Linux auf Filialgeräten– ein Use Case mit Foreman, Puppet und Gitlab

Timo Goebel | 04.10.19

dm TECH

Who am I

- Timo Goebel
- Foreman Core Committer
- Rubyist
- Sysadmin
- github.com/timogoebel

Timo Goebel
timogoebel

Handyman at dmTECH GmbH
@dm-drogeriemarkt
Karlsruhe, Germany

Organizations

Agenda

- Project Goals
- Tools
- Control repo
- Boot process

Project Goals

Business Goals

- Deploy a Linux operatingsystem on point of sale hardware all over Europe
- Manage the lifecycle of these 15.000 devices
- No budget for software licenses

- Scenario:
  - Cyberdyne Systems has 4.000 stores in Europe
  - Sells robots
  - Every store has
    - 2 to 8 points of sale that should run Linux
    - A broadband connection to the corporate datacenter

Cloud

- We can‘t migrate to the cloud as the hardware has to run locally in the stores

Technical Goals

- Automate everything
- Test everything
- Use open source tools

Challenges

- No management of the DHCP server possible
- Possibly unreliable Network

Tools

Foreman

- Inventory Database
- handles the OS installation via rich templating engine
- Integrates with
  - DNS
  - Puppet
- Reporting

FOREMAN »Any Organization« »Any Location« Admin User

»Monitor«
»Hosts«
»Configure«
»Infrastructure«
»Administer«
»Lab Features«
»Toolbox«

»Hosts«

»Filter ...« »Search«

»Export« »Select Action« »Create Host«

»0 of 103 selected«

	»Power«	»Name«	»Operating system«	»Puppet Environment«	»Model«	»Host group«	»Last report«	»Actions«
		allan-deschner.example.com	RHEL 7.1		ESX-LX-LAN	Test		»Edit«
		alton-buttner.example.com	RHEL 7.1		ESX-LX-LAN			»Edit«
		anna-massella.example.com	RHEL 7.1		ESX-LX-LAN			»Edit«
		blossom.example.com	redhat 7.4					»Edit«
		cara-kotrba.lxsbx.ka.de.dm-drogeriema...	RHEL 7.1			Test		»Edit«
		ejujuuj.example.com	RHEL 7.1			Test		»Edit«
		ffff-ffffff-01.lxsbx.ka.de.dm-drogeriema...	RHEL 7.1	production	ESX-LX-LAN			»Edit«
		flora-klenke.example.com	RHEL 7.1			Test		»Edit«
		floyd-falker						»Edit«
		garry-hodgkiss.example.com	RHEL 7.1			RollingUpdate		»Edit«
		gene-valorie.example.com	CoreOS 1465.7.0		ESX-LX-LAN			»Edit«
		host-sample-01.example.com	RHEL 7.1					»Edit«
		irvin-ertelta.lxsbx.ka.de.dm-drogeriema...	RHEL 7.1			Test		»Edit«
		jake-nippert.example.com	RHEL 7.1			RollingUpdate		»Edit«
		jess-asevedo.example.com	RHEL 7.2		ESX-LX-LAN			»Edit«
		jon-jamieson.example.com	RHEL 7.1			Test		»Edit«

Warning! This template is locked. You may only change the associations. Please clone it to customize.

