

Feeding, Watering, and Caring for GIS Servers

Mark Welsh
August 7, 2019

Overview

- Intro
- Launch a server
- Server configuration
- Managing server software
- Install and configure

Intro

- Why?
 - Quickly share content
 - Reliable
 - Industry standard – widely deployed
 - You love the command line!

Intro

- Caveats:
 - Security considerations
 - Configuration
 - Updates
 - You hate the command line!

Intro

- Good news:
 - Ubuntu widely supported
 - Cloud providers make it easier
 - Great learning opportunity
 - You want to be a command line guru!

Launch a Server

- Cloud service provider
- Microsoft Azure, Amazon Web Service, Digital Ocean...
- They all provide FOSS server instances
- Pay by hour, capped bandwidth
- Great laboratory

Launch a Server

- Create a private/public key pair (for secure login)
- Open command prompt (console)
- `cd ~/.ssh`
- If no directory exists: `mkdir ~/.ssh`
- `~/.ssh` is where the private/public keys will be stored
- `cd ~/.ssh`

Launch a Server

- Create key pair
- `cd ~/.ssh`
- `ssh-keygen -t rsa -b 4096`
- It will prompt you to define key name (enter or type in key name)
- Prompt for password (enter means no password)
- Creates public-private keys
- `ls -l`

