SSH 无法启动的原因分析及解决方法

* 简介

Secure Shell（缩写为SSH），由[IETF](https://zh.wikipedia.org/wiki/IETF" \o "IETF)的网络工作小组（Network Working Group）所制定；SSH为一项创建在[应用层](https://zh.wikipedia.org/wiki/%E5%BA%94%E7%94%A8%E5%B1%82" \o "应用层)和[传输层](https://zh.wikipedia.org/wiki/%E4%BC%A0%E8%BE%93%E5%B1%82)基础上的安全协议，为计算机上的[Shell](https://zh.wikipedia.org/wiki/Shell)（壳层）提供安全的传输和使用环境。

传统的网络服务程序，如[rsh](https://zh.wikipedia.org/wiki/Rsh)、[FTP](https://zh.wikipedia.org/wiki/%E6%96%87%E4%BB%B6%E4%BC%A0%E8%BE%93%E5%8D%8F%E8%AE%AE)、[POP](https://zh.wikipedia.org/wiki/POP3)和[Telnet](https://zh.wikipedia.org/wiki/Telnet)其本质上都是不安全的；因为它们在网络上用明文传送数据、用户帐号和用户口令，很容易受到[中间人](https://zh.wikipedia.org/wiki/%E4%B8%AD%E9%97%B4%E4%BA%BA%E6%94%BB%E5%87%BB)（man-in-the-middle）攻击方式的攻击。就是存在另一个人或者一台机器冒充真正的[服务器](https://zh.wikipedia.org/wiki/%E4%BC%BA%E6%9C%8D%E5%99%A8)接收用户传给服务器的数据，然后再冒充用户把数据传给真正的服务器。

而SSH是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用SSH协议可以有效防止远程管理过程中的信息泄露问题。通过SSH可以对所有传输的数据进行加密，也能够防止[DNS](https://zh.wikipedia.org/wiki/DNS)欺骗和[IP](https://zh.wikipedia.org/wiki/IP)欺骗。

SSH之另一项优点为其传输的数据可以是经过压缩的，所以可以加快传输的速度。SSH有很多功能，它既可以代替[Telnet](https://zh.wikipedia.org/wiki/Telnet)，又可以为FTP、POP、甚至为[PPP](https://zh.wikipedia.org/wiki/%E7%82%B9%E5%AF%B9%E7%82%B9%E5%8D%8F%E8%AE%AE)提供一个安全的“通道”。

关于SSH,详情参见如下:

https://zh.wikipedia.org/zh-cn/Secure\_Shell

* SSH无法正常启动的几种报错信息

1. ssh相关**文件权限有误**导致无法启动, 报错参考如下:  
   Starting sshd: /var/empty/sshd must be owned by root and not group or world-writable.
2. ssh**配置文件内容有误, 或语法有误**, 报错参考如下:

Starting sshd: [FAILED]

* 解决方案

**方案一:**

通过azure新portal的重置远程访问



**注意: 如果配置文件被删除, 该功能不会重建, 参考其他方案进行修复.**

**方案二:**

1. 删除虚拟机保留磁盘, 将该系统盘作为数据盘附加到临时虚拟机.
2. 登陆临时虚拟机, 进入到对应的目录, 进行手工修复.
3. 修复完毕以后, 分离该磁盘, 并基于此新建虚拟机.
4. 尝试通过SSH重新连接.