

Neil Ticktin

Neil not only plays host for all MacTech events, but aids the session chairs for all MacTech events (over 100 events since 2010). Neil has been the Editor-in-Chief and Publisher of MacTech Magazine since 1992. With both a technical and business background, Neil has authored hundreds of articles including most of MacTech's well known benchmarking articles on productivity applications, virtualization, and performance products. In addition to technical issues, Neil has a strong background in strategic planning especially when it comes to strategies that use technology by engaging an organization's leadership to use tech as a tool, and not be frightened off by tech speak.



Linux Servers:
Admin them in a more
“Mac-like” way.

What are we going to cover?

- OS X Server: Where you want to use it
- When and why Linux?
- If you go Linux...
 - Keep it simple
 - Keep it secure
 - Keep it monitored

OS X vs. Linux

- OS X:
 - It's what we know and love
 - It works well enough, unless
 - you need easy redundancy
 - you need real server software
 - you need “real” server level support
 - you need up to date open source packages
 - you don't want stuff to break with simple OS updates
 - Caching Server and Time Machine

OS X vs. Linux (cont)

- Linux
 - Many reasons
 - If you want to be, you can be on your own
 - You can pay for real, server level, support
 - But are a TON of free resources
 - Don't ignore security

Linux OSes

- Different Distributions
 - Arch Linux
 - CentOS
 - Debian
 - Fedora
 - Gentoo
 - openSUSE
 - Slackware
 - Ubuntu

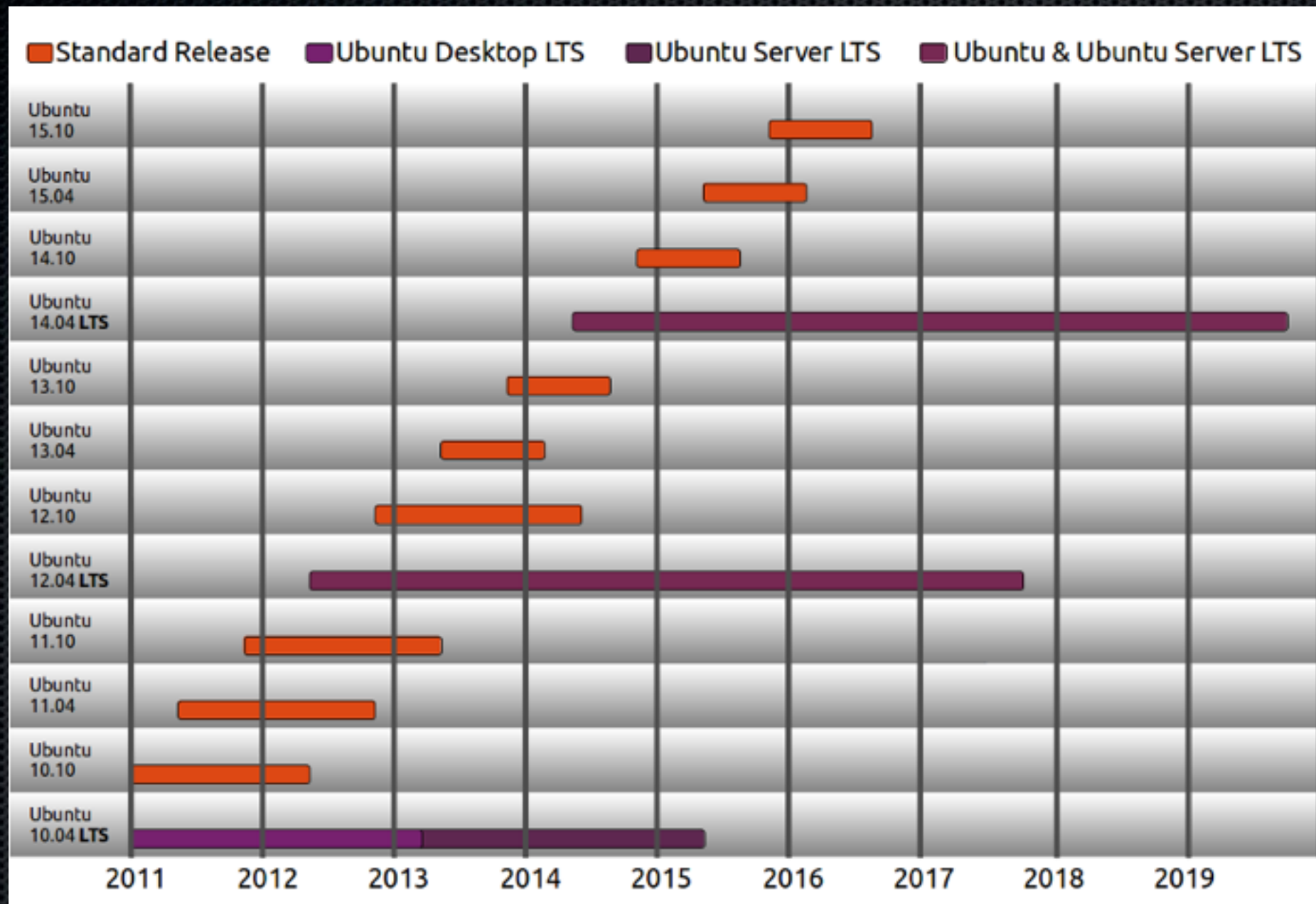
Linux OSes

- Choosing a distribution
 - Look at what you will do
 - What's supported and vibrant
 - What's compatible with your software choices
 - Pick the distro based on what you are doing, or one to standardize on.

Ubuntu LTS

- What's Ubuntu Long Term Solution (LTS)?
 - Every two years
 - Five year support
 - 14.04 LTS Supported until 2020 (16 until 2022)
 - Focus on hardening functionality of existing features, not new features (generally)

Ubuntu LTS



Note: LTS v16 is now out, but wait a bit longer

Providers

- In-house:
 - Why?
 - Don't.
- Traditional providers
 - HostGator, DreamHost, BlueHost, GoDaddy, I & I
- Linode, Digital Ocean, VPSie, VULTR, and others
- Specialized Providers
 - Drupal: Acquia, Pantheon, etc...
 - WordPress: WordPress.org, Pantheon, etc...

Real World Setup

- Examples for our process
- Tools selected important
 - Compatibility
 - Order of install:
 - Longview often first
 - Server management panel must be already installed, nor any web service

We're going to pick one.

Why we chose Linode

- Competitive pricing
- Better support
- Longview
- Interface easier to understand
- Backups that made more sense

Let's Build a Linode

- Add a linode (choosing size and data center)
- Deploy an Image
 - Ubuntu 14.04 LTS (or 16 when ready)
- Choose size for swap disk and main disk
 - Generally, use max size of 512MB for swap
 - Can do multiple disks
 - May want to reserve for later
- Settings > Linode Label (enter new name and save)

[Linodes](#) » **Add a Linode**

Select your plan

Linode 1024

24GB DISK
1 CPU Core
2TB XFER
.015/hr to \$10/mo

Linode 2048

48GB DISK
2 CPU Cores
3TB XFER
.03/hr to \$20/mo

Linode 4096

96GB DISK
4 CPU Cores
4TB XFER
.06/hr to \$40/mo

Linode 8192

192GB DISK
6 CPU Cores
8TB XFER
.12/hr to \$80/mo

Linode 16384

384GB DISK
8 CPU Cores
16TB XFER
.24/hr to \$160/mo

Linode 32768

768GB DISK
12 CPU Cores
20TB XFER
.48/hr to \$320/mo

Linode 49152

1152GB DISK
16 CPU Cores
20TB XFER
.72/hr to \$480/mo

Linode 65536

1536GB DISK
20 CPU Cores
20TB XFER
.96/hr to \$640/mo

Linode 98304


1920GB DISK
20 CPU Cores
20TB XFER
1.44/hr to \$960/mo

Location

- ✓ Newark, NJ
- Fremont, CA
- Atlanta, GA
- Dallas, TX
- London, UK
- Tokyo, JP
- Singapore, SG
- Frankfurt, DE

Add this Linode!

