Foreman e Ansible

one-click deploy totalmente open-source e escalável

Gabriel **Diab**

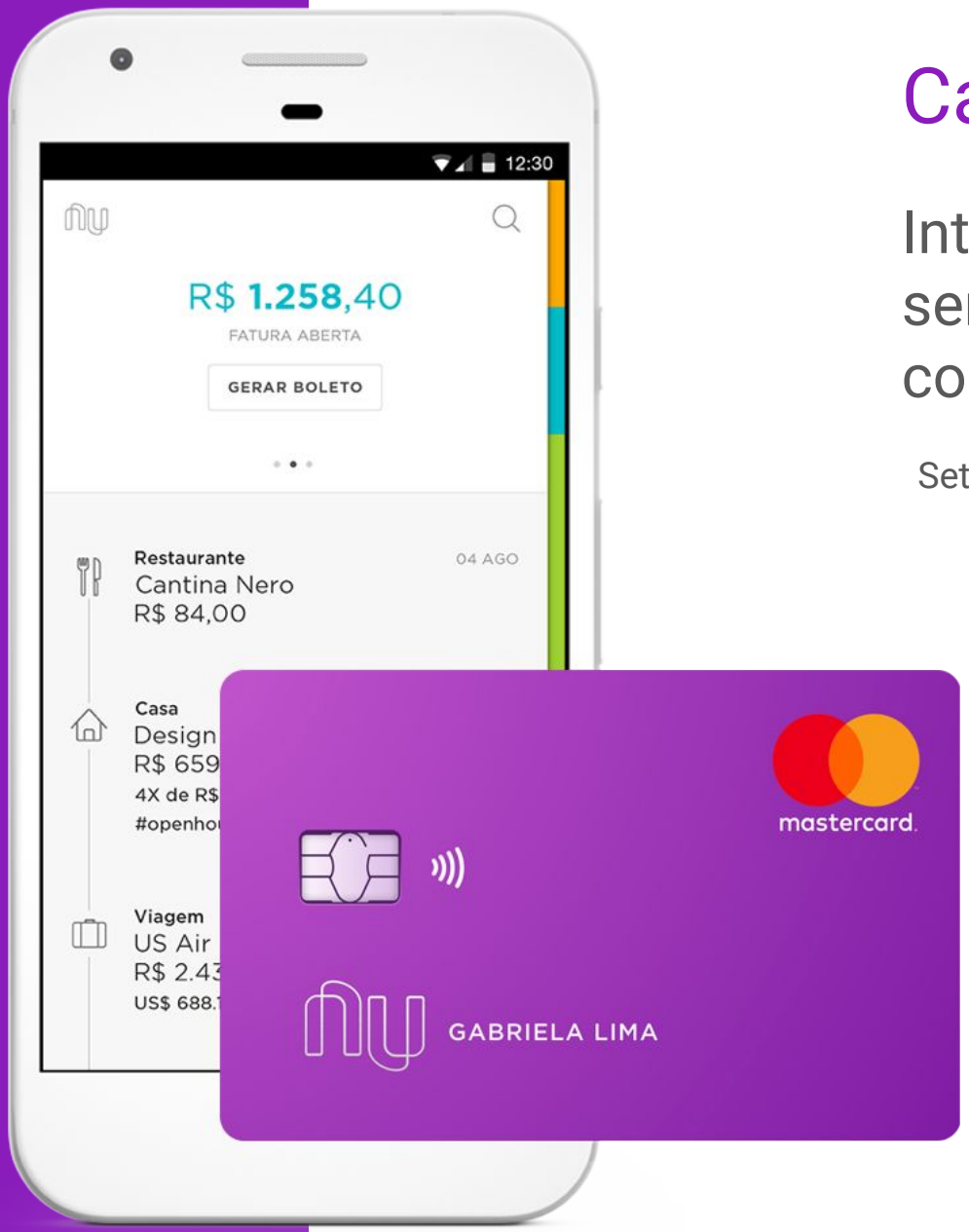
Security Software Engineer

Nubank

Foreman

Ansible

Como usamos



Cartão de Crédito

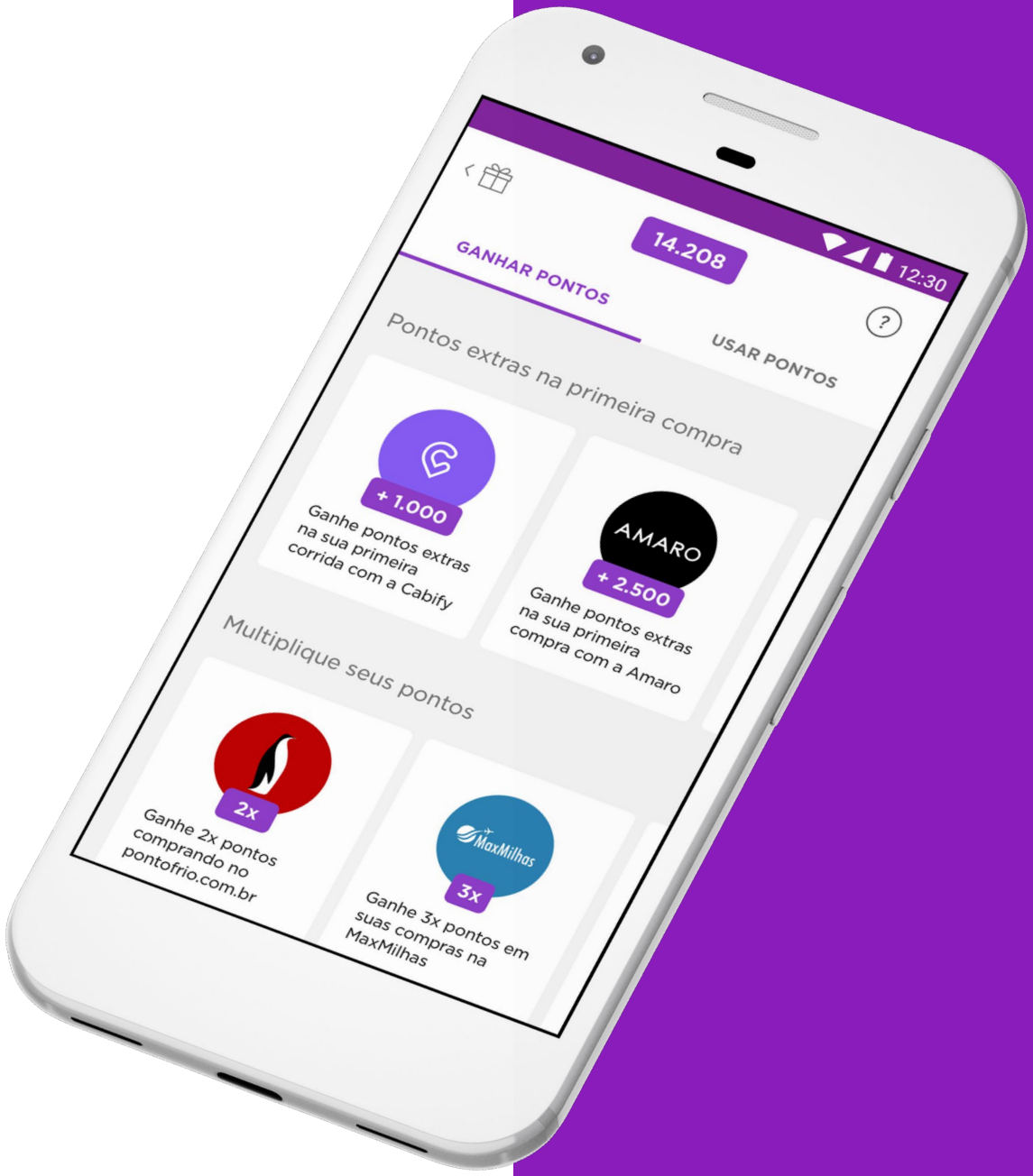
Internacional,
sem taxas e
controle total pelo app.

Setembro 2014

Rewards

um programa de pontos totalmente diferente de outras experiências no mercado brasileiro.

Agosto 2017



Nuconta

nossa visão de uma conta de banco simples e inteligente.

