DNS and Security

Julien Pivotto

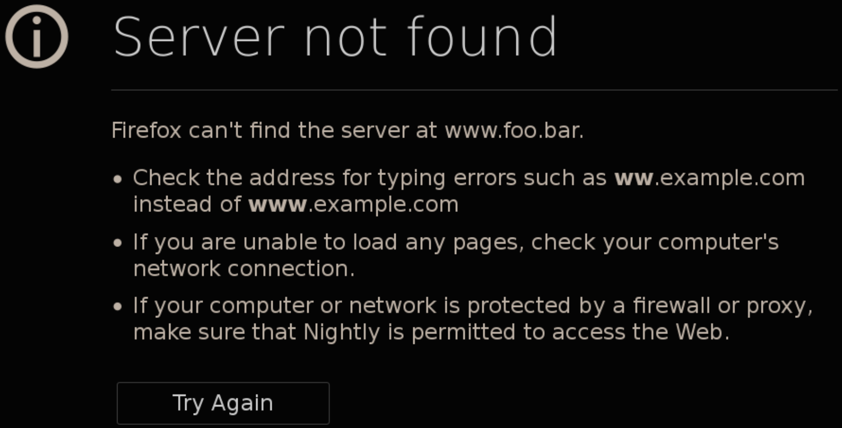
RMLL Security Track
July 5th, 2016

whois

Julien Pivotto

- Sysadmin at inuits.eu
- From small to large scale orgs
- Automation & Monitoring
- *@roidelapluie* on irc/twitter/github

inuits.eu



Server not found

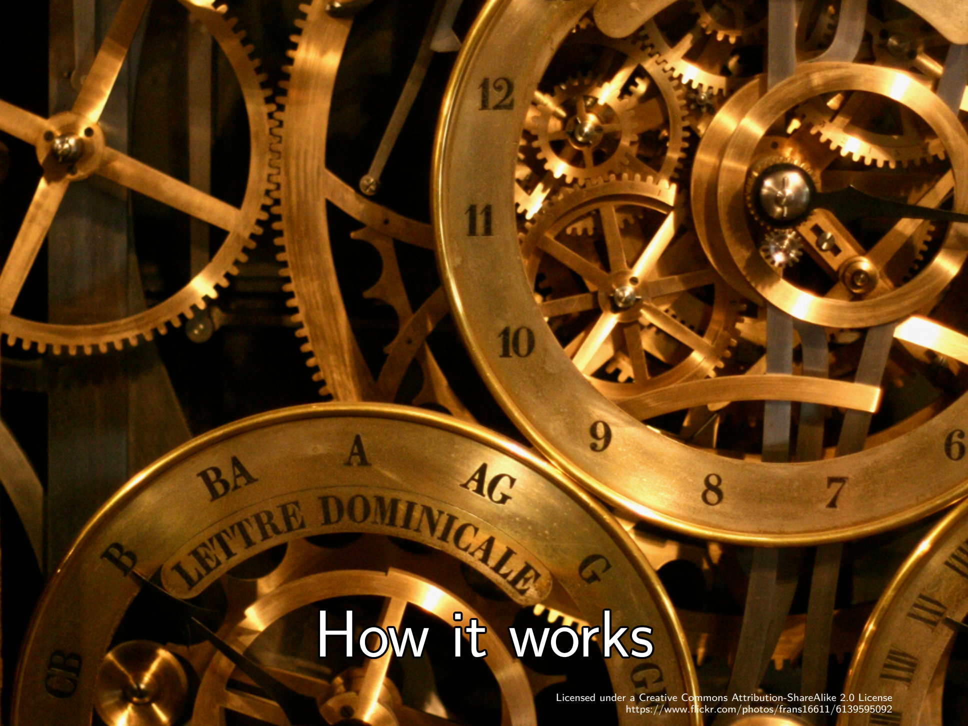
Firefox can't find the server at www.foo.bar.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Nightly is permitted to access the Web.

