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

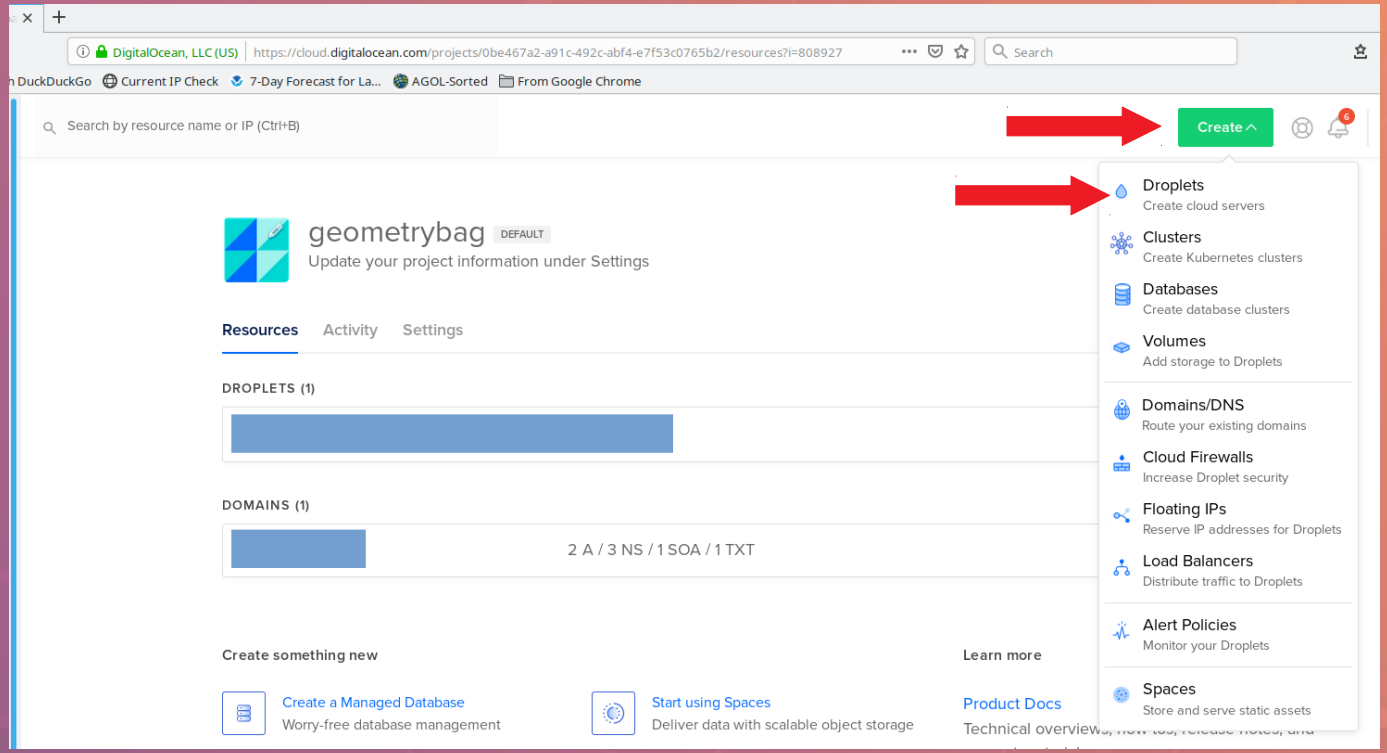
Launch a Server

- 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
```

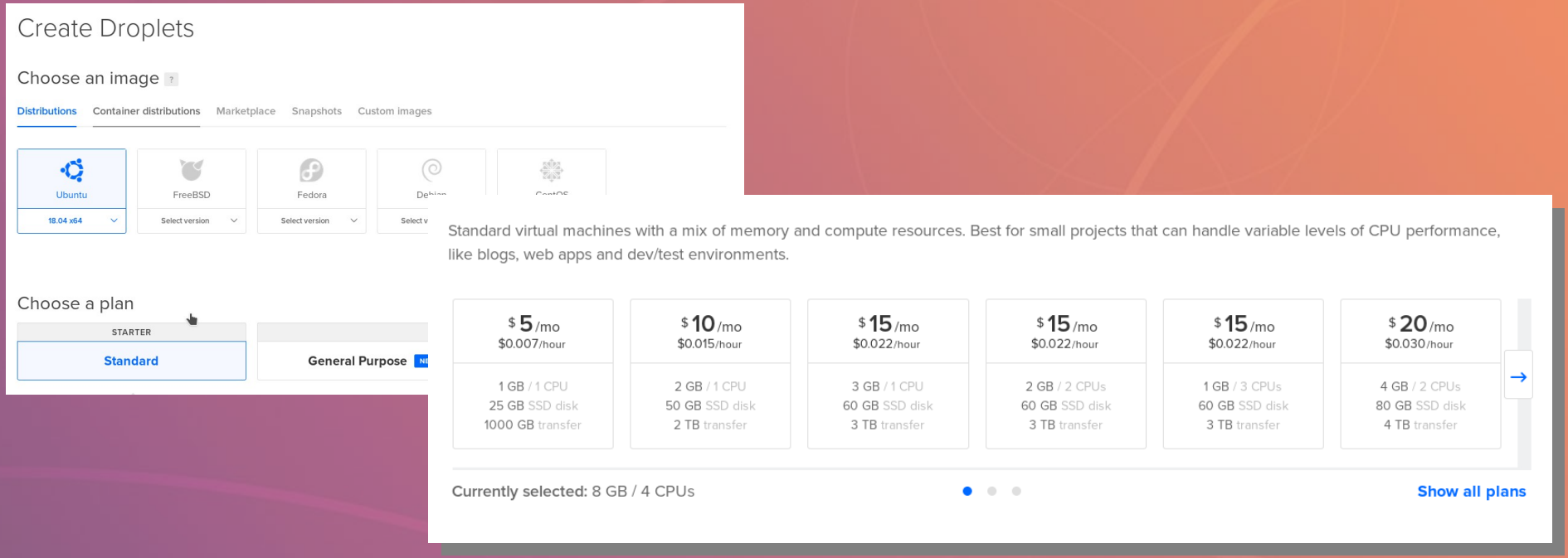
