- SSH
  - SSH 与 OpenSSH
    - SSH（Secure Shell 的缩写）是一种网络协议，用于加密两台计算机之间的通信，并且支持各种身份验证机制
    - OpenSSH 是 SSH 协议的免费开源实现
  - SSH 客户端
    - 安装
      - OpenSSH 官网
      - OpenSSH 的客户端是二进制程序 ssh
    - 基本命令使用
      - ssh hostname
      - ssh user@hostname
      - ssh -l username host
      - ssh -p 8821 host
    - 连接流程
      - ssh 首次连接服务器，会有一个验证过程，提醒是否确认连接
      - 每台 ssh 服务器都有唯一一对密钥，用于跟客户端通信，其中公钥的哈希值就可以用来识别服务器，简称服务器指纹
      - ssh 会将本机连接过的所有服务器公钥的指纹，都储存在本机的 ~/.ssh/known_hosts 文件中
    - 服务器密钥变更
      - 问题：主机服务器密钥变更(比如重装ssh服务器)，导致公钥指纹不匹配，连接会失败
      - 解决方式：1. 将 known_hosts 中保存的旧公钥指纹删除，然后再次 ssh 连接。2. 使用命令替换：ssh-keygen -R hostname
    - 命令行配置项
      - -c 指定加密算法：ssh -c blowfish,3des server.example.com
      - -C 表示压缩数据传输: ssh -C server.example.com
      - -d 设置打印的 debug 信息级别，数值越高，输出的内容越详细: ssh –d 1 foo.com
      - -D 指定本机的 Socks 监听端口，该端口收到的请求将转发到远程的 SSH 主机，又称动态端口转发: ssh -D 1080 server
      - -f 表示 SSH 连接在后台运行
      - -F 指定配置文件： ssh -F /usr/local/ssh/other_config
      - -i 指定私钥，默认私钥为 ~/.ssh/id_dsa
      - -l 指定远程登录的账户名
      - -L 设置本地端口转发：ssh -L 9999:targetServer:80 user@remoteserver
      - -m 指定校验数据完整性的算法: ssh -m hmac-sha1,hmac-md5 server.example.com
      - -p 指定 SSH 客户端连接的服务器端口: ssh -p 2035 server.example.com
      - -v 显示详细信息，-v可以重复多次，表示信息的详细程度：ssh -vvv server.example.com
      - -V 输出 ssh 客户端的版本
      - -1 指定使用 SSH 1 协议，-2 指定使用 SSH 2 协议
      - -4 指定使用 IPv4 协议（默认值），-6 指定使用 IPv6 协议
    - 配置文件
      - 全局配置文件是 /etc/ssh/ssh_config，用户个人的配置文件在 ~/.ssh/config，优先级高于全局配置文件
      - ~/.ssh 目录下常见文件
        - ~/.ssh/id_ecdsa：用户的 ECDSA 私钥
        - ~/.ssh/id_ecdsa.pub：用户的 ECDSA 公钥
        - ~/.ssh/id_rsa：用于 SSH 协议版本2 的 RSA 私钥
        - ~/.ssh/id_rsa.pub：用于SSH 协议版本2 的 RSA 公钥
        - ~/.ssh/identity：用于 SSH 协议版本1 的 RSA 私钥
        - ~/.ssh/identity.pub：用于 SSH 协议版本1 的 RSA 公钥
        - ~/.ssh/known_hosts：包含 SSH 服务器的公钥指纹
    - 配置命令
      - 语法
        - 配置文件的每一行，就是一个配置命令
        - 配置命令与对应的值之间，可以使用空格，也可以使用等号
        - #开头的行表示注释，会被忽略。空行等同于注释
      - 主要命令及范例值
  - SSH 密钥登录