



# Cooking with Splunk



*HOWTO build a powerful, secure,  
portable, and free (as in beer) log  
analysis platform*

*Justin Hall*





# A delicious forensic log analysis platform

Cook time: **1-2 hours**

## Ingredients

**1 virtual computing platform**

recommended: **Oracle VirtualBox**

**1 copy of Linux**

recommended: **Ubuntu Linux Server 10.04 LTS**

**1 copy of Splunk**

recommended: **Splunk 4.2 for Linux**

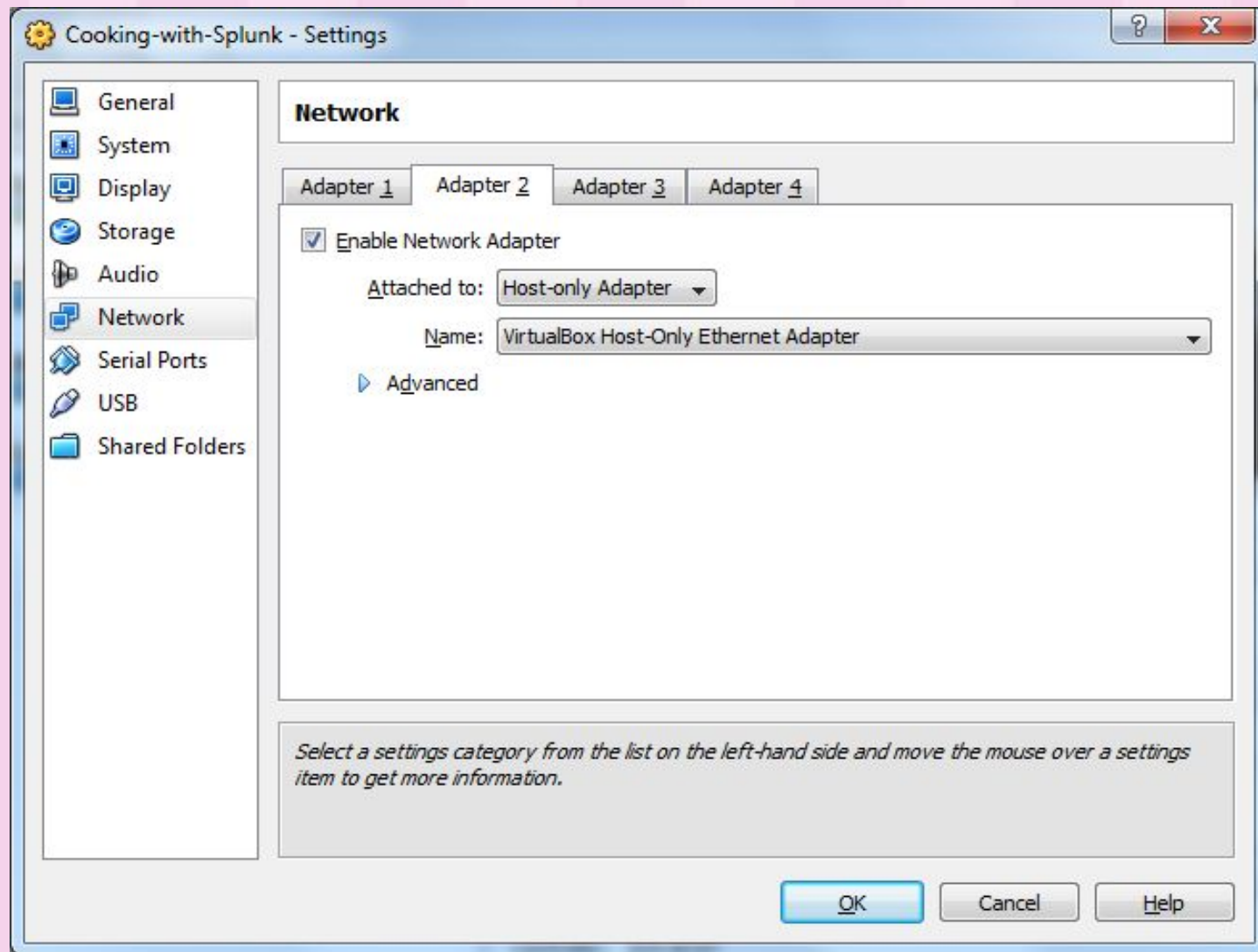
**12 oz cold beverage**

to consume while building





# Step 1: Install VirtualBox





## Step 2: Configure host-only network

Host-only Network Details

Applet DHCP Server

☒ Enable Server

Server Address: 192.168.57.100

Server Mask: 255.255.255.0

Lower Address Bound: 192.168.57.101

Upper Address Bound: 192.168.57.254

OK Cancel



## Step 3: Create new VM

?