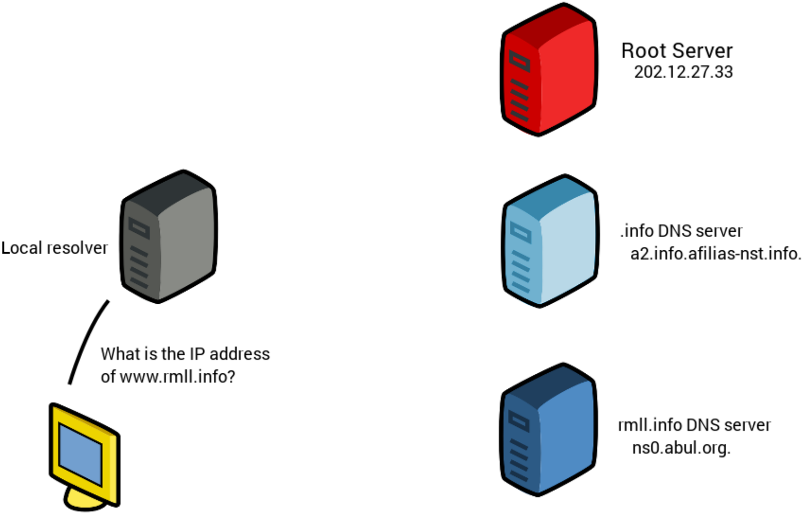
DNS

What is DNS?

- TL;DR Translates domain name to IP
- In facto, stores much more data than IP



How it works



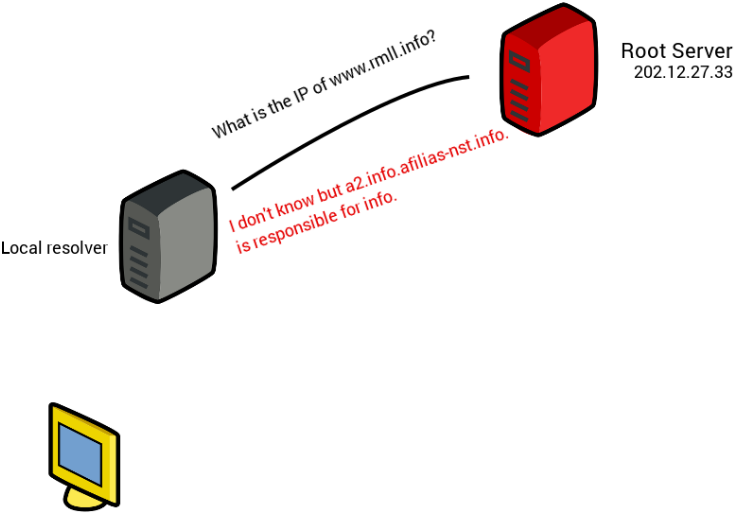
Root Server
202.12.27.33

Local resolver

.info DNS server
a2.info.afilias-nst.info.

What is the IP address
of www.rmll.info?

rmll.info DNS server
ns0.abul.org.

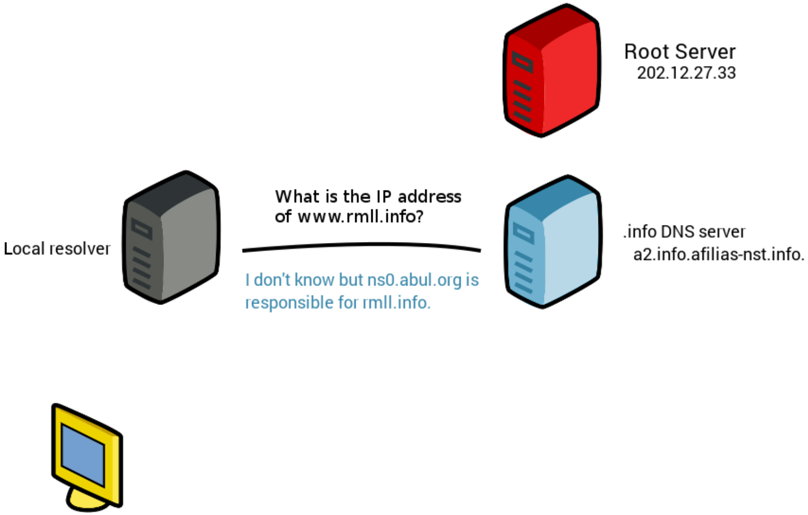


Root Server
202.12.27.33

What is the IP of www.rmll.info?

