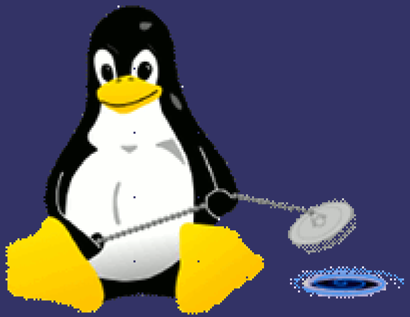


Remote Administration of Desktop Systems

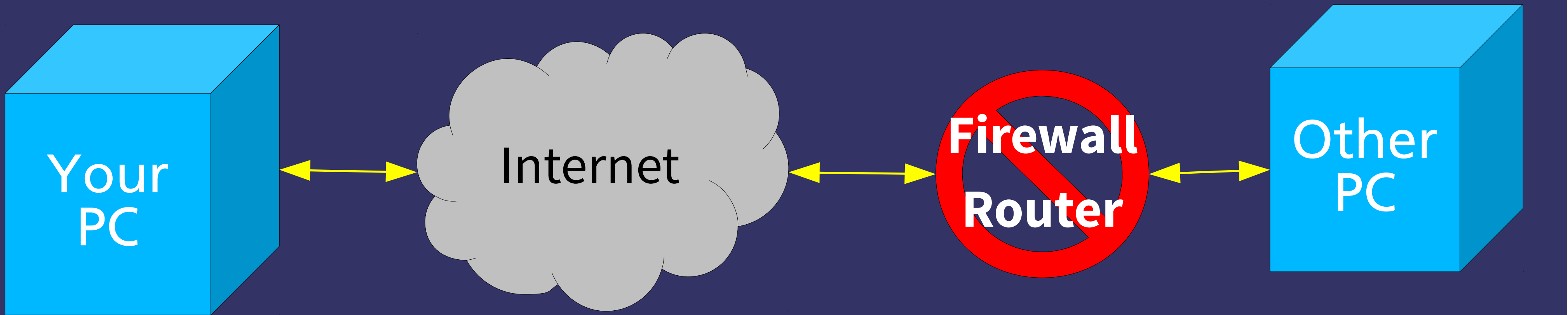
Adam John Trickett

www.iredale.net
adam.trickett@iredale.net
PGP Key: 0xAF0DB8C8

General problem

- You need to connect to a remote system
- You need to administer the system (upgrade, repair, extend etc.)
- You need to see the desktop as the user sees it
- The end user may not be technical

Topology



Technical problems

- Where is the other PC?
  - Most ISP only offer dynamic IP
- How do I get through the firewall?
  - Each make and model is different
- How do I reach the PC on the inside?
  - Most networks use dynamic & private IPs on the inside
- What needs to be installed on the target system?
  - Not all systems have everything installed by default

Where is the other PC

- The best solution is a static IP for the router/firewall
  - Standard with some ISPs
  - Optional cost extra with others
- If dynamic is the only option, then:
  - Some routers/firewalls will auto-update Dynamic DNS services
  - You can install a dynamic DNS client on the target PC
  - You can create a script to email you the external IP

Firewall - rules

- Most sane routers allow:
  - All ports outbound
  - All ports inbound that are part of an outbound pair
  - All ports inbound that are not part of a pair are denied
- You will need to tell it to allow at least one port inbound:
  - Some have virtual “DMZ”
  - Some have general rules

Router - Forwarding

- The remote system's firewall/router needs to forward incoming connections:
    - of type X, e.g. tcp
    - of port Y, e.g, 22
    - to IP address Z, e.g. 192.168.0.10
- External port number and internal port number are the same by default

Router – NAT/DHCP

- You need to ensure that the PC you want to reach has the same private IP so that the NAT rule points to the correct system every time:
  - DHCP reservation using MAC address
  - Static configuration in router and PC

Basic tools - SSH

- Secure Shell (“SSH”)
  - Replaces Telnet, rlogin, rsh, ftp etc
  - Standard on almost all Linux/Unix systems
  - Secure
  - Supports port forwarding
  - Creates a temporary on-demand instant “VPN-lite”

Extra tools

- Mobile Shell (“Mosh”)
  - Deals with lost connections better than SSH
  - Does not support port forwarding
- OpenVPN
  - Builds a permanent secure bridge between systems
  - Doesn't require user configuration to use
  - Requires administrative configuration to set-up
  - More complex than SSH

General installation

- OpenSSH server, though in all distros is not installed by default on all of them
- Mosh is widely available but not installed by default on most/all
- Sudo is widely available and installed by default on many but all
- Screen is widely available but not installed by default on most/all

Specific installation

- linuxvnc shares the physical console as VNC session, useful in emergencies or headless servers
- `x11vnc` shares the desktop X session as a VNC session and allows you to interact with the desktop at the same time as the user
- There are others but I'm not going to talk about them

Forwarding SSH ports

- The remote system's firewall/router needs to:
  - Forward TCP port on the external side to TCP port on the target PC
  - SSH normally uses tcp port 22
  - Mosh normally uses udp port 60001 (and up) plus SSH to start with only
- Many people change the external port to reduce the noise from script kiddies

Basic Administration

- Use SSH/Mosh to connect to the remote system
  - Default SSH configuration will work but you need to harden it
  - Run normal command line tools from login shell of your choice
  - Good for day to day administration and all standard tasks
  - No good if you need to see what the user sees or configure a desktop application

Harden SSH

- Open SSH is pretty good but it is not as secure as it can be out of the box on most Linux distributions:
  - Turn off password login – only allow SSH keys
  - Turn off root login – only allow real users
  - Specify the named users you want to allow
  - Turn off SSH protocol 1 – it may still be turned on in some distros

Configure SSH Client

- Edit your `~/.ssh/config` file:

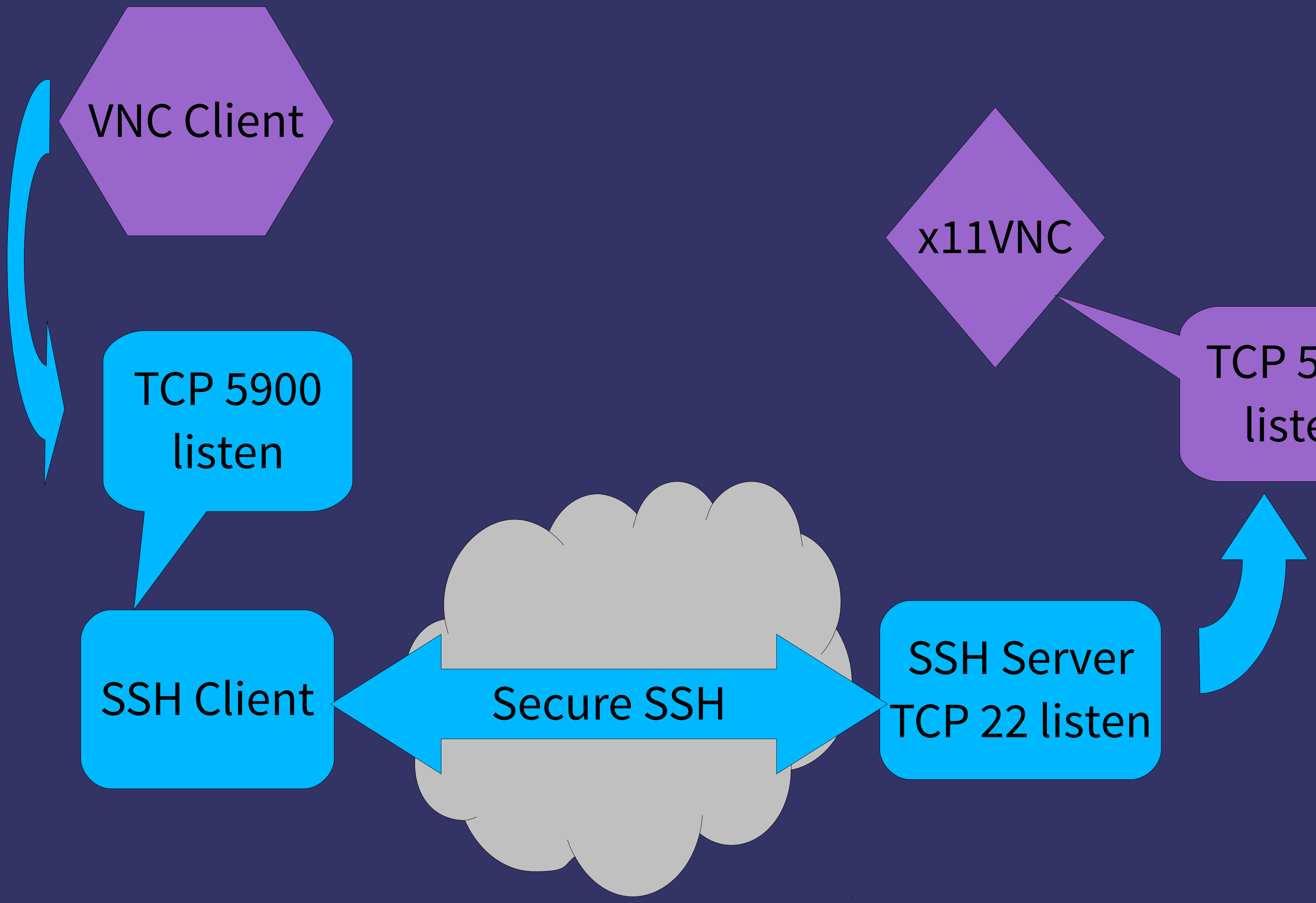
```
Host            <machinename>* <ip address>
HostName        <machinename.network.com>
user            <your username on machinename>
Port            <TCP port number>
ForwardX11      yes
Compression     yes
LocalForward    localhost:5900 localhost:5900
```

Procedure

- Add your SSH-Key to your SSH-Agent
- Start your SSH session to the other system
  - ssh machinename
- Your default shell starts at the other end
  - Start screen
  - Start any X programs
  - Start x11vnc or linuxvnc
- Start your VNC client on your desktop

What does SSH forwarding do?

- When you start x11vnc or linuxvnc they start to listen on the local host of the remote system on tcp port 5900 by default
- The SSH client on your PC also listens on TCP port 5900 locally, but forwards the packets to the remote system to its TCP port 5900
- That means an insecure protocol like VNC is now running over a secure and compressed SSH connection


VNC Client
x11VNC
TCP 5900 listen
TCP 5900 listen
SSH Client
Secure SSH
SSH Server TCP 22 listen

x11vnc configuration

- To automate and get the best out of x11vnc without end user interaction – there are a lot of options!
- Something like:

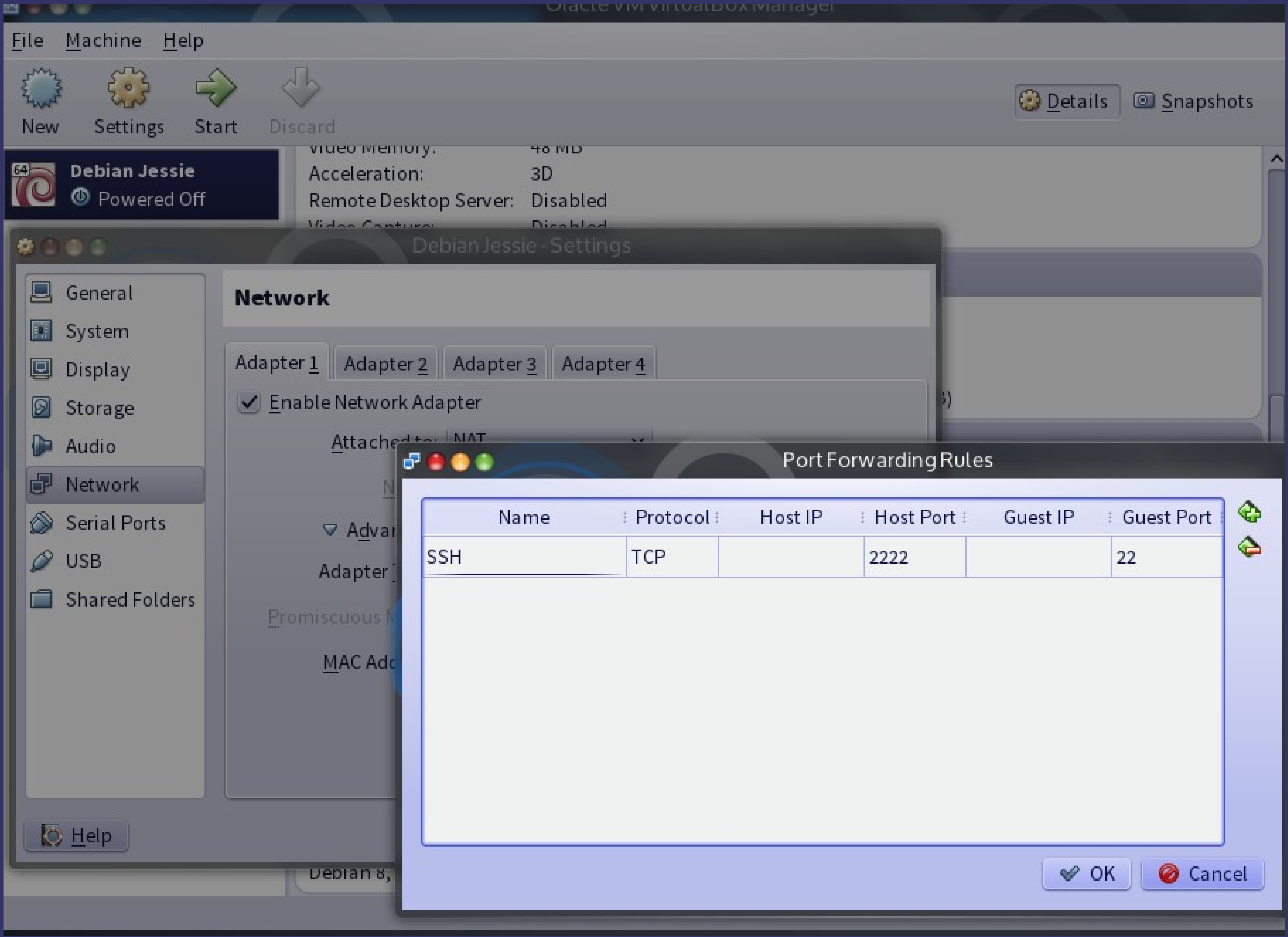
```
$ sudo x11vnc -nopw -localhost -ncache 10 -ncache_cr \
 -q -nodpms -auth <something>
```

linuxvnc configuration

- Exports a physical terminal
- Useful if X has failed to start
- Allows you to see kernel messages etc
- Of only limited use, but nice to know

```
$ sudo linuxvnc 1 -alwaysshared
```

Demo



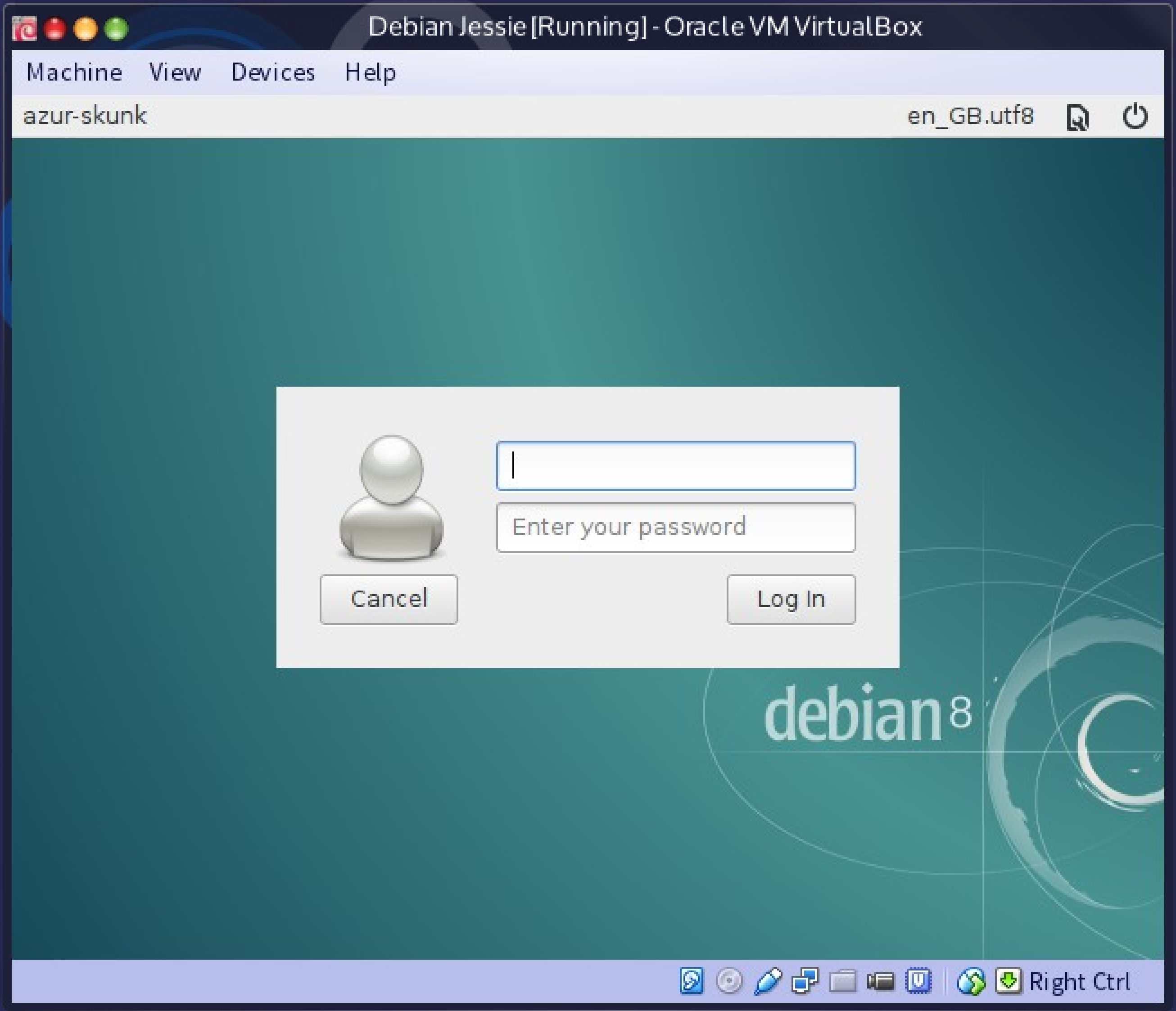
Video Memory: 48 MB
Acceleration: 3D
Remote Desktop Server: Disabled
Video Capture: Disabled

