Configuration, Accounting and Performance

CGS - Hugo Miranda

2021

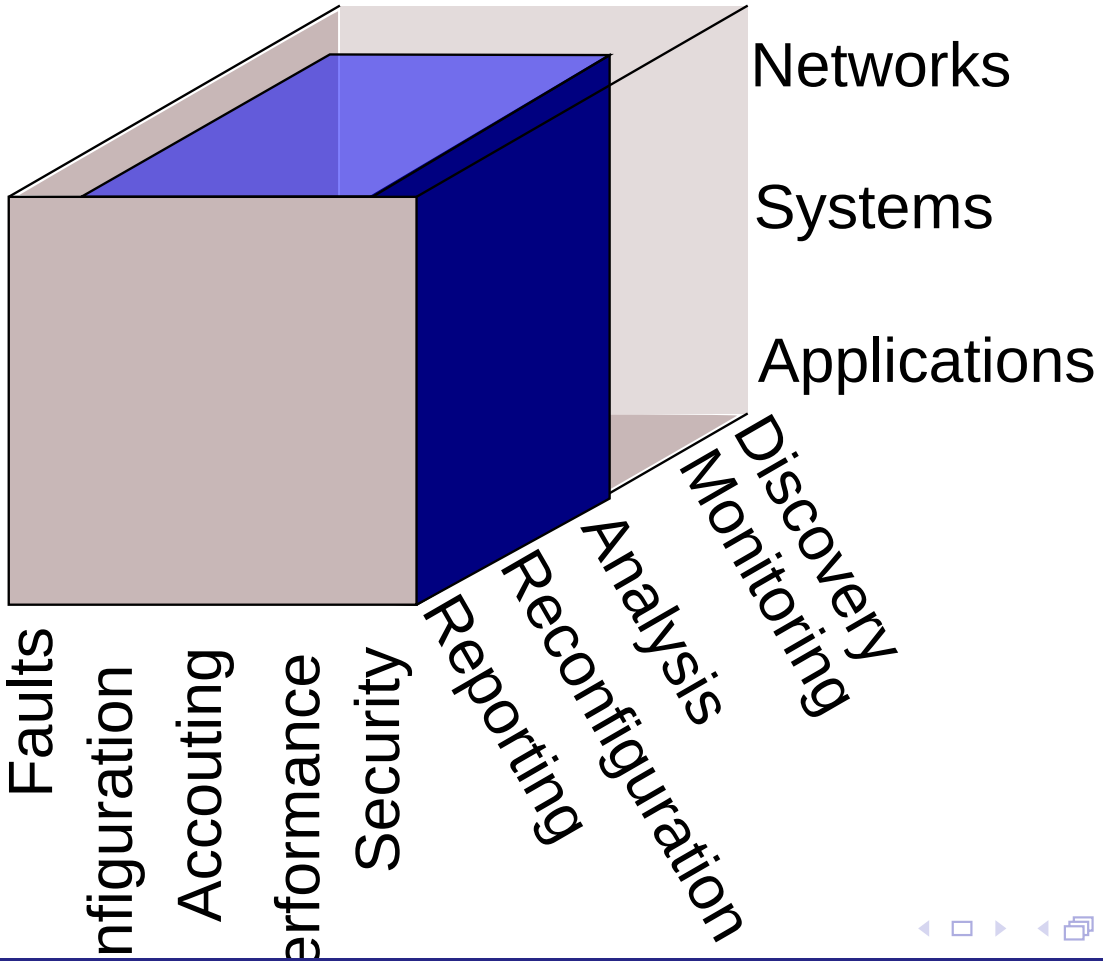
Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

Before we start

- The Agent assignment

The Cube


Networks
Systems
Applications
Discovery
Monitoring
Analysis
Reconfiguration
Reporting
Security
erformance
Accouting
nfiguration
Faults

The Challenges of Configuration

Configuration Values Management

- Preserve configuration files
- Keep configuration values "consistent"

Patch Management

- When and why to update software and hardware

Why Accounting and Performance

- To show that you meet the expectations/contracts
- To bill your clients
- To anticipate/detect performance problems
  - To keep the user happy
- To support management decisions

The Challenge

- Configuration parameters and values are a database
  - The challenge is to keep replicas consistent

Values replicated by all endpoints

- DNS server
- Default gateway address
- Print server address

IP/Port a public service is listening

- Must be configured in:
  - the service
  - the firewall
  - the reverse proxy
  - the HA server
  - the monitoring framework

New User ToDo List

Changing a web server's subnet

- DNS
- DHCP
- VLAN/Hypervisor
- Firewall
- Identify dependencies
  - Databases
  - Reverse proxy rules
- Monitoring framework
- Apache file
- Depending webservices

Problems

- No well-known unified database format
- Need to reconfigure/restart software and hardware
- No unified configuration file syntax or semantic
  - Makes hard to correlate information

sshd config file

```
#GatewayPorts no
#X11Forwarding no
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
PrintLastLog no
```

systemd config file

```
<!DOCTYPE busconfig PUBLIC "-//freedesktop//DTD D-BUS B
 "http://www.freedesktop.org/standards/dbus/1.0/busconf
<busconfig>
  <!-- Only root can send this message -->
  <policy user="root">
    <allow send_interface="com.redhat.PrinterSpooler"/>
  </policy>

  <!-- Allow any connection to receive the message -->
  <policy context="default">
    <allow receive_interface="com.redhat.PrinterSpooler
  </policy>
```

Cisco switch config file

```
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overloa
ip classless (default)
ip route 10.10.25.2 0.255.255.255 dialer 0
!
ip dhcp excluded-address 10.0.1.1 10.0.1.10
ip dhcp excluded-address 10.0.2.1 10.0.2.10
ip dhcp excluded-address 10.0.3.1 10.0.3.10
!
ip dhcp pool vlan1
network 10.0.1.0 255.255.255.0
default-router 10.0.1.1
```