I don't know but a2.info.afilias-nst.info.
is responsible for info.

Local resolver



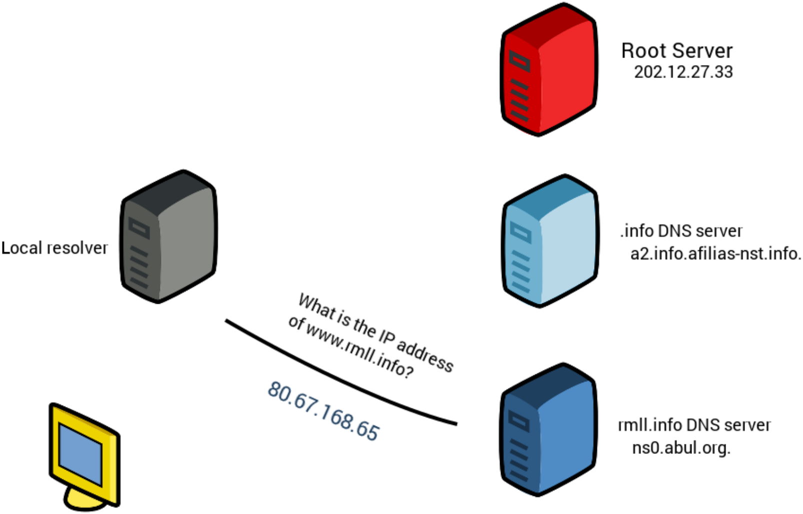
Root Server
202.12.27.33

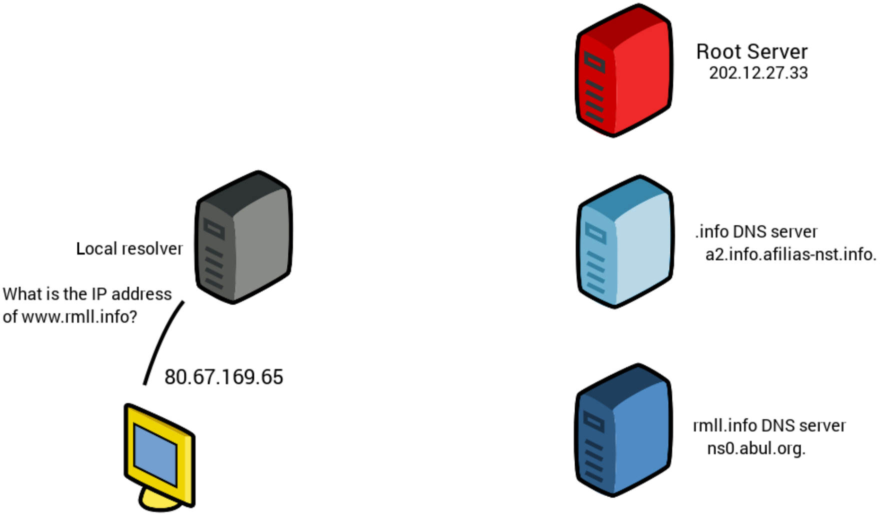
Local resolver

What is the IP address
of www.rmll.info?

I don't know but ns0.abul.org is
responsible for rmll.info.

.info DNS server
a2.info.afilias-nst.info.


Root Server
202.12.27.33
Local resolver
.info DNS server
a2.info.afilias-nst.info.
What is the IP address
of www.rmll.info?
80.67.168.65
rmll.info DNS server
ns0.abul.org.



