1.Linux的网络信息

1.1. 主机名称

- 临时修改
  - hostname school
- 长久修改
  - vi /etc/hostname

1.2. DNS解析

- 域名解析服务
- 可以将域名转换为IP地址
- DNS域名劫持
  - window -->
    C:\Windows\System32\drivers\etc\hosts
  - 123.56.138.186 www.baidu.com
    123.56.138.186 www.taodao.com
- 修改主机域名
  - vi /etc/hosts
  - 将来我们需要把所有的虚拟机都配置hosts文件
  - 192.168.31.101 bd1601
  - 192.168.31.102 bd1602

1.3. 网络相关命令

- ifconfig
  - 查看当前网卡的配置信息
  - 这个命令属于 net-tools中的一个命令，但是Centos7中minimal版并没有集成这个包 ○ 所以7的时候需要自己手动安装
  - 如果没有ifconfig ，可以使用ip addr 临时代替
- netstat
  - 查看当前网络的状态信息
  - 一个机器默认有65536个端口号[0,65535]
  - 这是一个逻辑的概念，将来我们需要使用程序监听指定的端口，等待别人的访问
  - 一个端口只能被一个程序所监听，端口已经被占用
  - netstat -anp
  - netstat -r 核心路由表 == route
- ping
  - 查看与目标IP地址是否能够连通
- telnet
  - 查看与目标IP的指定端口是否能够连通
  - yum install telnet -y
  - telnet 192.168.31.44 22
- curl
  - restful 我们所有的资源在网络上中都有唯一的定位
  - 那么我们可以通过这个唯一定位标识指定的资源
  - http://localhost:8080/lucky/user.action/666 ○ curl -X GET http://www.baidu.com

1.4. 防火墙

- 防火墙技术是通过有机结合各类用于安全管理与筛选的软件和硬件设备，帮助计算机网络于其内、外网之间构建一道相对隔绝的保护屏障，以保护用户资料与信息安全性的一种技术
- 在centOS7+中 使用firewalld代替以前的 iptables ；

```
#查看防火墙状态
systemctl status firewalld.service

#临时停止firewall
systemctl stop firewalld.service

#禁止firewall开机启动
systemctl disable firewalld.service

firewall-cmd --state                                ##查看防火墙状态，是否是
running
firewall-cmd  --reload                              ##重新载入配置，比如添加规则之
后，需要执行此命令
firewall-cmd --get-zones                            ##列出支持的zone
firewall-cmd --get-services                         ##列出支持的服务，在列表中的服
务是放行的
firewall-cmd --query-service ftp                    ##查看ftp服务是否支持，返回
yes或者no
firewall-cmd  --add-service=ftp                     ##临时开放ftp服务
firewall-cmd  --add-service=ftp  --permanent        ##永久开放ftp服务
firewall-cmd --remove-service=ftp --permanent  ##永久移除ftp服务
```

```
firewall-cmd  --add-port=80/tcp  --permanent       ##永久添加80端口
```