Linode Manager

 4macsadmin | [my profile](#) | [log out](#)

Linodes

NodeBalancers

64 bit Distributions - Recommended

Arch Linux 2015.08
CentOS 7
Debian 7
Debian 8
Fedora 22
Gentoo 2014.12
openSUSE 13.2
Slackware 14.1
Ubuntu 14.04 LTS
Ubuntu 15.10
Ubuntu 16.04 LTS

Older Distributions

Arch Linux 2015.02
CentOS 5.6
CentOS 6.5
Fedora 20
Fedora 21
Gentoo 2013-11-26
openSUSE 13.1
Slackware 13.37
Slackware 13.37 32bit
Ubuntu 12.04 LTS
Ubuntu 15.04

Account

Support

Documentation

Community

Dashboard

Remote Access

Linodes » (MACS Services) »

Deploy an Image

Image

Deployment Disk Size

Swap Disk

Root Password

Graphs

Backups

Settings

Extras

See also: [Deploying using StackScripts](#)

Linode Manager

4macsadmin | my profile | log out

Linodes NodeBalancers Longview DNS Manager Account Support Documentation Community

Dashboard Remote Access Rebuild Rescue Resize Clone Graphs Backups Settings

Linodes » (MACS Services) » linode1818909



Dashboard

Select	Configuration Profiles	Options
<input checked="" type="radio"/>	My Ubuntu 16.04 LTS Profile (Latest 64 bit (4.5.0-x86_64-linode65))	Edit Remove

Boot

[Rebuild](#) | [Deploy an Image](#) | [Create a new Configuration Profile](#)

Disks

 Ubuntu 16.04 LTS Disk (24320 MB, ext3)	Edit Remove
 256MB Swap Image (256 MB, swap)	Edit Remove

[Create a new Disk](#)

Host Job Queue [\(more\)](#)

Success	Create Filesystem - 256MB Swap Image Entered: 32 seconds ago - Took: 0 seconds
Success	Disk Create From Distribution - Ubuntu 16.04 LTS Entered: 33 seconds ago - Took: 8 seconds Setting password for root... done
Success	Linode Initial Configuration Entered: 4 minutes 58 seconds ago - Took: 0 seconds

Graphs

Server Status

Your Linode is currently

Powered Off

Network

- Transfer/mo: 2000 GB
- Incoming: 0 bytes
- Outgoing: 0 bytes
- Total: 0 bytes

You have used

0%
of your monthly transfer

Storage

- Total: 24576 MB
- Used: 24576 MB
- Free: 0 MB

You have allocated

100%
towards disk images

Backups

No - [Enable](#)

Host

newark1083	load
KVM	low

Linode Manager

 4macsadmin | [my profile](#) | [log out](#)

[Linodes](#)

[NodeBalancers](#)

[Longview](#)

[DNS Manager](#)

[Account](#)

[Support](#)

[Documentation](#)

[Community](#)

[Dashboard](#)

[Remote Access](#)

[Rebuild](#)

[Rescue](#)

[Resize](#)

[Clone](#)

[Graphs](#)

[Backups](#)

[Settings](#)

[Extras](#)

[Linodes](#) » [\(MACS Services\)](#) » [linode1818909](#) » **Rebuild**

Rebuilding will **destroy all data**, wipe your Linode clean, and start fresh.

Deploy an Image

Image

Ubuntu 14.04 LTS



Choosing a 64 bit distro is recommended.

See also: [Deploying using StackScripts](#)

Deployment Disk Size

4macs MB

750 MB min 24320 MB max

Swap Disk

256 MB



Root Password

.....



Rebuild

[Linodes](#) » [\(MACS Services\)](#) » [linode1818909](#) » **Settings**

Settings

Display Settings

Linode Label

Rename your Linode

Display Group

Group Linodes together on the Linodes tab using Display Groups!

Shutdown Watchdog

Description

Lassie is a Shutdown Watchdog that monitors your Linode and will reboot it if it powers off unexpectedly. It works by issuing a boot job when your Linode powers off without a shutdown job being responsible.

To prevent a loop, Lassie will give up if there have been more than 5 boot jobs issued within 15 minutes.

Lassie is currently

Email Alert Thresholds

Description

When an alert threshold is reached, an email is sent to all linode.com users that have the "access" privilege to this Linode.

Thresholds are compared to values once per hour, 15 minutes after the hour.

CPU Usage Enabled ☒ | %

Average CPU usage over 2 hours exceeding this value triggers this alert.

Disk IO Rate Enabled ☒ | IO Ops/sec

Average Disk IO ops/sec over 2 hours exceeding this value triggers this alert.

Incoming Traffic Enabled ☒ | Mbit/s

Average incoming traffic over a 2 hour period exceeding this value triggers this alert.

Outbound Traffic Enabled ☒ | Mbit/s

Average outbound traffic over a 2 hour period exceeding this value triggers this alert.

Transfer Quota Enabled ☒ | %

Percentage of network transfer quota used being greater than this value will trigger this alert.

Linode: IP and DNS

- Remote Access tab, and you'll see your server's IP address listed
- Add the IP to your DNS
- Set the reverse DNS
 - Remote Access » Reverse DNS
- Boot the Linode

Linodes » (MACS Services) » linode1818909 » Remote Access

Network Access

Public Network

SSH Access [ssh root@198.74.60.120](#)

[Getting Started Guide](#)

Public IPs 198.74.60.120 / 24 (li557-120.members.linode.com)
2600:3c03::f03c:91ff:fe55:62fc / 64
[IP Add](#) | [IP Remove](#) | [IP Failover](#) | [IP Swap](#) | [Reverse DNS](#)

[Static Networking Guide](#)
[IPv6 Networking Guide](#)

Default Gateways 198.74.60.1
fe80::1

DNS Resolvers

66.228.42.5
96.126.106.5
50.116.53.5
50.116.58.5
50.116.61.5
50.116.62.5
66.175.211.5
97.107.133.4
207.192.69.4
207.192.69.5
2600:3c03::5
2600:3c03::6
2600:3c03::7
2600:3c03::8
2600:3c03::9
2600:3c03::b
2600:3c03::c

Private/LAN Network

Private IPs None - [Add a Private IP](#)

Link-Local IP fe80::f03c:91ff:fe55:62fc/64

Console Access

Lish via Ajaxterm [Launch Lish Ajax Console »](#)


Lish via SSH [ssh -t 4macsadmin@lish-newark.linode.com linode1818909](#)

Lish listens on ports 22, 443, and 2200
([Lish Guide & Fingerprints](#))

Glish [Launch Graphical Web Console »](#)

Equivalent to plugging a monitor and keyboard into your server.
([Using Glish](#))

Linode Manager

 4macsadmin | [my profile](#) | [log out](#)

[Linodes](#)[NodeBalancers](#)[Longview](#)[DNS Manager](#)[Account](#)[Support](#)[Documentation](#)[Community](#)[Dashboard](#)[Remote Access](#)[Rebuild](#)[Rescue](#)[Resize](#)[Clone](#)[Graphs](#)[Backups](#)[Settings](#)[Extras](#)

[Linodes](#) » [\(MACS Services\)](#) » [linode1818909](#) » **Rescue**

Rescue Mode

Boots your Linode into Rescue Mode. Access it via the console.

/dev/sda

/dev/sdb

/dev/sdh

Reset Root Password

Filesystem

Linode must be shut down

New Password

Resize

Choose your new plan

- ☐ ~~Linode 1024~~ (current plan)
- ☐ Linode 2048
- ☐ Linode 4096
- ☐ Linode 8192
- ☐ Linode 16384
- ☐ Linode 32768
- ☐ Linode 49152
- ☐ Linode 65536
- ☐ Linode 98304

[Resize this Linode Now!](#)

How it works

1. Linode is shut down and migrated

You will experience downtime while your Linode is migrated. We estimate **18 minutes** to migrate your Linode, but that may vary based on host and network load.

2. Billing

Your account will be immediately charged (or credited) a prorated amount based upon the difference in cost and the number of days remaining in your billing cycle.

3. Enjoyment

After the migration completes, you can take advantage of the new resources by resizing your disks.

