos: debug2: 語言 stoc: debug2: first\_kex\_follows 0 debug2: 保留 0 debug3: send packet: 類型 5 debug3: receive packet: 類型 7 debug1: SSH2\_MSG\_EXT\_INFO 收到 debug3: kex\_input\_ext\_info: 扩展 server-sig-algs debug1: kex\_ext\_info\_client\_parse: server-sig-algs=<ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256> debug3: kex\_input\_ext\_info: 扩展 publickey-hostbound@openssh debug1: kex\_ext\_info\_check\_ver: publickey-hostbound@openssh.com=<0> debug3: kex\_input\_ext\_info: 扩展 ping@openssh.com debug1: kex\_ext\_info\_check\_ver: ping@openssh.com=<0> debug3: receive packet: 類型 6 debug2: service\_accept: ssh-userauth debug1: SSH2\_MSG\_SERVICE\_ACCEPT 收到 debug3: send packet: 類型 50 debug3: receive packet: 類型 7 debug1: SSH2\_MSG\_EXT\_INFO 收到 debug3: kex\_input\_ext\_info: 扩展 server-sig-algs debug1: kex\_ext\_info\_client\_parse: server-sig-algs=<ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256> debug3: receive packet: 類型 51 debug1: 可以繼續的認證: publickey,password debug3: 重新開始, 通過不同的列表 publickey,password debug3: 偏好 publickey,keyboard-interactive,password debug3: authmethod\_lookup publickey debug3: 剩餘偏好: keyboard-interactive,password debug3: authmethod\_is\_enabled publickey debug1: 下一個認證方法: publickey debug3: ssh\_get\_authentication\_socket\_path: 路徑 ‘/private/tmp/com.apple.launchd.cTjjoglh4V/Listeners’ debug1: get\_agent\_identities: 繫定代理到主機

密鑰 debug1: get\_agent\_identities: 代理返回 3 個密鑰 debug1: 將嘗試密鑰: /Users/lzwjava/.ssh/id\_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 explicit agent debug1: 將嘗試密鑰: lzwjava@Zhiweis-MacBook-Air.local RSA SHA256:ibpUGVDyOYKOQArPUs5ZSnp0oECaZJWSPWAthOYBX/8 agent debug1: 將嘗試密鑰: /Users/lzwjava/Downloads/LightsailDefaultKey-ap-northeast-1.pem RSA SHA256:QCwUpsEP8cawJtCQNidQq0poQgAgkUuP agent debug2: pubkey\_prepare: 已完成 debug1: 提供公鑰: /Users/lzwjava/.ssh/id\_rsa RSA SHA256:bF6g9+hPW6crim36xewb explicit agent debug3: send packet: 類型 50 debug2: 我們發送了一個 publickey 封包, 等待回應 debug3: receive packet: 類型 60 debug1: 服務器接受密鑰: /Users/lzwjava/.ssh/id\_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 explicit agent debug3: sign\_and\_send\_pubkey: 使用 publickey-hostbound-v00@openssh.com 和 RSA SHA256:bF6g9+hPW6c debug3: sign\_and\_send\_pubkey: 使用 rsa-sha2-512 簽名 SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 debug3: send packet: 類型 50 debug3: receive packet: 類型 52 已經通過代理使用 “publickey” 認證到 138.201.174.0。 debug1: 通道 0: 新會話 [client-session] (未活動超時: 0) debug3: ssh\_session2\_open: 通道新: 0 debug2: 通道 0: 發送開啟 debug3: send packet: 類型 90 debug1: 要求 no-more-sessions@openssh.com debug3: send packet: 類型 80 debug1: 進入交互式會話。 debug1: pledge: 文件系統 debug3: client\_repledge: 進入 debug3: receive packet: 類型 80 debug1: client\_input\_global\_request: rtype hostkeys-00@openssh.com want\_reply 0 debug3: client\_input\_hostkeys: 收到 RSA 密鑰 SHA256:iw5lSMAuL30RZCUE+w7sbdXV0DI/gJ+Jwua+mmBVGw debug3: client\_input\_hostkeys: 收到 ECDSA 密鑰 SHA256:XKwEiSX70VqFOFCxJ0sUl/Au0bbyOSUaaQz/9WSe8Gc debug3: client\_input\_hostkeys: 收到 ED25519 密鑰 SHA256:+5SaMkJXG9yZrsYjXgxFfRZpvb6qjc/arFG2Nk4Vv48 debug1: client\_input\_hostkeys: 搜索 /Users/lzwjava/.ssh/known\_hosts 以獲取 138.201.174.0 / (none) debug3: hostkeys\_foreach: 讀取文件 “/Users/lzwjava/.ssh/known\_hosts” debug3: hostkeys\_find: 在 /Users/lzwjava/.ssh/known\_hosts:164 中找到 ssh-ed25519 密鑰 debug3: hostkeys\_find: 在 /Users/lzwjava/.ssh/known\_hosts:165 中找到 ssh-rsa 密鑰 debug3: hostkeys\_find: 在 /Users/lzwjava/.ssh/known\_hosts:166 中找到 ecdsa-sha2-nistp256 密鑰 debug1: client\_input\_hostkeys: 搜索 /Users/lzwjava/.ssh/known\_hosts2 以獲取 138.201.174.0 / (none) debug1: client\_input\_hostkeys: 密鑰文件 /Users/lzwjava/.ssh/known\_hosts2 不存在 debug3: client\_input\_hostkeys: 3 個服務器密鑰: 0 新, 3 保留, 0 不完整匹配。