- 开启一个端口的正确操作
  - ```
    # 添加
    firewall-cmd  --zone=public  --add-port=80/tcp  --permanent

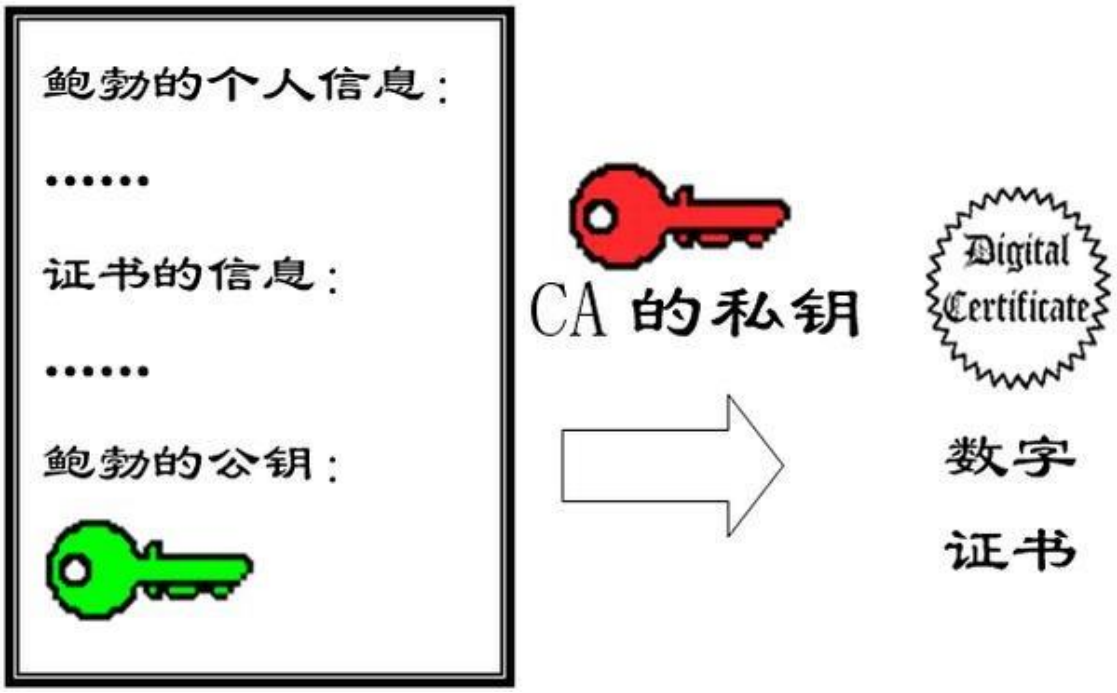
    #重新载入
    firewall-cmd  --reload

    #查看
    firewall-cmd  --zone=public  --query-port=80/tcp

    #删除
    firewall-cmd  --zone=public  --remove-port=80/tcp  --permanent
    ```

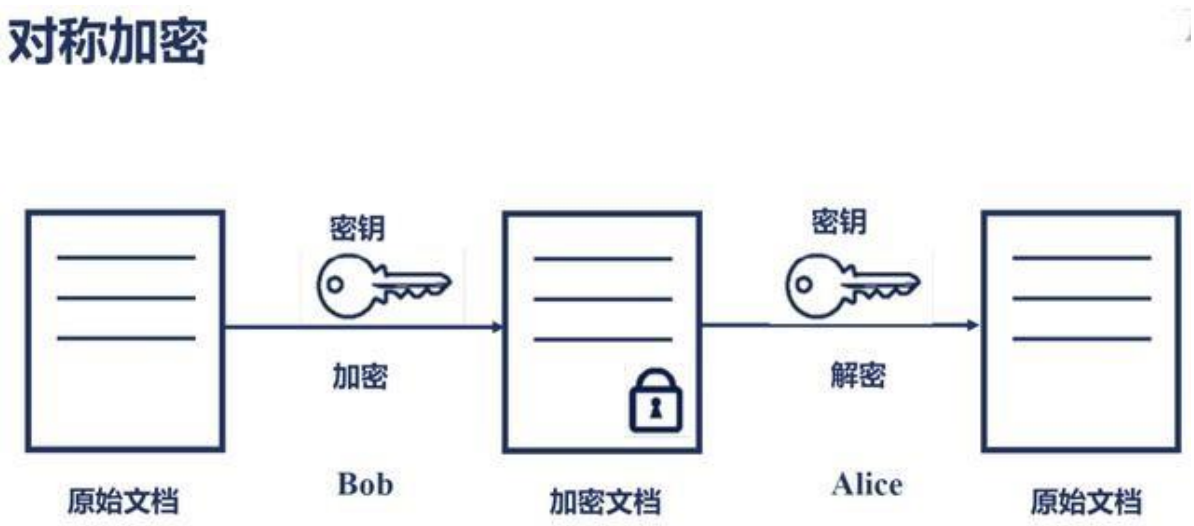
1.5. 加密算法

1.5.1. 不可逆加密算法
    ```



- 可以通过数据计算加密后的结果，但是通过结果无法计算出加密数据
- 应用场景
  - Hash算法常用在不可还原的密码存储、信息完整性校验。
  - 文档、音视频文件、软件安装包等用新老摘要对比是否一样(接收到的文件是否被修改)
  - 用户名或者密码加密后数据库存储(数据库大多数不会存储关键信息的明文，就像很多登录功能的忘记密码不能找回，只能重置)
- 案例
  - 123456
  - e10adc3949ba59abbe56e057f20f883e
  - md5(md5(123456))--------md5(654321)

1.5.2. 对称加密算法

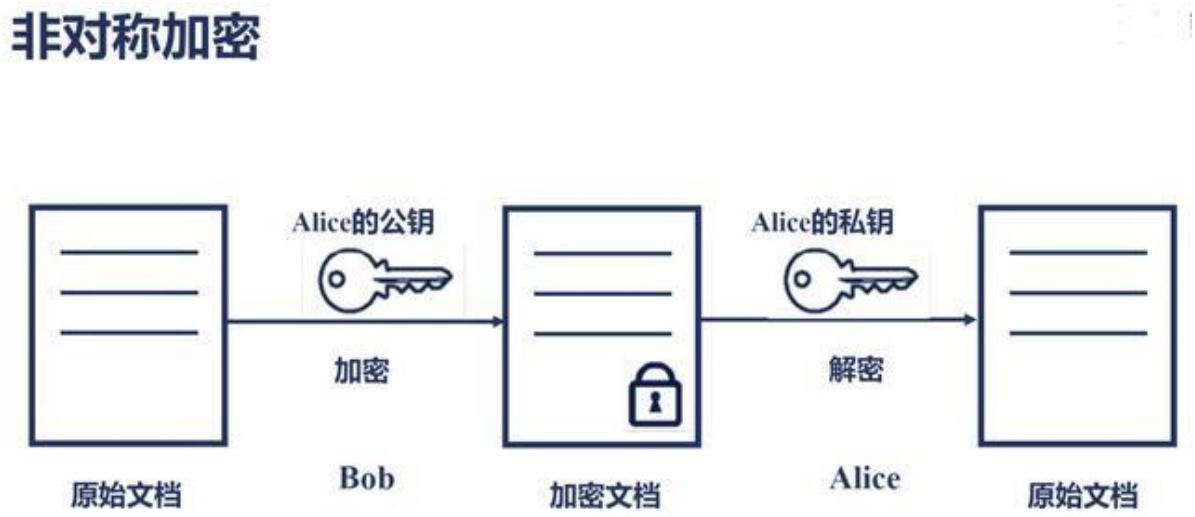


- Symmetric Key Encryption
- 代表性算法叫做 DES、3DES、Blowfish、IDEA、RC4、RC5、RC6和AES
- 特点

- 加密和解密使用相同的秘钥

- 优点
  - 生成密钥的算法公开、计算量小、加密速度快、加密效率高、密钥较短
- 缺点
  - 双方共同的密钥，有一方密钥被窃取，双方都影响
  - 如果为每个客户都生成不同密钥，则密钥数量巨大，密钥管理有压力
- 应用场景
  - 登录信息用户名和密码加密、传输加密、指令加密
- 案例:
  - 原文：今晚八点学校小树林
  见 ○ 密钥： love
  - 7gjM6FhIc89ACoel+jJ3VM26XGAdSlaHTj5NYg4VkKA=

1.5.3. 非对称加密算法



- Asymmetric Key Encryption
- 非对称加密算法需要一对密钥(两个密钥)：
  - 公开密钥(publickey)和私有密钥(privatekey)(简称公钥，私钥)。
  - 公开密钥与私有密钥生成时是一对
  - 用公钥加密只能是对应的私钥解密，同理用私钥加密只能用对应的公钥解密。
- 代表性算法叫做 RSA、ECC、Diffie-Hellman、El Gamal、DSA(数字签名用)
- 优点：
  - 安全高(几乎很难破解)
- 缺点
  - 加解密相对速度慢、密钥长、计算量大、效率低
- 应用场景
  - HTTPS(ssl)证书里制作、CRS请求证书、金融通信加密、蓝牙等硬件信息加密配对传输、关键的登录信息验证。
- http://tool.chacuo.net/cryptrsaprikey
  - ```
    -----BEGIN PUBLIC KEY-----
    MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDjlHREYDiL9p5bAPBsMCy+UIaH
    e4MAm7djkuHYW3aGQLgG9Rc1CSRaFeNXBw+llDsnIgBPgoUI4S8N2m87n25zJ5jH
    7pEyWoZsAeTgpqJ6fzfciRpGHsawZ+AxVs0PeIvBMVIIZfpP4tIK5WVau7mVt0gy
    /bU+PtX35wVymIKy7QIDAQAB
    -----END PUBLIC KEY-----
    ```
    ```

- ```
  -----BEGIN PRIVATE KEY-----
  MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBAOOUdERgOIv2nlsA
  8GwwLL5Qhod7gwCbt2OS4dhbdoZAuAb1FzUJJFoV41cHD6WUOyciAE+ChQjhLw3a
  bzufbnMnmMfukTJahmwB5OCmonp/N9yJGkYexrBn4DFWzQ94i8ExUghl+k/i0grl
  ZVq7uZW3SDL9tT4+1ffnBXKYgrLtAgMBAAECgYBOkrvNu7bqQ/yKiPl5MOzRzHWW
  I0OomxqnC1hkXbe/RGsFI+ueSQi+/Z2fN3XkghgmO6wFx5ds6GpZixgqarIz8z/Z
  AixGVx7BgUgAzIZ4OOsm7uLpPs7WEVLWn1I4/59HxnzWX85ShBsfJc4tFb566Bc2
  /5SaBurNXlOURFFs9QJBAPUL/qCWZ5JljXEtlLqaumEY54WT6+dJpLOj2bsmvktk
  CkMpzqCKy8ymiFPa5FyZDRsZfLQBoHWv7SVKDOwOFMcCQQDtwJcAsOrxWApQ19tr
  9wrrvOQBOXPkJjOL85x/I+6Q6CMd2YQs8ze2ex+J45VWtADQYi2VixgmtI9pNmW7
  eJ6rAkAe2s/I8KdB67+PjKm5hVoKd9RPIXOGtmMj3avAwPQdEg+ovU7jMBbRQfbQ
  eDNg5XSdAOyOzdWie/BkTZr3fJ5pAkEAr9OVGOK97ZxRjboyGRNMfVXdOwRV4YorJ
  5j9URkZ5gNrcVY/uixuX4TEvAte3MrbOPO3MLmL+imlQAdxD4h/zHwJBANYOvxVf
  8tzwPdXcNWK8ZCqmWLR8sDTrzRdwNejBraYbOOyEngGy1uALsDNevXtzrRkh8dzV
  QI5y+RliuFYWd14=
  -----END PRIVATE KEY-----
  ```

- ```
  IpaC8/W8s3UL9wDuz8pRUA3bG3jEOCh0MqCiVd3LXHBXSDRVckvD2OcUEnBkiG0N85NfY6rv
  M0iyb4fNkic4BhmLQg6AsV4L8LEIptSwPJwlVqJprqh7MHN+R9y/PekSmpZYAxitTaFFfgJP
  DhGYl45TmWLj2vhGoOQy/INK9boy=
  ```

