# TEMU使用

## Ubuntu9安装samba和图形管理界面

### 在终端下卸载samba,smbclient,samba-common

$sudo apt-get remove samba-common

$sudo apt-get remove smbclient

$sudo apt-get remove samba

### 安装Ubuntu samba服务器

命令: sudo apt-get install samba

sudo apt-get install smbfs

启动: sudo /etc/init.d/samba start

到这里，你已经可以去访问别人共享的目录了如smb://192.168.2.187/

### 安装Ubuntu samba图形管理界面

命令: sudo apt-get install system-config-samba

启动Ubuntu samba:

命令: sudo /etc/init.d/samba start

### 启动管理界面

命令: sudo system-config-samba

也可以在点击菜单项进去： 系统－系统管理－Samba

可添加共享目录,选中可访问用户. 设置用户smb密码命令为: sudo smbpasswd -a 用户名在配置时，要选上“可见”，否则就是隐藏的了，别人就看不到你的共享了这样重启之后别人就可以访问你共享的目录了

### 设置完毕之后要重启:

sudo /etc/init.d/samba restart

## Ubuntu10安装samba及图形界面

<http://bbs.chinaunix.net/thread-2302433-1-1.html>

<http://forum.ubuntu.org.cn/viewtopic.php?p=1892143>

### 方案1

sudo apt-get install samba

sudo apt-get install smbfs

sudo apt-get install samba-common-bin

此时init.d目录下没有samba这个文件，参考网上的，在/etc/cron.daily下有samba

将文件复制到对应目录

sudo cp /etc/cron.daily/samba /etc/init.d/

然后安装图形界面进行设置

### 方案2

sudo apt-get install samba samba-client samba-common

sudo apt-get install smbfs

sudo apt-get install samba-common-bin

然后执行

crifan@crifan-ubuntu10:~$ **sudo /etc/init.d/smbd start**

按照提示，执行

crifan@crifan-ubuntu10:~$ **sudo service smbd start**start: Job is already running: smbd

就可以启动samba服务了。接着安装samba图形管理界面

sudo apt-get install system-config-samba

然后，就可以通过 系统 -> 系统管理 -> Samba，启动samba的图形界面，对samba进行设置。设置完成后重新启动。

### 查看samba服务是否已经启动

|  |
| --- |
| **ps -aux** |

如果进程太多，那么就：

|  |
| --- |
| crifan@crifan-ubuntu10:~$ **ps -aux | grep smbd** Warning: bad ps syntax, perhaps a bogus '-'? See <http://procps.sf.net/faq.html> root 5426 0.0 0.2 16704 4160 ? Ss 20:02 0:00 smbd -F root 5439 0.0 0.0 16704 1236 ? S 20:02 0:00 smbd -F root 6527 0.0 0.2 17012 4176 ? S 20:23 0:00 smbd -F crifan 6873 0.0 0.0 5628 764 pts/0 S+ 20:55 0:00 grep --color=auto smbd |

其中找到smbd，就说明samba的服务已经启动了。   
另外，去查看nmbd服务是否也已经启动：

|  |
| --- |
| crifan@crifan-ubuntu10:~$ **ps -aux | grep nmbd** Warning: bad ps syntax, perhaps a bogus '-'? See <http://procps.sf.net/faq.html> crifan 6880 0.0 0.0 5628 764 pts/0 S+ 20:56 0:00 grep --color=auto nmbd |

其中smbd和nmbd的解释是：   
<http://hi.baidu.com/chenyangxin/blog/item/9c388050681bfd738535248e.html>  
“可以看到Samba服务会同时启动两个服务，其中smbd主要用来管理共享出来的目录，nmbd主要用来解析NetBIOS名。在Windows系统中，主机可以被加入一个组中，这样每个主机都必须有一个名字，这个名字是用于在网上被标志的名，并非机器的主机名，将其称为NetBIOS名。其中nmbd进程是随着smbd进程启动而启动。

# 简单的共享设置

<http://blog.csdn.net/tjhd1989/article/details/8189570>

启动虚拟机后，可以直接上网，但是主机和虚拟机共享需要配置，主机可以选择安装samba服务器，ubuntu下用图形工具system-config-samba配置很简单。