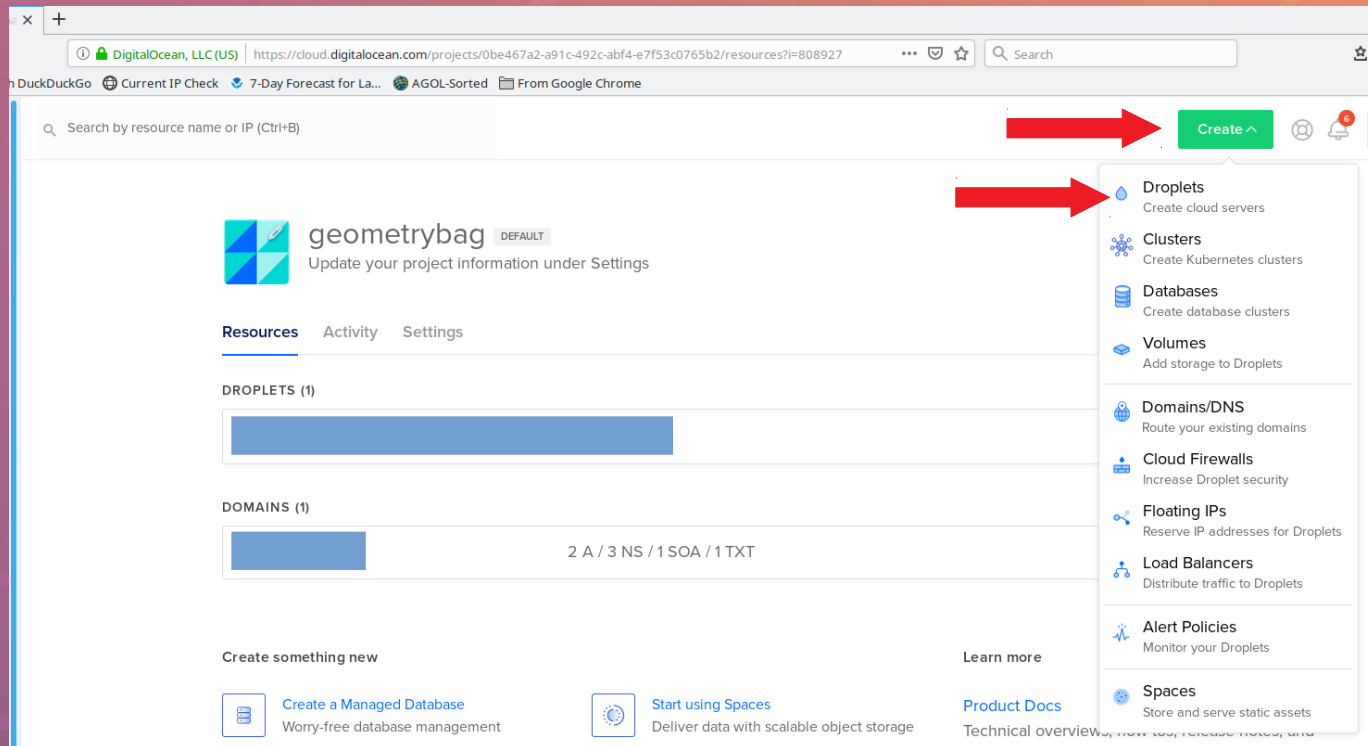
Launch a Server

- keys in ~/.ssh:

```
bug@Acerspin3:~/.ssh$ ls -l
total 24
drwxrwxr-x 2 bug bug 4096 Dec  1 2018 backup
-rw----- 1 bug bug 3326 Jul 20 20:34 digital_ocean_key_01
-rw-r--r-- 1 bug bug  739 Jul 20 20:34 digital_ocean_key_01.pub
-rw----- 1 bug bug 3326 Dec  1 2018 id_rsa
-rw-r--r-- 1 bug bug  739 Dec  1 2018 id_rsa.pub
-rwxrwxrwx 1 bug bug 1772 Jul 20 20:02 known_hosts
```

Launch a Server

- Login to cloud server provider (Digital Ocean):




Launch a Server


- Select configuration:


Create Droplets


Choose an image ?


[Distributions](#) [Container distributions](#) [Marketplace](#) [Snapshots](#) [Custom images](#)


Ubuntu
18.04 x64


FreeBSD
Select version


Fedora
Select version


Debian
Select v


CentOS
Select v

Choose a plan

STARTER

Standard

General Purpose

Standard virtual machines with a mix of memory and compute resources. Best for small projects that can handle variable levels of CPU performance, like blogs, web apps and dev/test environments.

\$ 5 /mo \$0.007/hour	\$ 10 /mo \$0.015/hour	\$ 15 /mo \$0.022/hour	\$ 15 /mo \$0.022/hour	\$ 15 /mo \$0.022/hour	\$ 20 /mo \$0.030/hour
1 GB / 1 CPU 25 GB SSD disk 1000 GB transfer	2 GB / 1 CPU 50 GB SSD disk 2 TB transfer	3 GB / 1 CPU 60 GB SSD disk 3 TB transfer	2 GB / 2 CPUs 60 GB SSD disk 3 TB transfer	1 GB / 3 CPUs 60 GB SSD disk 3 TB transfer	4 GB / 2 CPUs 80 GB SSD disk 4 TB transfer









Currently selected: 8 GB / 4 CPUs

[Show all plans](#)

Launch a Server

- Configuration:

Choose a datacenter region

 New York 1 2 3	 San Francisco 1 2	 Amsterdam 2 3	 Singapore 1	 London 1	 Frankfurt 1
 Toronto 1	 Bangalore 1				

Launch a Server

- Configuration:


Authentication ?

☒ **SSH keys**
A more secure authentication method

☐ **One-time password**
Emails a one-time root password to you (less secure)

☒ **Select all** ☒ pubKey2

New SSH Key



Launch a Server

- Configuration (new key):
- `cat id_rsa.pub`
- select output from the command to paste the public key contents:

Add public SSH key

Copy your public SSH key and paste it in the space below. For instructions on how, follow the steps on the right.

ssh-key-content
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCAQCIX4HDr3CvIEKehLPs9
ZbC8Oy/2Y5sNqq6uRRmMMLVL75T8B6sngL2x1jSsf7ExqDD2T
/nhppZEC...
HsmSwm
/Tr51j6u7
UTRUO3
Cii2B

Paste public key
contents here

GBYCY6wh
slwZ1xdFNn

Name
pubKey2

Add SSH Key

SSH Keys

Follow these instructions to create or add SSH keys on Linux, MacOS & Windows. Windows users without OpenSSH [can install and use PuTTY](#) instead.