Name * Kickstart default iPXE

Template *

Input | Diff | Preview | Fullscreen

ruby | Default

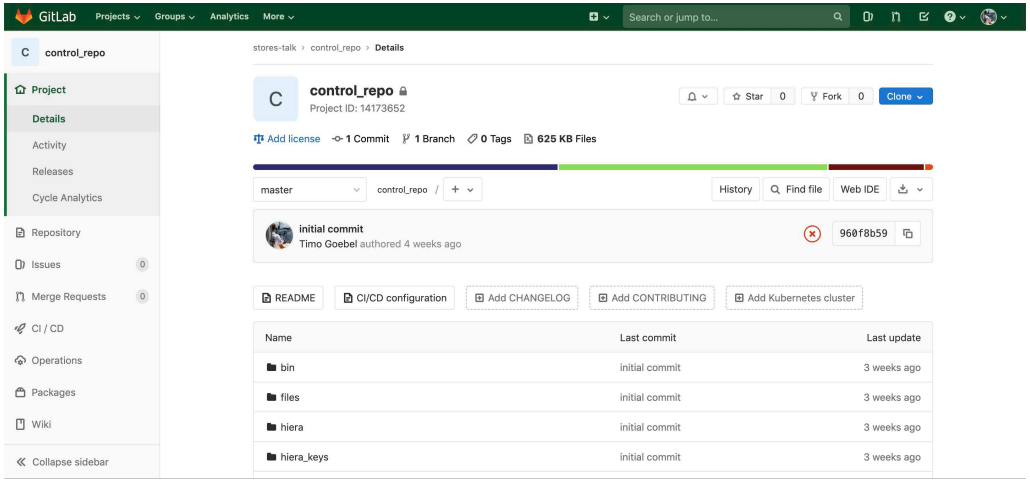
```
<%#
kind: iPXE
name: Kickstart default iPXE
model: ProvisioningTemplate
oses:
- CentOS
- Fedora
- RedHat
%>
<% subnet = @host.subnet -%>
<% if subnet.respond_to?(:dhcp_boot_mode?) && subnet.dhcp_boot_mode? -%>
  <% static = '' -%>
<% else -%>
  <% static_arg = 'static=yes' -%>
  <% static = (@host.token.nil? ? '?' : '&') + static_arg -%>
<% end -%>

<% stage2 = host_param('kickstart_liveimg') ? 'inst.stage2=' + @host.operatingsystem.medium_uri(@host).to_s : '' %>

kernel <%= "#{@host.url_for_boot(:kernel)}" %> initrd=initrd.img ks=<%= foreman_url('provision')%> inst.stage2=<%= @host.operatingsystem.medium_uri
initrd <%= "#{@host.url_for_boot(:initrd)}" %>
```

Puppet

- Config management
- Uses a pull approach, which scales better – especially with an unreliable network

Gitlab

- Hosts the git repositories
- Runs CI Pipelines



Test Kitchen

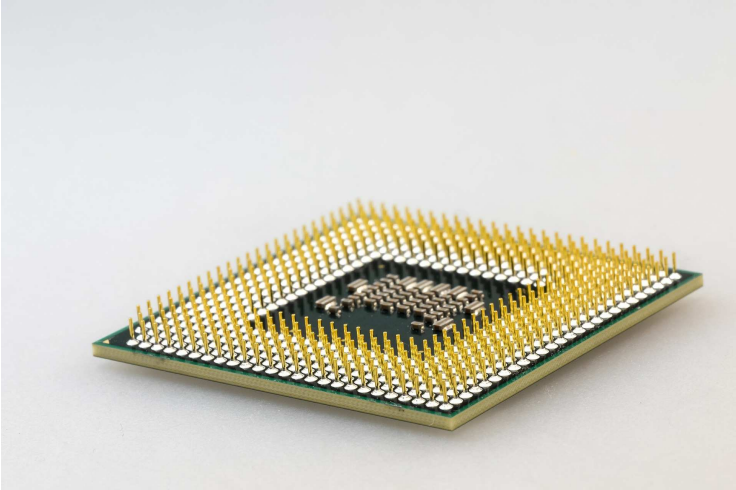
- Can run serverspec tests in a docker container

