GABRIELE ROMANATO

Evitare il blocco di rsync per la verifica dell'autenticità dell'host

Quando si utilizza Rsync per trasferire file su un server remoto tramite SSH, può capitare di imbattersi in un messaggio di autenticazione che interrompe il processo automatico richiedendo una conferma manuale. Questo comportamento può diventare un ostacolo, soprattutto in ambienti di automazione e scripting. In questo articolo vedremo perché si verifica questo problema e quali soluzioni adottare per evitarlo senza compromettere la sicurezza della connessione.

Può capitare di ricevere il seguente messaggio:

```
The authenticity of host '[192.168.1.5]:22
([192.168.1.5]:22)' can't be established.
ECDSA key fingerprint is
SHA256:sIWEU9G7yDvxZG2K+64DKkLHaMNjiILm+gzJB1o6+cF.
Are you sure you want to continue connecting
(yes/no/[fingerprint])?
```

Questo messaggio può bloccare l'esecuzione di `rsync` in attesa di un input manuale. Vediamo come evitarlo.

Soluzioni per Evitare il Blocco

Aggiungere l'Host ai `known_hosts`

Per confermare l'autenticità dell'host una sola volta ed evitare il blocco in futuro, eseguire:

```
ssh user@192.168.1.5
```

Rispondere `yes` alla richiesta e chiudere la connessione (`exit`).

Disabilitare il Controllo della Chiave

Se non si desidera verificare l'autenticità dell'host, si può usare l'opzione `StrictHostKeyChecking=no`:

```
rsync -az -e 'ssh -o StrictHostKeyChecking=no -o
UserKnownHostsFile=/dev/null' dir/
user@192.168.1.5:/home/user/dir/
```

Attenzione: Questa opzione riduce la sicurezza, in quanto accetta qualsiasi host senza verificarne la chiave.

Accettare Automaticamente Nuove Chiavi

Un compromesso tra sicurezza e praticità è usare:

```
rsync -az -e 'ssh -o StrictHostKeyChecking=accept-new' dir/
user@192.168.1.5:/home/user/dir/
```

Questo comando accetta automaticamente solo nuove chiavi, senza disabilitare la protezione in caso di cambiamenti sospetti.

Conclusione

Il metodo più sicuro è aggiungere l'host ai `known_hosts` manualmente (metodo 1). Per un'operazione automatizzata ma sicura, il metodo 3 è una buona scelta. Il metodo 2 è da usare solo se non si ha bisogno di verificare l'autenticità dell'host.