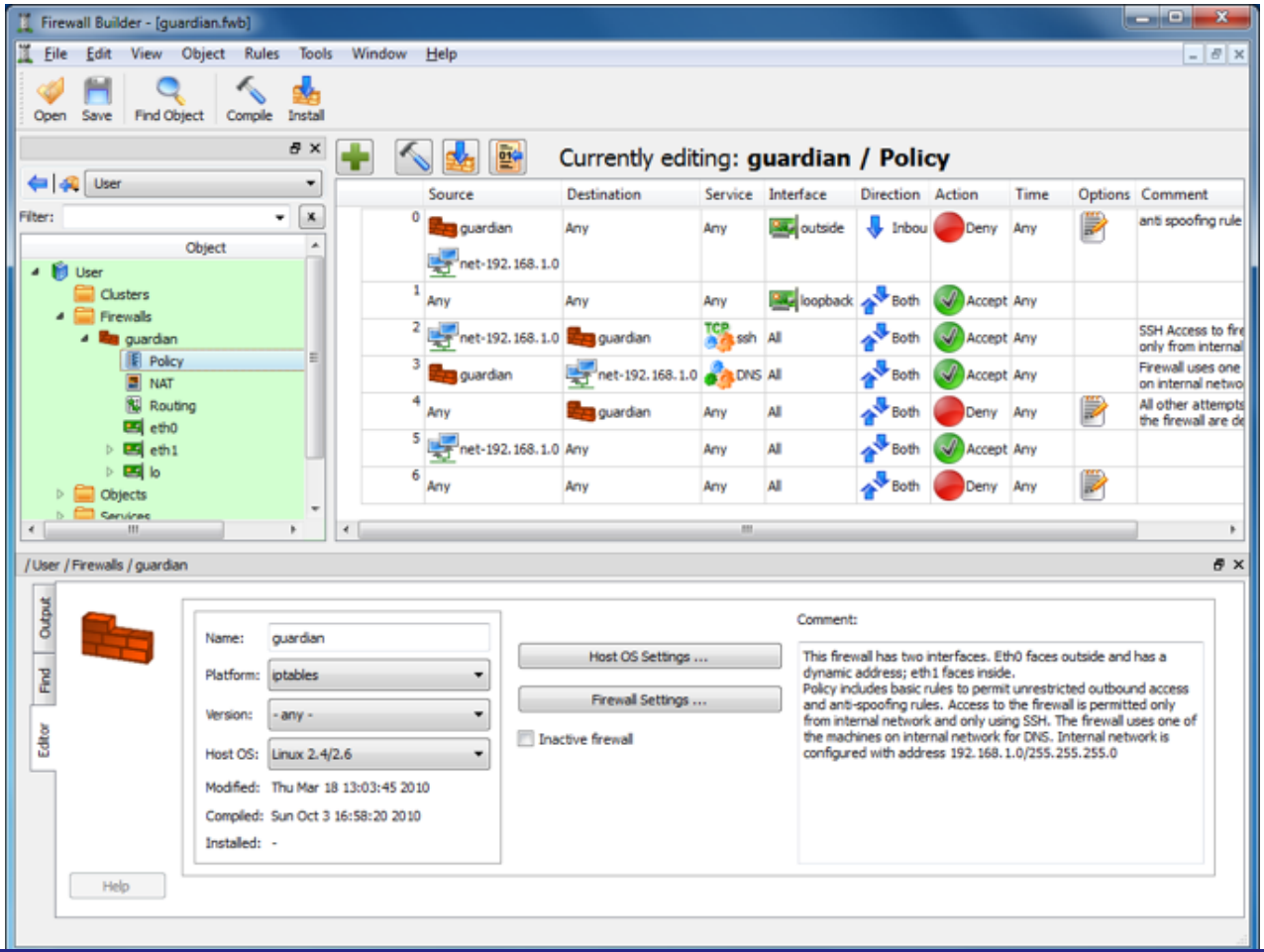
The Wishlist

- A centralized configuration management database (CMDB), i.e. a repository to:
  - Store configuration parameters
  - Look for problems
  - Identify dependencies
    - What If analysis
    - Validation
  - Quickly clone a device/service
  - Make bidirectional conversion from/to proprietary formats

Non-automated

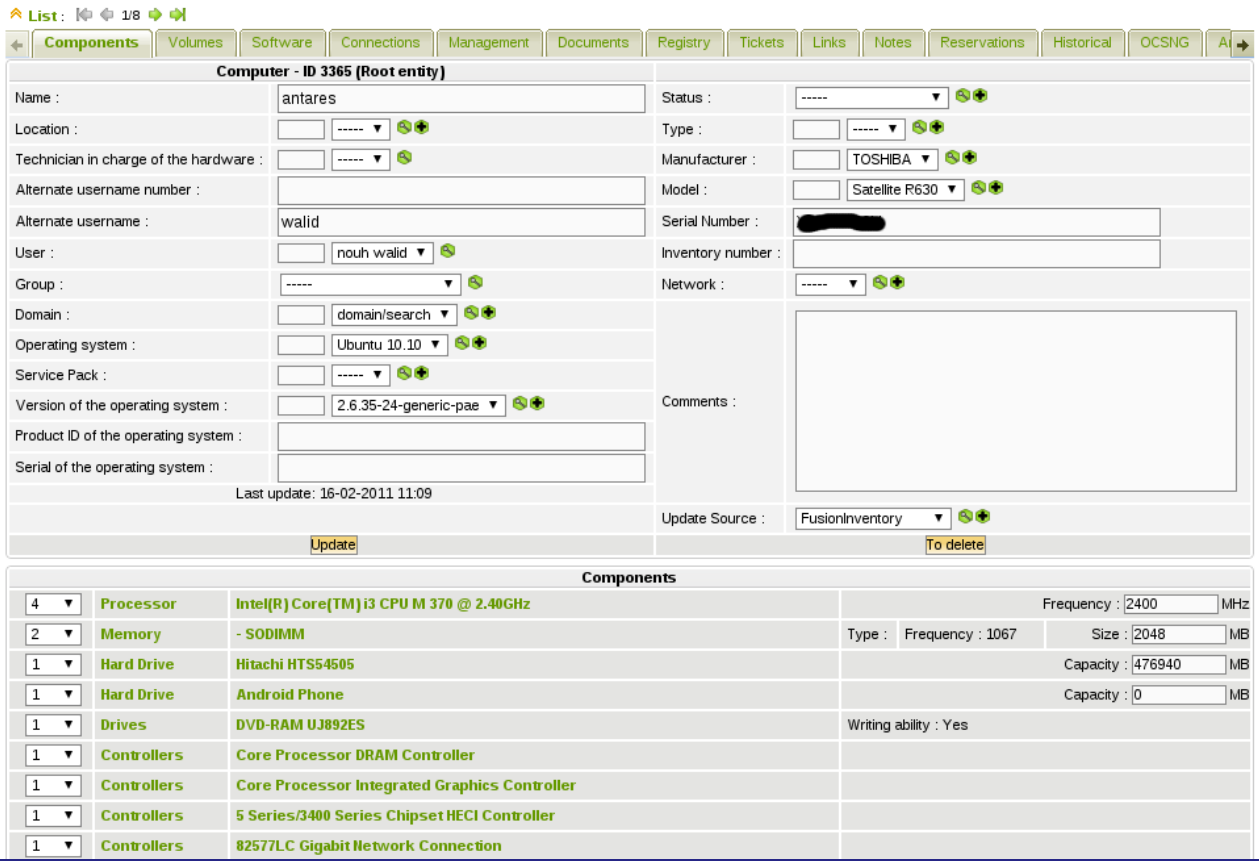
- UML models
  - For identifying dependencies
- Manual discovery
  - Topology analysis
  - Functional analysis
  - Library
- Workflows
- Reusable scripts (from workflows)
  - Placeholders
    - User creation
    - New website