X

← Create New Virtual Machine

### VM Name and OS Type

Enter a name for the new virtual machine and select the type of the guest operating system you plan to install onto the virtual machine.

The name of the virtual machine usually indicates its software and hardware configuration. It will be used by all VirtualBox components to identify your virtual machine.

Name

Cooking-with-Splunk

OS Type

Operating System: Linux

Version: Ubuntu

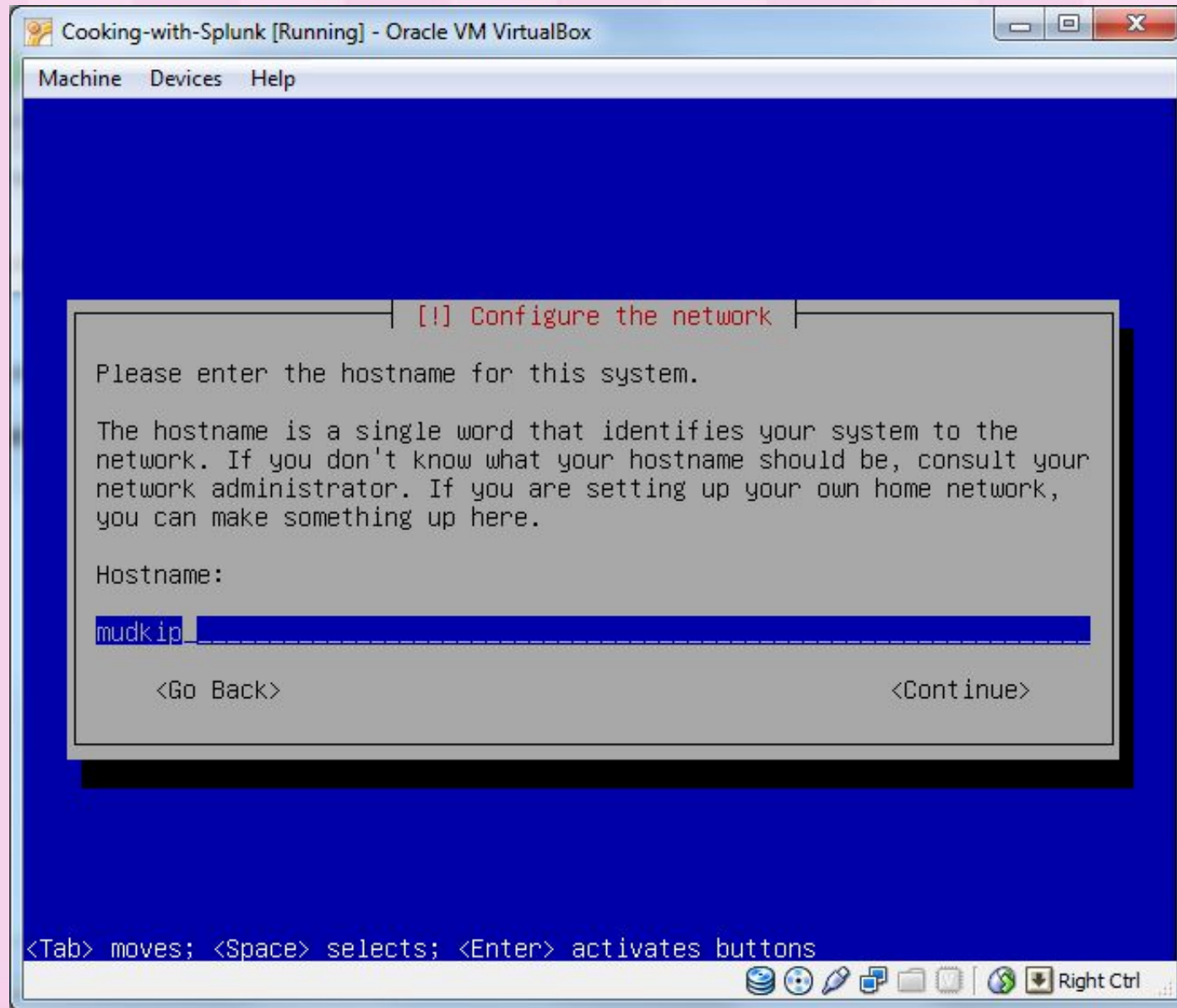
Next

Cancel



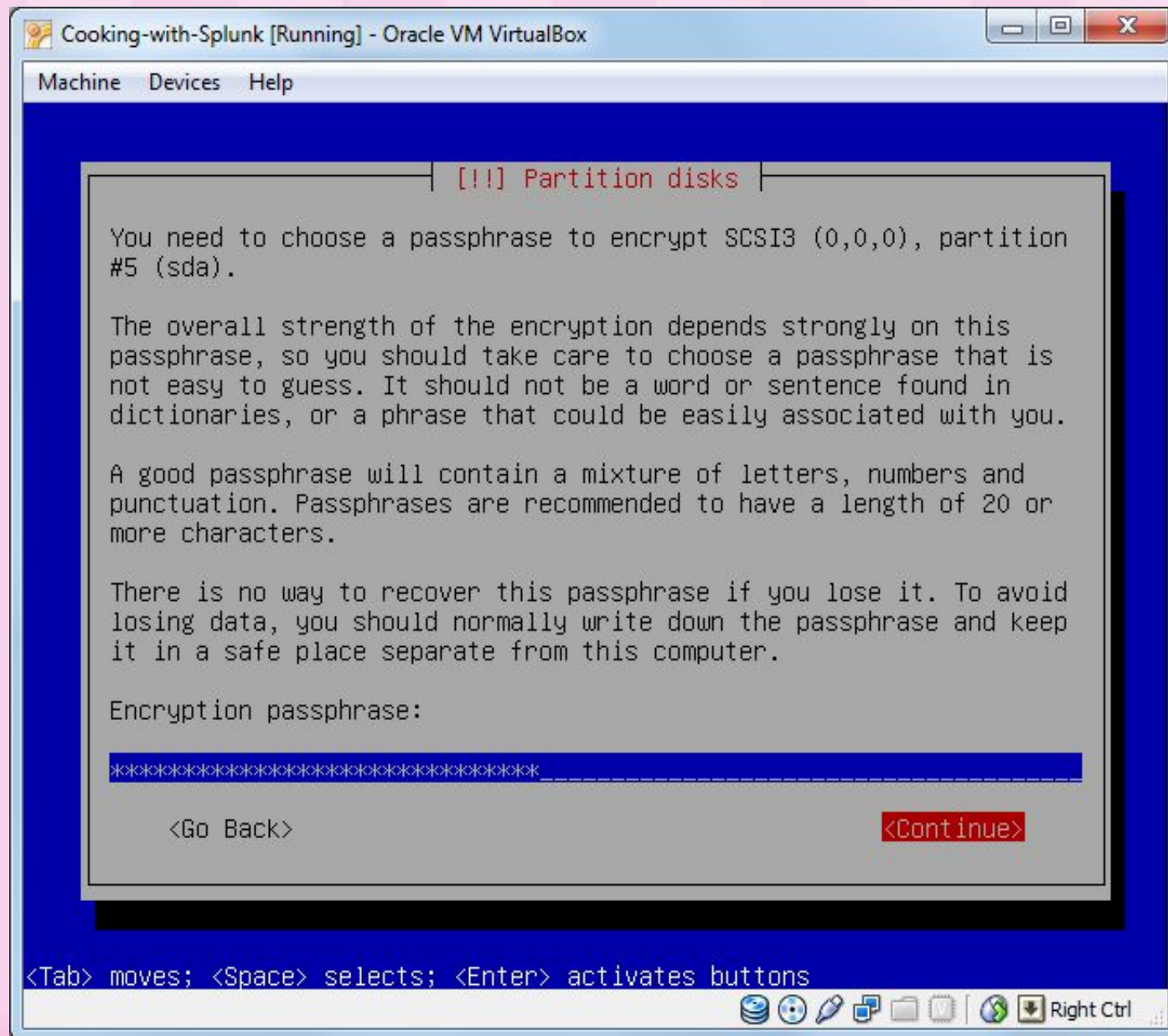


# Step 4: Install Linux



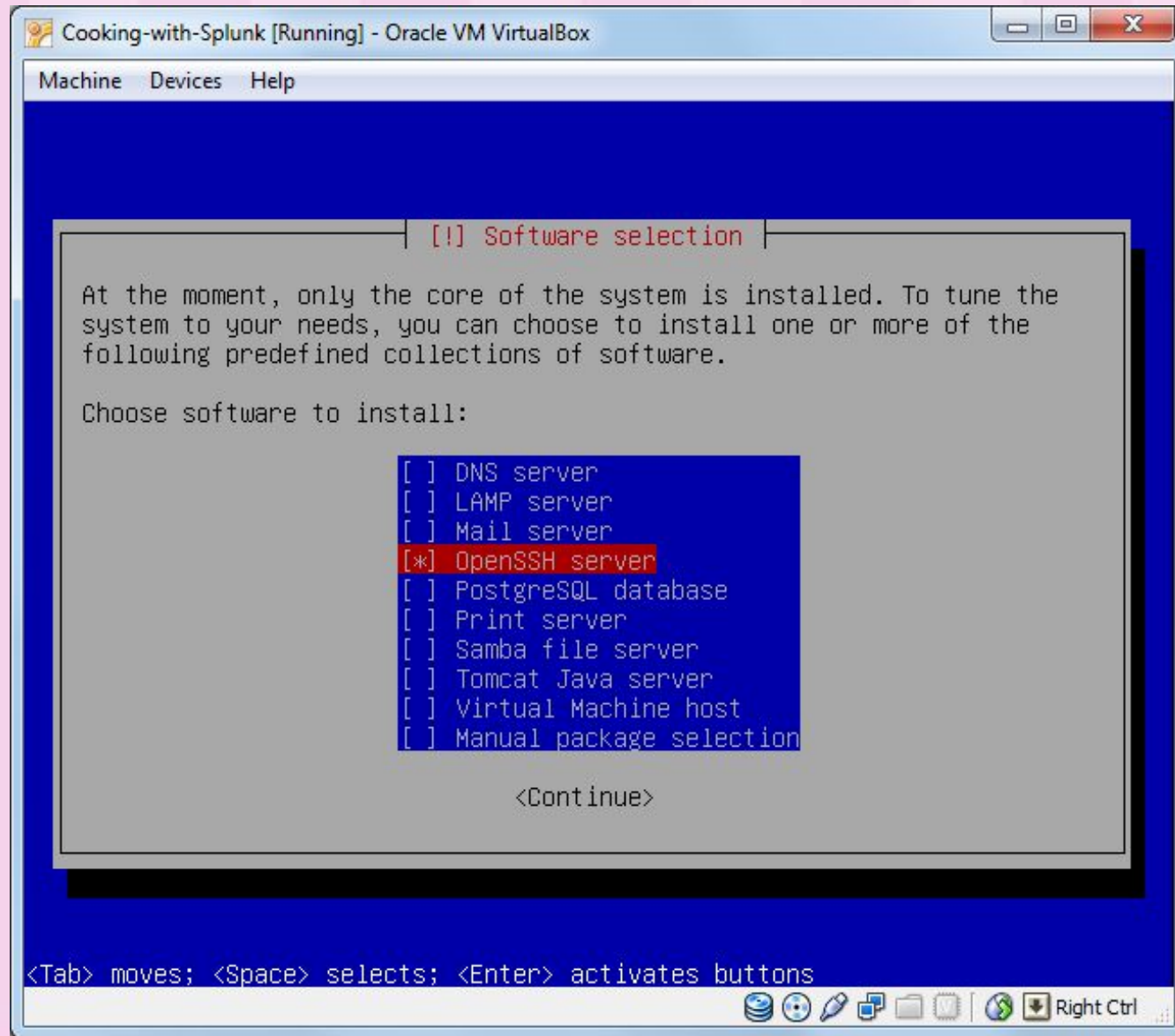