Docker

- Provides a container to simulate an endpoint and run tests inside

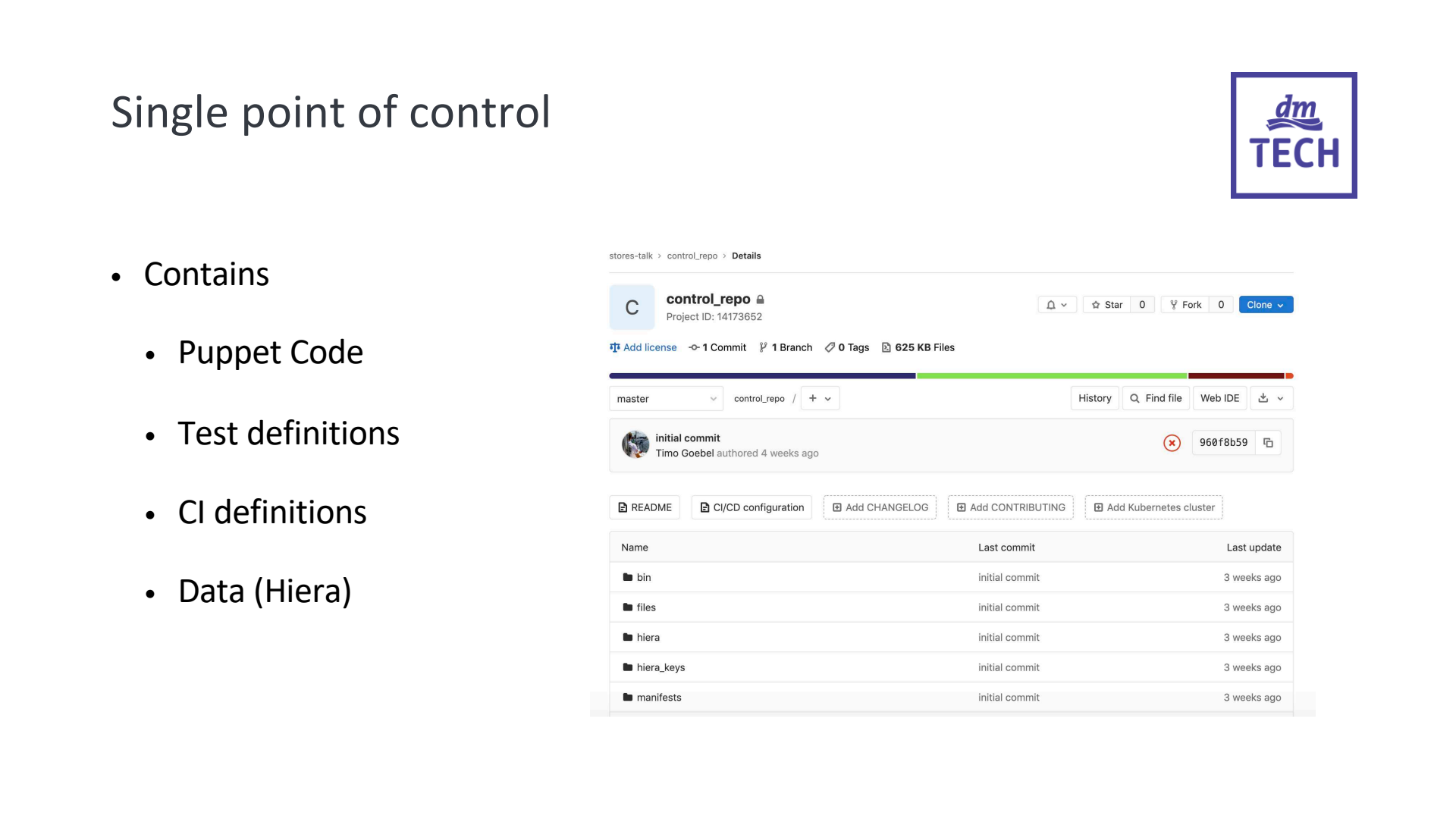
iPXE

- Boot Firmware
- We want to do as little TFTP as possible
- Can retrieve Kernel/Initrd via HTTP(s)