Create a new key pair, if needed

Open a terminal and run the following command:

ssh-keygen

Copy

You will be prompted to save and name the key.

Launch a Server

- Configuration (final settings):

Finalize and create

How many Droplets?

Deploy multiple Droplets with the same [configuration](#).

—1 Droplet+

Choose a hostname

Give your Droplets an identifying name you will remember them by. Your Droplet name can only contain alphanumeric characters, dashes, and periods.

DarkStar

Add tags

Use tags to organize and relate resources. Tags may contain letters, numbers, colons, dashes, and underscores.

Type tags here

Select Project











Assign Droplets to a project

geometrybag

Create Droplet

Launch a Server

- Server is launched:

Resources Activity Settings			
DROPLETS (2)			
  DarkStar	165.227.207.150		 
  RiverTrance			 

- Write down that IP address!

Launch a Server

- Connect to server (command prompt)
- `ssh root@XXX.XXX.XXX.XXX` (your server IP)
- `ssh root@165.227.207.150`
- ignore warning about identity
- Type password for key file (if applicable)

Launch a Server

- You're in!

```
bug@Acerspin3:~$ ssh root@165.227.207.150
The authenticity of host '165.227.207.150 (165.227.207.150)' can't be established.
ECDSA key fingerprint is SHA256:0kvgvIX0c5ETxHnAKQ8pBaw2fI7UCEKAplsTwVLRNaE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '165.227.207.150' (ECDSA) to the list of known hosts.
Enter passphrase for key '/home/bug/.ssh/id_rsa':
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Jul 21 03:14:33 UTC 2019

System load:  0.08          Processes:            90
Usage of /:   1.2% of 77.36GB Users logged in:       0
Memory usage: 3%           IP address for eth0: 165.227.207.150
Swap usage:   0%

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@DarkStar:~#
```

root@DarkStar:~#

Server Configuration

- but you're logged in as root!
- In server, create a new user:
- `adduser althea` (replace althea)
- Enter user password (write down!)
- Enter other info as prompted

Server Configuration

- Add the account to sudo group
- `usermod -aG sudo althea` (replace with your account name)
- `rsync --archive --chown=althea:althea ~/.ssh /home/althea`
- `logout`
- `ssh` using this new account (don't log in with root!)
- `ssh althea@165.227.207.150`

Server Configuration

- Turn on firewall (ufw)
- check if ufw installed (`sudo ufw status`)
- Allow ssh connections:
- `sudo ufw allow ssh`
- enable firewall:
- `sudo ufw enable`

Server Configuration

- Firewall on, ssh connections allowed:

```
althea@DarkStar:~$ sudo ufw status
[sudo] password for althea:
Status: active
```


To	Action	From
--	-----	----
22/tcp	ALLOW	Anywhere
22/tcp (v6)	ALLOW	Anywhere (v6)

```
althea@DarkStar:~$ █
```

Managing Server Software

- Ubuntu set to install security updates automatically
- But installing/updating other software up to you
- You get an indication when you log in:


Managing Server Software


Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-52-generic x86_64) 

* Documentation: <https://help.ubuntu.com>
* Management: <https://landscape.canonical.com>
* Support: <https://ubuntu.com/advantage>

System information as of Sun Jul 21 23:17:31 UTC 2019

System load:	0.0	Processes:	95
Usage of /:	1.7% of 77.36GB	Users logged in:	0
Memory usage:	5%	IP address for eth0:	165.227.207.150
Swap usage:	0%		

28 packages can be updated. 
0 updates are security updates.