# Step 5: Fold in Full Disk Encryption





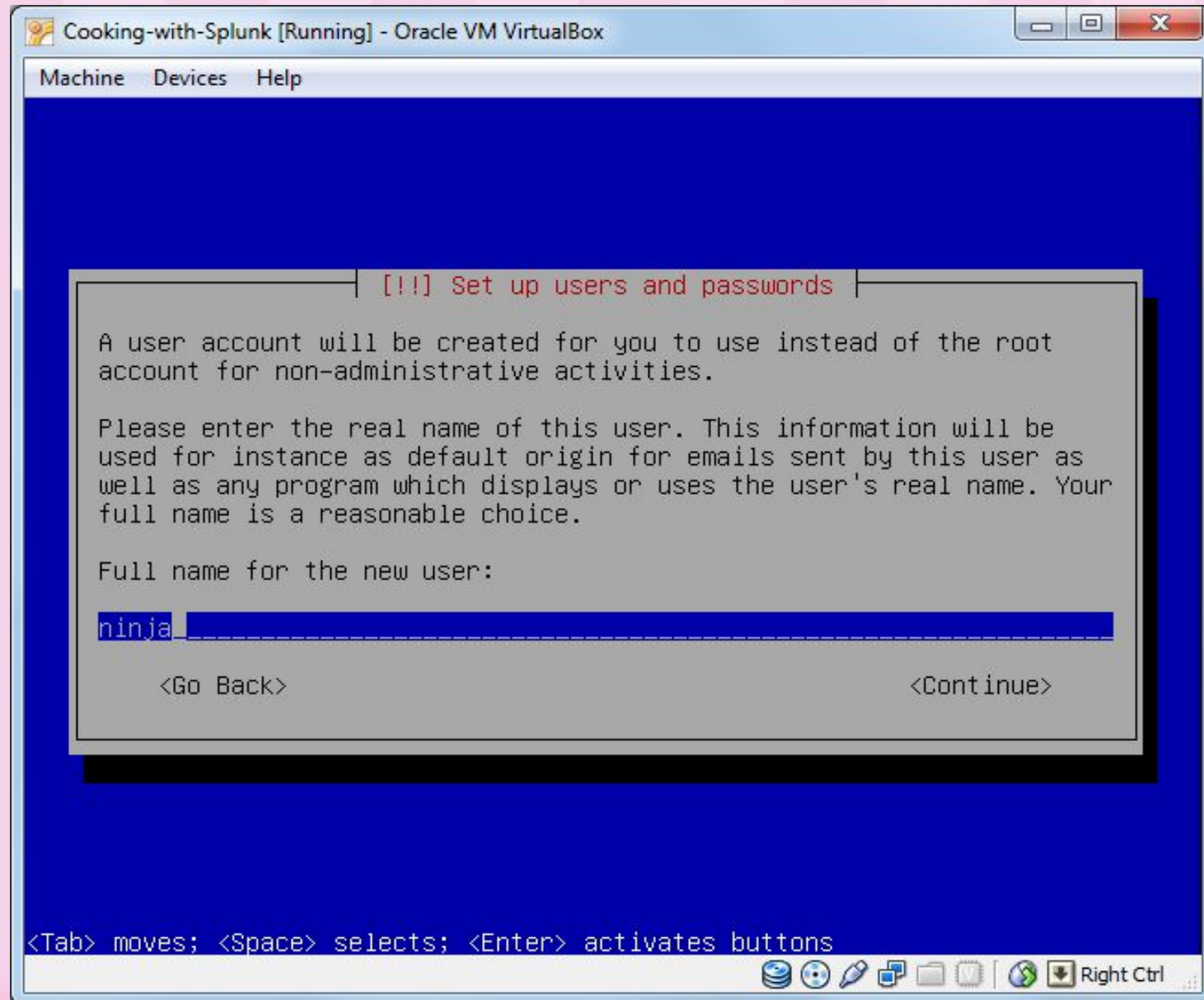
# Step 6: Add a dash of OpenSSH Server







# Step 7: Add two (2) users and one (1) group





# Step 8: Configure OpenSSH

```
Cooking-with-Splunk [Running] - Oracle VM VirtualBox
Machine  Devices  Help
GNU nano 2.2.2      File: /etc/ssh/sshd_config      Modified

UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 768

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no_
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile      %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell

[Icons] Right Ctrl
```