[Linodes](#) » [\(MACS Services\)](#) » [linode1818909](#) » **Clone**

Configuration Profiles

Select	Configuration Profiles	Kernel	Disks Attached
<input type="checkbox"/>	My Ubuntu 16.04 LTS Profile	Latest 64 bit (4.5.0-x86_64-linode65)	2

Select

Disks

Select	Disks	Type	Size
<input type="checkbox"/>	Ubuntu 16.04 LTS Disk	ext3	24320 MB
<input type="checkbox"/>	256MB Swap Image	swap	256 MB

Select

Linodes » (MACS Services) » screenconnect » Backups

Backups

Schedule

Backup Window (GMT-5) 0200 - 0400

Weekly Backup Sunday

Save Changes

Automatic Backups

Daily Backup From today
Restore to...

Weekly Backup From yesterday
Restore to...

Weekly Backup From 8 days ago
Restore to...

Manual Snapshot

Snapshot backup before upgrade
From 416 days ago
Restore to...

My New Snapshot Label

Take a New Snapshot Now

Backup History

Type	Started	Finished	Duration	Status	Message
auto	2016-04-25 02:31:58	2016-04-25 02:34:03	2 minutes, 5 seconds	successful	
auto	2016-04-24 02:31:21	2016-04-24 02:33:30	2 minutes, 9 seconds	successful	
auto	2016-04-23 02:31:14	2016-04-23 02:33:23	2 minutes, 9 seconds	successful	
auto	2016-04-22 02:31:13	2016-04-22 02:33:22	2 minutes, 9 seconds	successful	
auto	2016-04-21 02:31:31	2016-04-21 02:33:39	2 minutes, 8 seconds	successful	
auto	2016-04-20 02:32:19	2016-04-20 02:34:27	2 minutes, 8 seconds	successful	
auto	2016-04-19 02:31:58	2016-04-19 02:34:06	2 minutes, 8 seconds	successful	
auto	2016-04-18 02:31:30	2016-04-18 02:33:39	2 minutes, 9 seconds	successful	
auto	2016-04-17 02:31:38	2016-04-17 02:33:41	2 minutes, 3 seconds	successful	
auto	2016-04-16 02:32:31	2016-04-16 02:34:39	2 minutes, 8 seconds	successful	

Cancel Backups

Linode: Hostname

- ssh to server
 - Click on the Remote Access tab
- Set the hostname:
 - Replace *hostname* with a fqdn of your choice.
 - `echo "hostname" > /etc/hostname`
 - `hostname -F /etc/hostname`

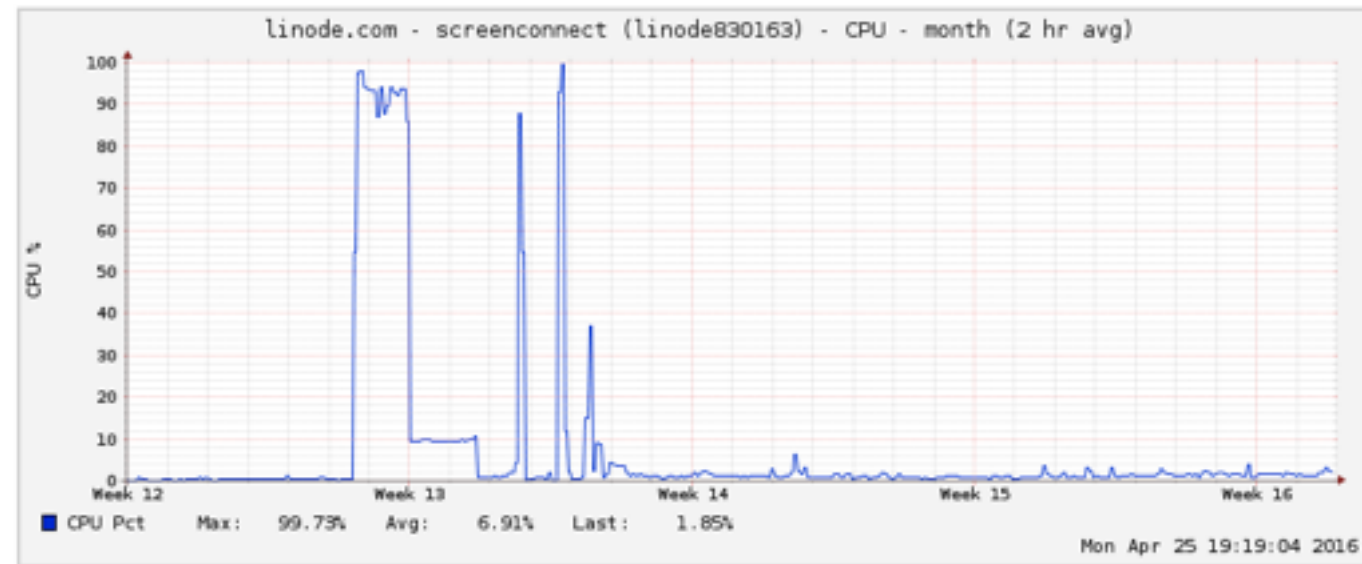
Linode:Time Zone

- Set the time zone for the server with this command:
 - `dpkg-reconfigure tzdata`
 - follow the on screen messages
 - select your region, and time zone

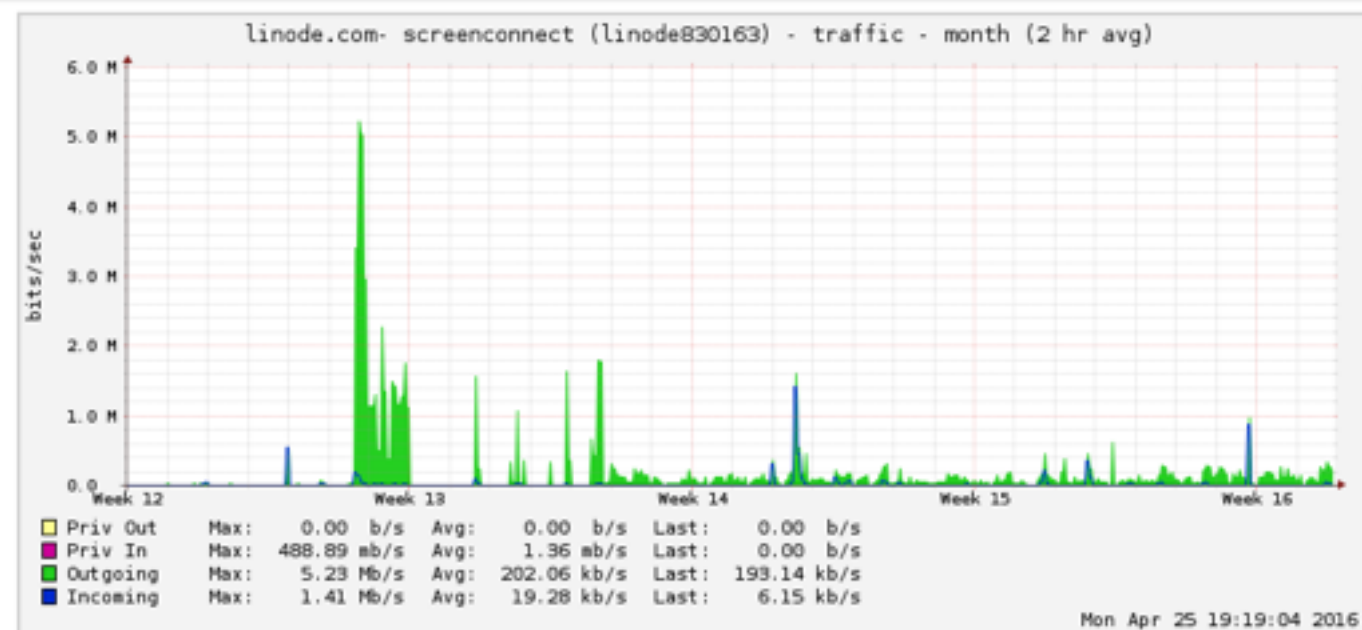
< 2015 2015 2015 2015 2015 2015 2015 2015 2016 2016 2016 LAST LAST
MAY JUN JUL AUG SEP OCT NOV DEC JAN FEB MAR 30D 24H