将temu-1.0文件或其他文件共享，在虚拟机的资源管理器中输入\\10.0.2.2就可以看到。

将temu-1.0\testdrv\driver目录下的testdrv.sys驱动文件拷贝至%SYSTEM32%\drivers目录下。然后双击testdrv.reg文件将内容拷贝至注册表来配置驱动程序，它将会在下次启动后加载。若要确认该驱动是否工作正常，在TEMU运行的目录中寻找是否创建了guest.log文件，其包含了一些TEMU收集的数据。

也可以打开dos窗口，用命令复制文件：

net use \\10.0.2.2

net view \\10.0.2.2

copy \\10.0.2.2\shared\testdrv.sys c:\

# [在Qemu/KVM下虚拟Windows XP中的鼠标位置偏移问题](http://blog.csdn.net/wangjingfei/article/details/6100966)

<http://blog.csdn.net/wangjingfei/article/details/6100966>

在Qemu/KVM中虚拟一个windows xp操作系统，发现用VNC（使用kvm -vnc :1参数启动qemu的VNC）登录windows的时候，出现严重的鼠标偏移现象，无法控制鼠标，很难对windows进行操作。

Google了一下，发现Xen中也出现了类似的问题：

<http://blog.csdn.net/jcwKyl/archive/2010/12/16/6079385.aspx>

以上博客中提到的解决方法一很简单，但是和实际操作有一些出入，不知道是不是因为windows XP版本的问题。具体修改方法如下：

控制面板->鼠标（如果没有，请先切换到经典模式）->指针选项

把其中“提高指针精度”选项去掉即可。

------------ 华丽的分割线 ----------

如此完成后，在刚通过VNC进入windows xp系统时，VNC中的鼠标和真实鼠标还是有一些偏移，只不过这个偏移的大小是不会乱变的。这是因为相对定位鼠标引起的，解决的方法也比较简单，在Qemu启动的时候，把所有的相对定位设备改为绝对定位设备，即在Qemu启动参数中加入以下参数即可：

**-usbdevice tablet**

# 安装temu驱动

<http://blog.sina.com.cn/s/blog_55a8a96d0100rkor.html>

在虚拟机中将[TEMU源码中](http://bitblaze.cs.berkeley.edu/release/temu-1.0/temu-1.0.tar.gz)的testdrv/driver目录下的testdrv.sys驱动文件拷贝至%SYSTEM32%\drivers目录下。然后双击testdrv.reg文件将内容拷贝至注册表来配置驱动程序，它将会在下次启动后加载。若要确认该驱动是否工作正常，在TEMU运行的目录中寻找一个创建是guest.log文件，包含一些TEMU收集的数据。注意，虚拟机可以正常连接网络，但无法与host OS交互，若要实现此功能，还需要进行一些其它配置，这里省略。

驱动安装成功后，一个用于TEMU分析的Windows映像就做好了，为了避免今后误操作将该映像损坏，在进行动态分析时可以使用映像的快照进行分析，启动时输入

temu -snapshot -monitor stdio -kernel-kqemu winxp.qcow2

# 存在的问题与解决

针对TEMU-0.1.0

<http://blog.163.com/wuzhiyong_430/blog/static/488830522010111765422286/>

1）在安装guest系统的过程中，有时最好添加下面选项：

"-k en-us": 这样guest系统中的键盘不会失效，如在guest系统中安装ubuntu1004系统；

“no-kqemu": kqemu固然可以加速，但是如果添加此项，才能够顺利进入X界面；

2）如果guest系统是windows，则使用sp1的windows，或者使用sp2的windows。sp3的windows是没有用的。（安装目录下taintcheck.c文件增加支持）

如：TEMU中的插件tracecap运行将会失效，不能够把tainted的instructions记录到trace文件当中。

# 6 黑帽案例

## 设置

(qemu) load\_plugin ./tracecap/tracecap.so

Could not find INI file: /etc/bitblaze/tracecap/main.ini

Use the command 'load\_config <filename> to provide it.

Cannot determine file system type

Cannot determine file system type

Cannot determine file system type

./tracecap/tracecap.so is loaded successfully!

(qemu) load\_config ./tracecap/main.ini