Root Server
202.12.27.33

Local resolver

.info DNS server
a2.info.afilias-nst.info.

What is the IP address
of www.rmll.info?

80.67.169.65

rmll.info DNS server
ns0.abul.org.

DNS is mission-critical

- Holds IP addresses
- Holds service definitions
- Holds hostnames, TXT records

DNS practices

- Do not mix Authoritative and Recursive servers
- Mix your DNS server `brand'
- Hide your DNS masters
- Do not invent new TLD

Data stored in DNS

- A records: IP addresses
- CNAME: Cannonical names
- SRV: Service record
- MX: Mail servers
- TXT: Text record

SRV records

```
_xmpp—client._tcp.inuits.eu. IN      SRV
       0 5 5222 xmpp.inuits.eu.
```

TXT Records

- SPF record: Sender Policy Framework
- DKIM
- Keybase.io
- Let's Encrypt DNS challenge

Not secure by design

- 1983
- Designed for scale, not security
- Early 2000: birth of DNSSec

DNSSec

- 2000's DNSSec RFC
- DNSSec hit DNS root in 2010
- Multiple iteration of RFC

The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System.

RFC 4033

What is DNS Sec?

- Proof of origin and integrity
- Zones and records signing
- Proof of non-existence

Two types of keys

- ZSK: Zone Signing Key
- KSK: Key Signing Key

Zone Signing key

- Private/Public key pair
- Sign the Records
- e.g sign the A records, the MX records …
- Rolled out frequently

Key Signing Key

- Private/Public key pair
- Sign the ZSK
- Designed to be stronger than the ZSK
- Its fingerprint is stored in parent zone

DNS Records types

- RRSIG: Signature
- DNSKEY: Public key
- DS: Hash of a DNSKEY (parent zone)

DNS Records types

- NSEC: Next secure
- Returns the next secure entry
- Returned when next secure is not found
- NSEC/NSEC3 records are signed
- NSEC3 prevents zone walking

In Practice

Bind

- Reference DNS Server
- Developed by the Internet Systems Consortium
- Current version: bind9
- bind10 project is abandoned

Bind features

- Supports everything
- Recurive, Authoritative
- Dynamic updates
- DNSSec

Bind and DNSSec

- Full support + NSEC3
- Manual signing
- Automated signing
- DNSSec and dynamic zones

Generating keys

```
mkdir /etc/bind/keys
cd /etc/bind/keys
dnssec-keygen rmll.example
dnssec-keygen -f KSK rmll.example
```

Generating keys

```
dnssec—keygen —a NSEC3RSASHA1 —b 2048 rmll
    .example
dnssec—keygen —a NSEC3RSASHA1 —b 4096 —f
    KSK rmll.example
```

Generating DS keys

```
dnssec-dsfromkey  -f /var/bind/rmll.
   example -K /etc/bind/keys/ rmll.example

rmll.example. IN DS 18025 8 1
   E223065EE5EE66F08CA1C89D8
rmll.example. IN DS 18025 8 2 522
   D8EA3287FFF41186169A30
```

Enable DNSSec in bind

```
options {
  dnssec-enable yes;
  dnssec-validation yes;
}
```

Enable DNSSec for a zone

Manually signed

```
zone ”rmll.example” IN {
        type master;
        file ”rmll.example.zone.signed”;
};
```

Enable DNSSec for a zone

Auto Signing

```
zone "rmll.example" IN {
    type master;
    file "rmll.example.zone";
    key-directory "/etc/bind/keys";
    auto-dnssec maintain;
    inline-signing yes;
};
```

Manually Sign a zone

```
dnssec—signzone —S —o rmll.example —K /etc/bind/keys/ /var/bind/master/rmll.example.zone
```

- Creates a .signed zone file

DANE

DANE

- DNS-based Authentication of Named Entities
- New record types to store public keys hashes
- Independant from DNSSec (!)