Outubro 2017

Nubank

Maior fintech fora da Asia

1847

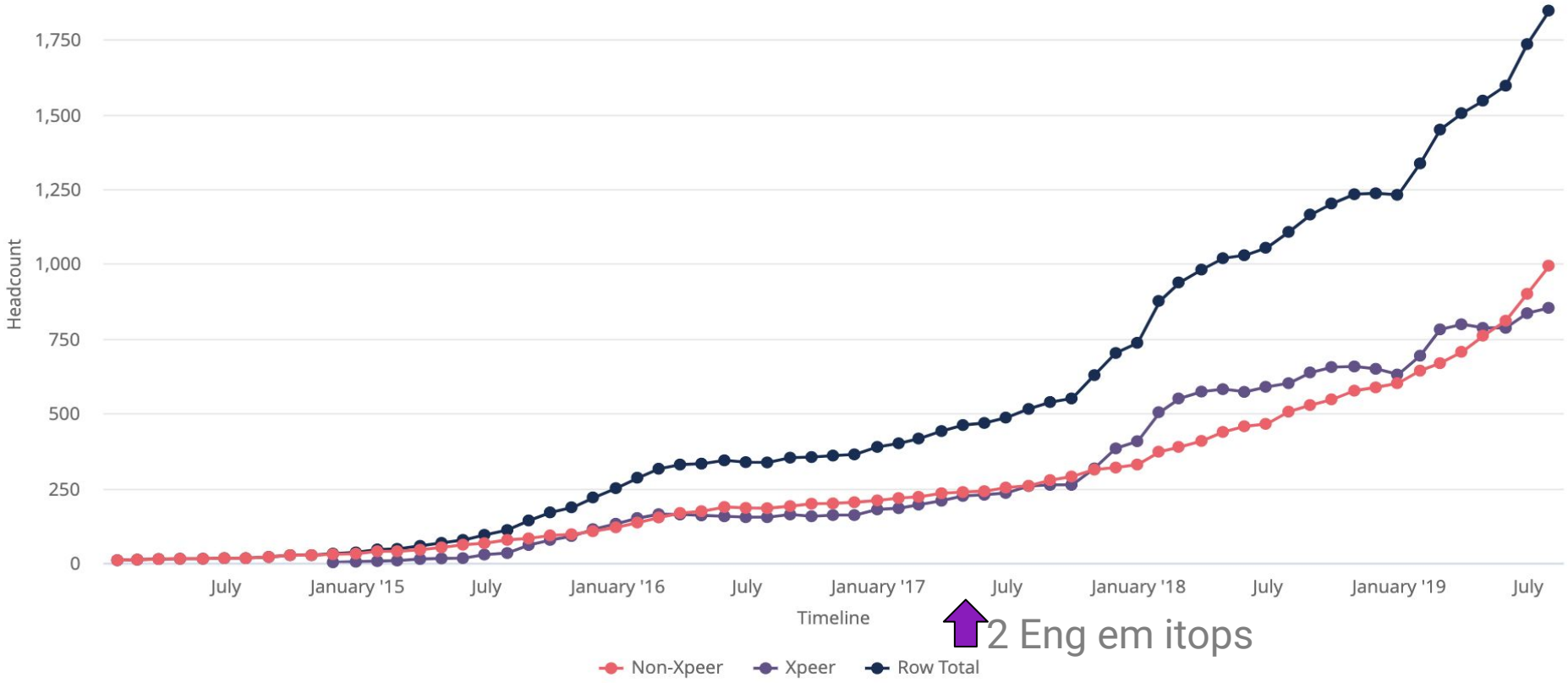
Nubankers

16/70

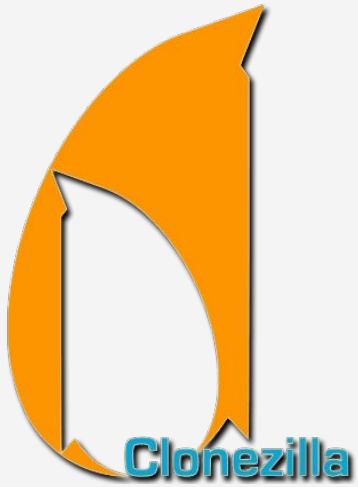
Tribes/Squads

10M+

Clientes



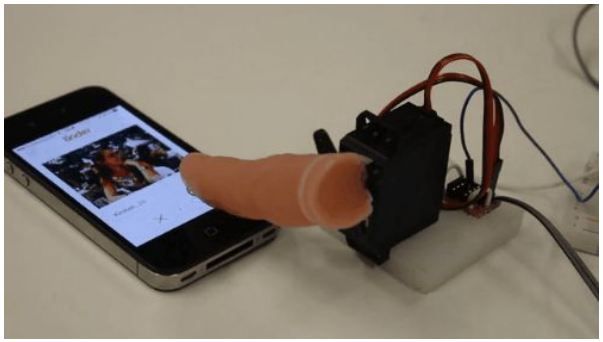

```
        }).done(function(response) {
            for (var i = 0; i < response.length; i++) {
                var layer = L.marker(
                    [response[i].latitude, response[i].longitude]
                    // ,{icon: myIcon}
                );
                layer.addTo(group);

                layer.bindPopup(
                    "<p>" + "Species: " + response[i].species + "
                    "<p>" + "Description: " + response[i].descript
                    "<p>" + "Seen at: " + response[i].latitude + "
                    "<p>" + "On: " + response[i].sighted_at + "</
            }

            $('select').change(function() {
                species = this.value;
            });
        });
    }
$.ajax({
        url: queryURL,
        method: "GET"
        }).done(function(response) {
            for (var i = 0; i < response.length; i++) {
                var layer = L.marker(
                    [response[i].latitude, response[i].longitude]
                    // ,{icon: myIcon}
                );
                layer.addTo(group);
```



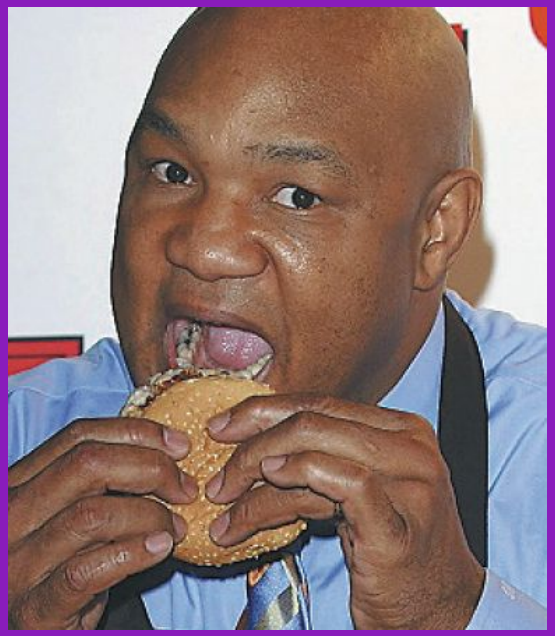
Itops

Mindset de automatizar tudo
Um parque que vem crescendo em média de
~50 maquinas por mes

joined #general along with 51 others.



Foreman



Foreman

Foreman Grill

Foreman

"O Foreman é uma ferramenta completa de gerenciamento de ciclo de vida para servidores físicos e virtuais. Que dá aos administradores de sistema o poder de automatizar facilmente tarefas repetitivas, implantar rapidamente aplicativos e gerenciar proativamente servidores, no local ou na nuvem."

https://theforeman.org

Foreman

FOREMAN

Host Groups

O dimensionamento horizontal é uma arquitetura onipresente em TI. Agrupe seus hosts e modifique sua configuração como se fossem apenas um com o Foreman.

API

API RESTful para fornecer a você o poder de automatizar a maioria das tarefas, como registrar hosts, atribuir funções a usuários e muito mais.

CLI

UIs te atrapalhar? O Hammer CLI oferece acesso fácil a todas as chamadas de API que você precisa para ficar no topo do seu data center.

Audit

Não é mais necessário saber por que seu balanceador de carga de repente se tornou um banco de dados. Veja como, quem e quando no nosso sistema de auditorias.