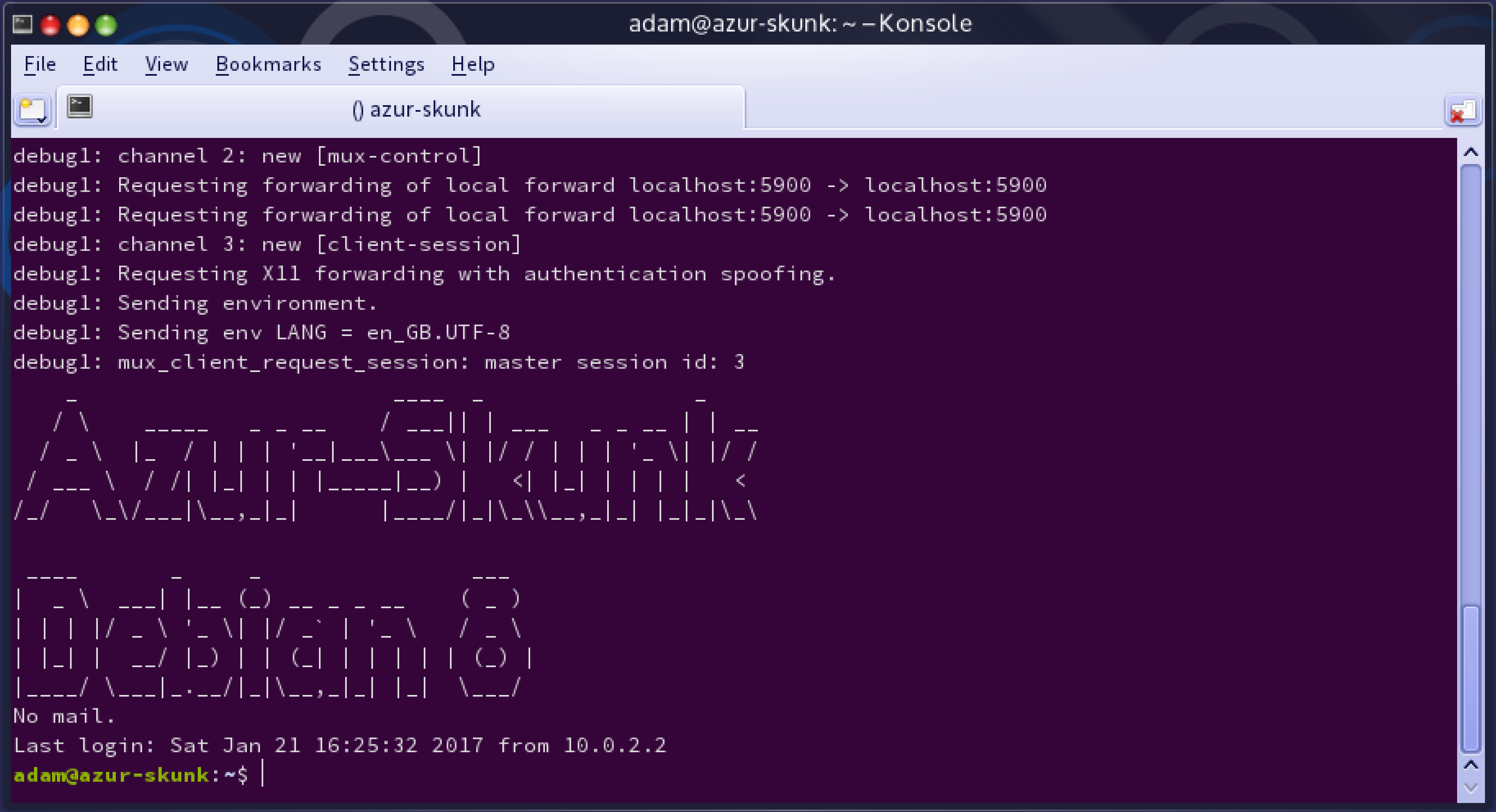
Network

☑ Enable Network Adapter

Attached to: NAT

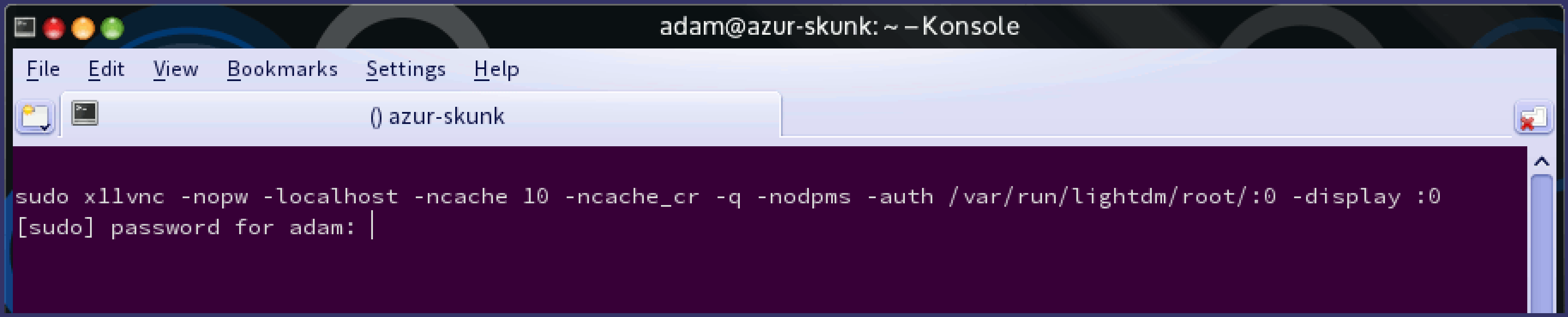
Name	Protocol	Host IP	Host Port	Guest IP	Guest Port
SSH	TCP		2222		22


Debian Jessie [Running] - Oracle VM VirtualBox
Machine
View
Devices
Help
azur-skunk
en_GB.utf8
Enter your password
Cancel
Log In
debian 8
Right Ctrl

