Bastion使用指南

堡垒机通过bastion软件实现，可以实现如下功能：

1. 所有经过堡垒机登录内部服务器的用户无需使用密码登录，这有效地解决的用户密码管理问题。
2. 提供用户WEB UI管理界面，且用户管理基于角色管控，大大降低了用户管理维护工作量。
3. 所有用户的所有操作及输出均已日志方式保存，做到了有据可查，极大地方便了用户操作审计工作；
4. 防止用户随意上传下载文件，访问公网等【可选】【需要在目标服务器做防火墙策略】

# 一、堡垒机用户配置

下面以实现“z00190465@10.120.5.3无密码登陆zvisit18@10.120.5.18和zvisit20@10.120.5.20”为例说明整个配置步骤：

步骤一：参考《廊坊BigData环境VPN用户授权管理指导.docx》创建vpn用户z00190465；

步骤二：在堡垒机10.120.5.3上创建z00190465用户,设置密码；

10.120.5.3:~ # useradd –m -g bastion z00190465

10.120.5.3:~ # passwd z00190465

步骤三：在目标机器10.120.5.18和10.120.5.20上分别创建zvisit18和zvisit20用户（如果事先已存在可不创建）；

10.120.5.18:~ #useradd -m zvisit18

10.120.5.18:~ #passwd zvisit18

10.120.5.20:~ #useradd -m zvisit20

10.120.5.20:~ #passwd zvisit20

步骤三：切换到z00190465用户后，创建ssh的公钥密钥对；

10.120.5.3:~ #su - z00190465

z00190465@10.120.5.3:~ > ssh-keygen

步骤四：将公钥部署到目标机器的目标用户上；

z00190465@10.120.5.3:~ >ssh-copy-id -i /home/z00190465/.ssh/id\_rsa.pub [zvisit18@10.120.5.18](mailto:zvisit18@10.120.5.18)

z00190465@10.120.5.3:~ >sh-copy-id -i /home/z00190465/.ssh/id\_rsa.pub [zvisit20@10.120.5.20](mailto:zvisit20@10.120.5.20) 步骤五：测试是否可以不输密码登陆；

z00190465@10.120.5.3:~ >ssh [zvisit18@10.120.5.18](mailto:zvisit18@10.120.5.18)

z00190465@10.120.5.3:~ >ssh [zvisit20@10.120.5.20](mailto:zvisit20@10.120.5.20)

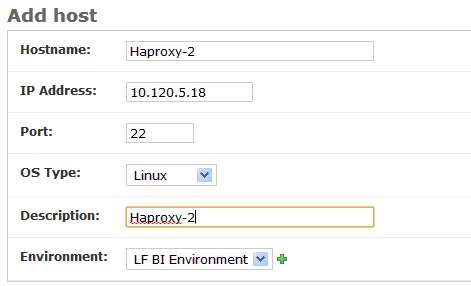
步骤六：root用户下修改10.120.5.3的z00190465用户的壳类型为/usr/local/bastion/main.py；

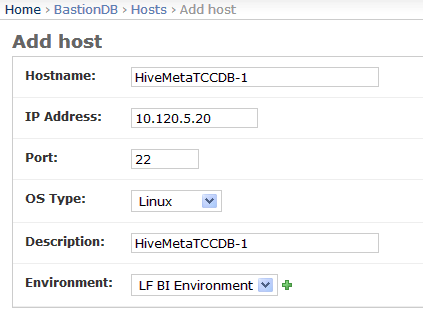
10.120.5.3:#chsh -s /usr/local/bastion/main.py z00190465