TLSA records

- Hash the fingerprint of a TLS key
- "Replacement" for the CA (https)
- Not implemented natively in browsers
- Implemented in IRC clients (irssi)

TLSA records

```
_443._tcp IN TLSA 3 0 1 2
   bfa3214fda53315b140e65fe66
_443._tcp.www IN TLSA 3 0 1 2
   bfa3214fda53315b140e65
_6697._tcp.irc IN TLSA 3 0 1 2
   bfa3214fda53315b140e6
```

Generating a hash

```
openssl x509 —in cert.pem —outform DER |
    openssl sha256
```

SSH

TOFU

- Trust on first use
- Works on slowly moving env's
- Nowadays we populate new hosts all the time
- Nowadays we rebuild existing hosts

SSHFP records

- Hash the fingerprint of a SSH server
- Implemented in OpenSSH
- Uses DNS to recognize SSH key

```
IN SSHFP 1 1
   e0fd9112d2fc6974597fe8968665ad6b420c
IN SSHFP 1 2 9
   de5bc066a898733420bcfaae8f43e80e532
IN SSHFP 2 1 223
   e89447a53a3178be02fee6fdd5b44228a
IN SSHFP 2 2 2644
   fcbd2a1b179091a195207e395d009b16
```

```
VerifyHostKeyDNS no
VerifyHostKeyDNS yes
VerifyHostKeyDNS ask
```

```
$ ssh —o VerifyHostKeyDNS=yes rmll.example
The authenticity of host ’rmll.example
   (1.2.3.4)’ can’t be established.
ECDSA key fingerprint is SHA256:
   f8zwQD3RU62PXgwCw5WRk2OIyVY.
Matching host key fingerprint found in DNS
Are you sure you want to continue?
```

Populating SSHFP fields

- What if we have a single source of truth?
- Something that can scale, and be quick enough?

Config Management

- Quickly moving env often use Cfgmgmt Tools
- They know the env, store data
- We use Puppet+The foreman

Puppet

- A Config Management Tool
- Declarative
- Enforces a desired state

Puppet Facts

- Values collected on the host
- OS version, Uptime, kernel
- SSH fingerprints
- Sent back to master

facts2sshfp

- https://github.com/jpmens/facts2sshfp
- Python script
- Read facts yaml files
- Converts Puppet facts to SSHFP records
- Uses Puppet as single source of truth
- facts2sshfp.py -T nsupdate.template -D a.aa.
- Output to templates, nsupdate commands...

