



链滴

fix the error “host key verification failed”

作者: [tuchief](#)

原文链接: <https://ld246.com/article/1586489351745>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      B: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
9a:55:de:ad:be:ef:00:00:08:67:53:09.
Please contact your system administrator.
Add correct host key in /home/briane/.ssh/known_hosts to get rid of this message.
Offending key in /home/briane/.ssh/known_hosts: 6
Host key verification failed.
```

错误信息

在使用iterms通过ssh连接某服务器时，报了如下提示：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
dd:cf:50:31:7a:78:93:13:dd:99:67:c2:a2:19:22:13.
Please contact your system administrator.
Add correct host key in /home/user01/.ssh/known_hosts to get rid of this message.
Offending key in /home/lcz/.ssh/known_hosts:7
RSA host key for 192.168.21.49 has changed and you have requested strict checking.
Host key verification failed.
```

修复方式：

1. 手动删除旧的秘钥

```
# vi ~/.ssh/known_hosts
192.168.1.113 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
TYAAABBBLrY91bQOihgFZQ2Ay9KiBG0rg51/YxJAK7dvAlopRaWzFEEis3fQJiYZNLzLgQtlz6ple2t
9m/Za33W6WirN8=
192.168.19.11 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
TYAAABBBCrY/m16MdFt/Ym51Cc7kxZW3R2pcHV1jlOclv6sXix1UhMuPdtobj+b7+NLITcjfrUc
L+1bkg8EblYucymeU=
# 根据提示的IP地址，将该秘钥删除
192.168.21.49 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
TYAAABBBCrY/m16MdFt/Ym51Cc7kxZW3R2pcHV1jlOclv6sXix1UhMuPdtobj+b7+NLITcjfrUc
L+1bkg8EblYucymeU=
```

2. 使用ssh-keygen目录删除旧秘钥

```
$ ssh-keygen -R [hostname | IP address]
```

```
$ ssh-keygen -R 192.168.21.49
```

```
# Host 192.168.21.49 found: line 4
```

```
/home/user01/.ssh/known_hosts updated.
```

```
Original contents retained as /home/user01/.ssh/known_hosts.old
```

最后，再重新使用ssh连接服务器；

```
$ ssh root@192.168.21.49
```

```
The authenticity of host '192.168.21.49(192.168.21.49)' can't be established.
```

```
ECDSA key fingerprint is SHA256:V+iGp3gwSlnpbtYv4Niq6tcMMSZivSnYWQlaJnUvHb4.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '192.168.21.49' (ECDSA) to the list of known hosts.
```