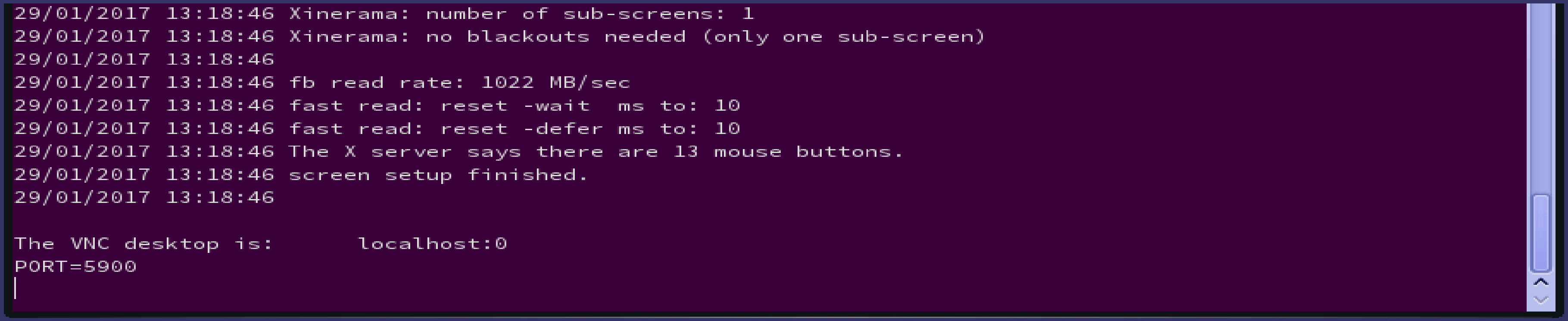


```
debug1: channel 2: new [mux-control]
debug1: Requesting forwarding of local forward localhost:5900 -> localhost:5900
debug1: Requesting forwarding of local forward localhost:5900 -> localhost:5900
debug1: channel 3: new [client-session]
debug1: Requesting X11 forwarding with authentication spoofing.
debug1: Sending environment.
debug1: Sending env LANG = en_GB.UTF-8
debug1: mux_client_request_session: master session id: 3
    _                         ____  _                _
   / \    _____   _ _ __    / ___|| | ___   _ _ __ | | __
  / _ \  |_  / | | | '__|___\___ \| |/ / | | | '_ \| |/ /
 / ___ \  / /| |_| | | |_____|__) |   <| |_| | | | |   <
/_/   \_\/___|\__,_|_|      |____/|_|\_\\__,_|_| |_|_|\_\


 ____       _     _                ___
|  _ \  ___| |__ (_) __ _ _ __    ( _ )
| | | |/ _ \ '_ \| |/ _` | '_ \   / _ \
| |_| |  __/ |_) | | (_| | | | | | (_) |
|____/ \___|_.__/|_|\__,_|_| |_|  \___/
No mail.
Last login: Sat Jan 21 16:25:32 2017 from 10.0.2.2
adam@azur-skunk:~$ 
```

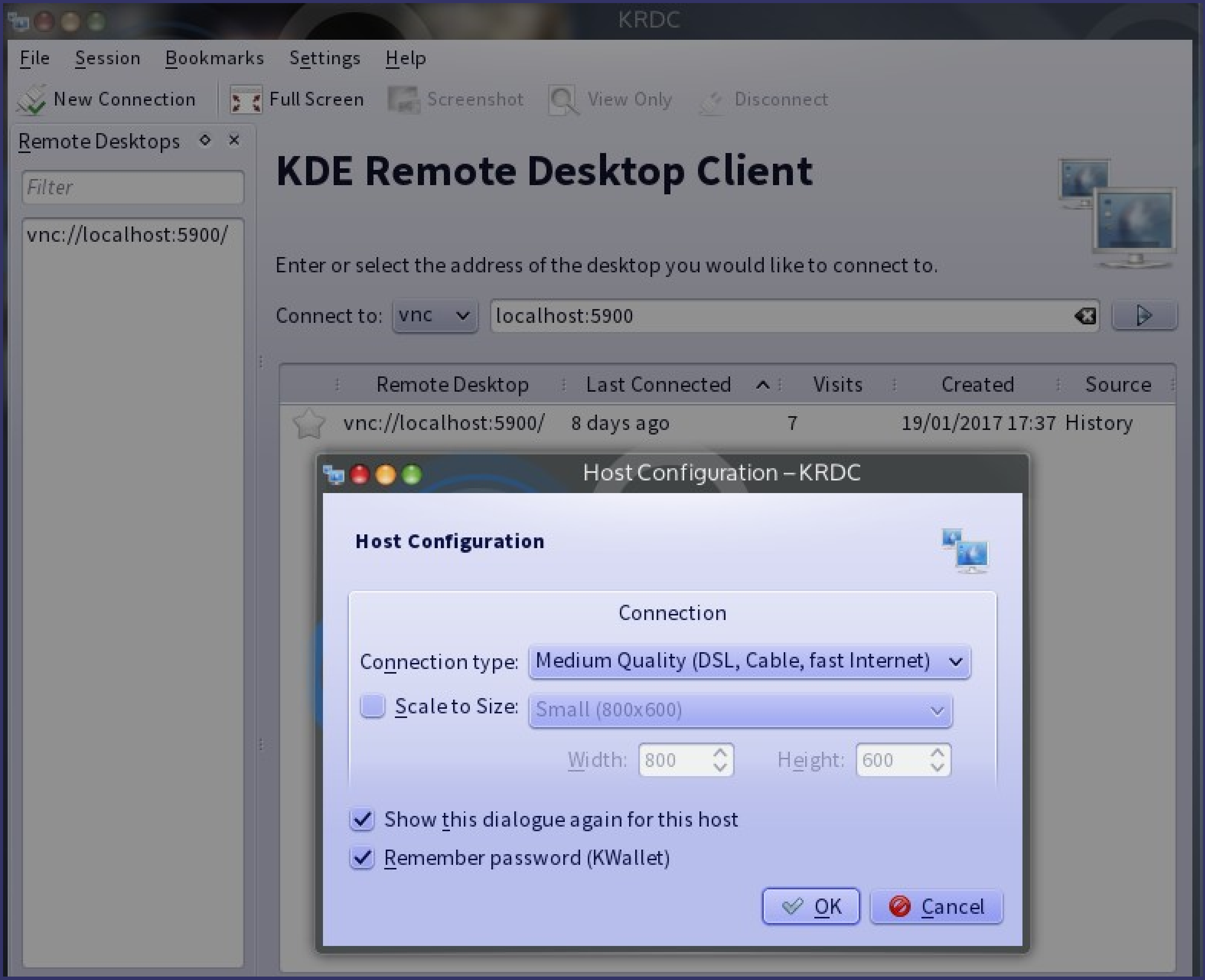


```
sudo x11vnc -nopw -localhost -ncache 10 -ncache_cr -q -nodpms -auth /var/run/lightdm/root/:0 -display :0
[sudo] password for adam: 
```



```
29/01/2017 13:18:46 Xinerama: number of sub-screens: 1
29/01/2017 13:18:46 Xinerama: no blackouts needed (only one sub-screen)
29/01/2017 13:18:46
29/01/2017 13:18:46 fb read rate: 1022 MB/sec
29/01/2017 13:18:46 fast read: reset -wait  ms to: 10
29/01/2017 13:18:46 fast read: reset -defer ms to: 10
29/01/2017 13:18:46 The X server says there are 13 mouse buttons.
29/01/2017 13:18:46 screen setup finished.
29/01/2017 13:18:46

The VNC desktop is:      localhost:0
PORT=5900
```