Last 30 Days

CPU



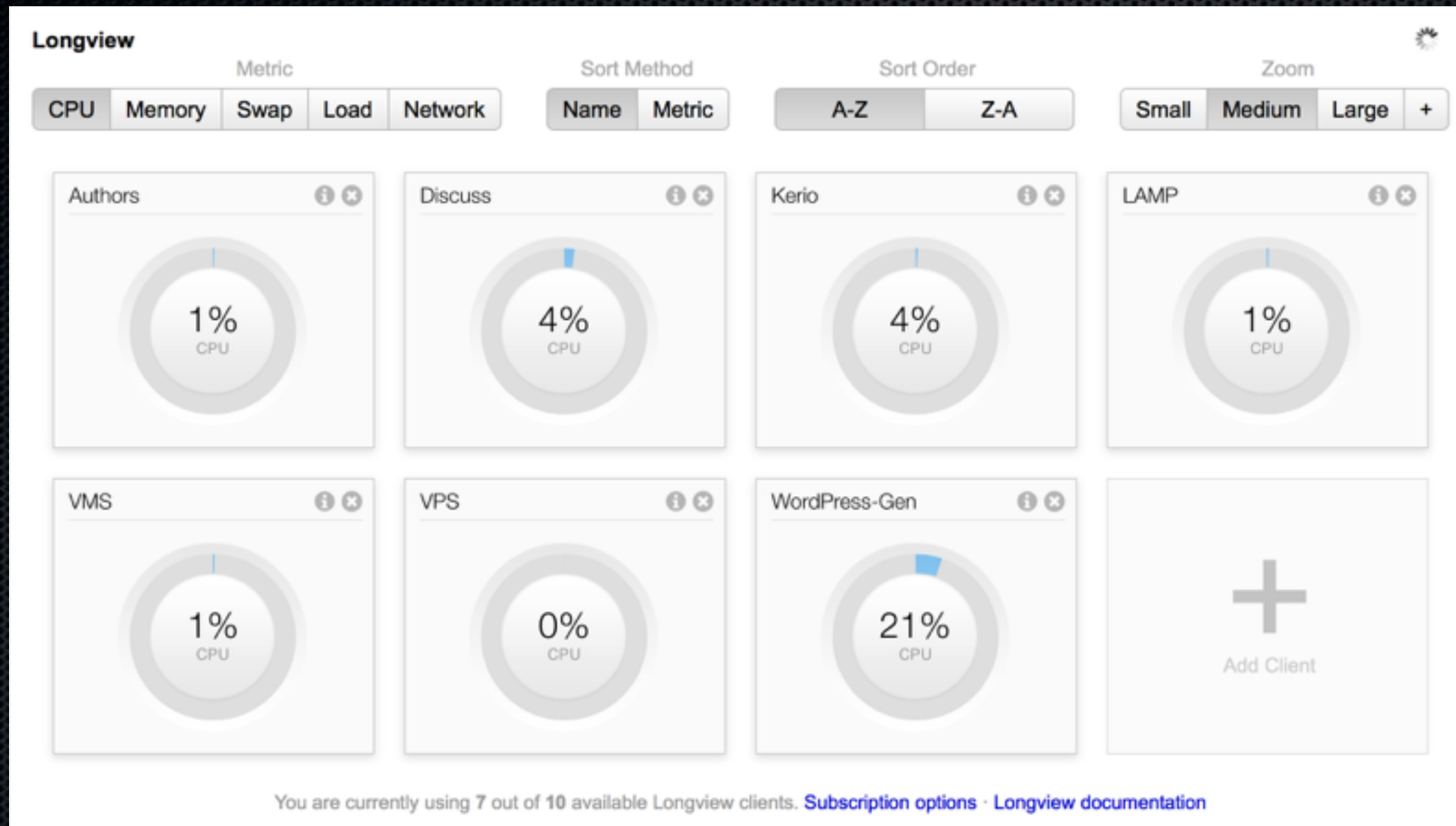
Network



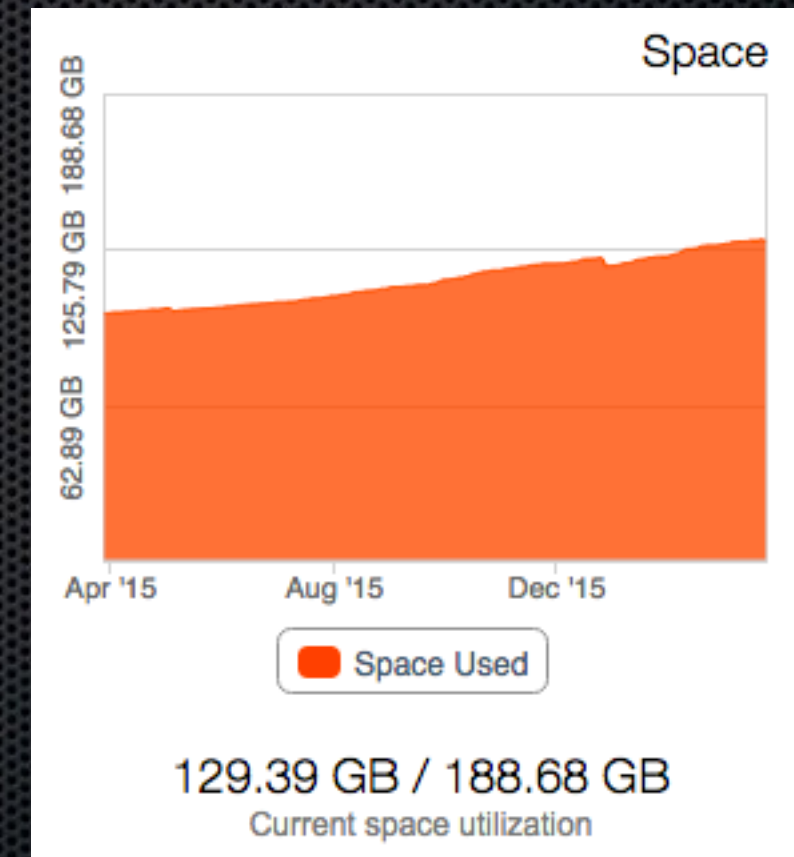
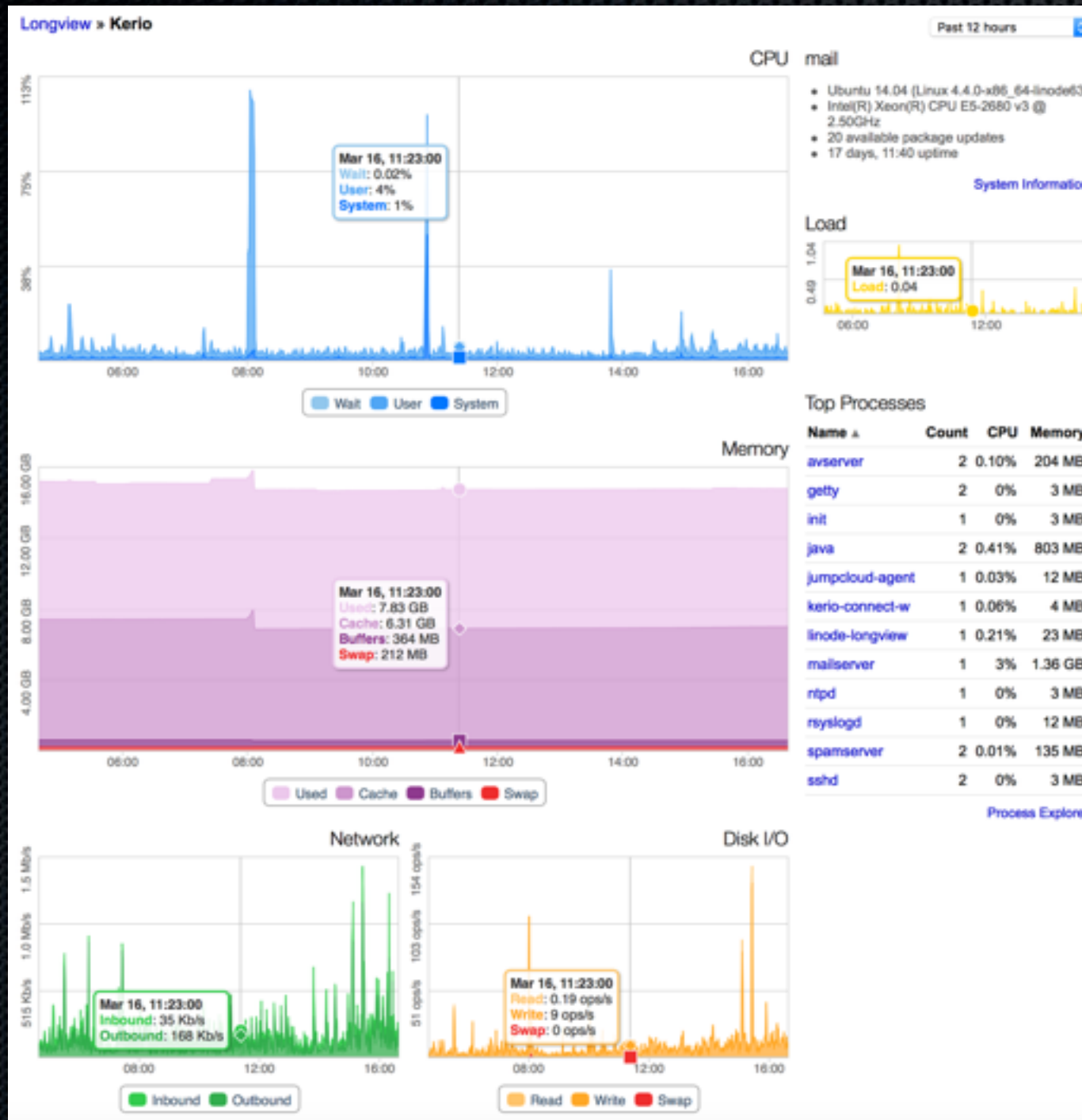
Linode: Monitoring