Tools: Firewall Builder



Tools: FusionInventory

- Software database (nice for Discovery)



Tools

- Puppet/Chef
  - Software configuration
- Fog Project
  - Desktop computer cloning

How Fog Works

Policies

- Microsoft ActiveDirectory
  - Policies
  - Objects
    - Users
    - Devices
    - Groups
  - Enforces policies on objects
    - Which software must be installed
    - Which desktop background to use
    - Password changing rules

Software/firmware versions

- Software is creative but the typical is:
- MAJOR.MINOR[.MOREMINOR[.EVENMINOR]]

  MAJOR changes in functionality and interfaces

  MINOR patches to known problems, minor improvements to functionality
- Expect more problems with major updates

When to Update?

- By default, Never
  - It is working! Why mess with it?
- Unless there are good reasons

Steps toward an update (1/3)

1. Patch discovery
   - Package managers
   - Software alerts
   - Foruns

Steps toward an update (2/3)

1. Evaluation
   1. Security vulnerabilities
   2. Compatibility
      - Critical functions?
      - Improves performance?
      - Dependencies?
   3. Relevance
   4. Operational impact of the patch update
      - Cost of the system being down
   5. Cost
      - Work hours
      - Hardware upgrade
      - Human resources

Steps toward an update (2/3)

3. Test
   - Possibly on backup hardware
4. Install
   - Minimize downtime
     - If replicated
   - At non-working hours
     - Be prepared for problems at the early working hours after

Updates

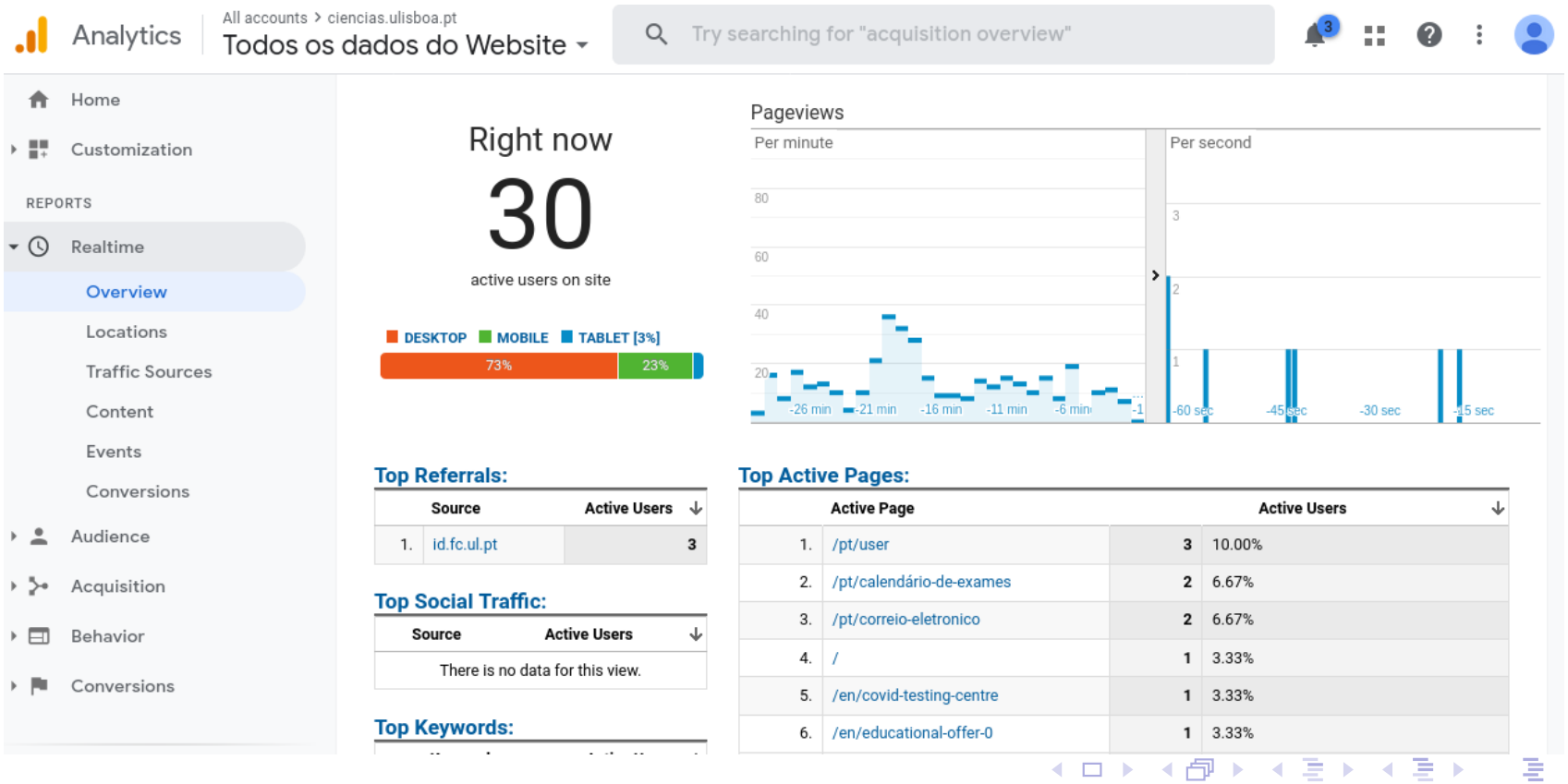
- Plan, plan, plan
- Make contingency/reversion plans
- Accumulate several updates
  - Beware of dependencies
- Policy may be required
  - E.g. multisite web hosting frameworks

Why Accounting?