# Step 9: Patch that \$#&@!

```
Machine  Devices  Help
Hit http://us.archive.ubuntu.com lucid-updates/main Sources
Hit http://us.archive.ubuntu.com lucid-updates/restricted Sources
Hit http://us.archive.ubuntu.com lucid-updates/universe Packages
Hit http://us.archive.ubuntu.com lucid-updates/universe Sources
Hit http://us.archive.ubuntu.com lucid-updates/multiverse Packages
Hit http://us.archive.ubuntu.com lucid-updates/multiverse Sources
Reading package lists... Done
ninja@mudkip:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  landscape-common linux-generic linux-image-generic
The following packages will be upgraded:
  apparmor apparmor-utils apt apt-transport-https apt-utils at base-files
  bind9-host bsduutils bzip2 coreutils dmsetup dnsutils dpkg e2fslibs e2fsprogs
  fuse-utils gzip ifupdown libapparmor-perl libapparmor1 libbind9-60 libblkid1
  libbz2-1.0 libc-bin libc6 libc6-i686 libcomerr2 libdbus-1-3
  libdevmapper-event1.02.1 libdevmapper1.02.1 libdns64 libfuse2
  libgssapi-krb5-2 libisc60 libisc60c60 libisc60c60g60 libk5crypto3 libkrb5-3
  libkrb5support0 liblwres60 libplymouth2 libss2 libssl0.9.8 libudev0 libuuid1
  libwww-perl libxml2 linux-firmware linux-image-2.6.32-24-generic login lvm2
  man-db mount mountall openssh-client openssh-server openssl passwd plymouth
  plymouth-theme-ubuntu-text python-lazr.restfulclient rsyslog screen sudo tar
  tzdata udev unattended-upgrades update-manager-core upstart ureadahead
  util-linux uuid-runtime wget xkb-data
76 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
Need to get 72.2MB of archives.
After this operation, 1,573kB of additional disk space will be used.
Do you want to continue [Y/n]? 
```





# Step 10: Install Splunk

```
Cooking-with-Splunk [Running] - Oracle VM VirtualBox
Machine  Devices  Help
ninja@mudkip:~$ sudo dpkg -i splunk-4.2-96430-linux-2.6-intel.deb
Selecting previously deselected package splunk.
(Reading database ... 24349 files and directories currently installed.)
Unpacking splunk (from splunk-4.2-96430-linux-2.6-intel.deb) ...
Setting up splunk (4.2-96430) ...

-----
Splunk has been installed in:
    /opt/splunk

To start Splunk, run the command:
    /opt/splunk/bin/splunk start

To use the Splunk Web interface, point your browser at:
    http://mudkip:8000

Complete documentation is at http://www.splunk.com/r/docs
-----

ninja@mudkip:~$ _
```







## Step 11: Create log directory

```
Command Prompt

C:\temp>pscp seclogs.csv ninja@192.168.57.101:/logs/
ninja@192.168.57.101's password:
seclogs.csv          | 9233 kB | 1538.9 kB/s | ETA: 00:00:00 | 100%

C:\temp>_
```



# Step 12: Fire up Splunk

The screenshot shows a web browser window with the address bar displaying `192.168.57.101:8000/en-US/app/launcher/home`. The page title is "(home) - Home - Splunk ...". The Splunk logo and "Home" text are visible in the top left. In the top right, it says "Logged in as admin" with links for "App", "Manager", and "Jobs". Below the navigation bar, there are two tabs: "Welcome" and "Splunk Home", with "Splunk Home" being the active tab. The main content area has a heading "Welcome to Splunk". On the left, there are two prominent cards: "Add data" with a green arrow icon and text explaining the need to index IT data, and "Launch search app" with a green arrow icon and text describing the Search app. On the right, there is a "Need help?" section with links to "Getting started tutorial", "What's new in this release", "Splunk documentation", and "Splunk answers". At the bottom, a link says "Don't want to see this screen? Change your default settings in Manager."

(home) - Home - Splunk ...