The Foreman

The Foreman

Provisioning

The Foreman

Provisioning

Configuration

The Foreman

Provisioning

Configuration

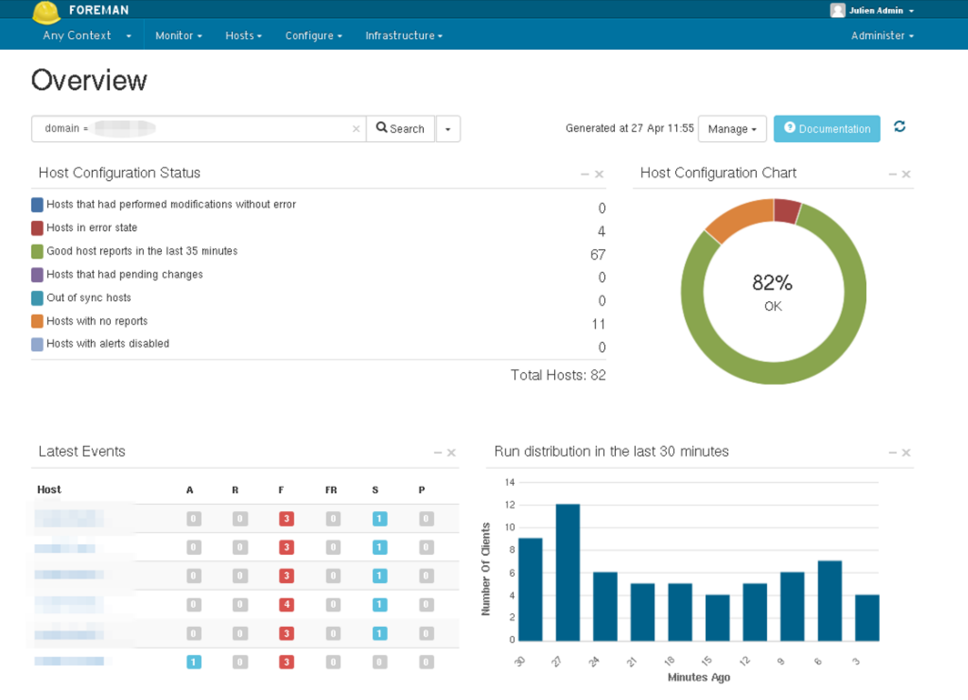
Monitoring

The Foreman

Provisioning

Configuration

~~Monitoring~~
Reporting



Overview

Generated at 27 Apr 11:55

Host Configuration Status

🟦 Hosts that had performed modifications without error	0
🟥 Hosts in error state	4
🟩 Good host reports in the last 35 minutes	67
🟪 Hosts that had pending changes	0
🟦 Out of sync hosts	0
🟧 Hosts with no reports	11
🟦 Hosts with alerts disabled	0