0 將被移除 debug1: client\_input\_hostkeys: 從服務器沒有新的或過時的密鑰 debug3: client\_repledge: 進入 debug3: receive packet: 類型 4 debug1: 遠程: /root/.ssh/authorized\_keys:1: 密鑰選項: agent-forwarding port-forwarding pty user-rc x11-forwarding debug3: receive packet: 類型 4 debug1: 遠程: /root/.ssh/authorized\_keys:1: 密鑰選項: agent-forwarding port-forwarding pty user-rc x11-forwarding debug3: receive packet: 類型 91 debug2: channel\_input\_open\_confirmation: 通道 0: 回調開始 debug2: client\_session2\_setup: id 0 debug2: 通道 0: 要求 pty-req 確認 1 debug3: send packet: 類型 98 debug1: 發送環境。 debug3: 忽略 env TERM\_SESSION\_ID debug3: 忽略 env SSH\_AUTH\_SOCK debug1: 通道 0: 設置 env LC\_TERMINAL\_VERSION = “3.4.19” debug2: 通道 0: 要求 env 確認 0 debug3: send packet: 類型 98 debug3: 忽略 env COLORFGBG debug3: 忽略 env ITERM\_PROFILE debug3: 忽略 env XPC\_FLAGS debug3: 忽略 env PWD debug3: 忽略 env SHELL debug3: 忽略 env \_\_CFBundleIdentifier debug1: 通道 0: 設置 env LC\_CTYPE = “UTF-8” debug2: 通道 0: 要求 env 確認 0 debug3: send packet: 類型 98 debug3: 忽略 env TERM\_PROGRAM\_VERSION debug3: 忽略 env TERM\_PROGRAM debug3: 忽略 env PATH debug1: 通道 0: 設置 env LC\_TERMINAL = “iTerm2” debug2: 通道 0: 要求 env 確認 0 debug3: send packet: 類型 98 debug3: 忽略 env COLORTERM debug3: 忽略 env COMMAND\_MODE debug3: 忽略 env TERM debug3: 忽略 env HOME debug3: 忽略 env TMPDIR debug3: 忽略 env USER debug3: 忽略 env XPC\_SERVICE\_NAME debug3: 忽略 env LOGNAME debug3: 忽略 env ITERM\_SESSION\_ID debug3: 忽略 env \_\_CF\_USER\_TEXT\_ENCODING debug3: 忽略 env SHLVL debug3: 忽略 env OLDPWD debug3: 忽略 env GLOBAL\_PROXY debug3: 忽略 env NO\_PROXY debug3: 忽略 env HOMEBREW\_PREFIX debug3: 忽略 env

HOMEBREW\_CELLAR debug3: 忽略 env HOMEBREW\_REPOSITORY debug3: 忽略 env INFOPATH debug3: 忽略 env  
HTTP\_PROXY debug3: 忽略 env HTTPS\_PROXY debug3: 忽略 env http\_proxy debug3: 忽略 env https\_proxy debug3:  
忽略 env HTTP\_PROXY\_REQUEST\_FULLURI debug3: 忽略 env HTTPS\_PROXY\_REQUEST\_FULLURI debug3: 忽略 env  
ALL\_PROXY debug3: 忽略 env SSL\_CERT\_FILE debug3: 忽略 env HOMEBREW\_NO\_AUTO\_UPDATE debug3: 忽略 env  
GOOGLE\_APPLICATION\_CREDENTIALS debug3: 忽略 env DEEPSEEK\_API\_KEY debug3: 忽略 env MISTRAL\_API\_KEY  
debug3: 忽略 env CODESTRAL\_API\_KEY debug3: 忽略 env SPEECH\_ENDPOINT debug3: 忽略 env DO\_API\_KEY  
debug3: 忽略 env GEMINI\_API\_KEY debug3: 忽略 env HERTZNER\_API\_KEY debug3: 忽略 env GROK\_API\_KEY  
debug3: 忽略 env \_debug2: 通道 0: 要求 shell 確認 1 debug3: send packet: 類型 98 debug3: client\_repledge: 進  
入 debug1: pledge: fork debug2: channel\_input\_open\_confirmation: 通道 0: 回調完成 debug2: 通道 0: 開啟確  
認 rwindow 0 rmax 32768 debug3: receive packet: 類型 99 debug2: channel\_input\_status\_confirm: 類型 99 id 0  
debug2: PTY 分配請求在通道 0 上被接受 debug2: 通道 0: rcvd adjust 2097152 debug3: receive packet: 類型 99  
debug2: channel\_input\_status\_confirm: 類型 99 id 0 debug2: 通道 0: shell 確認 請求接受