192.168.57.101:8000/en-US/app/launcher/home

splunk> Home

Logged in as admin | App | Manager | Jobs


Welcome Splunk Home

## Welcome to Splunk



### Add data

Before you can use Search, you'll need to index some IT data. Index event logs, local logs, syslog, and more.



### Launch search app

The Search app is Splunk's default interface for searching and analyzing IT data. It allows you to index data into Splunk, add knowledge, create dashboards, and create alerts.

#### Need help?

- Getting started tutorial
- What's new in this release
- Splunk documentation
- Splunk answers

Don't want to see this screen? [Change your default settings](#) in Manager.



# Step 13: Switch to Free license

Change license group - ...

192.168.57.101:8000/en-US/manager/system/licensing/switch?return\_tc

« Back to Search Logged in as admin | Alerts | Jobs | Logout

splunk> Manager » Licensing » Change license group Help

### Change license group

The type of license group determines what sorts of licenses can be used in the pools on this license server. [Learn more](#)

- ☐ Enterprise license  
Splunk Enterprise adds capabilities to support multi-user, distributed deployments and includes alerting, role-based security, single sign-on, scheduled PDF delivery and support for unlimited data volumes.  
*There are no valid Splunk Enterprise licenses installed. You will be prompted to install a license if you choose this option.*
- ☐ Forwarder license  
Use this group when configuring Splunk as a forwarder. [Learn more](#)
- ☒ Free license  
Use this group when you are running Splunk Free. This license has a 500MB/day daily indexing volume. [Learn more](#)
- ☐ Enterprise Trial license  
This is your included download trial. IMPORTANT: If you switch to another license, you cannot return to the Trial. You must install an Enterprise license or switch to Splunk Free.

Cancel Save





# Step 14: Configure Splunk to read /logs

Splunk Manager - Splunk... x

192.168.57.101:8000/en-US/manager/launcher/data/inputs/monitor?msgid=4096270.33

« Back to Home Logged in as admin | Jobs

splunk> Manager » Data inputs » Files & directories Help

Disabled \$SPLUNK\_HOME/var/spool/splunk.

Data inputs (files) New

Showing 1-5 of 5 items Results per page 25

Full path to your data ↕	Set host ↕	Source type ↕	Set the destination index ↕	Number of files ↕	App ↕	Status ↕	Actions
<a href="#">\$SPLUNK_HOME/etc/splunk.version</a>	None	splunk_version	_internal		system	Disabled   Enable	Clone
<a href="#">\$SPLUNK_HOME/var/log/splunk</a>	None	Automatic	_internal		system	Disabled   Enable	Clone
<a href="#">\$SPLUNK_HOME/var/spool/splunk</a>	None	Automatic	default		system	Disabled   Enable	Clone
<a href="#">\$SPLUNK_HOME/var/spool/splunk/...stash_new</a>	None	stash_new	default		system	Disabled   Enable	Clone
<a href="#">/logs</a>	None	Automatic	default	1	launcher	Enabled   Disable	Clone   Delete





# Step 15: Give it a try!

The screenshot shows the Splunk Search dashboard interface. At the top, there's a navigation bar with 'Summary', 'Search', 'Status', 'Views', and 'Searches & Reports'. The 'Summary' tab is active. Below the navigation bar, there's a search bar and a 'All time' filter. The main content area is divided into four sections: 'All indexed data', 'Sources (≥ 1)', 'Sourcetypes (≥ 1)', and 'Hosts (≥ 1)'. Each section contains a table with data.

**All indexed data**

This lists all of the data you have loaded into your default indexes. [Add more data.](#)

Events indexed	Earliest event	Latest event
36,333	06/22/2010 07:28:16	03/22/2011 14:47:24