- Longview
 - Press the “+” to add a client
 - Copy command to install Longview via the curl
 - Rename your Longview
 - the “i” icon for the new Longview
- Watchman Monitoring (to come)
- Enable Backups:
 - Costs 20% of the cost of your Linode

Linode's Longview



Linode's Longview



Control Panels

- Why?
 - Base server config
 - Services Configuration
 - Scripted Installers
 - User Access
 - Database Configuration
 - Security
- Industry Standards:
 - cPanel, Plesk, InterWorx, zPanel, ISPConfig

Control Panels

- Light, fast, and secure with modern interface
- New Breed, multi-servers
 - ServerPilot.io
 - webmin / virtualmin / usermin
 - Sentora <http://sentora.org>
 - virtualizor
- Single Servers
 - Webuzo
 - VestaCP

Types of Services

- Nginx Web Server
- Apache Web Server (as backend)
- Bind DNS Server
- Exim or other mail server
- Antivirus Antispam
- Dovecot POP3/IMAP Server or others
- MySQL Database Server
- FTP Server
- Firewall and automatic banning
- ... and others

ServerPilot.io

The screenshot shows the 'Apps' management page in the ServerPilot.io dashboard. The browser address bar shows 'manage.serverpilot.io/#apps'. The page has a sidebar with navigation links: Servers, Apps, Account, Support, and Log out. A green '+ Create App' button is in the top right. A light blue banner states 'We now offer free SSL certificates! [Learn more.](#)'. Below this is a search bar labeled 'Search Apps'. The main content is a table with columns: APP, SERVER, DISK, and MEMORY. It lists five apps: 'authors' (0 MB disk, 0 MB memory), 'images' (0.34 MB disk, 0 MB memory), 'pagewatch' (7.7 MB disk, 0 MB memory), 'phpq' (0.71 MB disk, 0 MB memory), and 'redirect' (21 MB disk, 0 MB memory). All apps show '0 processes'.

APP	SERVER	DISK	MEMORY
authors <small>authors.mactech.com</small>	authors.mactech.com	0 MB	0 MB <small>0 processes</small>
images <small>images.mactech.com</small>	vps.xplain.com	0.34 MB	0 MB <small>0 processes</small>
pagewatch <small>pagewatch.mactech.com</small>	vps.xplain.com	7.7 MB	0 MB <small>0 processes</small>
phpq <small>forms.mactech.com</small>	lamp.xplain.com	0.71 MB	0 MB <small>0 processes</small>
redirect <small>redirect.mactech.com</small>	vps.xplain.com	21 MB	0 MB <small>0 processes</small>

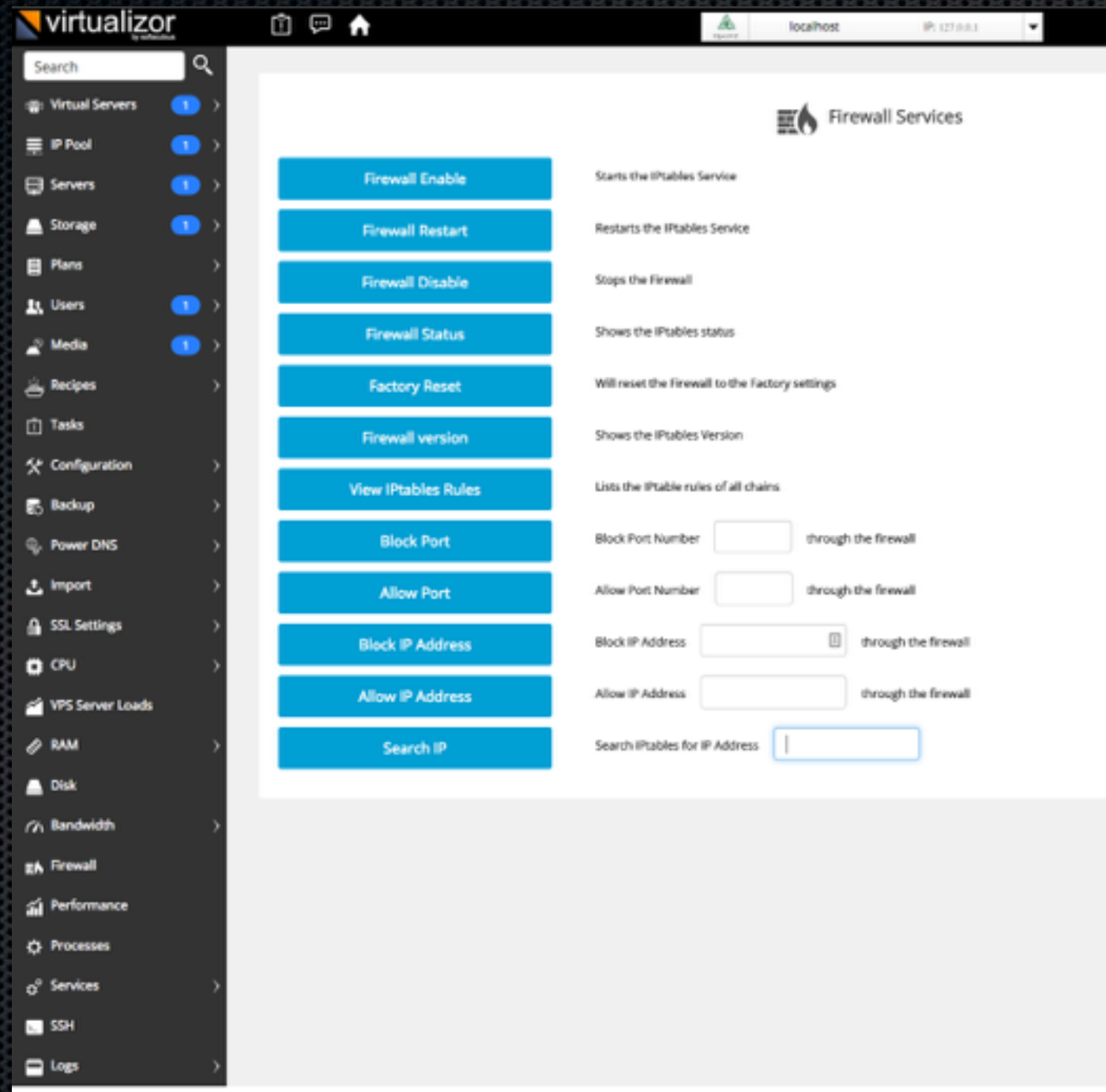
VestaCP

The screenshot displays the VestaCP web interface in a browser window. The address bar shows the URL `vps.xplain.com:8083/list/user/`. The interface includes a top navigation bar with various links like 'ClipOneNote', 'KM', 'SipNumCart', etc., and a secondary bar with 'VESTA' and navigation options like 'Packages', 'IP', 'Graphs', etc. The main content area is titled 'USER' and shows a summary of system statistics across seven categories: USER, WEB, DNS, MAIL, DB, CRON, and BACKUP. Below this, a table lists the details for the 'admin' user, including their role as 'System Administrator', bandwidth usage, disk usage, and various system settings like email, package, SSH access, and name servers.