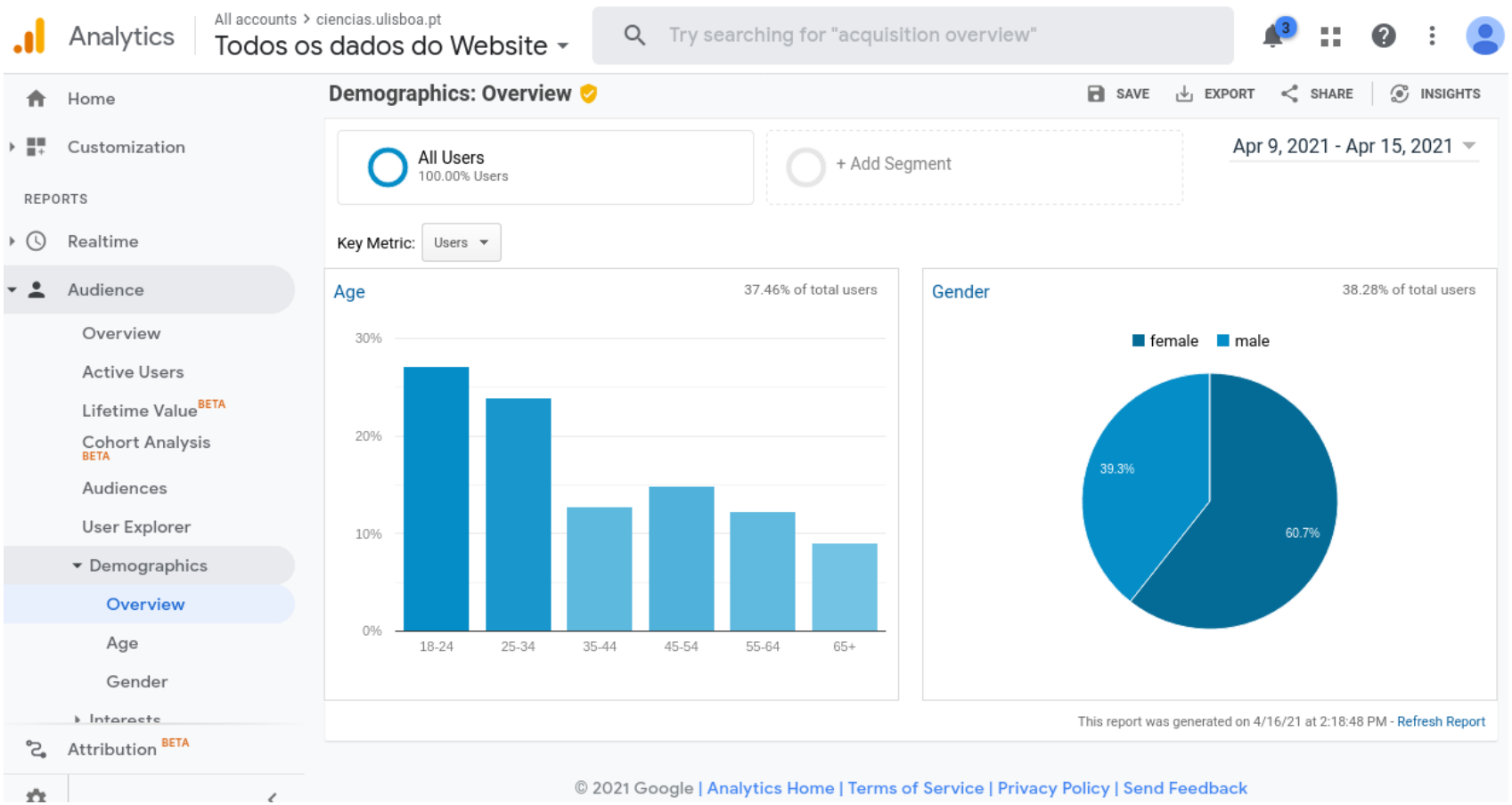
- To bill your clients
  - ISP
  - Number of printed pages
  - Satisfaction of SLA
- To show how well the team is performing
- To support strategic planning