*** System restart required *** 
Last login: Sun Jul 21 21:32:02 2019 from 98.192.130.94

Managing Server Software

- apt – Advanced Package Tool
- Update, then upgrade
- Keeps software up to date
- Security

Managing Server Software

- First, update the package index:
- `sudo apt update`

```
althea@DarkStar:~$ sudo apt update
[sudo] password for althea:
Hit:1 http://mirrors.digitalocean.com/ubuntu bionic InRelease
Get:2 http://security.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Hit:3 http://mirrors.digitalocean.com/ubuntu bionic-updates InRelease
Hit:4 http://mirrors.digitalocean.com/ubuntu bionic-backports InRelease
Fetched 88.7 kB in 1s (129 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
28 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Managing Server Software

- List packages that will be upgraded:
- `apt list --upgradable`

```
althea@DarkStar:~$ apt list --upgradable
Listing... Done
base-files/bionic-updates 10.1ubuntu2.5 amd64 [upgradable from: 10.1ubuntu2.4]
bash/bionic-updates 4.4.18-2ubuntu1.2 amd64 [upgradable from: 4.4.18-2ubuntu1.1]
dmeventd/bionic-updates 2:1.02.145-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2:1.02.145-4.1ubuntu3]
dmsetup/bionic-updates 2:1.02.145-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2:1.02.145-4.1ubuntu3]
friendly-recovery/bionic-updates 0.2.38ubuntu1.1 all [upgradable from: 0.2.38ubuntu1]
iputils-ping/bionic-updates 3:20161105-1ubuntu3 amd64 [upgradable from: 3:20161105-1ubuntu2]
iputils-tracepath/bionic-updates 3:20161105-1ubuntu3 amd64 [upgradable from: 3:20161105-1ubuntu2]
language-selector-common/bionic-updates 0.188.3 all [upgradable from: 0.188.2]
libdevmapper-event1.02.1/bionic-updates 2:1.02.145-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2:1.02.145-4.1ubuntu3]
libdevmapper1.02.1/bionic-updates 2:1.02.145-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2:1.02.145-4.1ubuntu3]
libdrm-common/bionic-updates 2.4.97-1ubuntu1~18.04.1 all [upgradable from: 2.4.95-1~18.04.1]
libdrm2/bionic-updates 2.4.97-1ubuntu1~18.04.1 amd64 [upgradable from: 2.4.95-1~18.04.1]
liblvm2app2.2/bionic-updates 2.02.176-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2.02.176-4.1ubuntu3]
liblvm2cmd2.02/bionic-updates 2.02.176-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2.02.176-4.1ubuntu3]
libnss-systemd/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
libpam-systemd/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
libssl1.1/bionic-updates 1.1.1-1ubuntu2.1~18.04.4 amd64 [upgradable from: 1.1.1-1ubuntu2.1~18.04.2]
libsystemd0/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
libudev1/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
lvm2/bionic-updates 2.02.176-4.1ubuntu3.18.04.1 amd64 [upgradable from: 2.02.176-4.1ubuntu3]
openssl/bionic-updates 1.1.1-1ubuntu2.1~18.04.4 amd64 [upgradable from: 1.1.1-1ubuntu2.1~18.04.2]
python3-distupgrade/bionic-updates 1:18.04.34 all [upgradable from: 1:18.04.33]
snapd/bionic-updates 2.39.2+18.04 amd64 [upgradable from: 2.38+18.04]
systemd/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
systemd-sysv/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
tmux/bionic-updates 2.6-3ubuntu0.2 amd64 [upgradable from: 2.6-3ubuntu0.1]
ubuntu-release-upgrader-core/bionic-updates 1:18.04.34 all [upgradable from: 1:18.04.33]
udev/bionic-updates 237-3ubuntu10.24 amd64 [upgradable from: 237-3ubuntu10.22]
```

Managing Server Software

- Upgrade software:
- `sudo apt upgrade`