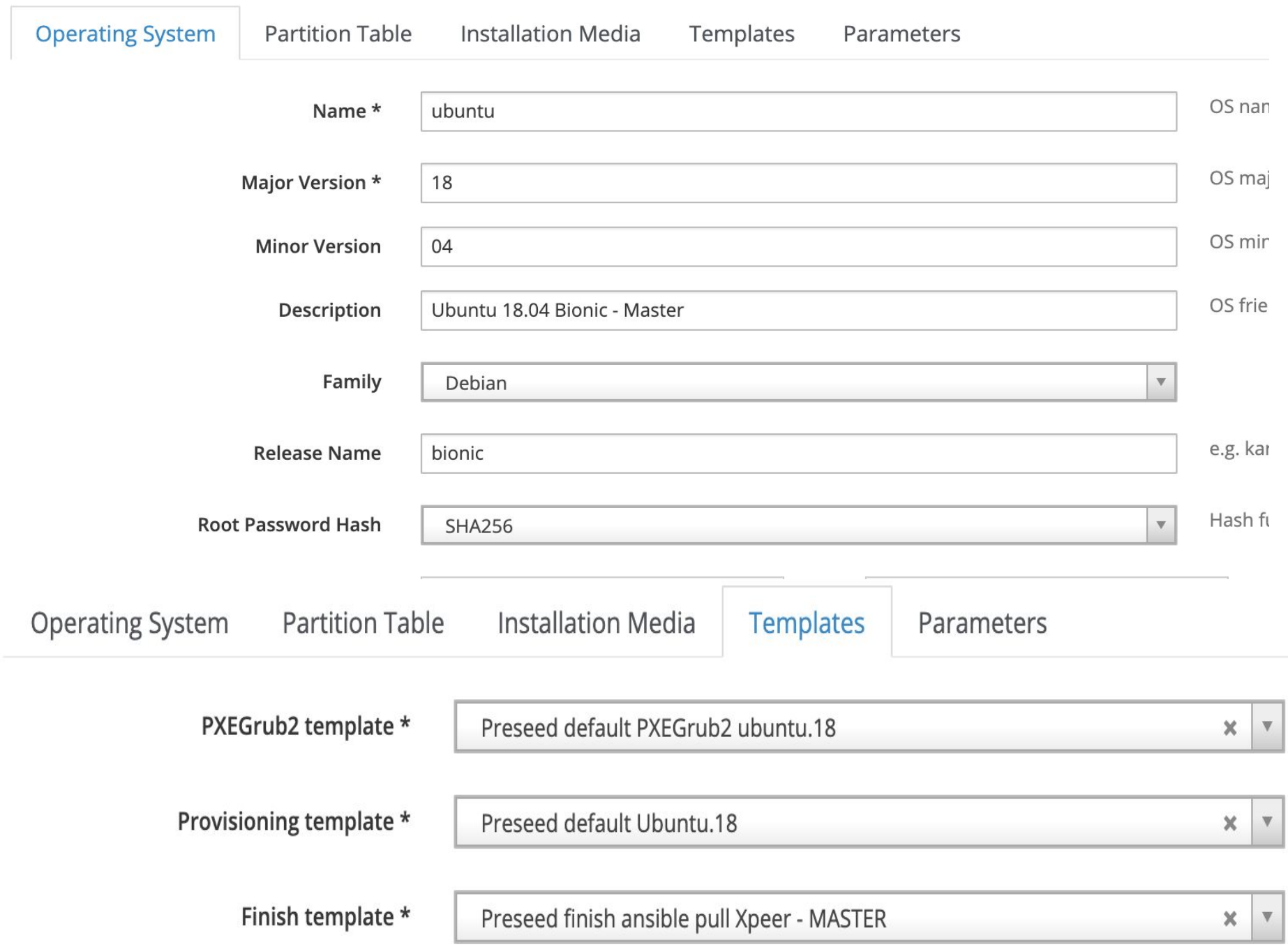
Plugins

Uma arquitetura conectável permite estender o Foreman em praticamente qualquer direção. Visite nossa lista de plugins para um vislumbre.

RBAC and LDAP integration

Um sistema de autorização completo com base no controle de acesso baseado em função (RBAC) permite políticas rígidas para os usuários do Foreman. Se você usar o LDAP ou o FreeIPA, poderá continuar usando-os para autenticação e autorização.

https://theforeman.org


Operating System
Partition Table
Installation Media
Templates
Parameters
Name *
ubuntu
OS nan
Major Version *
18
OS maj
Minor Version
04
OS mir
Description
Ubuntu 18.04 Bionic - Master
OS frie
Family
Debian
Release Name
bionic
e.g. kar
Root Password Hash
SHA256
Hash fu
Operating System
Partition Table
Installation Media
Templates
Parameters
PXEGrub2 template *
Preseed default PXEGrub2 ubuntu.18
Provisioning template *
Preseed default Ubuntu.18
Finish template *
Preseed finish ansible pull Xpeer - MASTER

Hosts » 6672.nubank.com.br ⇄

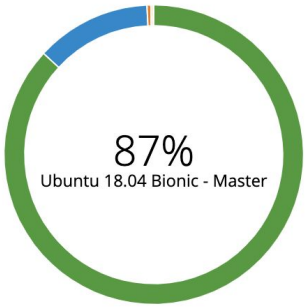
Details

Audits | YAML

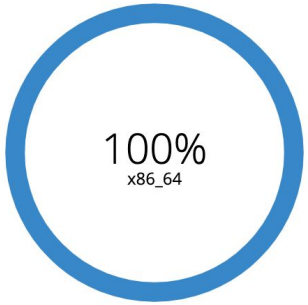
Properties | Metrics | Templates | NICs

Properties	
Status	OK
Build	Installed
Build duration	31 minutes
Token	N/A
Domain	nubank.com.br
MAC Address	4c:d9:8f:fc:a2:bc
Puppet Environment	production
Architecture	x86_64
Operating System	Ubuntu 18.04 Bionic - Master
PXE Loader	Grub2 UEFI SecureBoot
Host group	foreman.nubank.com.br
Owner	evandro ananias