To report on the success of a web site

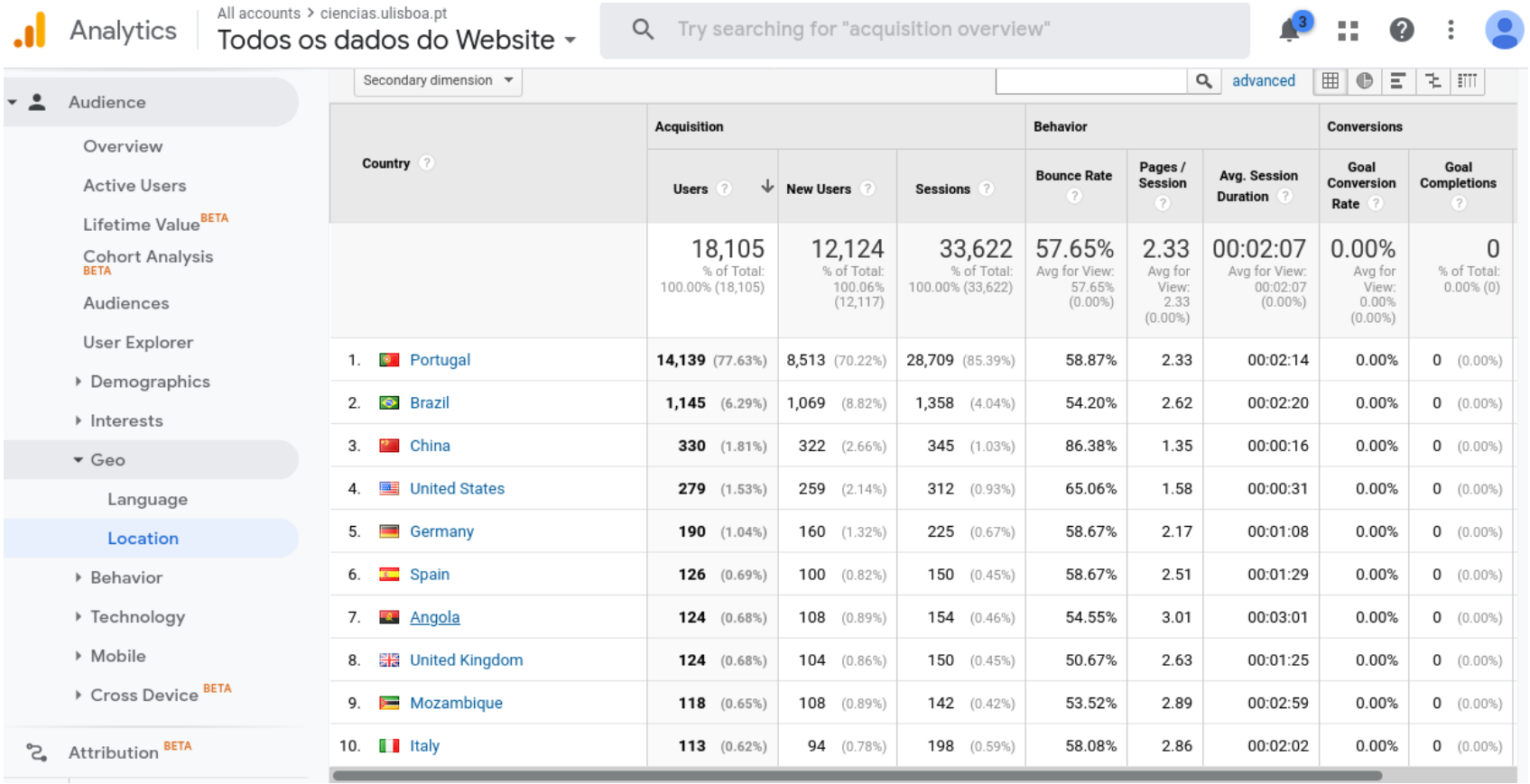
E.g. Google Analytics



To know who your clients are

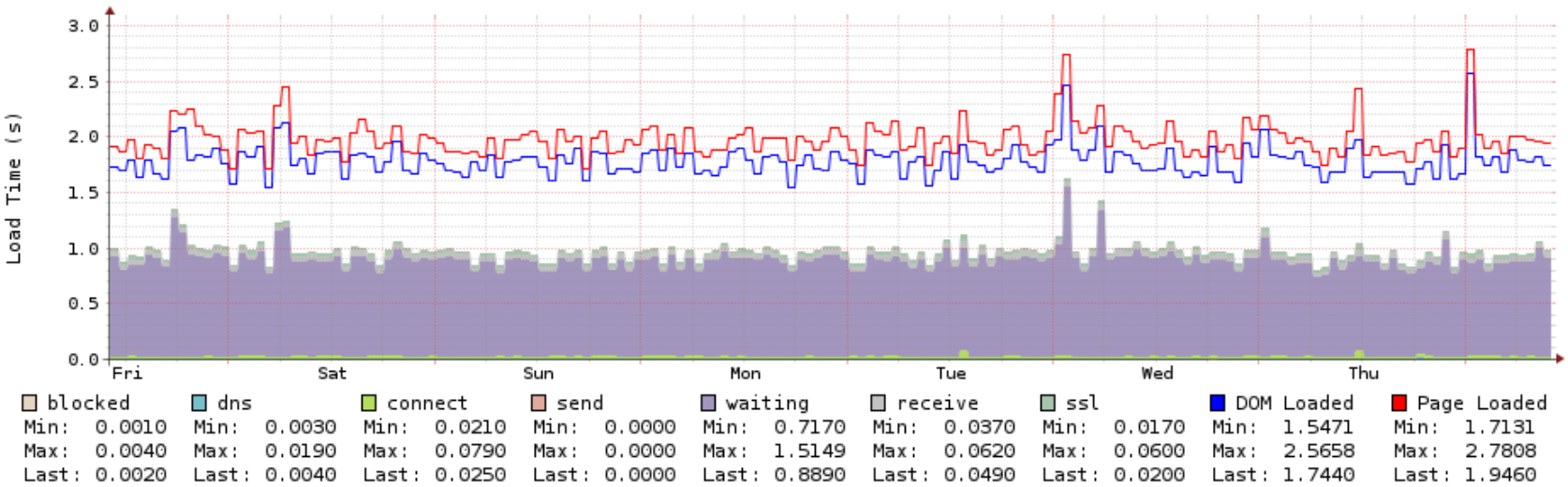


Or where are they from

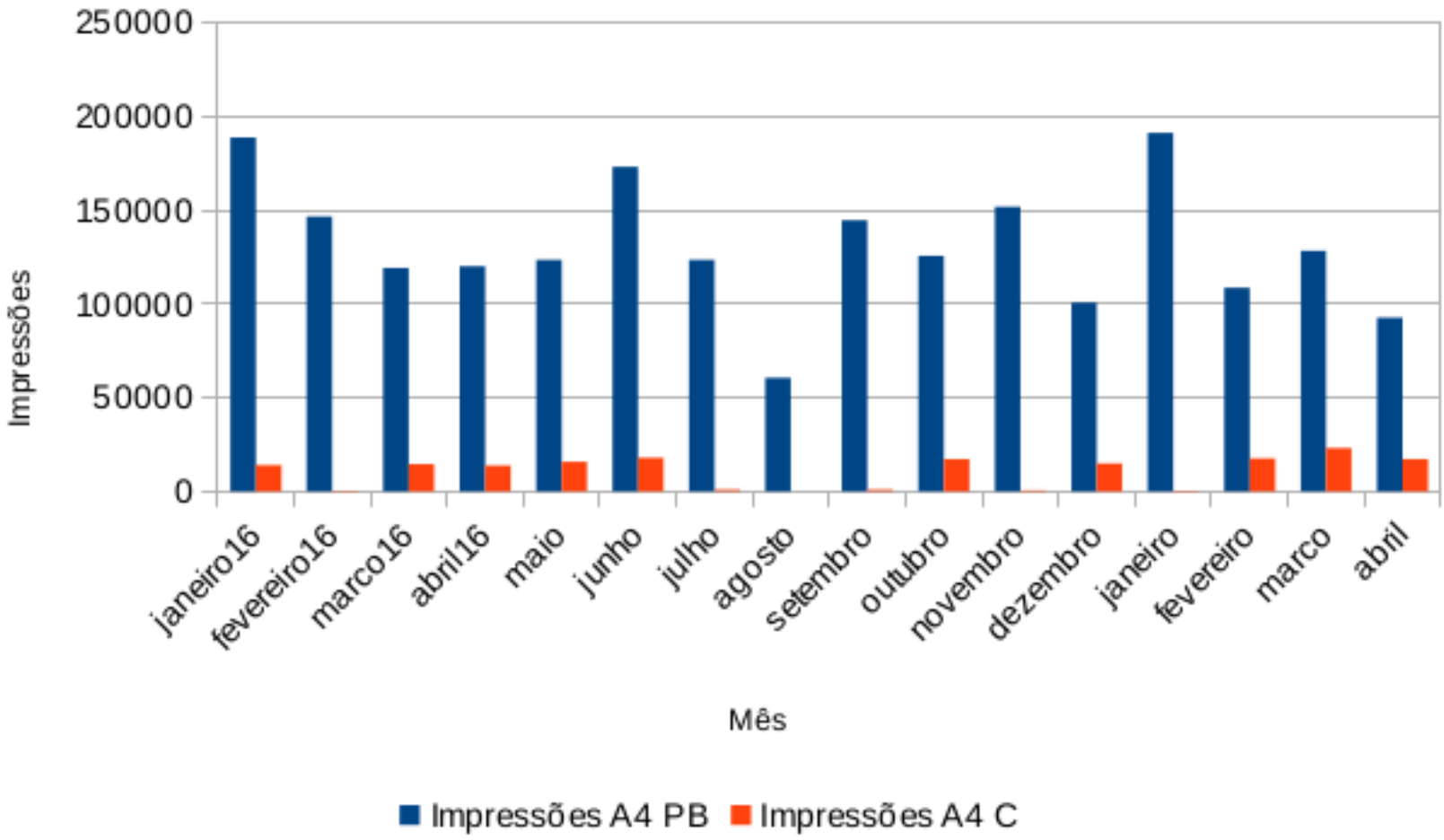


Country	Acquisition			Behavior			Conversions	
	Users	New Users	Sessions	Bounce Rate	Pages / Session	Avg. Session Duration	Goal Conversion Rate	Goal Completions
	18,105 % of Total: 100.00% (18,105)	12,124 % of Total: 100.06% (12,117)	33,622 % of Total: 100.00% (33,622)	57.65% Avg for View: 57.65% (0.00%)	2.33 Avg for View: 2.33 (0.00%)	00:02:07 Avg for View: 00:02:07 (0.00%)	0.00% Avg for View: 0.00% (0.00%)	0 % of Total: 0.00% (0)
1. Portugal	14,139 (77.63%)	8,513 (70.22%)	28,709 (85.39%)	58.87%	2.33	00:02:14	0.00%	0 (0.00%)