Launch a Server

- Login to cloud server provider (Digital Ocean):



Launch a Server

- Select configuration:

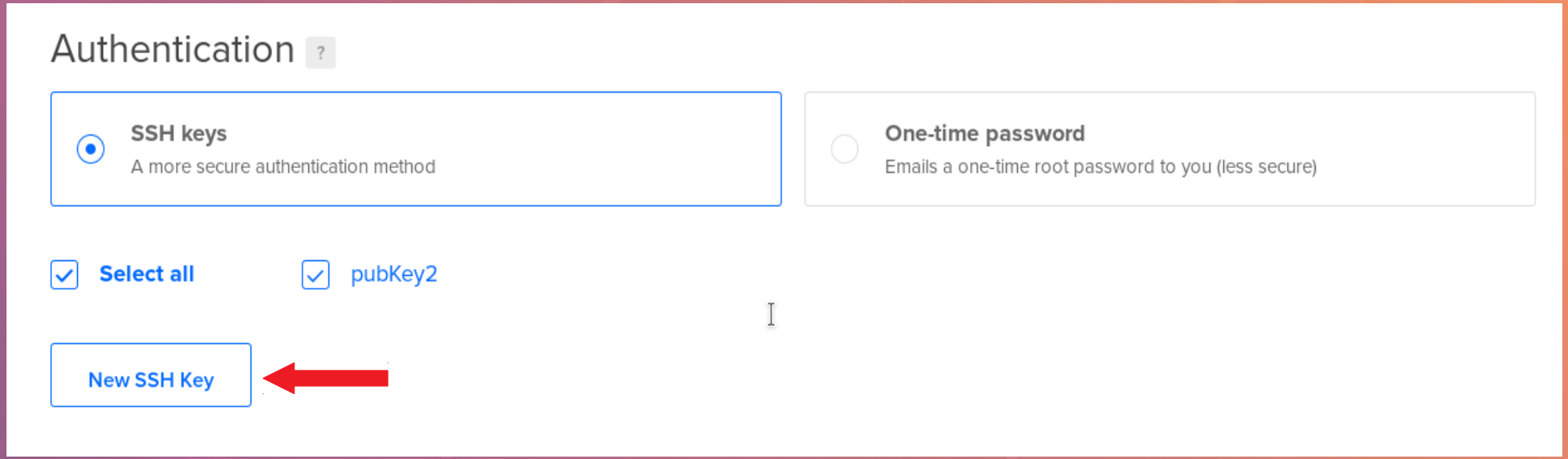


Launch a Server

- Configuration:

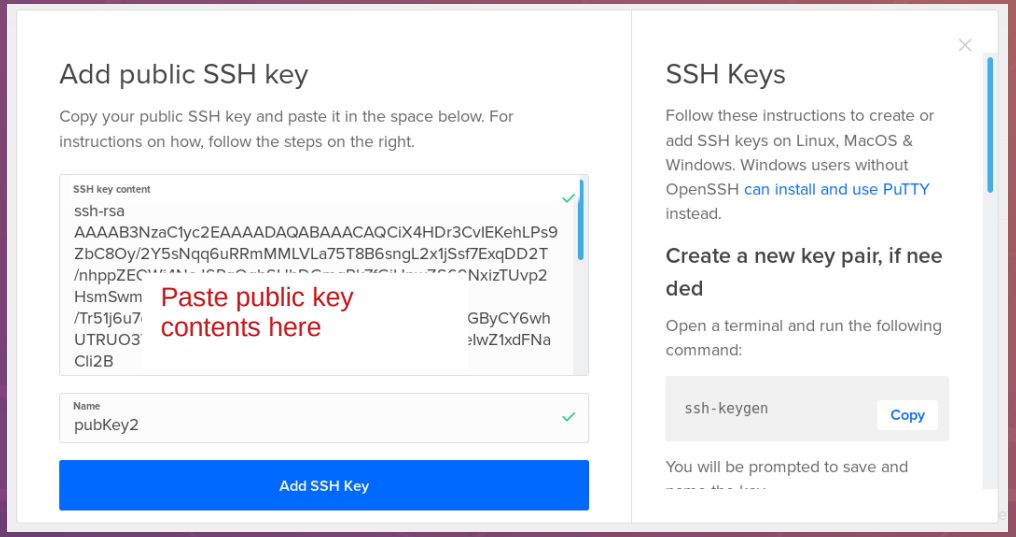
Launch a Server

- Configuration:



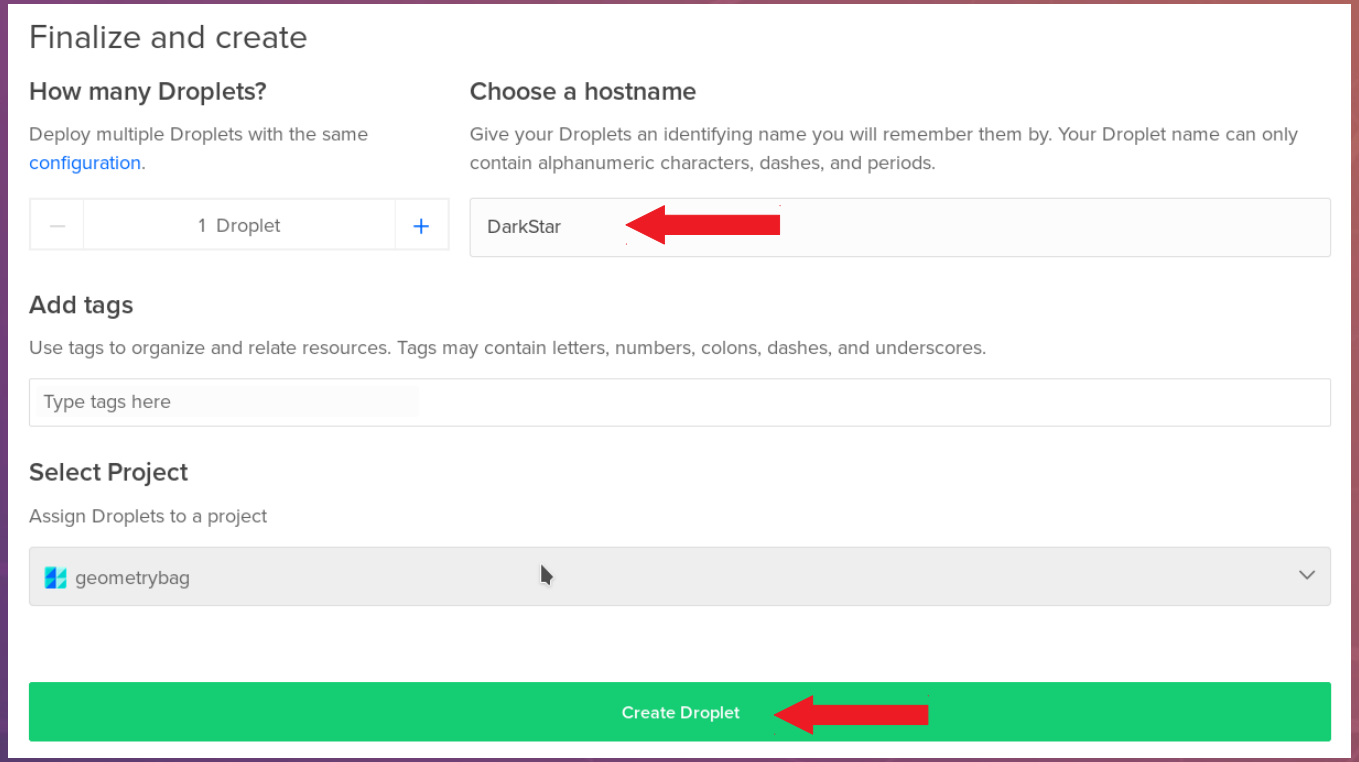
Launch a Server

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