- 今晚八点学校小树林见

1.6. 主机间的相互免秘钥

- 可以通过ssh命令免秘钥连接到其他的主

机 • 如果是第一次建立连接，需要输入yes

  - 在 ~/.ssh/known_hosts 文件记录了以前访问地址(ip hostname)的信息 ○ 在访问地址的时候如果没有收录到known_hosts文件中，就需要输入yes ○ 如果以前收录到known_hosts中，直接输入密码即可

- 需要输入密码
  - 生成秘钥
    - ```
      [root@basenode ~]# ssh-keygen -t rsa -P '' -f ~/.ssh/id_rsa
      Generating public/private rsa key pair.
      /root/.ssh/id_rsa already exists.
      Overwrite (y/n)? y
      Your identification has been saved in /root/.ssh/id_rsa.
      Your public key has been saved in /root/.ssh/id_rsa.pub.
      The key fingerprint is:
      SHA256:A187RixRSgQxCLUpssDbMuvxhb/4MmMoYP1jTE6RXhM root@basenode
      The key's randomart image is:
      +---[RSA 2048]----+
      |  .o..+++..      |
      |.   .o E +       |
      |o.. o o + +      |
      |.oo. o = + .     |
      |.+... o S +      |
      |..+..+   o .     |
      |oo..*.           |
      |o.o=+*           |
      |...o*+o          |
      +----[SHA256]-----+
      ```
    - ssh-keygen -t rsa -P '' -f ~/.ssh/id_rsa
      ```