The control repo

Single point of control



- Contains
  - Puppet Code
  - Test definitions
  - CI definitions
  - Data (Hiera)

stores-talk › control_repo › Details

C

control_repo
Project ID: 14173652

Star 0 | Fork 0 | Clone

Add license | 1 Commit | 1 Branch | 0 Tags | 625 KB Files

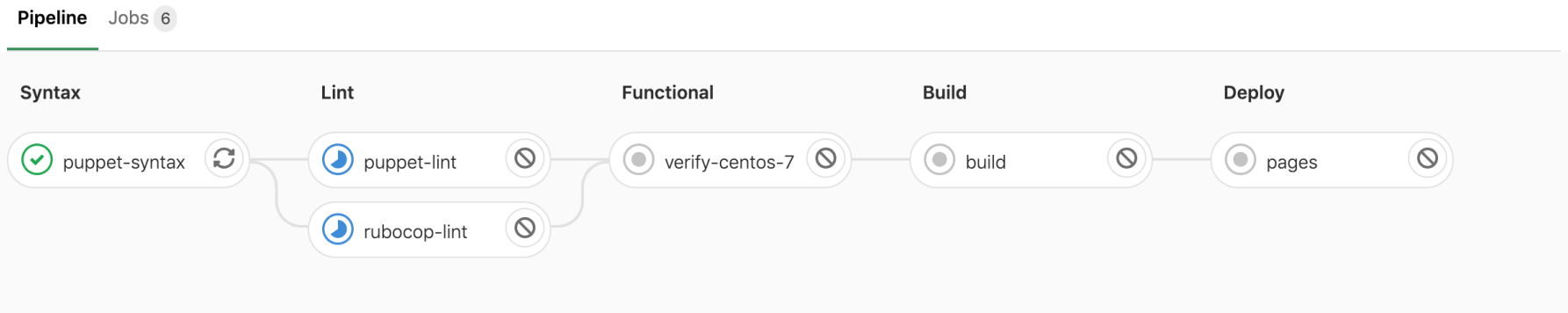
master | control_repo / | History | Find file | Web IDE

initial commit
Timo Goebel authored 4 weeks ago
960f8b59

README | CI/CD configuration | Add CHANGELOG | Add CONTRIBUTING | Add Kubernetes cluster

Name	Last commit	Last update
bin	initial commit	3 weeks ago
files	initial commit	3 weeks ago
hiera	initial commit	3 weeks ago
hiera_keys	initial commit	3 weeks ago
manifests	initial commit	3 weeks ago

Test driven



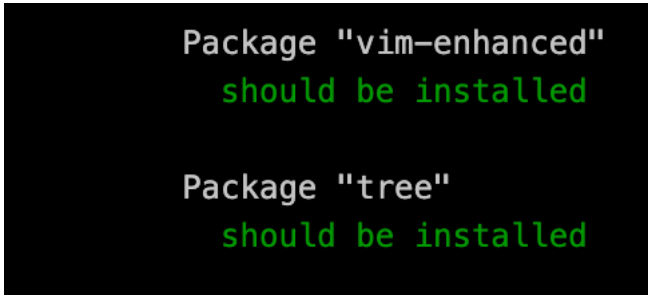

```
before_script:
  - apk add bash build-base git
  - bundle install --without kitchen

puppet-syntax:
  stage: syntax
  script:
    - ./bin/puppet_check_syntax.sh all
```

Test driven

```yaml
verify-centos-7:
  services:
    - docker:dind
  before_script:
    - echo "${PUPPET_EYAML_PRIVATE_KEY}" > hiera_keys/private_key.pkcs7.pem
    - cat hiera_keys/private_key.pkcs7.pem | head -n 1
    - apk add build-base docker libffi-dev patch git
    - docker info
    - bundle install --with kitchen
  stage: functional
  artifacts:
    expire_in: 7d
    when: on_failure
    paths:
      - .kitchen/logs
  script:
    - kitchen test default-centos-7 -d always
```

Test driven

```ruby
require 'serverspec'

# Required by serverspec
set :backend, :exec

describe package('vim-enhanced') do
  it { should be_installed }
end

describe package('tree') do
  it { should be_installed }
end
```



```
Package "vim-enhanced"
  should be installed

Package "tree"
  should be installed
```