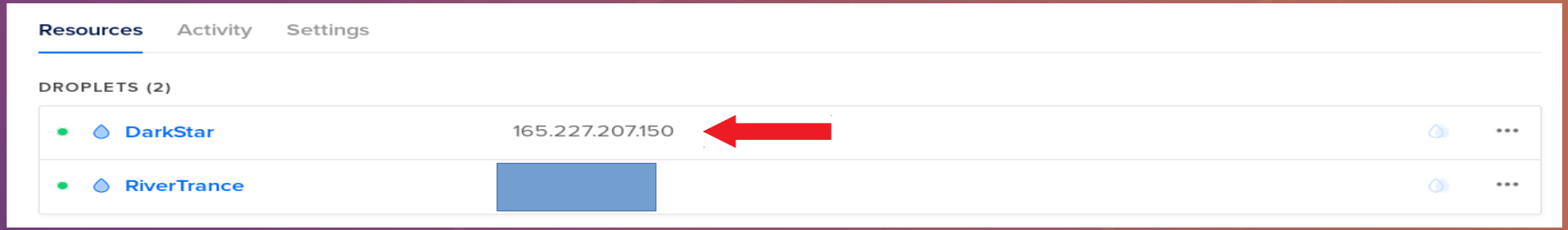
Launch a Server

- Configuration (final settings):



Launch a Server

- Server is launched:



- 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:~#
```