KDE Remote Desktop Client

Enter or select the address of the desktop you would like to connect to.

Connect to: vnc localhost:5900

vnc://localhost:5900/

Remote Desktop	Last Connected	Visits	Created	Source
vnc://localhost:5900/	8 days ago	7	19/01/2017 17:37	History

Host Configuration

Connection

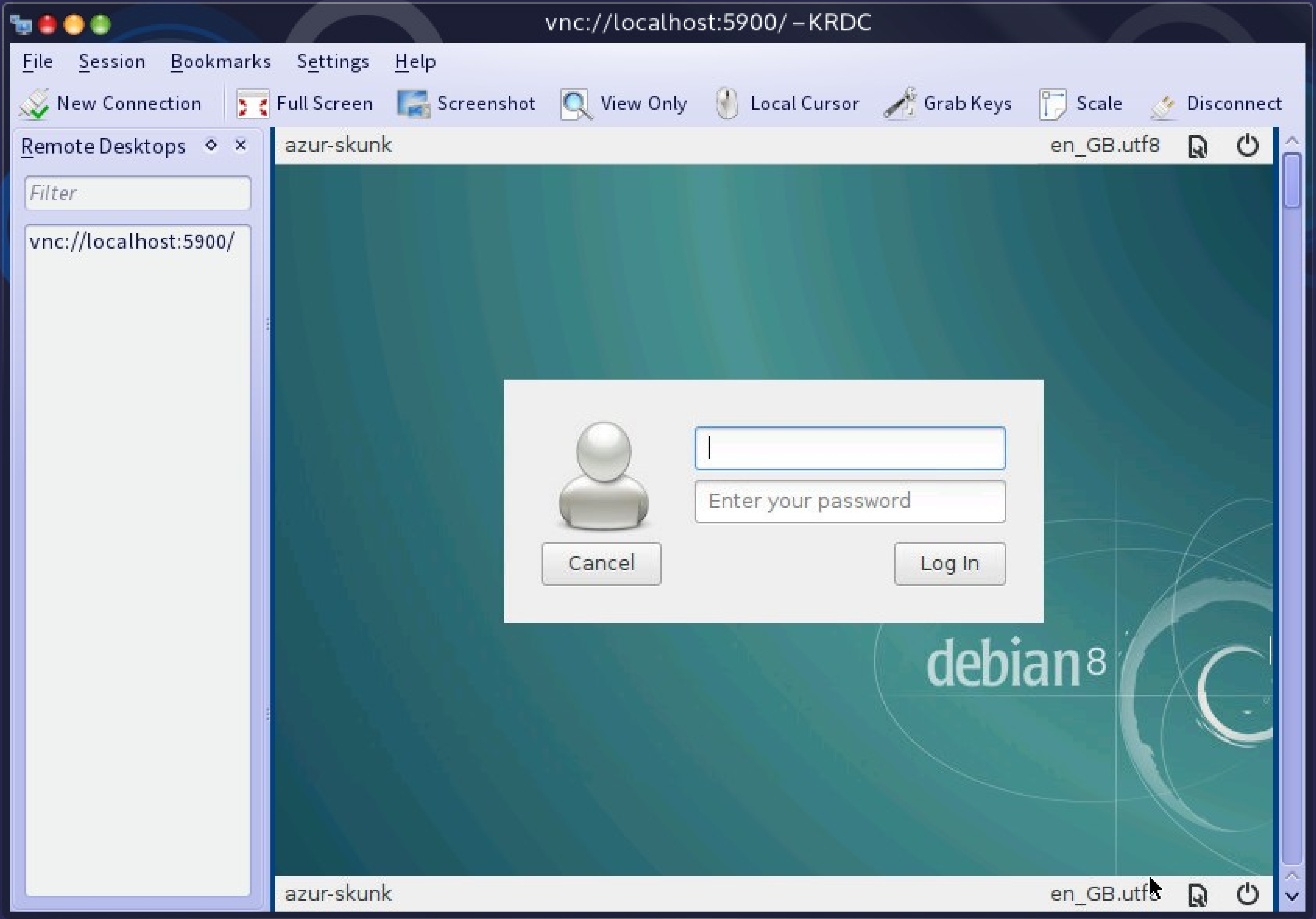
Connection type: Medium Quality (DSL, Cable, fast Internet)