2. Brazil	1,145 (6.29%)	1,069 (8.82%)	1,358 (4.04%)	54.20%	2.62	00:02:20	0.00%	0 (0.00%)
3. China	330 (1.81%)	322 (2.66%)	345 (1.03%)	86.38%	1.35	00:00:16	0.00%	0 (0.00%)
4. United States	279 (1.53%)	259 (2.14%)	312 (0.93%)	65.06%	1.58	00:00:31	0.00%	0 (0.00%)
5. Germany	190 (1.04%)	160 (1.32%)	225 (0.67%)	58.67%	2.17	00:01:08	0.00%	0 (0.00%)
6. Spain	126 (0.69%)	100 (0.82%)	150 (0.45%)	58.67%	2.51	00:01:29	0.00%	0 (0.00%)
7. Angola	124 (0.68%)	108 (0.89%)	154 (0.46%)	54.55%	3.01	00:03:01	0.00%	0 (0.00%)
8. United Kingdom	124 (0.68%)	104 (0.86%)	150 (0.45%)	50.67%	2.63	00:01:25	0.00%	0 (0.00%)
9. Mozambique	118 (0.65%)	108 (0.89%)	142 (0.42%)	53.52%	2.89	00:02:59	0.00%	0 (0.00%)
10. Italy	113 (0.62%)	94 (0.78%)	198 (0.59%)	58.08%	2.86	00:02:02	0.00%	0 (0.00%)

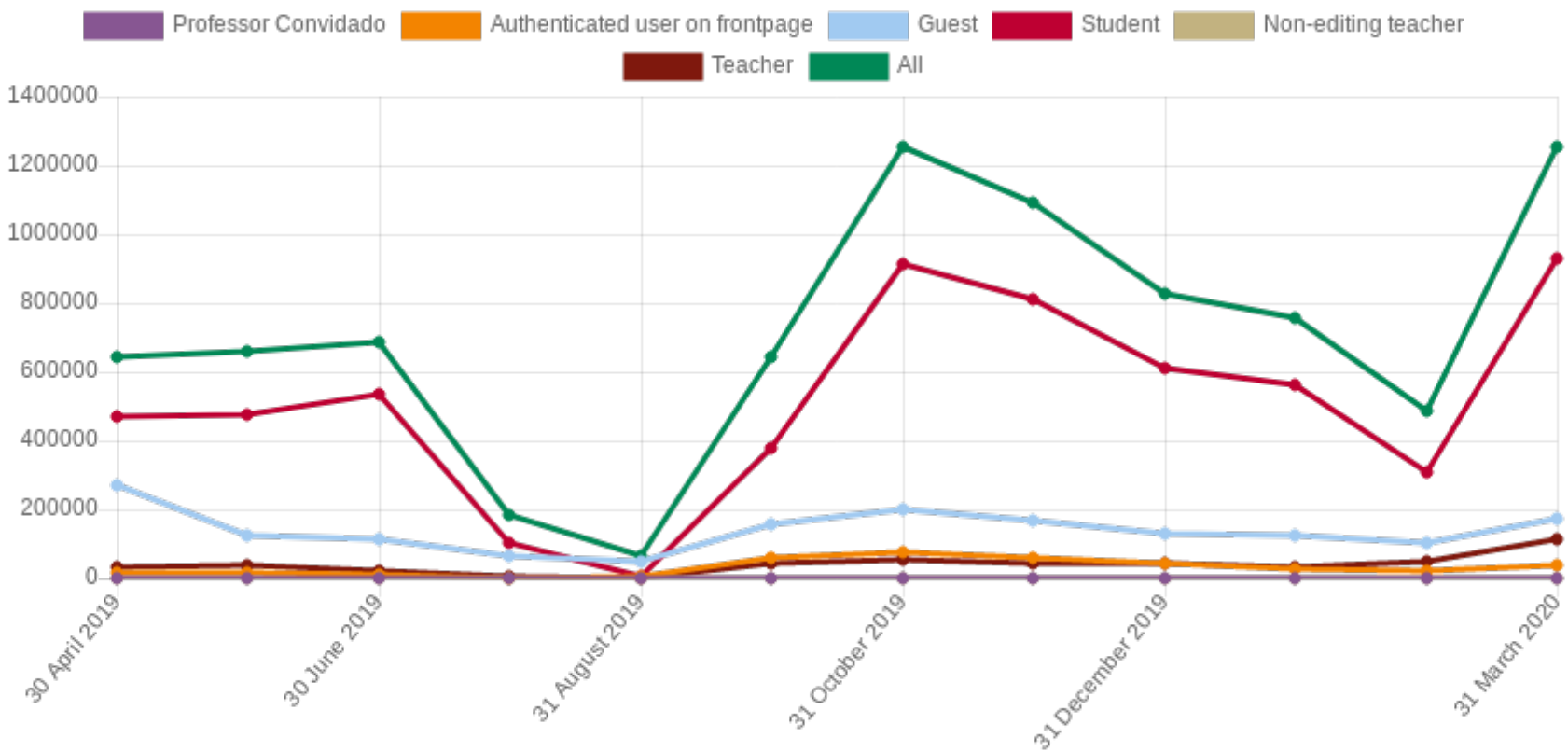
Or see how much time it takes to load a web page