Launch a Server

- 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

Launch a Server

- 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

Launch a Server

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

Launch a Server

- 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:~$
```

Maintaining 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:

Maintaining 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
```

Maintaining Server Software

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

Maintaining 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.
```

Maintaining 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]
```

Maintaining 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:~$
```

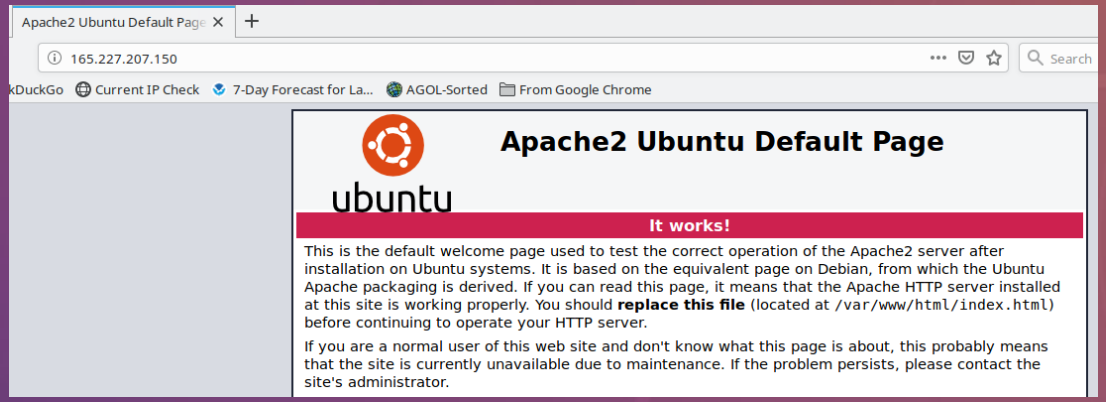
Installing Server Applications

- Apache Web Server
- Use apt to install applications

Installing Server Applications

- 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:

Installing Server Applications

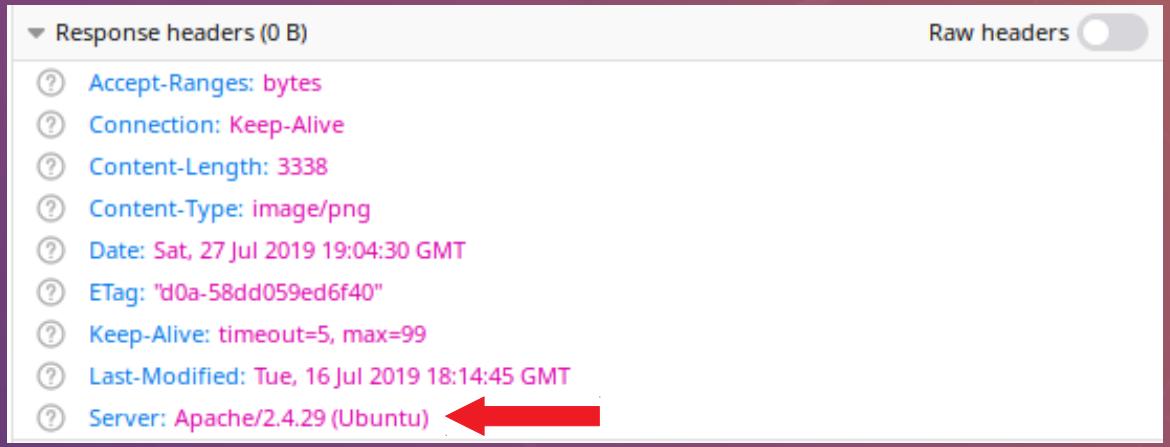


- sudo systemctl status apache2