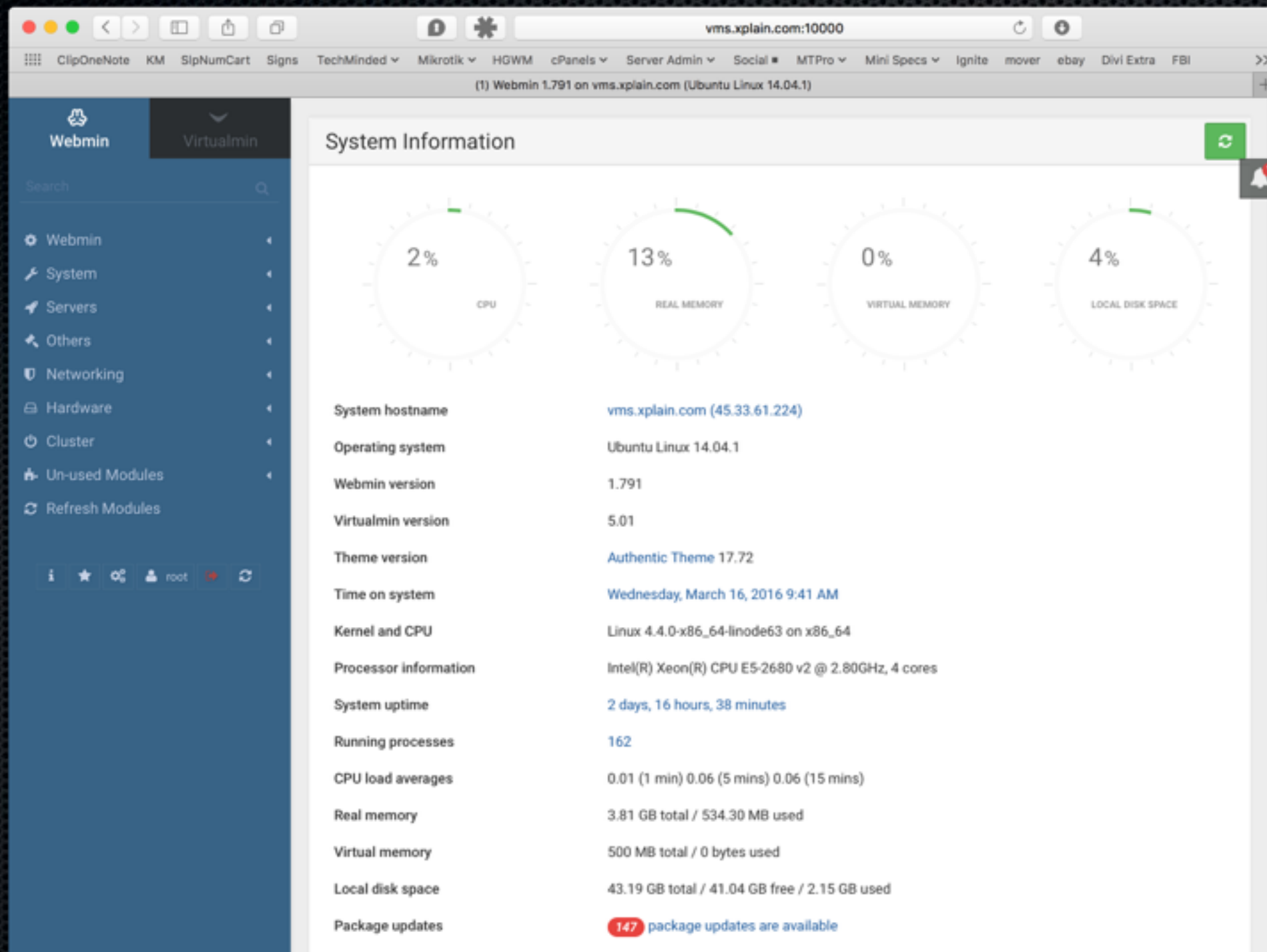
USER	WEB	DNS	MAIL	DB	CRON	BACKUP
users: 1	domains: 1	domains: 0	domains: 1	databases: 1	jobs: 7	backups: 3
suspended: 0	aliases: 1	records: 0	accounts: 0	suspended: 0	suspended: 0	
	suspended: 0	suspended: 0	suspended: 0			

admin	
System Administrator	
Bandwidth	0 mb
Disk:	2 mb
Web: 1 mb	Databases: 0 mb
Mail: 0 mb	User Directories: 1 mb
Web Domains:	1 / 100
DNS Domains:	0 / 100
Mail Domains:	1 / 100
Databases:	1 / 100
Cron Jobs:	7 / 100
Backups:	3 / 3
Email:	netadmin@xplain.com
Package:	default
SSH Access:	bash
IP Addresses:	1
Name Servers:	ns1.localhost.ltd ns2.localhost.ltd

virtualizor



webmin



webmin fun

- For Webmin, don't forget...
 - Set time zone, and time server:
 - Webmin > Hardware > System Time
- Fix permissions, and validate
 - Virtualmin > Limits and Validations > Validate Virtual Servers
 - May want to set up schedule for regular validation
- webmin vs. virtualmin vs. cloudmin vs. usermin

Or choose none...

- Remember...
 - Ask yourself why?
- And if none, you need to remember
 - Updates and Security Patches
 - Prevent password and root login
 - Firewall
 - Monitoring

Auto-Updates

- `sudo apt-get install unattended-upgrades`
- `sudo dpkg-reconfigure -p low unattended-upgrades`

Check the Schedule

```
mactech@someserver:~$ cat /etc/apt/apt.conf.d/10periodic
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "0";
APT::Periodic::AutocleanInterval "0";

mactech@someserver:~$ cat /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Note: The 1 means it will update every day. 7 is weekly

Forcing Updates

- Find available updates, and force an upgrade now:
`sudo apt-get update`
`sudo apt-get dist-upgrade`
- Testing it?
 - list available updates
`sudo apt-get -u upgrade`
 - simulate update process
`sudo apt-get -s upgrade`
- Brute Force Testing
 - `sudo reboot now`
 - you should not see updates now

Firewall

Configure the firewall

Typical ports you may want to open:

```
sudo ufw allow ssh
sudo ufw allow 80/tcp
sudo ufw allow 443/tcp
sudo ufw allow 25/tcp
sudo ufw show added
sudo ufw enable
```


Disable Access

- Disable password access for root