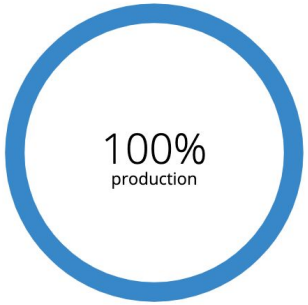
OS Distribution



Architecture Distribution



Environment Distribution

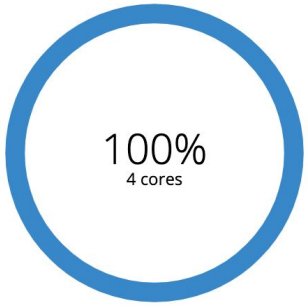


Host Group Distribution

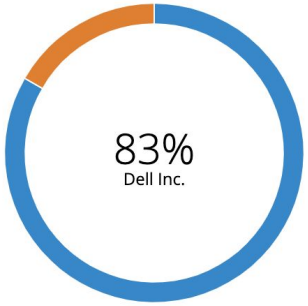
Compute Resource Distribution

No Data Available

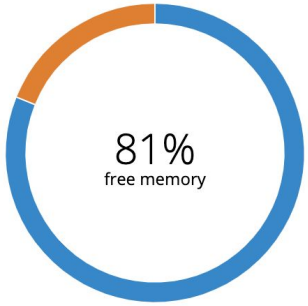
Number of CPUs



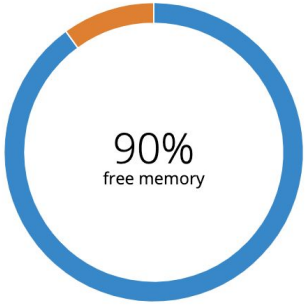
Hardware



Average Memory Usage



Average Swap Usage



Class Distribution

No Data Available

Template | Type | Association | History | Help

Name * Preseed finish ansible pull Xpeer - MASTER

Template *

Input | Diff | Preview | Import | Fullscreen

ruby | Default

```
apt-get install software-properties-common
apt-add-repository ppa:ansible/ansible -y
apt-get update
apt-get install ansible -y
ansible-pull --accept-host-key --private-key=/home/root/.ssh/id_rsa --url=ssh://git@github.com/nubank/ansible-pull.git -i 'localhost,'

cat > /etc/cron.d/ansible-pull <<EOF
*/10 * * * * root ansible-pull --accept-host-key --private-key=/home/root/.ssh/id_rsa --url=ssh://git@github.com/nubank/ansible-pull.git -i 'localhost,'
EOF

#Unity desktop manager on ubuntu 18
apt remove gdm3 --purge -y
apt remove gnome-shell ubuntu-gnome-desktop --purge -y
apt install lightdm -y
apt install ubuntu-unity-desktop -y
apt remove gnome-initial-setup -y
cat > /home/nubank/.bashrc <<EOF
alias ansi="sudo ansible-pull --accept-host-key --private-key=/home/root/.ssh/id_rsa --url=ssh://git@github.com/nubank/ansible-pull.git -i localhost,"
EOF

#Touchpad manager
```

Audit Comment

The Audit Comment field is saved with the template auditing to document the template changes

Submit | Cancel

Ansible

Ferramenta open source de automação e provisionamento. E de fácil aprendizagem(yaml) e utiliza SSH para se comunicar com os clientes (nodes/máquinas) não precisa de agent local, tendo como única dependência ter o Python e o ansible instalados no client. Uma das vantagens e que atualmente ele é mantido pela comunidade e pela Red Hat

Ansible

Playbook

São a forma pelo qual o Ansible consegue configurar uma política ou passos de um processo de configuração

Handler

São opcionais, sendo estruturas que são ativadas por tasks e são executadas quando são notificadas por uma task.

Task

São onde o trabalho vai ser efetivamente realizado. Elas contém as definições do que será instalado ou qual arquivo será copiado para o servidor que está sendo configurado,

Files

Contém os arquivos que podem ser deployados via role

Module

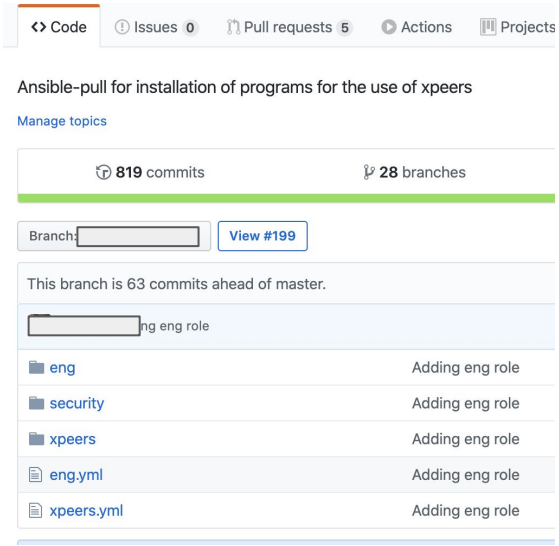
As tasks são o local onde o trabalho ocorrerá, mas quem efetivamente o realiza são os modules.

Templates

São alterados em tempo de execução de acordo com as variáveis pré-definidas

Ansible-pull

Em vez de enviar um playbook para host, o host vai atrás do playbook...