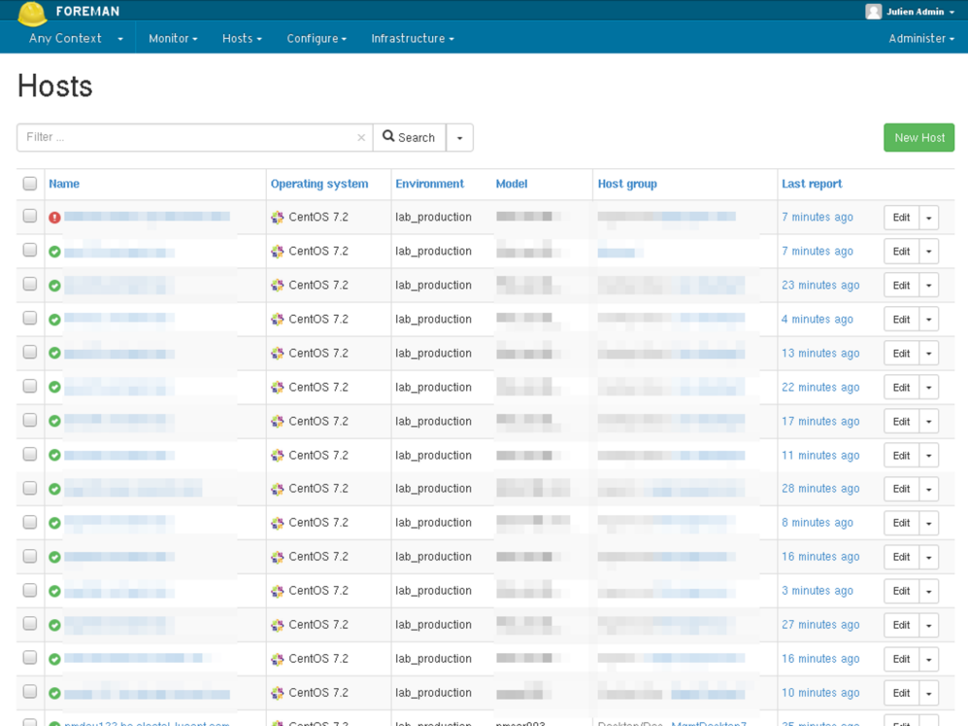
Total Hosts: 82

Host Configuration Chart

Latest Events

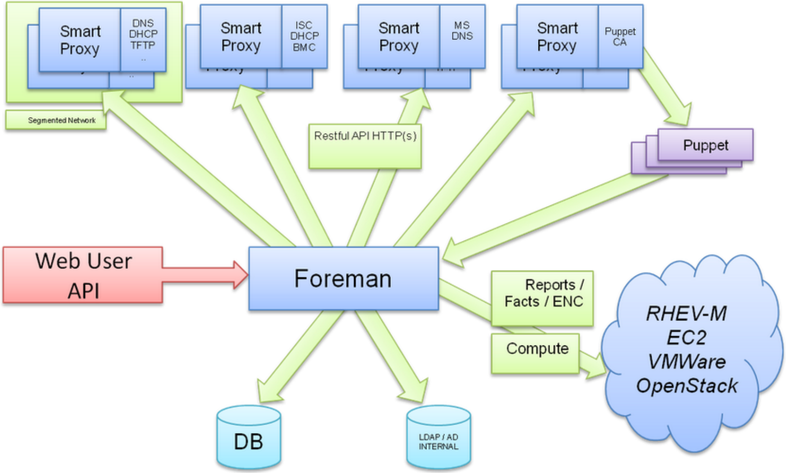
Host	A	R	F	FR	S	P
[redacted]	0	0	3	0	1	0
[redacted]	0	0	3	0	1	0
[redacted]	0	0	3	0	1	0
[redacted]	0	0	4	0	1	0
[redacted]	0	0	3	0	1	0
[redacted]	1	0	3	0	0	0

Run distribution in the last 30 minutes



Hosts

☐	Name	Operating system	Environment	Model	Host group	Last report	
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	7 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	7 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	23 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	4 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	13 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	22 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	17 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	11 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	28 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	8 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	16 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	3 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	27 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	16 minutes ago	Edit
☐	[redacted]	CentOS 7.2	lab_production	[redacted]	[redacted]	10 minutes ago	Edit
☐	pmdeu123.be.alcatel-lucent.com	CentOS 7.2	lab_production	pmcar003	Desktop/Dec MgmtDesktop7	35 minutes ago	Edit


Smart Proxy
DNS DHCP TFTP ..
Segmented Network
Smart Proxy
ISC DHCP BMC
Smart Proxy
MS DNS
Smart Proxy
Puppet CA
Restful API HTTP(s)
Puppet
Web User API
Foreman
Reports / Facts / ENC
Compute
RHEV-M EC2 VMWare OpenStack
DB
LDAP / AD INTERNAL

Foreman Proxies

- Foreman works with a GUI + Proxies
- DHCP proxy, Puppet Proxy, DNS proxy…
- DNS Proxy is pluggable: bind9, powerdns…

Foreman is great

- Open Source
- Backed by Red Hat
- The main brick behind Red Hat Satellite 6
- Provides a REST API

Building a (libvirt) host

- Create/update DNS entries
- Create/update DHCP entries
- Create the VM in libvirt
- Boot the VM
- Serve a kickstart
- Run Puppet

The Foreman - Puppet proxy

- Puppet Collects and save Facts on the machines
- It can send it back to the Foreman
- Foreman can graph them, query them…

facts2sshfp

- https://github.com/jpmens/facts2sshfp
- facts2sshfp.py -T nsupdate.template --foreman-url=https://foreman.example -D a.aa.

Conclusion

Licensed under a Creative Commons Attribution 2.0 License
https://www.flickr.com/photos/haslamdigital/17191280202/sizes/h/

DNS rocks

- Needed everywhere
- Distributed
- Contains lots of data
- Makes our life easier

DNSSec is easy to implement

- Automation is key
- Implemented in most of the tools
- And most of the DNS servers

DANE adds more security

- SSH fingerprint
- IRC, SMTP certificates hashes
- Existing client-side implementations

DNSSec+DANE

- DNSSec and Dane are more useful together
- Make sure your resolver supports DNSsec!
- The power to check certificates without CA

Contact

Julien Pivotto
julien@inuits.eu
@roidelapluie

https://inuits.eu
info@inuits.eu
+32 473 441 636