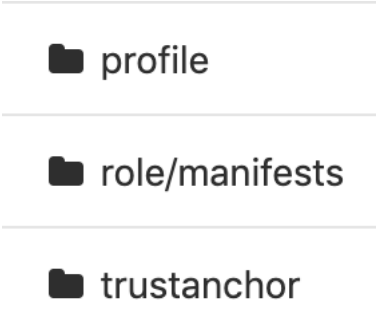
Test driven

```
34  platforms:
35    - name: centos-7
36      driver_config:
37        image: centos:7
38        platform: centos
39        run_command: /usr/sbin/init
40
41  verifier:
42    name: serverspec
43    default_pattern: true
44
45  suites:
46    - name: default
```

- We can easily test
  - if our config works with different OS versions
  - If a code change breaks a special configuration
  - in a local (debug) environment

The site folder

- Contains
  - Custom Puppet Modules
  - Roles
  - Profiles



The Puppetfile

- Contains
  - Puppet Modules from the forge

Puppetfile 317 Bytes

```
forge 'https://forgeapi.puppetlabs.com'

mod 'blackknight36-chrony', '0.2.3'
mod 'camptocamp-systemd', '2.1.0'
mod 'puppet-yum', '4.0.0'
mod 'puppetlabs-inifile', '2.4.0'
mod 'puppetlabs/stdlib'
mod 'saz-timezone', '5.0.2'

mod 'firewalld',
  git: 'https://github.com/crayfishx/puppet-firewalld.git',
  ref: 'master'
```

Code deploy

```
48  build:
49    script:
50      - ./bin/build.sh
51    stage: build
52    artifacts:
53      paths:
54        - build/puppet_archive.tar.gz
55      expire_in: 1 week
56
57  pages:
58    stage: deploy
59    script:
60      - mkdir public/
61      - cp index.html public/
62      - cp build/puppet_archive.tar.gz public/
63    dependencies:
64      - build
65    artifacts:
66      paths:
67        - public
68    only:
69      - master
```

- Deploy to Gitlab Pages is easy
- No branch support, yet.
- Won‘t support a phased rollout.

Code deploy

- Deploy Code to Puppetmaster(s)
- Create Puppet environment in Foreman
- `hammer --fetch-ca-cert https://foreman.example.com/`
- `hammer environment create --name #{env} --organizations #{organization} --locations #{location}`
- `hammer proxy import-classes --environment #{env} --name #{puppetmaster_name}`

The boot process

The boot process

- Store computers boot via PXE
  - DHCP Request to (local) router
  - Router tells the network card firmware
    - The IP-Address of a TFTP server
    - A filename on the TFTP server
  - TFTP is very trivial, not a good fit for WAN

Prerequisites

- Stores have a router running Cisco iOS
- Router is a pretty dumb DHCP server
- Router can server files locally via TFTP
- Let‘s serve „undionly.kpxe“ (iPXE) via TFTP, distribute via Ansible