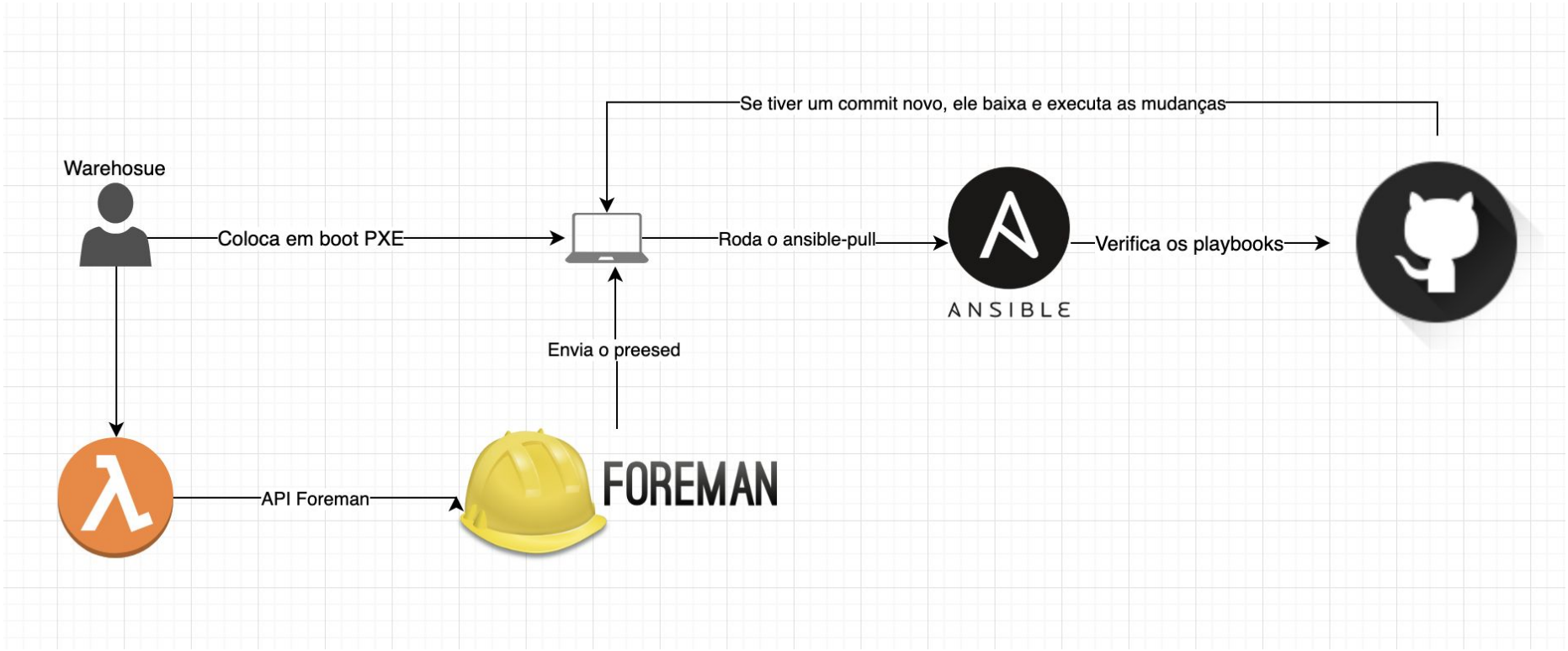


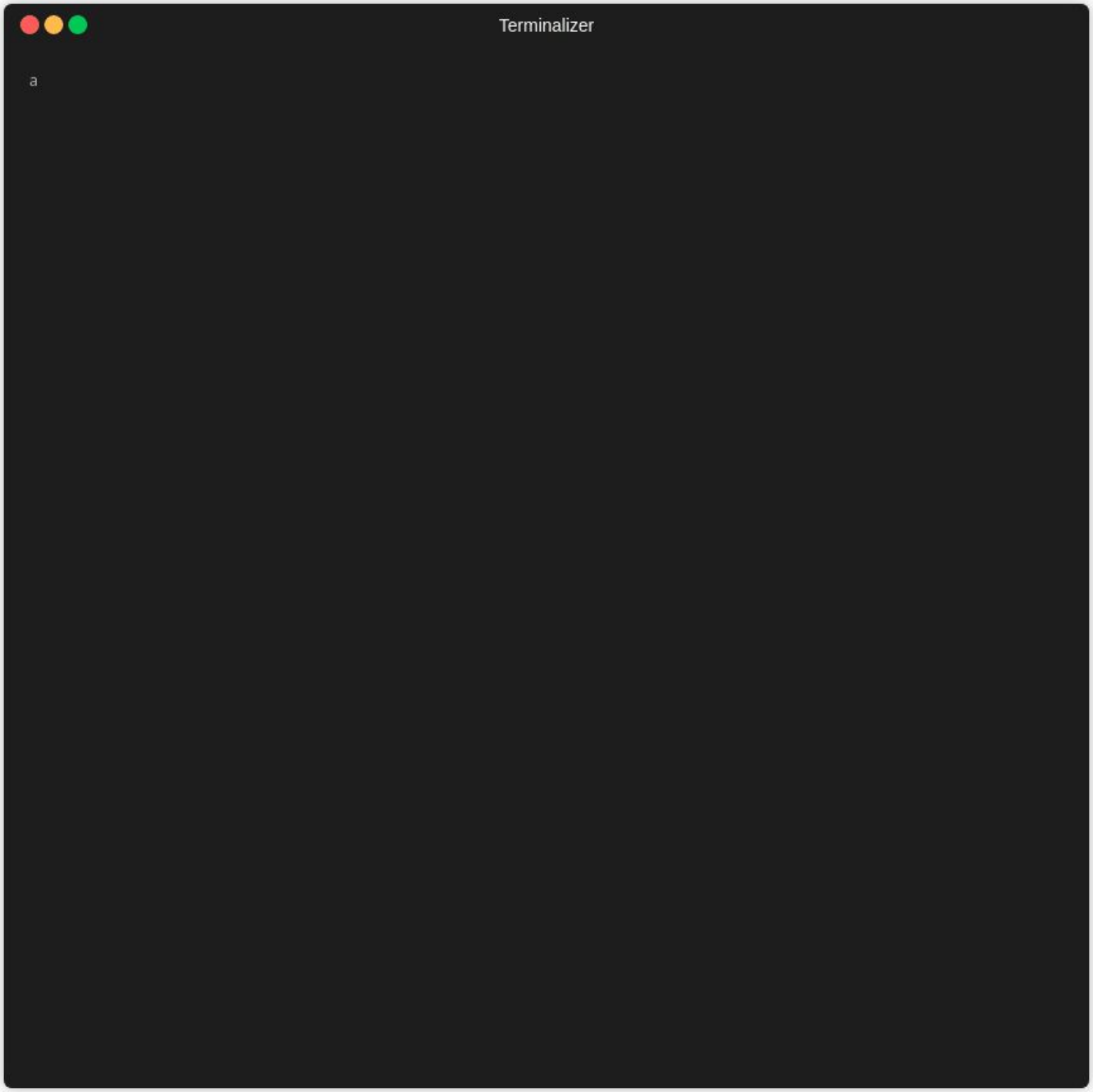

```yaml
- hosts: all      Rodolfo Ponteado, 22 days ago • Changing hosts

  roles:
    - xpeers
    - security
```

```yaml
# tasks file for xpeers role

- include: 01_repos.yml
- include: 02_packages.yml
- include: 03_commands.yml
- include: 04_configuration.yml
- include: 05_personalize.yml
- include: 06_cleanup.yml
```