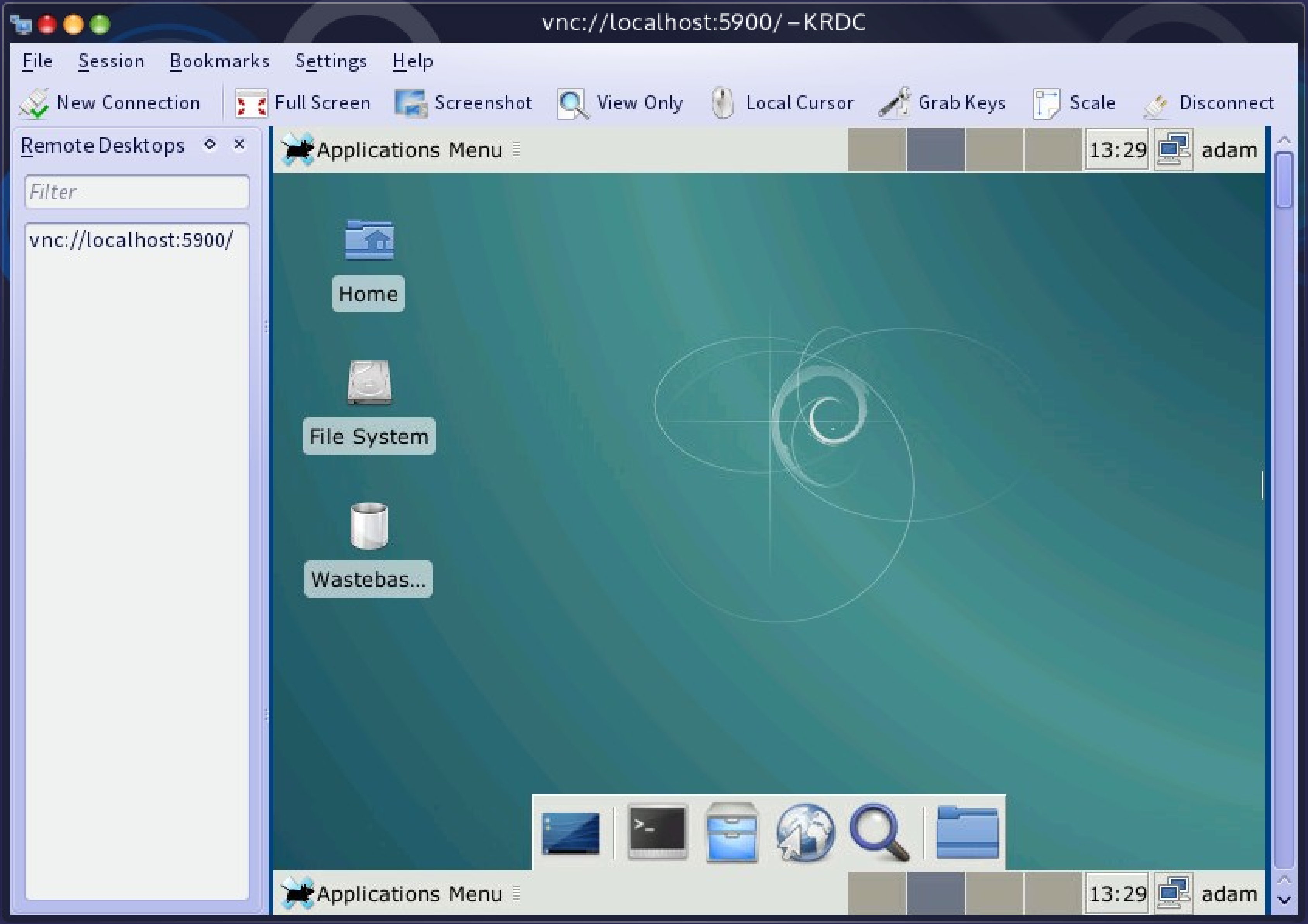
□ Scale to Size: Small (800x600)

Width: 800 Height: 600

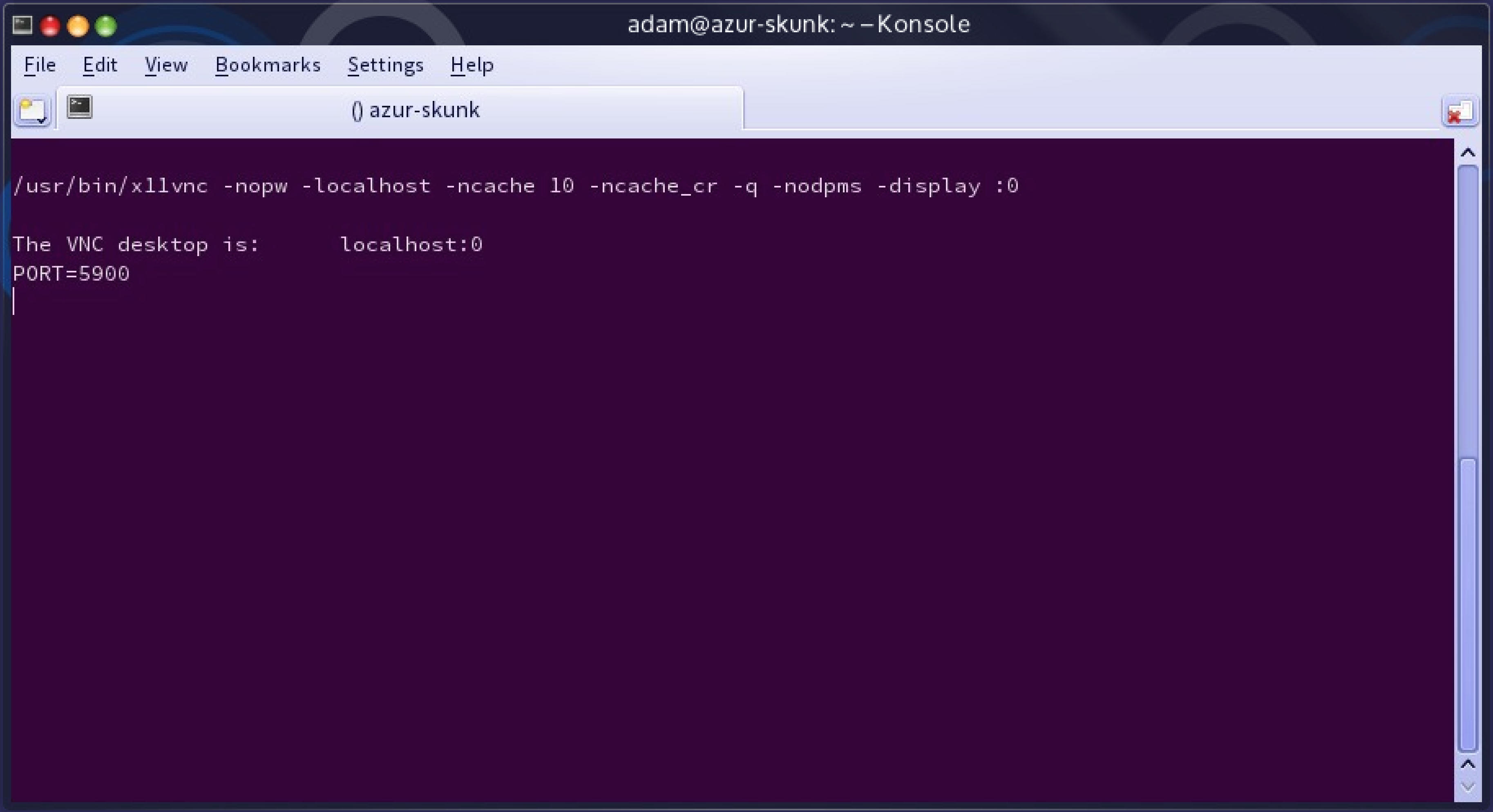
☑ Show this dialogue again for this host

