A+

ssh使用密钥进行认证

ssh可以基于密码进行认证，也可以基于密钥去认证用户，基于密钥认证时可以实现免密码登录的效果。

生成私钥与公钥

比如，张三平常使用密码连接到服务器A的root账户，现在可以利用公钥，免密码连接到服务器A的root账户，首先，张三要生成一对密钥，私钥与公钥，私钥是自
定不要泄露给它人，公钥是给别人用的，张三把公钥发给自己的朋友，朋友们就能用张三的公钥加密信息或者验证身份，当张三准备好了私钥与公钥，只要把公钥交
root账户"，当张三再次连接服务器A的root账户时，root账户就会使用张三的公钥验证张三的身份，此时，张三只要拿出自己的私钥，即可通过身份验证，成功的
的root账户中，当然，张三还可以把公钥交给服务器B的zsy账户，也可以把公钥交给服务器C的think账户，或者任意一个张三想要连接的服务器账户，都能够通过
通过认证，当然，如果有些心怀不轨的人窃取了张三的私钥，那么这个人就能冒充张三，因为拥有张三公钥的服务器"只认密钥不认人"，所以，我们一定要保管好自
对称加密并不是此处总结的重点，此处主要总结一下与ssh相关的一些命令，我们使用ssh-keygen命令即可生成私钥与公钥。

直接执行ssh-keygen命令，会进入交互模式，并等待用户输入生成密钥文件的路径，在不输入任何路径的情况下，私钥与公钥默认生成在当前用户家目录下的 .ssh
图所示，因为当前系统账户为root，所以，默认生成密钥路径为/root/.ssh/id_rsa，如果不指定其他路径，直接回车即可，如果对应目录下已经存在了同名的密钥文
你是否覆盖，在没有搞清楚是谁的密钥之前，最好不要覆盖，否则可能会导致私钥的丢失，下图中的情况为第一次生成密钥的情况，所以对应目录下并不存在同名的
接回车即可，随后，出现了Enter passphrase（输入密码）的提示，为了安全起见，我们可以为生成的私钥设置密码，如果为私钥设置了密码，在每次使用私钥的时
我们输入私钥的密码，直接回车，代表不为私钥设置密码，Enter same passphrase again表示确认密码，如果上一步没有输入密码，此处直接回车即可。

```
# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
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:
63:77:29:f0:a5:9c:f5:fc:08:34:63:a6:d5:eb:4b:76 root@cos72ini
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|               .   |
|        .   X .  |
|         + @ * . |
|        S O + +  |
|       . o o o o |
|              = E|
|             o o |
|              .  |
+-----------------+
```


ssh-keygen还有一些常用选项，文章结尾会对这些常用选项进行总结。

完成上述步骤后，即在用户家目录的.ssh目录中生成了一对密钥文件，私钥文件id_rsa与公钥文件id_rsa.pub

从文件名称可以看出，我们生成的是rsa密钥，我们也可以选择其他算法，从而生成其他类型的密钥文件，但是我们在生成秘钥时并未指定算法类型，所以，默认生成
密钥，现在大家都在版本2的ssh协议，在版本2的ssh协议中我们可以使用的密钥类型有： "dsa", "ecdsa", "ed25519", "rsa"

现在，我们已经拥有了自己的私钥与公钥，但是，我们并没有把公钥交给任何人，所以，其他人还无法利用我们的公钥对我们进行认证。

比如，我现在所在的服务器IP为10.1.0.1，我想通过10.1.0.1中的ssh客户端连接到10.1.0.3的zsy账户中，那么，我可能会执行如下命令。

```
10.1.0.1   10.1.0.3   +
# ssh zsy@10.1.0.3
zsy@10.1.0.3's password:
```

正如上图所示，10.1.0.3的zsy账户要求我输入密码，我必须输入10.1.0.3的zsy账户的密码才能够登录，有可能在某些场景下，你需要自动连接到10.1.0.3，比如在执
本的时候，所以，我们我要有一种方法，可以不用每次输入密码，也可以进行认证登录。

没错，聪明如你，一定想到了，我们需要把自己的公钥交给10.1.0.3的zsy账户，这样，zsy账户就能够通过我们公钥对我们进行身份认证了，于是，我现在需要做的
给10.1.0.3的zsy账户，我们可以使用一条命令，完成交付公钥的操作，这个命令就是ssh-copy-id