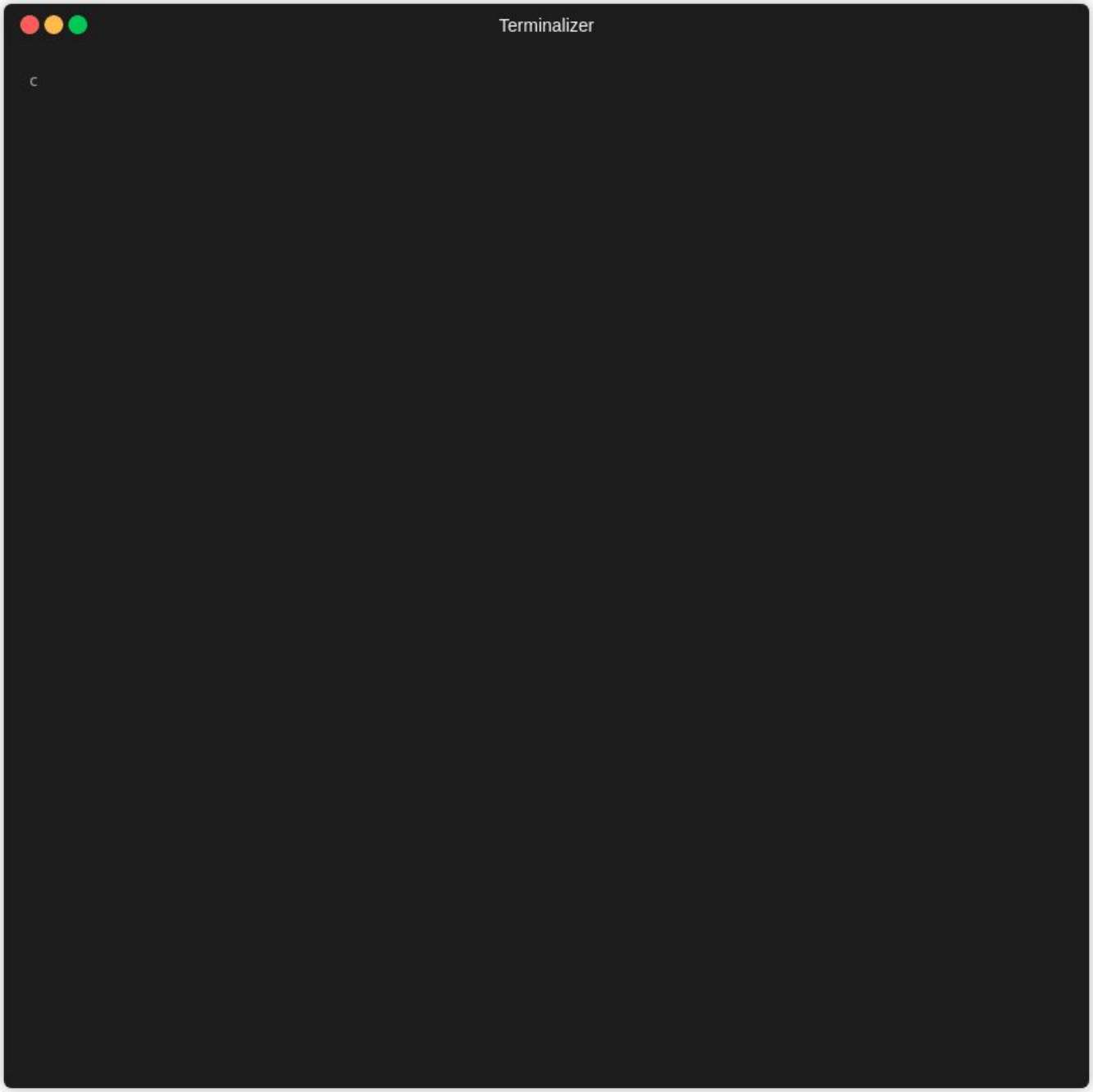
```yaml
- name: Configuring osquery daemon      Rodolfo Ponteado, 23 days ago • Adding handlers and changing
  template:
    src: "{{ item.src }}"
    dest: "{{ item.dest }}"
    mode: 0640
  notify: "restart osquery"
  with_items:
    - {src: 'osqueryd.service.j2',dest: '/usr/lib/systemd/system/osqueryd.service'}
    - {src: 'nubank-pack.conf.j2',dest: '/usr/share/osquery/packs/nubank-pack.conf'}
    - {src: 'audit.rules.j2',dest: '/etc/audit/rules.d/audit.rules'}
  tags:
    - always

- name: Configuring auto updates
  template:
    src: "{{ item.src }}"
    dest: "{{ item.dest }}"
    mode: 0640
  with_items:
    - {src: '20auto-upgrades.j2',dest: '/etc/apt/apt.conf.d/20auto-upgrades'}
    - {src: '50unattended-upgrades.j2',dest: '/etc/apt/apt.conf.d/50unattended-upgrades'}
  tags:
    - always

- name: Configuring fail2ban daemon
  template:
    src: "{{ item.src }}"
    dest: "{{ item.dest }}"
    mode: 0640
  notify: "restart fail2ban"
  with_items:
    - {src: 'sshd_jail.conf.j2',dest: '/etc/fail2ban/jail.d/sshd_jail.conf'}
    - {src: 'defaults-debian.conf.j2',dest: '/etc/fail2ban/jail.d/defaults-debian.conf'}
  tags:
    - always

- name: Configuring cups for xpeers
  template:
    src: "{{ item.src }}"
    dest: "{{ item.dest }}"
    mode: "{{ item.mode }}"
  notify: "restart cups"
  with_items:
    - {src: 'rh.ppd.j2',dest: '/usr/share/cups/model/rh.ppd', mode: '0755'}
    - {src: 'printers.conf.j2',dest: '/etc/cups/printers.conf', mode: '0600'}
  tags:
    - always

- name: Configuring conky for xpeers
  template:
    src: "{{ item.src }}"
    dest: "{{ item.dest }}"
    mode: "{{ item.mode }}"
  notify: "configure conky"
  with_items:
    - {src: 'startup.sh.j2',dest: '/etc/profile.d/startup.sh', mode: '0755'}
    - {src: 'conky-new.j2',dest: '/etc/conky/conky-nubank.conf', mode: '0655'}
  tags:
    - always

- name: Configuring X11 drivers
  template:
    src: "{{ item.src }}"
    dest: "{{ item.dest }}"
    mode: "{{ item.mode }}"
  with_items:
    - {src: '20-intel.conf.j2',dest: '/usr/share/X11/xorg.conf.d/20-intel.conf', mode: '0644'}
  tags:
    - always

- name: Configuring nu-stress for xpeers
  template:
```