```
Setting up libdrm2:amd64 (2.4.97-1ubuntu1~18.04.1) ...
Setting up snapd (2.39.2+18.04) ...
Installing new version of config file /etc/apparmor.d/usr.lib.snapd.snap-confine.real ...
md5sum: /etc/apparmor.d/usr.lib.snapd.snap-confine: No such file or directory
snapd.failure.service is a disabled or a static unit, not starting it.
snapd.snap-repair.service is a disabled or a static unit, not starting it.
Setting up liblvm2cmd2.02:amd64 (2.02.176-4.1ubuntu3.18.04.1) ...
Setting up dmeventd (2:1.02.145-4.1ubuntu3.18.04.1) ...
dm-event.service is a disabled or a static unit not running, not starting it.
Setting up lvm2 (2.02.176-4.1ubuntu3.18.04.1) ...
update-initramfs: deferring update (trigger activated)
Processing triggers for initramfs-tools (0.130ubuntu3.8) ...
update-initramfs: Generating /boot/initrd.img-4.15.0-54-generic
Processing triggers for libc-bin (2.27-3ubuntu1) ...
althea@DarkStar:~$
```

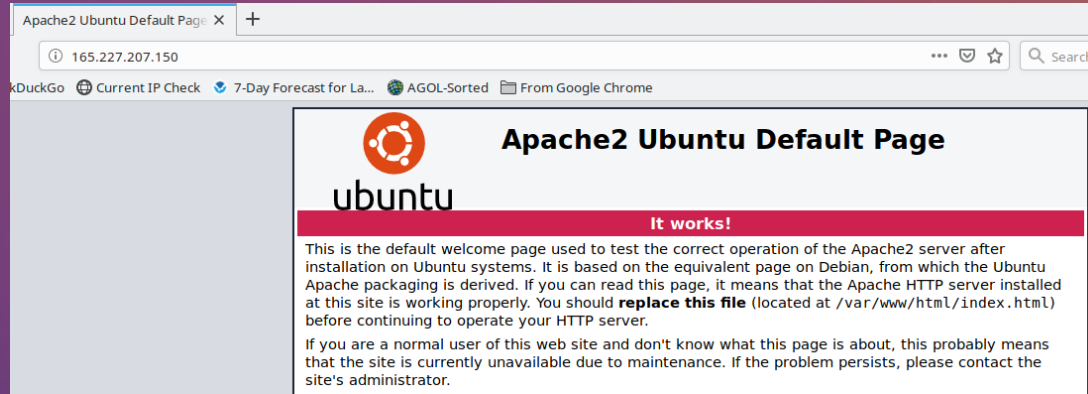
Managing Server Software

- Apache Web Server
- Use apt to install applications

Managing Server Software

- Use apt to install applications
- `sudo apt update`
- `sudo apt install apache2`
- `sudo ufw allow 'Apache'`
- `sudo ufw status`
- You can now reach the web server:

Managing Server Software

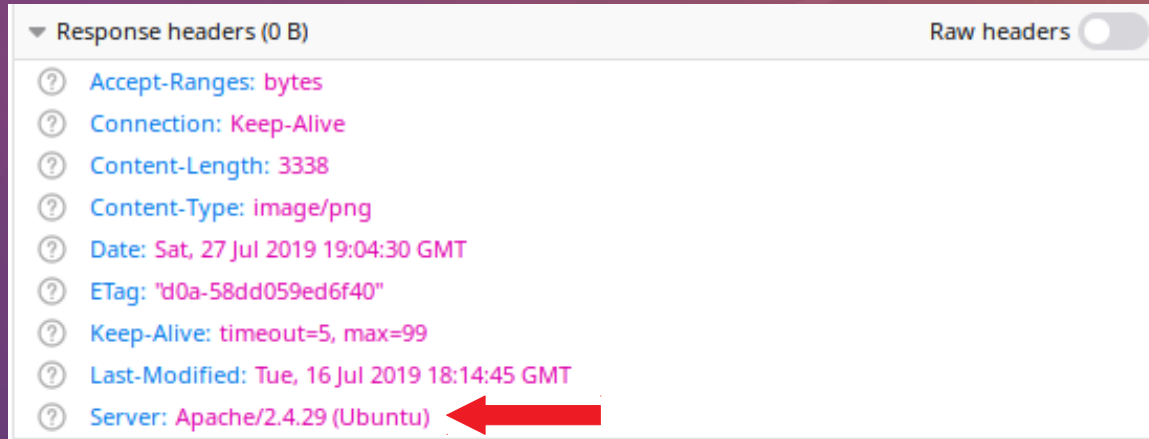


- `sudo systemctl status apache2`