通过如下命令，可以将本机上指定的的公钥交给10.1.0.3的zsy账户

ssh-copy-id -i ~/.ssh/id_rsa.pub zsy@10.1.0.3

使用"-i"选项指定要传输的公钥，然后指明账户与IP地址，如下图所示，传输公钥时，要求我们输入zsy账户的密码，因为我们必须要知道密码，才能合法的连接到zs
然，这种密码验证只需要进行一次即可。

输入zsy用户的密码后，会出现类似如下提示

提示我们已经添加了1个密钥，并且提示我们尝试使用'ssh zsy@10.1.0.3'进行验证。

好了，完成上述步骤后，以后再从10.1.0.1的root账户连接10.1.0.3的zsy账户，就不用输入密码了，我们来试试看，如下。

如上图所示，已经可以免密码登录到对应的账户中。

我们已经把公钥交给了10.1.0.3的zsy账户，那么，zsy账户把我们的公钥放在了哪里呢？其实，用户会把别人的公钥放在家目录的.ssh/authorized_keys文件中

我们来一起看一下，zsy账户的authorized_keys中的内容，如下图

经过对比，你可以发现，上图中显示的公钥内容与10.1.0.1中root账户中的id_rsa.pub中的内容相同。

当然，目前只有一个公钥交给了zsy账户，如果有更多的人把自己的公钥交给zsy账户，那么authorized_keys文件中则会有更多条内容，分别代表不同的公钥。

聪明如你，一定想象到了，ssh-copy-id命令的作用是将公钥交给某个账户，如果不使用ssh-copy-id命令，我们是否也能够手动的将10.1.0.1中root账户中的id_rsa
拷贝到10.1.0.3的zsy账户的authorized_keys文件中呢？答案是肯定的，比如，我们可以直接在10.1.0.1上使用如下命令

cat ~/.ssh/id_rsa.pub | ssh -p 22 zsy@10.1.0.3 "umask 077;mkdir -p ~/.ssh;cat - >> ~/.ssh/authorized_keys"

这条命令与之前ssh-copy-id的命令效果是相同的，其实就是通过一连串的命令的将公钥内容加入到了对方服务器zsy账户的authorized_keys文件中。

你也可以不使用上述命令，而是纯手动的去'复制'、'粘贴'公钥中的内容，但是这样容易出错，因为对方服务器的账户中可能还没有对应的.ssh目录，也没有authoriz
件，你需要手动的创建它们，权限设置也容易出错，所以还是建议使用ssh-copy-id命令。

在大多数时候，公司中的sshd服务不会使用默认端口，所以，在使用ssh-copy-id命令时，可能需要指定sshd服务端的端口号。

但是在centos6与centos7中，使用ssh-copy-id指定sshd服务器端口的方法略有不同，假设对方sshd服务器端口号为22222，示例如下

当前系统为centos6：ssh-copy-id -i ~/.ssh/id_rsa.pub "zsy@10.1.0.3 -p 22222"

当前系统为centos7：ssh-copy-id -i ~/.ssh/id_rsa.pub zsy@10.1.0.3 -p 22222

没错，上述两种写法的细微差别就在于是否有引号。

当然，上述示例中，我们是将自己的公钥交给对方服务器的某个账户，我们再连接对方账户时，对方账户就可以使用我们的公钥对我们进行身份认证，如果反过来，
免密码连接到我们的账户，那么对方则需要将对方的公钥交给我们，操作步骤都是一样的。

相关问题

通常的问题是，你已经将本机的公钥推送到了对方服务器的某个账户中，但是仍然不能免密码登录对应账户。

出现上述问题，通常可能是由于如下原因引起的：

1、ssh服务端不支持基于公钥认证或者修改了默认的公钥认证文件

服务端可以禁用使用公钥认证的机制，PubkeyAuthentication配置项用于控制是否可以使用公钥进行认证，PubkeyAuthentication默认值为yes，表示支持公钥认
认使用authorized_keys作为存储用户公钥的文件，在服务端的sshd_config配置文件中可以使用AuthorizedKeysFile配置项指定其他文件为认证文件。

2、ssh服务端相关目录或者文件的权限过大

服务端用户家目录.ssh目录的权限正常700，服务端用户家目录.ssh/authorized_keys文件的权限默认为600

3、ssh服务端的authorized_keys文件中包含windows字符

通常纯手动复制粘贴公钥内容到authorized_keys并且操作时经过windows系统处理，会出现这种情况

4、ssh客户端连接服务端时，没有指定对应账户的用户名

如果我们想要从hostB的B账户连接到hostA的A账户，则需要在hostB中执行命令ssh A@hostA，如果在hostB的B账户中直接执行命令ssh hostA，并没有指定连接
表示连接到hostA中的B账户，也就是说，如果你在hostB的B账户中执行ssh hostA，相当于执行了ssh B@hostA，如果你把B的公钥交给了hostA的A账户，却在链
A账户，则很有可能会连错账户，自然无法认证成功，这种低级错误在你有些疲惫的时候很难发觉。

5、ssh客户端的私钥权限过大，正常情况下，将私钥的权限设置为600即可，如果权限过大，可能会在连接ssh服务端时看到如下提示

Permissions 0644 for '/root/.ssh/id_rsa' are too open.