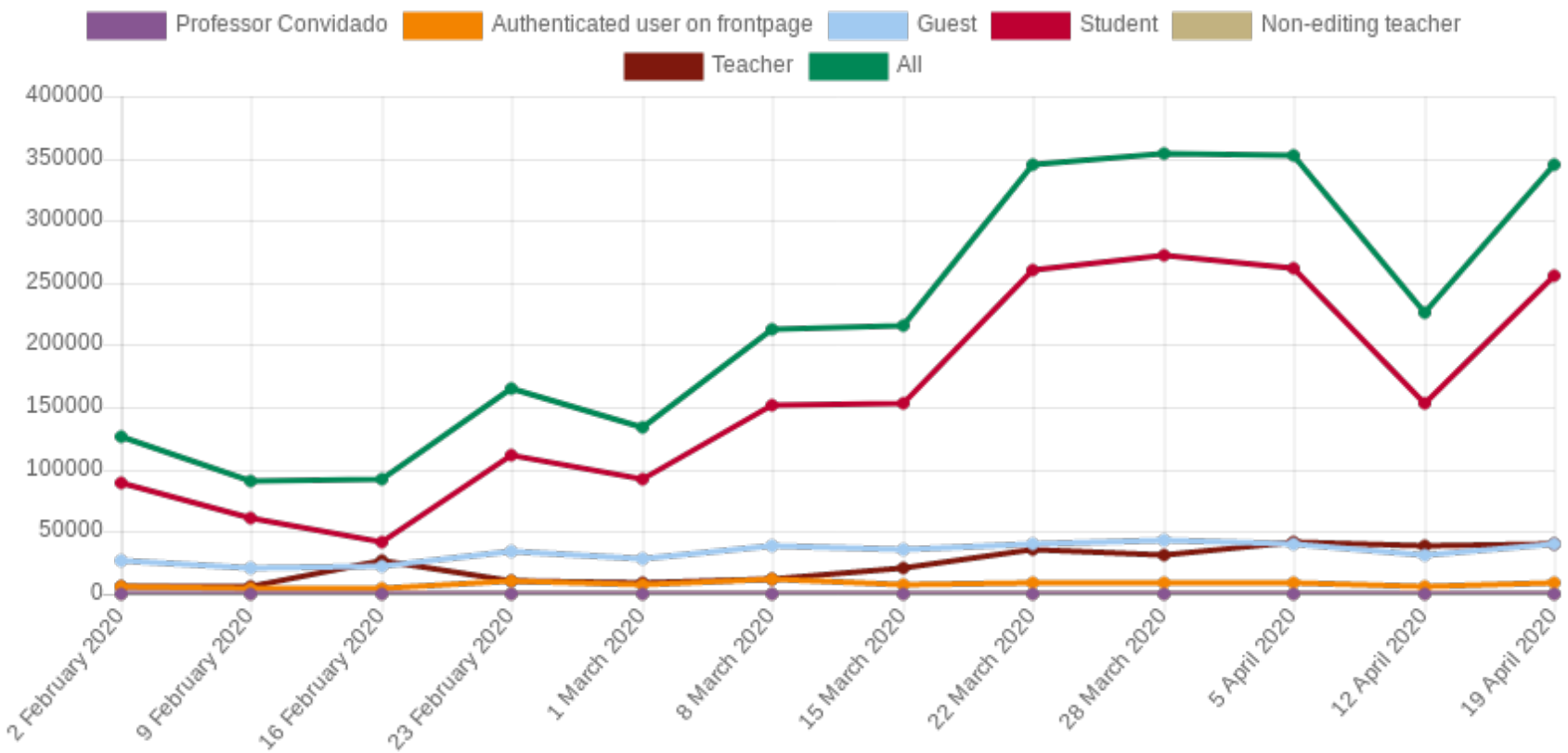
Understand how the printing system should grow



