Guida tecnica all’installazione e utilizzo di Secure Socket Shell (SSH) per la connessione remota

Mauro Bellone

Guida tecnica

Versione 0.1 – 20/07/2021

Abstract

Questo documento contiene le istruzioni operative per l'utilizzo del ssh per la connessione a macchine remote in ambiente linux.

1 Introduzione

L'accesso a macchine remote è ormai diventato un elemento imprescindibile nel lavoro dei computer scientists. Esistono principalmente due metodi per accedere in maniera remota ad una macchina, usare il remote desktop protocol (RDP) o usare il secure socket shell (ssh). Nell'ambito dei lavori ad alte performance (big data, intelligenza artificiale etc.), dove la massimizzazione utilizzo delle risorse e la minimizzazione degli sprechi computazionali è essenziale, il più utilizzato è ssh che unisce semplicità di utilizzo e flessibilità a performance molto elevate su shell. Questo significa che ssh si utilizza principalmente in assenza di interfaccia grafica ma solo tramite terminale.

1.1 Prerequisiti

I prerequisiti di base per avviare una connessione sicura sono:

1. Computer remoto acceso e connesso ad una rete
2. Abilitazione di client e server
3. Conoscenza dell'indirizzo IP di connessione alla macchina remota
4. Permessi utente per la connessione al computer remoto
5. Permessi di accesso dal firewall di sistema della macchina remota

2 SSH – Secure Socket Shell

Secure socket shell è un protocolo di rete client-server con crittografia che consente la connessione e il trasferimento sicuro tra computer remoti usando una interfaccia di testo (NO GUI). Tipicamente una shell si avvia all'attivazione di una connessione consentendo la manipolazione del server remoto tramite la digitazione di comandi a schermo. I maggiori utilizzatori di questo sistema sono amministratori di rete e amministratori di sistema che hanno la necessità di manipolare computer remoti con un alto livello di sicurezza.

Il protocollo ssh è, di fatto, un protocollo client-server, quindi per stabilire una connessione di rete è necessario che sulla macchina remota sia installato il lato server, mentre sulla macchina locale sia installato il lato client. Entrambi, client e server, possono essere installati sulle macchine lo switch tra client e server dipende dal lato della connessione, da client verso server. Il client fornisce le informazioni al server, indirizzo IP e credenziali di accesso, prima di stabilire la connessione. Molte versioni di linux (ubuntu ad esempio) hanno il software openSSH installato di default, per verificare l'installazione è sufficiente chiamare il comando "`ssh`" da finestra terminale senza ulteriori opzioni, se presente il comando fornirà l'help di utilizzo. In alternativa, per installare il client è possibile usare il comando:

```
sudo apt-get install openssh-client
```

Chiaramente è necessario disporre delle credenziali "`sudo`" per installare software su qualunque delle macchine (server o client).

Sul lato server è presente un software, chiamato sshd (dove la lettera "d" sta per deamon) che ha il compito di ascoltare costantemente una specifica porta TPC/IP in attesa di una connessione da parte di un client. Quando il client avvia una connessione al server, ssh-deamon risponde con la versione del software installato e supporta lo scambio dati per la sola identificazione, se le credenziali sono corrette si avvia l'ambiente di controllo della macchina remota.

Per verificare se è presente sulla macchina il server è possibile tentare una connessione usando "`localhost`" come destinazione, avviando quindi il comando:

```
username@host:~$ ssh localhost
ssh: connect to host localhost port 22: Connection refused username@host:~$
```

normalmente è sempre possibile connettersi a localhost in quanto, di fatto, si chiede a ssh di stabilire una connessione con la stessa macchina. Se la risposta al comando è quella indicata nella linea precedente, quindi connessione rifiutata, è necessario installare il server, semplicemente avviando il comando:

```
sudo apt-get install openssh-server ii
```

A valle dell'installazione è possibile nuovamente testare che il server sia in esecuzione tentando nuovamente la conessione sull'host locale, se il server è attivo dovrebbe essere possibile connettersi a se stessi con l'inserimento delle credenziali utente.

```
ssh localhost

The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:Fxc1BvgaR+mQ5aYFOXTUkluJy/9Qlmk2rJ0Lvnu61rI.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Un altro modo per verificare che il server sia attivo è il comando `ssh server status` (lanciato eventualmente con i privilegi sudo), la risposta dovrebbe essere analoga alla seguente:

La porta predefinita di connessione è la porta n. 22, la porta di connessione di default è modificabile (per garantire maggiore sicurezza) editando sul lato server il file `/etc/ssh/sshd_config` e riavviando il server tramite il comando `service ssh restart`.

3 Connessione remota tramite SSH

Una volta installati client e server è possibile avviare una connessione alla macchina remota, il comando per avviare la connessione è:

```
ssh remote_user_name@host_ip_address
```

nel caso in sui la porta di ascolto del server sia stata modificata, è necessario aggiungere l'opzione "-p" ed indicare il numero della porta di ascolto del server, es "`-p 22`".

La chiusura della connessione avviene tramite il comando "`exit`", oppure alla chiusura del terminale (processo) che ha richiesto la connessione sul client.

Una volta connessi è possibile usare qualunque comando (dati i privilegi associati all'utente connesso) sul lato server. Il comando tipicamente più utilizzato è quello per la copia dei file da client a server e viceversa tramite "`scp`" o secure copy, usato nella forma seguente:

```
scp [option] user@SOURCE_HOST:file user@DESTINATION_HOST:file
```

usando l'opzione "`-r`" è possibile copiare in maniera ricorsiva, inserendo intere cartelle.

Data 20 luglio 2021 Mauro Bellone