```
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
```

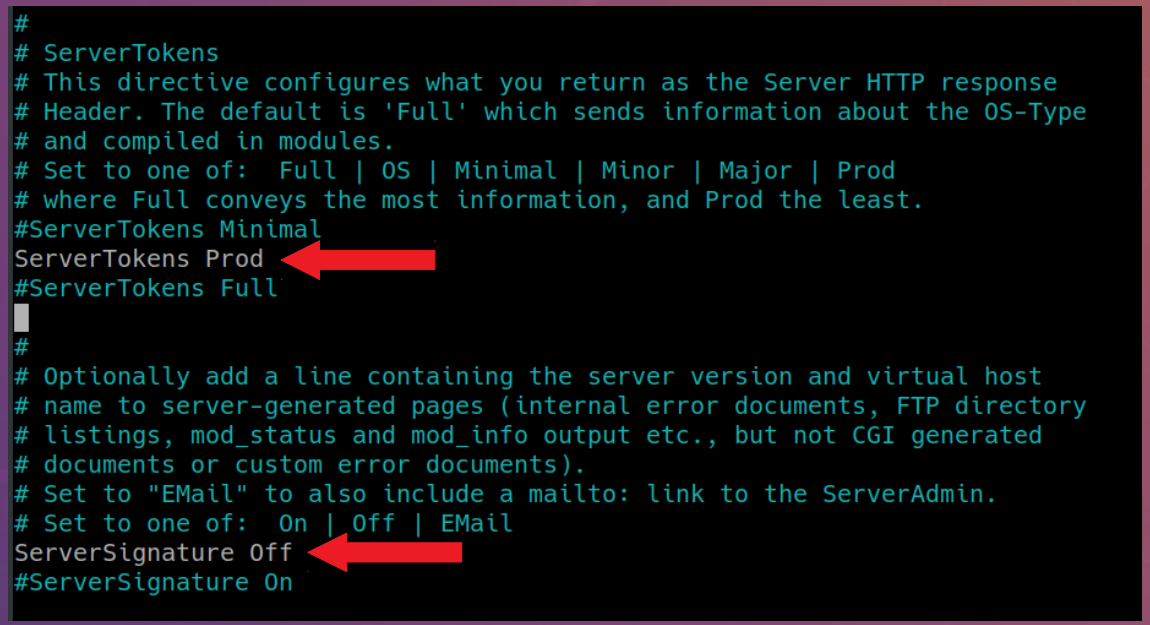
Installing Server Applications

- Configure Apache to not show server info:



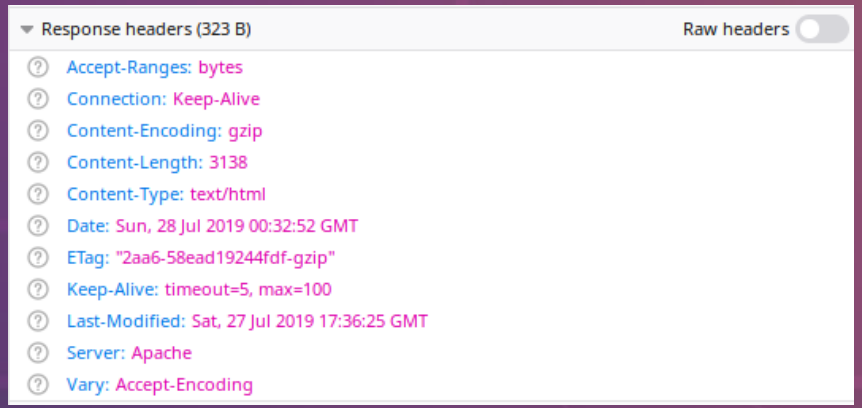
Installing Server Applications

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



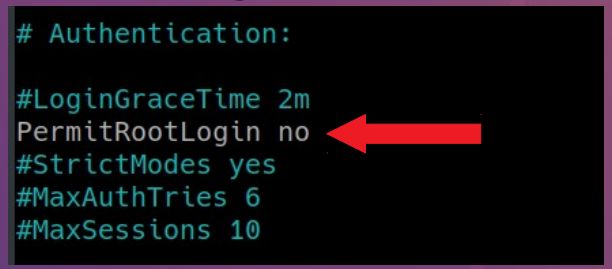
Installing Server Applications

- 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:



- 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