SSH 代理隧道

```
% GIT_TRACE=1 GIT_CURL_VERBOSE=1 git push
21:32:14.216308 exec-cmd.c:139          trace: 从 Darwin 堆栈解析可执行路径: /Applications/Xcode.app/Contents/D
21:32:14.216594 exec-cmd.c:238          trace: 解析可执行目录: /Applications/Xcode.app/Contents/Developer/usr/b
21:32:14.216949 git.c:460               trace: 内置: git push
21:32:14.218655 run-command.c:655       trace: run_command: 取消设置 GIT_PREFIX; ssh git@github.com 'git-recei
```

一切都已更新

我遇到 `git push` 操作缓慢，延迟发生在 `ssh git@github.com` 阶段。为了解决这个问题，我配置了 SSH 使用代理。

要使用 `corkscrew` 进行 SSH 隧道，首先需要安装它。在 macOS 上，可以使用 Homebrew 运行命令: `brew install corkscrew`

`~/.ssh/config`:

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

日志:

“ ‘bash % ssh root@138.201.174.0 -vvv ☒ **检测到代理设置:** - HTTP_PROXY: http://127.0.0.1:7890 - HTTPS_PROXY: http://127.0.0.1:7890

OpenSSH_9.8p1, LibreSSL 3.3.6 debug1: 读取配置数据 /Users/lzwjava/.ssh/config debug1: /Users/lzwjava/.ssh/config 第 1 行: 适用于 * 的选项 debug1: 读取配置数据 /etc/ssh/ssh_config debug1: /etc/ssh/ssh_config 第 21 行: 匹配 0 个文件 include /etc/ssh/ssh_config.d/ debug1: /etc/ssh/ssh_config 第 54 行: 适用于 的选项 debug2: resolve_canonicalize: 主机名 138.201.174.0 是地址 debug3: 扩展 UserKnownHostsFile ‘~/.ssh/known_hosts’ -> ‘/Users/lzwjava/.ssh/known_hosts’debug3: 扩展 UserKnownHostsFile‘~/.ssh/known_hosts2’->‘/Users/lzwjava/.ssh/known_h debug1: 无法解析 Authenticator 提供程序 $SSH_SK_PROVIDER; 禁用 debug3: channel_clear_timeouts: 清除 debug1: 执行代理命令: exec corkscrew localhost 7890 138.201.174.0 22 debug1: 身份文件 /Users/lzwjava/.ssh/id_rsa 类型 0 debug1: 身份文件 /Users/lzwjava/.ssh/id_rsa-cert 类型 -1 debug1: 本地版本字符串 SSH-2.0-OpenSSH_9.8 debug1: 远程协议版本 2.0, 远程软件版本 OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 debug1: compat_banner: 匹配: OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 兼容 0x04000000 debug2: 设置 fd 5 O_NONBLOCK debug2: 设置 fd 4 O_NONBLOCK debug1: 认证到 138.201.174.0:22 作为 ‘root’ debug3: record_hostkey: 在文件 /Users/lzwjava/.ssh/known_hosts:164 中找到密钥类型 ED25519 debug3: record_hostkey: 在文件 /Users/lzwjava/.ssh/known_hosts:165 中找到密钥类型 RSA debug3: record_hostkey: 在文件 /Users/lzwjava/.ssh/known_hos 中找到密钥类型 ECDSA debug3: load_hostkeys_file: 从 138.201.174.0 加载 3 个密钥 debug1: 打开 /Users/lzwjava/.ssh/known 没有该文件或目录 debug1: 打开 /etc/ssh/ssh_known_hosts: 没有该文件或目录 debug1: 打开 /etc/ssh/ssh_known_hosts2:

没有该文件或目录 debug3: order_hostkeyalgs: 具有匹配的最佳偏好密钥类型 ssh-ed25519-cert-v01@openssh.com,
使用 HostkeyAlgorithms 直接 debug3: 发送数据包: 类型 20 debug1: 发送 SSH2_MSG_KEXINIT debug3:
接收数据包: 类型 20 debug1: 接收 SSH2_MSG_KEXINIT debug2: 本地客户端 KEXINIT 提议 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: 主机密钥算法: 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: 密码 ctos: chacha20-poly1305@openssh.com,aes128-
ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: 密码 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,u
128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 压缩 ctos: none,zlib@openssh.com,zlib de-
bug2: 压缩 stoc: none,zlib@openssh.com,zlib debug2: 语言 ctos: debug2: 语言 stoc: debug2: first_kex_follows 0 de-
bug2: reserved 0 debug2: 服务器 KEXINIT 提议 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: 主机密钥算法: rsa-sha2-512,rsa-sha2-256,ecdsa-
sha2-nistp256,ssh-ed25519 debug2: 密码 ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-
ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: 密码 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,h
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,hm
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: 压缩 ctos: none,zlib@openssh.com debug2: 压缩 stoc: none,zlib@openssh.com
debug2: 语言 ctos: debug2: 语言 stoc: debug2: first_kex_follows 0 debug2: reserved 0 debug3: kex_choose_conf:
将使用严格的 KEX 顺序 debug1: KEX 算法: sntrup761x25519-sha512@openssh.com debug1: 主机密钥算法:
ssh-ed25519 debug1: 服务器到客户端密码: chacha20-poly1305@openssh.com MAC: 压缩: none debug1: 客户端
到服务器密码: chacha20-poly1305@openssh.com MAC: 压缩: none debug3: 发送数据包: 类型 30 debug1: 期待
SSH2_MSG_KEX_ECDH_REPLY debug3: 接收数据包: 类型 31 debug1: 接收 SSH2_MSG_KEX_ECDH_REPLY debug1:
服务器主机密钥: ssh-ed25519 SHA256:+5SaMkJXG9yZrsYjXgxFfRZpvb6qjc/arFG2Nk4Vv48 debug3: record_hostkey:
在文件 /Users/lzwjava/.ssh/known_hosts:164 中找到密钥类型 ED25519 debug3: record_hostkey: 在文件
/Users/lzwjava/.ssh/known_hosts:165 中找到密钥类型 RSA debug3: record_hostkey: 在文件 /Users/lzwjava/.ssh/known_hos
中找到密钥类型 ECDSA debug3: load_hostkeys_file: 从 138.201.174.0 加载 3 个密钥 debug1: 打开 /Users/lzwjava/.ssh/known

没有该文件或目录 debug1: 打开 /etc/ssh/ssh_known_hosts: 没有该文件或目录 debug1: 打开 /etc/ssh/ssh_known_hosts2: 没有该文件或目录 debug1: 主机‘138.201.174.0’已知且与 ED25519 主机密钥匹配。debug1: 在 /Users/lzwjava/.ssh/known_hosts:164 中找到密钥 debug3: 发送数据包: 类型 21 debug1: ssh_packet_send2_wrapped: 重置发送 seqnr 3 debug2: ssh_set_newkeys: 模式 1 debug1: 在 134217728 块后重新加密 debug1: 发送 SSH2_MSG_NEWKEYS debug1: 发送 SSH2_MSG_EXT_INFO debug3: 发送数据包: 类型 7 debug1: 期待 SSH2_MSG_NEWKEYS debug3: 接收数据包: 类型 21 debug1: ssh_packet_read_poll2: 重置读 seqnr 3 debug1: 接收 SSH2_MSG_NEWKEYS debug2: ssh_set_newkeys: 模式 0 debug1: 在 134217728 块后重新加密 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: 主机密钥算法: 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: 密码 ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com debug2: 密码 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,u 128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1 debug2: 压缩 ctos: none,zlib@openssh.com,zlib debug2: 压缩 stoc: none,zlib@openssh.com,zlib debug2: 语言 ctos: debug2: 语言 stoc: debug2: first_kex_follows 0 debug2: reserved 0 debug3: 发送数据包: 类型 5 debug3: 接收数据包: 类型 7 debug1: 接收 SSH2_MSG_EXT_INFO 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: 接收数据包: 类型 6 debug2: service_accept: ssh-userauth debug1: 接收 SSH2_MSG_SERVICE_ACCEPT debug3: 发送数据包: 类型 50 debug3: 接收数据包: 类型 7 debug1: 接收 SSH2_MSG_EXT_INFO 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: 接收数据包: 类型 51 debug1: 继续认证: publickey,password debug3: 重新开始，传递了不同的列表 publickey,password debug3: 优先 publickey,keyboard-interactive,password debug3: 认证方法查找 publickey debug3: 剩余优先: keyboard-interactive,password debug3: 认证方法是否启用 publickey debug1: 下一个认证方法: publickey debug3: ssh_get_authentication_socket_path: 路径‘/private/tmp/com.apple.launchd.cTjjogIh4V/Listeners’ debug1: 绑定代理到主机密钥 debug1: 代理返回 3 个密钥 debug1: 将尝试密钥: /Users/lzwjava/.ssh/id_rsa RSA SHA256:bF6g9+hPW6crim36xewb/0Pvl/Y34 隐式代理