步骤六：通过管理页面<http://10.120.5.3/admin/>完成剩余配置。



添加主机10.120.5.18和10.120.5.20后，完成后单击页面右下角的save按钮保存。

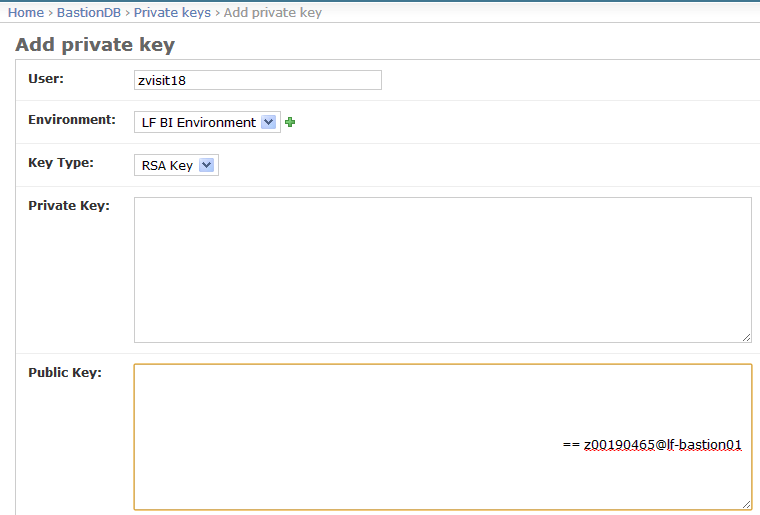


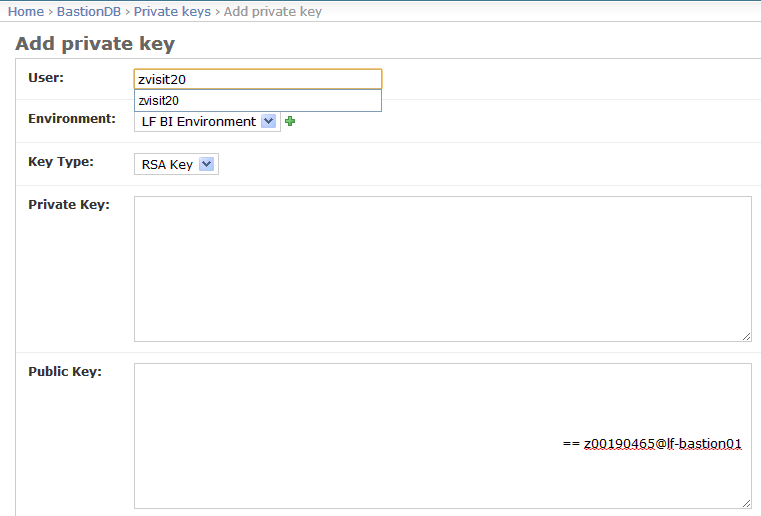


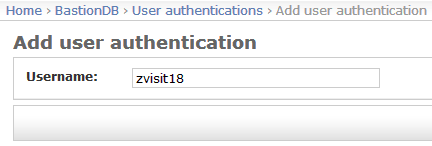
为需要登陆的目标主机用户(10.120.5.18,zvisit18)以及(10.120.5.20,zvisit20)添加认证用的公密钥对，private key和public key字段分别来源于如下命令，完成后单击页面右下角的save按钮保存。

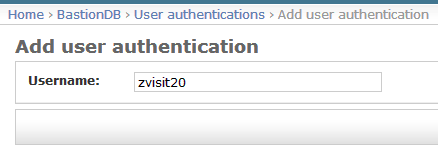
10.120.5.3~ #cat /home/z00190465/.ssh/id\_rsa