- 如果你想免秘钥登录谁，只需要把自己的公钥传递给对方主机即可

- 这个秘钥要放在 ~/.ssh/authorized_keys

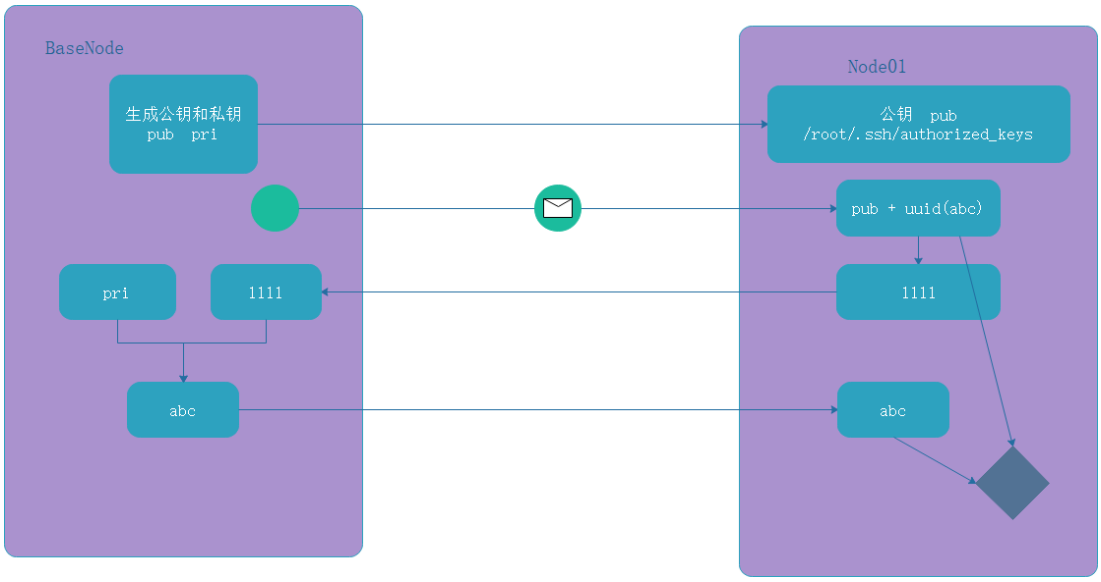
```
[root@basenode ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.58.100
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.58.100 (192.168.58.100)' can't be established.
ECDSA key fingerprint is SHA256:XkqG1QTiXPbFbKpPZIH0WPpAjsohJItzJvXFGg1drKY.
ECDSA key fingerprint is MD5:f7:b7:da:60:16:1b:18:b3:c4:9b:53:f6:65:32:7c:29.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.58.100's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.58.100'"
and check to make sure that only the key(s) you wanted were added.
```

  - ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.58.201

- 相互面秘钥工作流程



1.7. 主机名与Host校验

```
[root@sxtnode ~]# ssh localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:WvGciSiHIaSXdXciUY1M2f4fUiP04+H41z3+kWpgHUg.
ECDSA key fingerprint is MD5:ae:08:fc:68:ab:2d:a1:c5:39:2e:4b:33:16:c6:17:94.
Are you sure you want to continue connecting (yes/no)? yes
```

- 错误原因:
- Cannot determine realm for numeric host
- 解决方案1--本次
  - ssh -v -o GSSAPIAuthentication=no root@192.168.189.201

- 解决方案2--所有
    - 修改/etc/ssh/ssh_config文件的配置，以后则不会再

    出现此问题 ○ 最后面添加：

    - StrictHostKeyChecking no

      UserKnownHostsFile

      /dev/null