It is required that your private key files are NOT accessible by others.

This private key will be ignored.

bad permissions: ignore key: /root/.ssh/id_rsa

6、在创建密钥对时，没有使用默认的密钥名称，比如id_rsa或者id_dsa，而是使用了自定义的密钥名称，如果将自定义名称密钥对中的公钥拷贝到了远程主机中，在
主机时，需要指定对应的自定义名称的私钥才能够实现免密码连接，使用"-i"选项可以指定密钥，当指定密钥后，ssh会使用指定的密钥与远程主机上的公钥进行认证
然使用默认名称的私钥进行认证，如果你自定义了密钥对的名称，但是在连接时没有指定对应私钥，由于默认私钥与远程主机中的自定义公钥不匹配，自然无法基于
证，会再次提示你输入密码。

相关命令总结

此处，对上文中的命令以及一些常用选项进行总结，以便以后回顾。

交互式生成密钥对

```
ssh-keygen
```

上述命令表示在完全交互的模式下生成密钥对

指定密钥对生成位置与名称

```
ssh-keygen -f /testdir/test/id_rsa
```

上述命令表示在/testdir/test目录下生成私钥id_rsa以及对应的公钥，-f选项表示直接指定密钥生成位置以及密钥的名称，但是还是会交互式的提示用户为私钥设置密
钥生成位置与名称后，在使用ssh命令连接到对应主机时，可以使用-i选项指定对应的密钥，比如:

```
ssh -i /testdir/id_rsa_zsy_testkey zsy@192.168.50.50
```

直接生成密钥对并设置密码

```
ssh-keygen -P '123456' -f /testdir/test/id_rsa
```

上述命令表示在/testdir/test目录下生成私钥id_rsa以及对应的公钥，并且为将私钥的密码设置为123456，-P (大写P)表示指定私钥的密码，上述命令不会进入交互
户不用输入任何信息即可生成密钥对，如果想要生成没有密码的私钥，只需要将 -P '123456' 改为 -P '' 即可。

为私钥添加密码，取消密码，修改密码

```
ssh-keygen -f /testdir/test/id_rsa -p
```

上述命令表示为私钥设置新密码，-p（小写p）表示为私钥设置新密码，无论私钥原来是否有密码，都可以使用此命令对私钥设置新密码，输入上述命令后，会进入
果原来私钥没有密码，则会直接提示输入新密码，即为私钥添加密码，如果私钥原来就有密码，则会提示先输入老密码，再提示输入新密码，即为修改私钥密码，如
有密码，现在想要取消原来的密码，只需要在提示输入新密码时直接回车即可。

生成指定类型的密钥

```
ssh-keygen -t dsa -P '' -f /testdir/test/id_dsa
```

上述命令表示生成dsa类型的密钥对，-t选项表示指定密钥的类型，即指定算法，版本2的ssh协议可以指定的密钥类型有 "dsa", "ecdsa", "ed25519", "rsa"

生成指定位数的密钥

```
ssh-keygen -t rsa -b 1024 -P '' -f /testdir/test/id_rsa
```

上述命令表示生成1024位长的密钥，-b用于指定密钥的位数。

根据私钥生成公钥

```
ssh-keygen -f /testdir/test/id_rsa -y
```

上述命令表示根据私钥生成对应的公钥，-y选项表示根据私钥生成对应的公钥，生成的公钥会打印在屏幕中，我们可以使用重定向生成公钥文件。

```
ssh-keygen -f /testdir/test/id_rsa -y > id_rsa.pub
```

如果私钥有密码，则需要在生成公钥是提供密码，用户需要在交互式模式中输入密码，如果不想使用交互式输入密码，可以使用-P选项（大写P）提供密码。

将公钥加入到指定账户的认证文件中

当ssh服务器使用默认端口号时，使用如下命令

```
ssh-copy-id -i ~/.ssh/id_rsa.pub zsy@10.1.0.3
```