10.120.5.3~ #cat /home/z00190465/.ssh/id\_rsa.pub

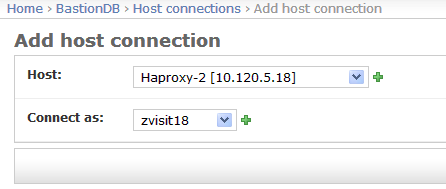


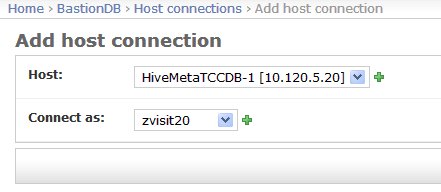


添加待认证用户zvisit18，zvisit20(Username必需和目标主机上的用户名一致)，完成后单击页面右下角的save按钮保存； 

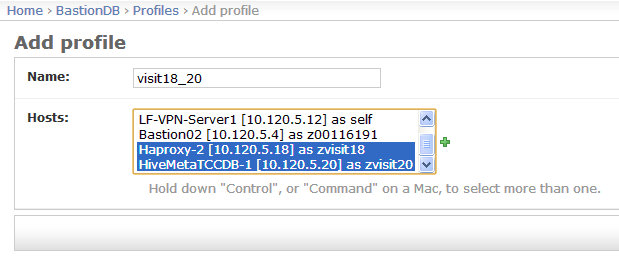


为zvisit18，zvisit20用户分别添加10.120.5.18和10.120.5.20的主机连接，完成后单击页面右下角的save按钮保存；

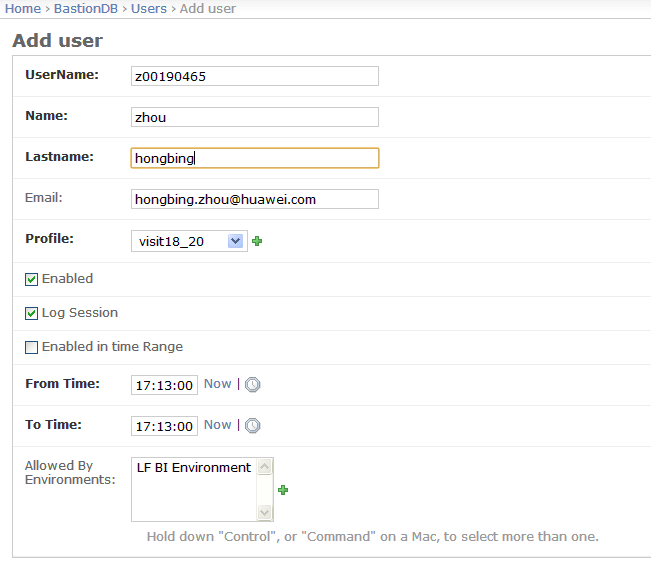




添加profile，hosts列表框可以通过ctrl和shift实现多选，完成后单击页面右下角的save按钮保存；



创建最终用户（UserName必需和堡垒机上分配的OS用户名z00190465一致），可用于禁用或者启用该用户以及限制可登陆的时间点（中文名支持的不太好），完成后单击页面右下角的save按钮保存。



步骤七：限制zvisit18、zvisit20访问公网【可选】

1. 使用root账号编辑suse的防火墙配置文件，配置FW\_CUSTOMRULES参数为；

FW\_CUSTOMRULES="/etc/sysconfig/scripts/SuSEfirewall2-custom"

10.120.5.18~ #vi /etc/sysconfig/SuSEfirewall2

b、替换/etc/sysconfig/scripts/SuSEfirewall2-custom文件以增加iptables的规则（首次配置需要替换，以后只需处理c）；

c、在/etc/sysconfig/bastion文件的BASTION\_POLICY\_NOINTERNET项中增加要限制访问公网的用户；



BASTION\_POLICY\_NOINTERNET="zvisit18"

d、重启防火墙；

10.120.5.18~ #SuSEfirewall2 stop

10.120.5.18~ #SuSEfirewall2 start

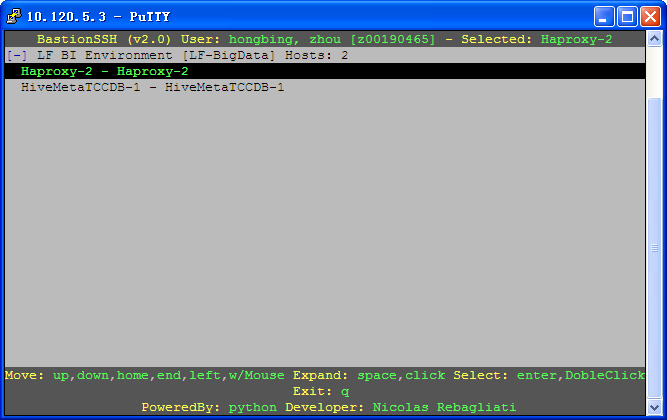
# 二、bastion维护信息

1. 应用程序目录：/usr/local/bastion/
2. 日志目录：/var/log/bastion/
3. 管理后台启动命令：nohup /usr/local/bastion/BastionSSH/manage.py runserver 10.120.5.3:80 > /var/log/bastion/bastion.log 2>&1 &

# 三、bastion用户使用

步骤一：参考《廊坊BigData环境VPN拨入指导.docx》使用z00190465（vpn）账户接入廊坊BI网络；

步骤二：利用putty等ssh客户端工具使用z00190465（OS系统用户）账户登陆10.120.5.3堡垒机；



选择指定的目标主机回车即可登陆成功