```
sudo passwd -l root
```

- But there's an easier way.

Managing Users

- JumpCloud
 - <https://console.jumpcloud.com/#/systems>
 - get your Linux install curl command and execute it at the command line for the ssh session you have to the server
 - add a tag to the system so you can manage it
 - make sure to assign yourself (and anyone else) and the server
- Other solutions as well

JumpCloud

 JumpCloud

USERS

SYSTEMS

TAGS

APPLICATIONS

DIRECTORIES

COMMANDS

SETTINGS

SUPPORT

Users All your users at-a-glance

greg.keller@jumpcloud.com

!

All Users: No users selected

Resend Email

+ Add User


- Del User


Search


	Status	Last Name	First Name	Username	Email	System Admin/Sudo	
<input type="checkbox"/>	✓	Keller	Gregory	GREGORYMKELLER	greg@jumpcloud.com	✓	Details
<input type="checkbox"/>	✓	Dietrich	Amy	adietrich	amy@jumpcloud.com		Details
<input type="checkbox"/>	✓	Christianson	Billy	billyc	billyc@jumpcloud.com	✓	Details
<input type="checkbox"/>	⚠	Brown	Bob	bob	bob@test-jumpcloud.com		Details
<input type="checkbox"/>	✓	O'Connor	Beth	bocconor	beth@jumpcloud.com		Details
<input type="checkbox"/>	✓	McGloughlin	Cindi	cindi	cindi@jumpcloud.com	✓	Details
<input type="checkbox"/>	✓	Johnson	Eric	⚠ ejohnson (Password Expired)	ejohnson@jumpcloud.com	✓	Details
<input type="checkbox"/>	✓	User	GADS	⚠ gadsuser	ITAdmin@jumpcloud.com		Details
<input type="checkbox"/>	⚠	Blackborow	Josh	jblaclborow	jblaclborow@test-jumpcloud.com		Details
<input type="checkbox"/>	✓	Blow	Joe	jblow	joe@jumpcloud.com	✓	Details


Showing 1 to 10 of 30 entries


First Previous 1 2 3 Next Last



JumpCloud



 USERS



SYSTEMS



 TAGS



 APPLICATIONS


 DIRECTORIES



 COMMANDS



 RADIUS


 SETTINGS


 SUPPORT

Systems
 All your systems at-a-glance


 Search


 20 systems










<input type="checkbox"/>	Status	System Name ^	OS	Primary Adapter IP	Last Contact
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago
<input type="checkbox"/>	✓		Ubuntu 14.04 x86_64		a few seconds ago

Commands All your executable system commands at-a-glance

 Search



10 commands

<input type="checkbox"/>	Name 	Command	System / Tag Count
<input type="checkbox"/>	Download & Install Kerio Connect <small>Launch Manually</small>	<code>#edit url! cd /tmp; curl -O http://cdn.kerio</code>	 2 Systems
<input type="checkbox"/>	add text to mail server login page <small>Launch Manually</small>	<code>sed -i "107i /tmp/kerio.connect.login.page.:</code>	 1 Tag
<input type="checkbox"/>	install watchman <small>Launch Manually</small>	<code>wget -N https://macs.monitoringclient.com/di</code>	 5 Systems
<input type="checkbox"/>	install watchman pt 2 <small>Launch Manually</small>	<code>sudo dpkg -i MonitoringClient.deb</code>	 1 System
<input type="checkbox"/>	jumpcloud <small>Launch Manually</small>	<code>curl -s https://lv.linode.com/A3F95E96-D19A-</code>	 1 System
<input type="checkbox"/>	set watchman group <small>Launch Manually</small>	<code>sudo echo "Tech2000" > /var/tmp/ClientGroup-</code>	 1 System
<input type="checkbox"/>	set watchman to auto update <small>Launch Manually</small>	<code>sudo run-client --auto-update true</code>	 19 Systems
<input type="checkbox"/>	update (1 of 2) <small>Launch Manually</small>	<code>apt-get update</code>	 14 Systems

Details

User Bindings

Display Name:

PT Management

Status:

Active, System Reporting

Last Contact:

a few seconds ago

Host Name:

Instance ID:

Unknown

Operating System:

Ubuntu 14.04

Architecture:

x86_64

Primary Adapter IP:

Remote IP Address:

SSH Root Login:

☐ Allow

SSH Password Login:

☐ Allow

Multifactor Authentication:

☐ Enable

Public Key Authentication:

☒ Enable

Integrated Monitoring

- Go to your watchman setup:
- define the group
- install on (two commands) watchman client

```
run-client --auto-update true  
sudo run-client -F
```


Computer Overview

[Actions](#)

All Clear



0 Muted Plugins



2 Expirations

Last User: xadmin

[Copy Specs](#)

Computer Name:

Group:

Serial Number: No Serial Found

INTEGRATIONS

Monkey Box:

[View in MonkeyBox](#)

TECH SPECS

Operating System: Ubuntu 14.04.4 LTS

Serial Number: No Serial Found

Installed RAM: 3.9 GB

Processor: Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz 2800 (4 core 1 processor)

System MAC: F2:3C:91:89:F0:B7

Flash Version: Unknown

REPORTING

Last Report: 2016-04-25 7:18 PM

Agent Version: 3.0.218

Uptime: 133 days 15 hours 58 minutes

First Report: 2014-11-30 10:42 AM

Watchman ID: 20141130-L27J-GXKGWA

Plugin Results

[Notes \(0\)](#)[History](#)[Edit](#)

Last Reboot

2016-04-25 7:18 PM

Last System Boot Time: 2015-12-14 at 02:19 (Monday)

[?](#) [Actions](#)

Local IP Address

2016-04-25 7:18 PM

Primary IP: on eth0

[?](#) [Actions](#)

Monitoring Agent

2016-04-25 7:18 PM

Monitoring Client version 3.0.218

The internal check of the client software reports no issues.

[?](#) [Actions](#)

Network Errors

2016-04-25 7:18 PM

[2016-04-25] lo: 0 Send Errors, 0 Receive Errors; eth0: 0 Send Errors, 0 Receive Errors

[?](#) [Actions](#)

RAM Errors

2016-04-25 7:18 PM

Memory: 3998MiB total, 1979MiB used, 2019MiB free

Swap: 255MiB total, 254MiB used, 1MiB free

[?](#) [Actions](#)

Report Failed Logins

2016-04-25 7:18 PM

No new failed logins to report

[?](#) [Actions](#)

Report Kerio Status

2016-04-25 7:18 PM

License:

License Expires: 31 Jan 2017

Subscription Expires: 31 Jan 2017

Licensed Users: 10000 (43 Local Used)

Company: Mid-Atlantic Computer Solutions

E-Mail: woneal@4macsolutions.com

[?](#) [Actions](#)

Key Directory, path, size:

Mailstore, /opt/kerio/mailserver/store, 89.16GB

Backups, /var/backup, does not exist.

Archives, /opt/kerio/mailserver/store/archive, 0.00GB

Logs, /opt/kerio/mailserver/store/logs/, 0.63GB

FullTextSearch, /opt/kerio/mailserver/store/fulltext, 1.97GB

Domains - Users (Total Storage, Public Folders):

adasafrica.com - 5 (15.25GB, 0.00GB)

docshutventure.com - 2 (0.00GB, 0.00GB)

PCI and SSL

- PCI Security:
<https://www.virtualmin.com/documentation/security/pci>
- Check your vulnerabilities and SSL installation with tools.
 - <https://www.digicert.com/help/>
 - <https://www.sslshopper.com/ssl-checker.html>

Mitigating Poodle / SSL 3.0 Issue

- Apache, VirtualMin, Usermin
 - See full description and steps at:
<https://www.digicert.com/ssl-support/apache-disabling-ssl-v3.htm>

<https://www.virtualmin.com/node/34811>

Tools and Utilities

- ncdu: “GUI” for file browsing

```
ncdu install  
apt-get install ncdu  
apt-get install yum  
apt-get install yum-utils  
yum-config-manager --enable
```

- mtr: “GUI” to help with packet trace and loss

```
apt-get install mtr
```


ncdu

```
ncdu 1.10 ~ Use the arrow keys to navigate, press ? for help
--- /opt/kerio ---
      ..
321.7GiB [#####] /mailserver
16.0KiB [          ] .DS_Store

Scanning...
Total items: 2279188 size: 123.3GiB
Current item: /opt/kerio/mailserver/sto...il/02 - Q4/#msgs/00000ded.eml

ning...                               Press q to abort

Total disk usage: 321.7GiB Apparent size: 315.5GiB Items: 3198720
```


ncdu

```
neil — neil@mail: / — ssh mail — 80x24
ncdu 1.10 ~ Use the arrow keys to navigate, press ? for help
--- /opt/kerio/mailserver/store/backup -----
/..
2.0GiB [#####] C20160227T190203Z.11.zip
2.0GiB [##### ] C20160227T190203Z.1.zip
2.0GiB [##### ] ncdu help 1:Keys 2:Format 3>About
2.0GiB
2.0GiB      C Sort by items (ascending/descending)
2.0GiB      d Delete selected file or directory
2.0GiB      t Toggle dirs before files when sorting
2.0GiB      g Show percentage and/or graph
2.0GiB      a Toggle between apparent size and disk usage
2.0GiB      c Toggle display of child item counts
2.0GiB      e Show/hide hidden or excluded files
2.0GiB      i Show information about selected item
2.0GiB      r Recalculate the current directory
2.0GiB      q Quit ncdu
2.0GiB
2.0GiB                                     Press q to continue
2.0GiB [##### ] C20160227T190203Z.9.zip
2.0GiB [##### ] F20160305T080103Z.27.zip
2.0GiB [##### ] F20160305T080103Z.28.zip
Total disk usage: 145.8GiB Apparent size: 145.8GiB Items: 120
```


mtr