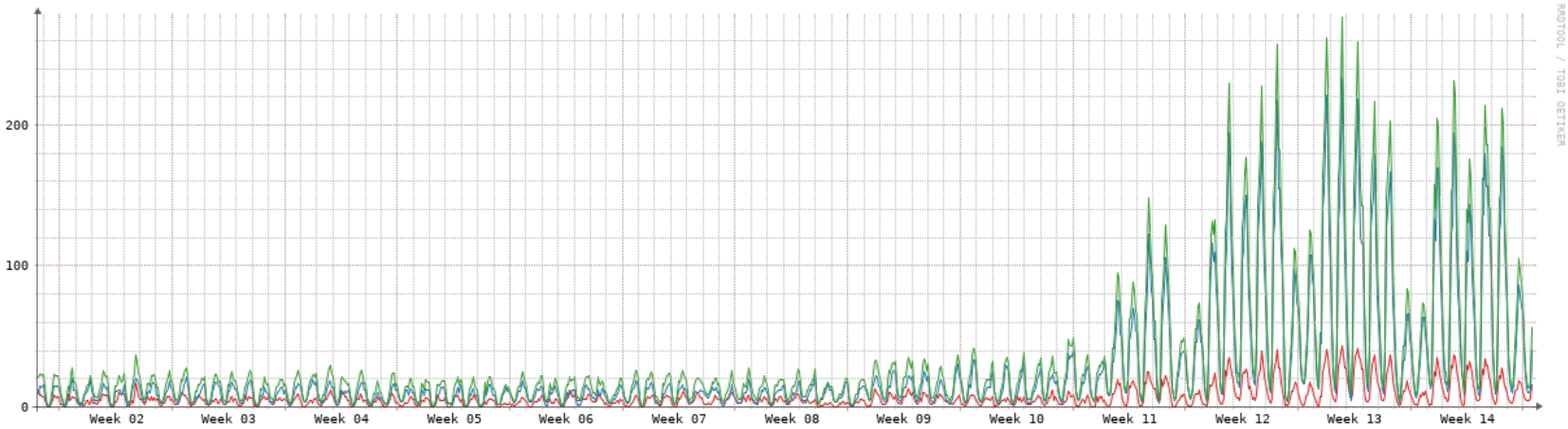
Moodle 11 months



Moodle 3 months



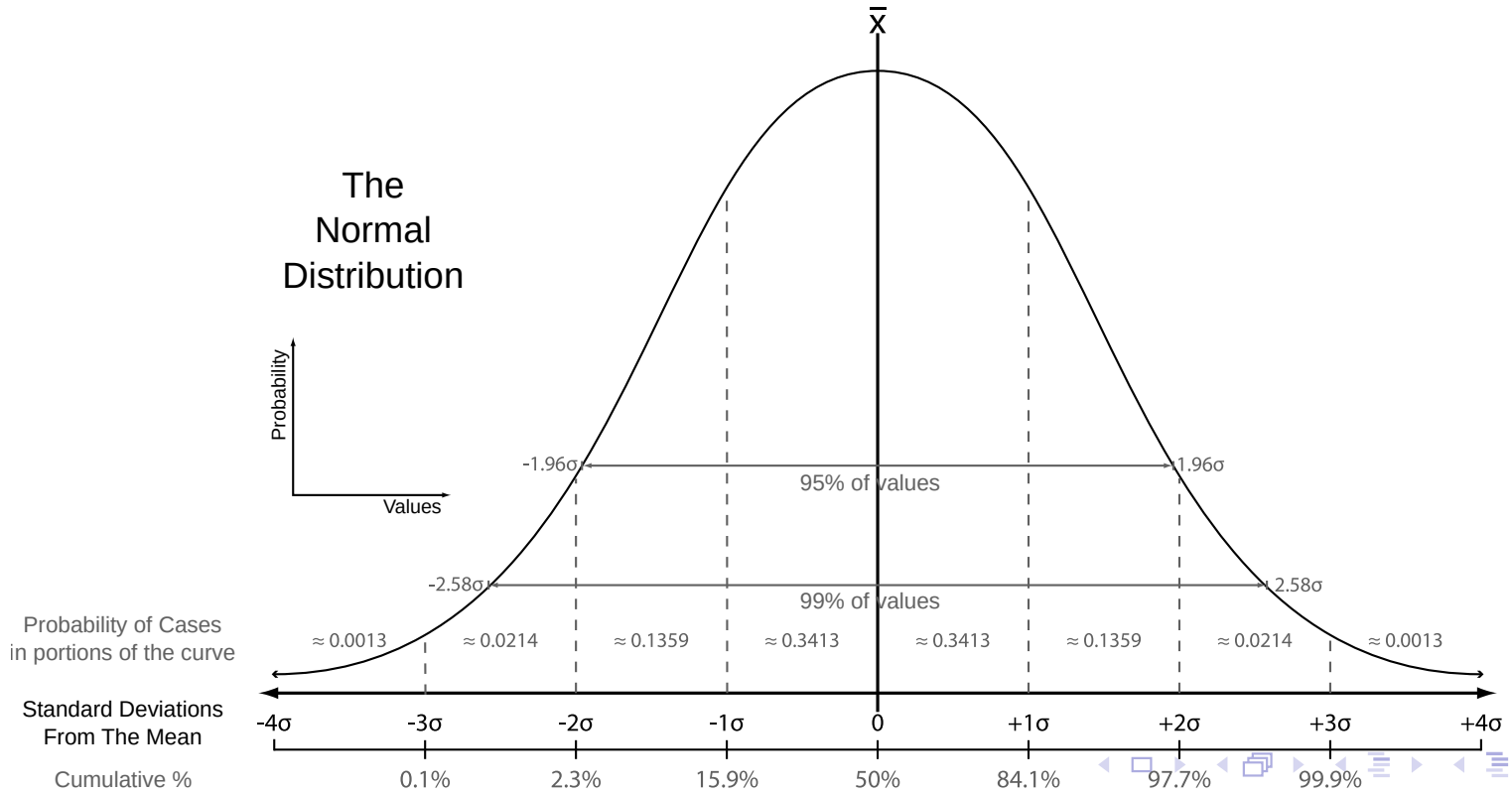
VPN utilization



Performance Problems

- Not boolean values
  - Things can be working but not as expected
- Learn that something is wrong
  - Users complaints
  - Abnormal behavior
    - Expected results from time series
    - the 3σ rule

The 3σ rule



Example 1: Configuration Problem

Example 2: Slashdot Effect

Performance Data

- Needs to be compressed
  - As discussed in monitoring
  - Not just average
    - Max, min, stdev, ...

Common Performance Metrics

(To be discussed in planning class)

- Workload packets/s
- Utilization 35%
- Throughput packets/s
- Response time 25ms
- Loss rate 2%

Performance Common Root Causes

- Configuration errors
  - Incorrect routing of requests
  - Concurrency problems
- Not enough resources
- Updates
- Utilization spikes

Estimation

- Trend lines
  - Over time series
- ARIMA (AutoRegressive Integrated Moving Average)
  - See `https://machinelearningmastery.com/arima-for-time-series-forecasting-with-python/`
- Fourier Transforms

Wrap Up

- Configuration is divided in:
  - Configuration values management
    - Challenge is to keep them consistent to keep the system working
  - Patch Management
    - When and why to update software and hardware
- Accounting
  - Keep track of a number of indicators
    - More than performance
- Performance
  - Like with faults, requires identification and diagnostic
  - Challenge is on identification