☑ Remember password (KWallet)


vnc://localhost:5900/ – KRDC
File
Session
Bookmarks
Settings
Help
New Connection
Full Screen
Screenshot
View Only
Local Cursor
Grab Keys
Scale
Disconnect
Remote Desktops
Filter
vnc://localhost:5900/
azur-skunk
en_GB.utf8
Enter your password
Cancel
Log In
debian 8
azur-skunk
en_GB.utf8



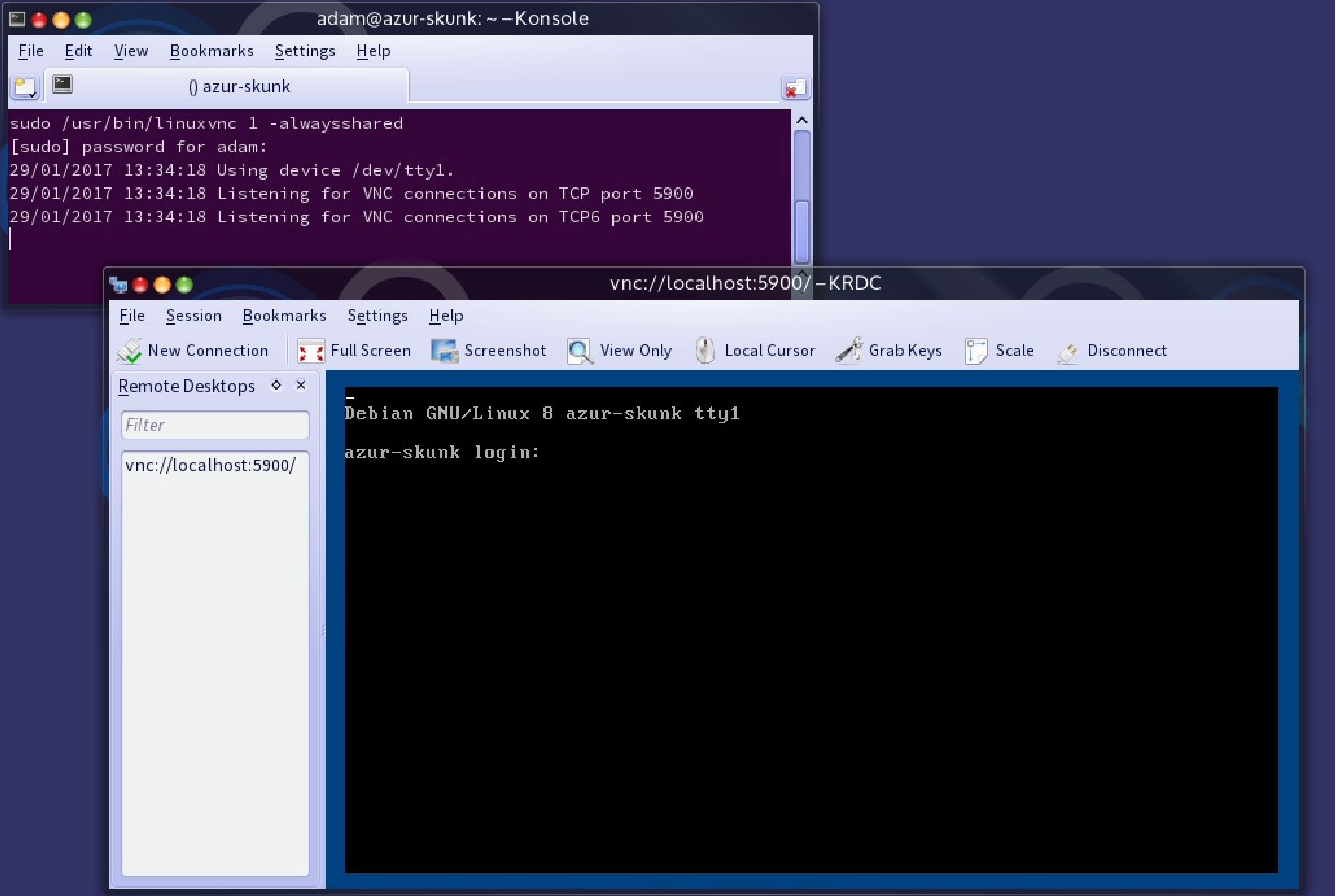
vnc://localhost:5900/ – KRDC
File
Session
Bookmarks
Settings
Help
New Connection
Full Screen
Screenshot
View Only
Local Cursor
Grab Keys
Scale
Disconnect
Remote Desktops
Filter
vnc://localhost:5900/
Applications Menu
13:29
adam
Home
File System
Wastebas...
Applications Menu
13:29
adam



adam@azur-skunk: ~ – Konsole
File Edit View Bookmarks Settings Help
() azur-skunk

```
/usr/bin/x11vnc -nopw -localhost -ncache 10 -ncache_cr -q -nodpms -display :0

The VNC desktop is:      localhost:0
PORT=5900
```



adam@azur-skunk: ~ – Konsole
File Edit View Bookmarks Settings Help
() azur-skunk

```
sudo /usr/bin/linuxvnc 1 -alwaysshared
[sudo] password for adam:
29/01/2017 13:34:18 Using device /dev/tty1.
29/01/2017 13:34:18 Listening for VNC connections on TCP port 5900
29/01/2017 13:34:18 Listening for VNC connections on TCP6 port 5900
```

```
_
Debian GNU/Linux 8 azur-skunk tty1

azur-skunk login:
```

Thank You

Any Questions?