**Sources (≥ 1)**

source	Count	Last Update
1 /logs/seclogs.csv	36,333	03/22/2011 14:47:49

**Sourcetypes (≥ 1)**

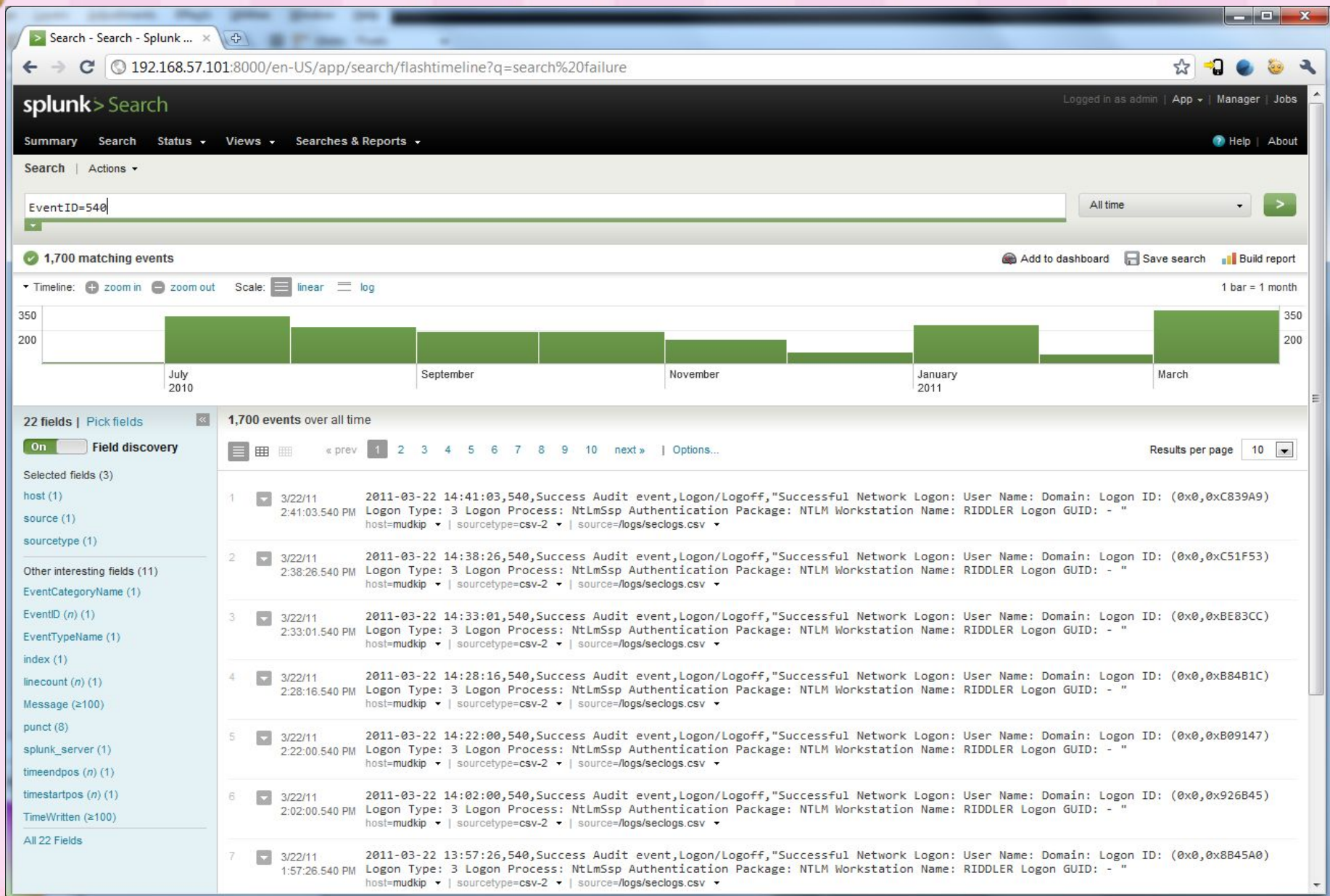
sourcetype	Count	Last Update
1 csv-2	36,333	03/22/2011 14:47:49

**Hosts (≥ 1)**

host	Count	Last Update
1 mudkip	36,333	03/22/2011 14:47:49



# Step 16: Enable boot-start





# Final Notes

- To wipe the slate clean, run:  
`/opt/splunk/bin/splunk clean eventdata`
- To distribute the VM, pass along the .VBOX config file and .VDI disk to others
  - Remember to change passwords!
- Watch your license!







MMM MMMM GOOD



Questions?







Download this preso:  
[sandwichsecurity.com](http://sandwichsecurity.com)

Thanks!  
Justin Hall  
[justin.hall@cbts.cinbell.com](mailto:justin.hall@cbts.cinbell.com)