```
althea@DarkStar:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Drop-In: /lib/systemd/system/apache2.service.d
            └─apache2-systemd.conf
   Active: active (running) since Sat 2019-07-27 17:36:27 UTC; 1h 33min ago
   Main PID: 29492 (apache2)
     Tasks: 55 (limit: 4703)
    CGroup: /system.slice/apache2.service
            └─29492 /usr/sbin/apache2 -k start
               29493 /usr/sbin/apache2 -k start
               29494 /usr/sbin/apache2 -k start
```


Managing Server Software

- Configure Apache to not show server info:



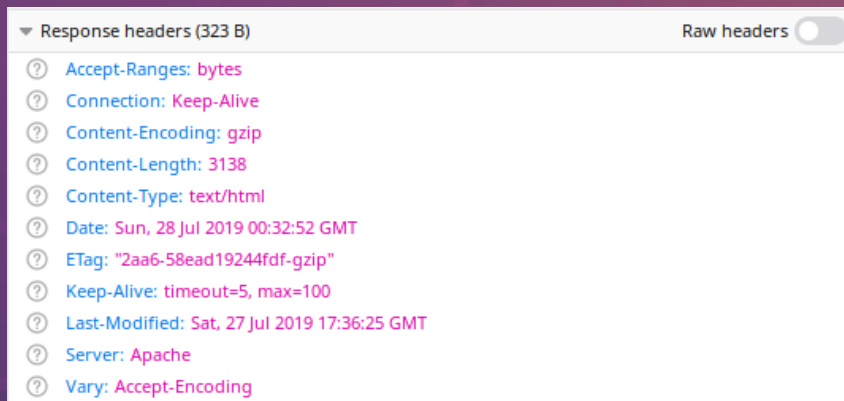
Managing Server Software

- `sudo nano`
`/etc/apache2/conf-enabled/security.conf`

```
#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens Prod
#ServerTokens Full
■
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
ServerSignature Off
#ServerSignature On
```

Managing Server Software

- Ctrl-X ends nano text edit, you'll be prompted to save changes...
- Restart Apache to implement changes
- `sudo systemctl reload apache2`



One Last Configuration

- Don't allow root login
- `sudo nano /etc/ssh/sshd_config`
- Change PermitRootLogin to no:

```
# Authentication:
```

```
#LoginGraceTime 2m
```

```
PermitRootLogin no
```

```
#StrictModes yes
```

```
#MaxAuthTries 6
```

```
#MaxSessions 10
```



- `sudo systemctl restart ssh`

What's Next?

- Additional security configuration
 - <https://askubuntu.com/questions/151440/important-things-to-do-after-installing-ubuntu-server>
 - <https://hostadvice.com/how-to/how-to-harden-your-ubuntu-18-04-server/>
 - <https://www.nuharborsecurity.com/ubuntu-server-hardening-guide-2/>
- Domain Name
- Certificate
- Spatial software (postgresql, mapserver etc)
- Logwatch (and other log utilities like GoAccess)

Summary

- Server makes your content shareable
- Linux community is very helpful
- Linux and FOSS is an internet force
- How to set up a basic platform to build on
- Questions