Fluxo de vida das maquinas

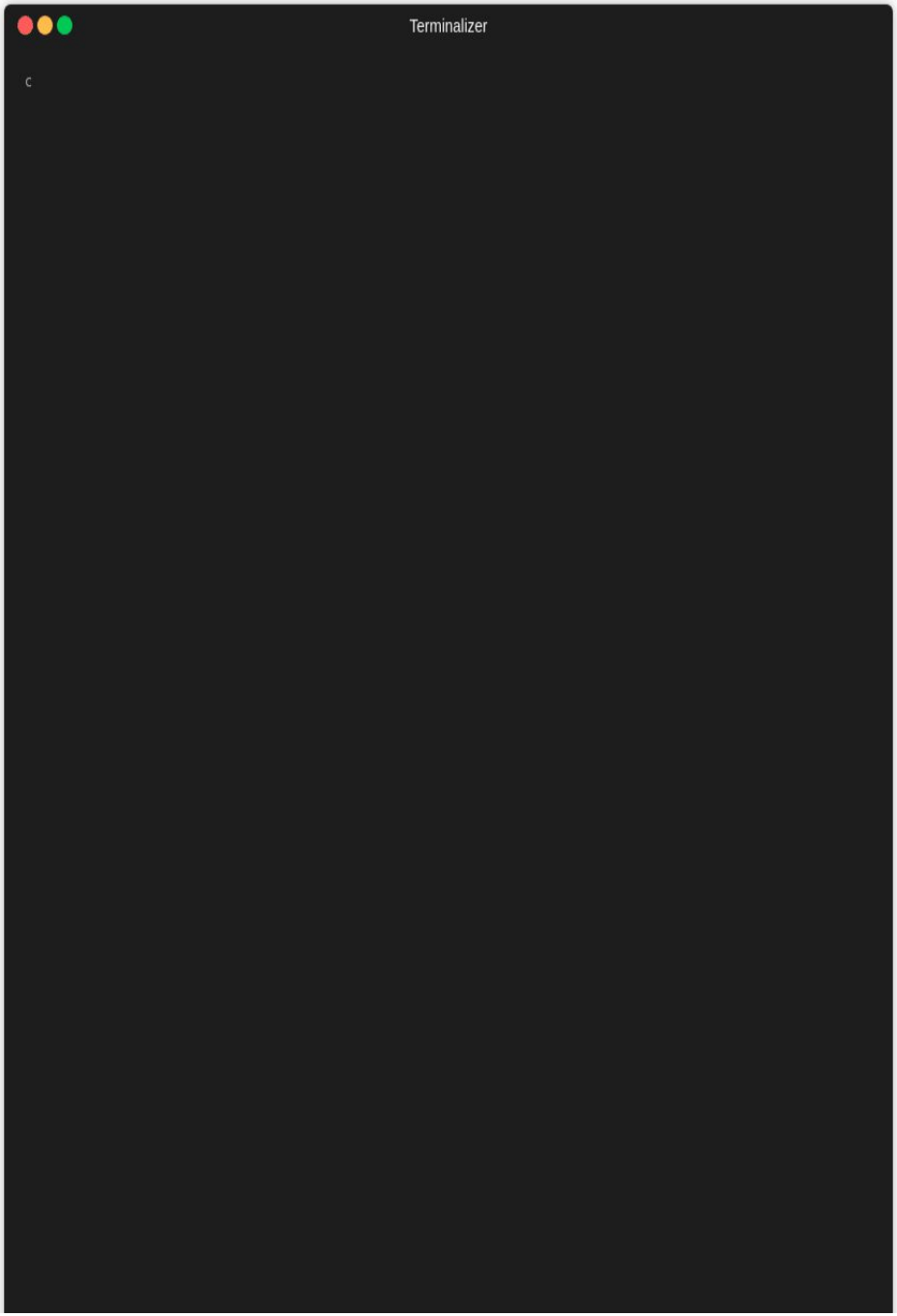




Tags First-time
01_repos.yml
02_packages.yml
03_commands.yml
04_configuration.yml



Tags security - Roda sempre
01_packages.yml
02_configuration.yml

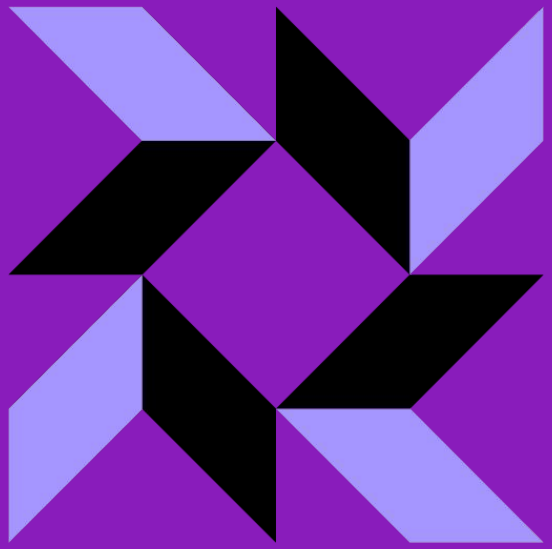


Tags personalize
05_personalize.yml
06_cleanup.yml

Estamos contratando

sou.nu/jobs-at-nubank

Bonus



Osquery

Com o ansible-pull colocamos as maquinas para enviar os logs das queries feitas pelo osquery para o splunk

splunk>

Splunk

18k eventos a cada 15 min

As máquinas fazem um post com o resultado das queries para um serviço que envia os logs para o splunk

Assim temos todo do audit e alertas feito pelo time de SOC usando o splunk


bank