```
ssh root@198.74.60.120 — -ssh -l root 198.74.60.120 — 100x35

My traceroute [v0.86]
ubuntu (0.0.0.0) Tue Apr 26 17:34:49 2016
Keys: Help Display mode Restart statistics Order of fields quit

Host      Loss%  Snt  Last  Avg  Best  Wrst StDev
1. router2-nac.linode.com 0.0%  291  0.7  0.6  0.5  1.9  0.1
2. 173.255.239.2          0.0%  291  0.7  0.8  0.6  2.1  0.2
3. 207.99.109.69          0.0%  291  0.8  1.7  0.4  12.8 2.8
4. 0.e1-1.tbr1.tl9.nac.net 0.0%  291  10.8 3.7  1.5  12.7 3.4
5. 0.e1-3.tbr2.tl9.nac.net 0.0%  291  1.5  2.6  1.4  22.1 2.9
6. ae-30.r08.nycmny01.us.bb.gin.ntt.net 0.0%  291  3.1  2.2  1.8  5.2  0.4
7. lag-17.ear2.NewYork1.Level3.net 78.6% 291 54464 52695 51162 55082 866.7
8. b.resolvers.Level3.net 0.0%  291  1.5  1.5  1.4  2.0  0.0
```


System Logging

- syslog - or System Logging
 - papertrailapp.com will let you send your log files to them for parsing & storage
 - they will let you set up defined searches and the system will send you emails when something needs your attention


```

Apr 25 19:12:19 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: associa
Apr 25 19:12:19 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac RADIUS: starting acc
Apr 25 19:12:19 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac WPA: pairwise key ha
Apr 25 19:12:30 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_LEAVE ath1: 2
Apr 25 19:12:30 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: sta_sta
Apr 25 19:12:30 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: disasso
Apr 25 19:13:35 l logger: Attempt to deliver to unknown recipient <lmattis@t2000inc.com>, from <uemlmm2_595416893
Apr 25 19:13:36 l logger: Attempt to deliver to unknown recipient <zafar.ghadar@t2000inc.com>, from <bounce-18682
Apr 25 19:15:05 l logger: Attempt to deliver to unknown recipient <smalomo@t2000inc.com>, from <www-data@ccb1.lea
Apr 25 19:18:16 acsolutions.com logger: Connection attempt to service SMTP from IP address 195.22.126.189 rejecte
Apr 25 19:18:30 l logger: HTTP/CardDav: User demison@t2000inc.com doesn't exist. Attempt from IP address 207.235.
Apr 25 19:18:30 l logger: HTTP/CardDav: User demison@t2000inc.com doesn't exist. Attempt from IP address 207.235.
Apr 25 19:22:12 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: associa
Apr 25 19:22:12 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_JOIN ath1: 70:48:0f:
Apr 25 19:22:12 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac RADIUS: starting acc
Apr 25 19:22:12 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac WPA: pairwise key ha
Apr 25 19:22:20 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_LEAVE ath1: 2
Apr 25 19:22:20 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: sta_sta
Apr 25 19:22:20 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: disasso
Apr 25 19:22:22 l logger: Attempt to deliver to unknown recipient <lmattis@t2000inc.com>, from <uemlmm3_683517444
Apr 25 19:27:43 i_Control KerioControl: IPS: Alert, severity: Blacklist, Rule ID: 1:2520074 ET TOR Known Tor Exit
Apr 25 19:29:28 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_JOIN ath1: b8:09:8a:
Apr 25 19:29:28 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA b8:09:8a:ca:3b:2b IEEE 802.11: associa
Apr 25 19:29:28 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA b8:09:8a:ca:3b:2b RADIUS: starting acc
Apr 25 19:29:28 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA b8:09:8a:ca:3b:2b WPA: pairwise key ha
Apr 25 19:30:05 l logger: Attempt to deliver to unknown recipient <smalomo@t2000inc.com>, from <www-data@ccb1.lea
Apr 25 19:30:26 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_LEAVE ath1: 2
Apr 25 19:30:26 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA b8:09:8a:ca:3b:2b IEEE 802.11: sta_sta
Apr 25 19:30:26 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA b8:09:8a:ca:3b:2b IEEE 802.11: disasso
Apr 25 19:32:34 acsolutions.com logger: Connection attempt to service SMTP from IP address 195.22.126.189 rejecte
Apr 25 19:33:02 l logger: HTTP/CardDav: Invalid password for user kbroe@t2000inc.com. Attempt from IP address 96.
Apr 25 19:33:02 l logger: HTTP/CardDav: Invalid password for user kbroe@t2000inc.com. Attempt from IP address 96.
Apr 25 19:37:17 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_JOIN ath1: 70:48:0f:
Apr 25 19:37:17 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: associa
Apr 25 19:37:17 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac RADIUS: starting acc
Apr 25 19:37:17 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac WPA: pairwise key ha
Apr 25 19:37:43 106.143 (U7P: ,0418d6027439,v3.2.7.2816) syslog: wevent.recv_msg(): EVENT_STA_LEAVE ath1: 2
Apr 25 19:37:43 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: sta_sta
Apr 25 19:37:43 106.143 (U7P: ,0418d6027439,v3.2.7.2816) hostapd: ath1: STA 70:48:0f:ae:e7:ac IEEE 802.11: disasso
Apr 25 19:42:33 l logger: HTTP/WebDav: User rvanalastine@t2000inc.com doesn't exist. Attempt from IP address 68.2
Apr 25 19:42:36 l logger: HTTP/CardDav: User @ doesn't exist. Attempt from IP address 68.203.29.69.
Apr 25 19:42:39 l logger: HTTP/CardDav: User rvanalastine@t2000inc.com doesn't exist. Attempt from IP address 68.
Apr 25 19:42:42 l logger: HTTP/CardDav: User @ doesn't exist. Attempt from IP address 68.203.29.69.
Apr 25 19:42:46 l logger: HTTP/CalDav: User rvanalastine@t2000inc.com doesn't exist. Attempt from IP address 68.2
Apr 25 19:42:50 i_Control KerioControl: IPS: Packet drop, severity: Blacklist, Rule ID: 1:2400007 ET DROP Spamhau
172.98.114.196
Apr 25 19:45:05 l logger: Attempt to deliver to unknown recipient <smalomo@t2000inc.com>, from <www-data@ccb1.lea
Apr 25 19:46:13 l logger: Connection attempt to service SMTP from IP address 192.162.101.80 rejected: access from
Apr 25 19:47:05 acsolutions.com logger: Connection attempt to service SMTP from IP address 195.22.126.189 rejecte

```


Cloud Based Storage

- Storing files in Cloud as primary storage isn't backup
- 3-2-1 still applies, even to the Cloud
 - Have 3 copies of your data
 - Store on 2 different media types
 - Store 1 backup offsite (offsite = cloud in this case)
- Backup client machine that's synced to cloud
- Cloud-based data transfer and backup (briefly)
 - <https://mover.io>
 - <https://www.multicloud.com>
 - <http://www.cloudsfer.com>
 - <http://www.otixo.com>

Useful Links

- <https://www.linode.com>
- <https://www.digitalocean.com>
- <https://wiki.ubuntu.com/LTS>
- <http://serverpilot.io>
- <https://vestacp.com>
- <http://www.webmin.com>
- <http://jumpcloud.com>

Questions?



Neil Ticktin
neilt@mactech.com