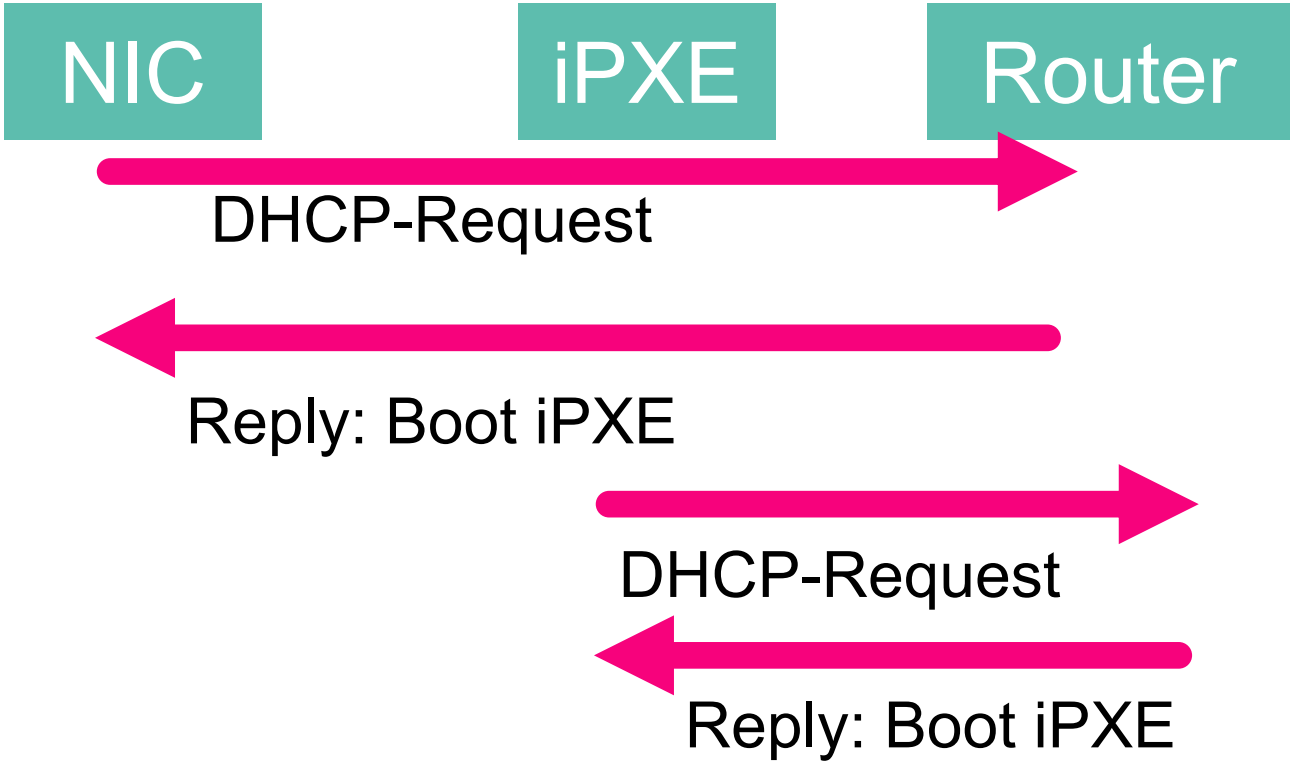
```
Router#sho run | begin pool 1
ip dhcp pool 1
network 192.168.1.0 255.255.255.0
bootfile undionly.kpxe
next-server 192.168.1.1
default-router 192.168.1.1
dns-server 192.168.1.1 192.168.1.2
domain-name store.de.example.com
lease 0 4
```

Breaking the infinite loop

- When iPXE starts, it issues a DHCP request to determine what to do next
- The DHCP server (being dumb) tells iPXE to load iPXE via tftp
- We‘re stuck in an infinite loop

- We can use an embedded script to break the loop

Infinite Loop Com Flow



Embedded Script

- We need to build our own iPXE image

```
#!ipxe

dhcp
chain http://boot.ipxe.org/demo/boot.php
```

```
make bin/undionly.kpxe EMBED=demo.ipxe
```

Foreman Handoff

- We need to build our own iPXE image

```
#!ipxe
dhcp
chain
http://foreman.example.com/unattended/iPXE?mac=${net0/mac}
```

iPXE Templates

theforeman / community-templates

Watch 30 | Star 126 | Fork 174

Code | Issues 12 | Pull requests 25 | Actions | Security | Insights

Branch: develop | community-templates / provisioning_templates / iPXE / | Create new file | Upload files | Find file | History

jcpunk and mmoll Fixes #22742 - Add link delay option to kickstart — Latest commit 381b38f 10 days ago

..	
autoyast_default_ipxe.erb	last year
ipxe_default_local_boot.erb	last year
ipxe_global_default.erb	10 days ago
ipxe_intermediate_script.erb	6 months ago
kickstart_default_ipxe.erb	10 days ago
preseed_default_ipxe.erb	3 months ago

- Install SLES Kernel/Initrd
- Boot from disk
- Unknown Host
- What we bake into iPXE
- Install RHEL Kernel/Initrd
- Install Debian Kernel/Initrd

Limitations

- How to configure the iOS device to serve either „undionly.kpxe“ for BIOS boots or „ipxe.efi“ for EFI boots?

Thank you.

Images taken from pixabay.com