



Welcome to

Drift af en infrastruktur med Ansible

Henrik Lund Kramshøj hk@zencurity.dk

Slides are available as PDF, [kramshoej@Github](https://github.com/kramshoej)

Try searching for `automate-it-2017.tex` in the repo

slide are available as PDF [kramshoej@Github](https://github.com/kramshoej)

Goal and Agenda: Ansible and more



PatientSky is rolling out new health infrastructure of connected clinics in Norway.

We are very few people running the systems, so we need to automate.

... but automation has other benefits.

Prerequisites: Python, SSH, SSH keys, sudo

Ansible introduction, what is this Ansible

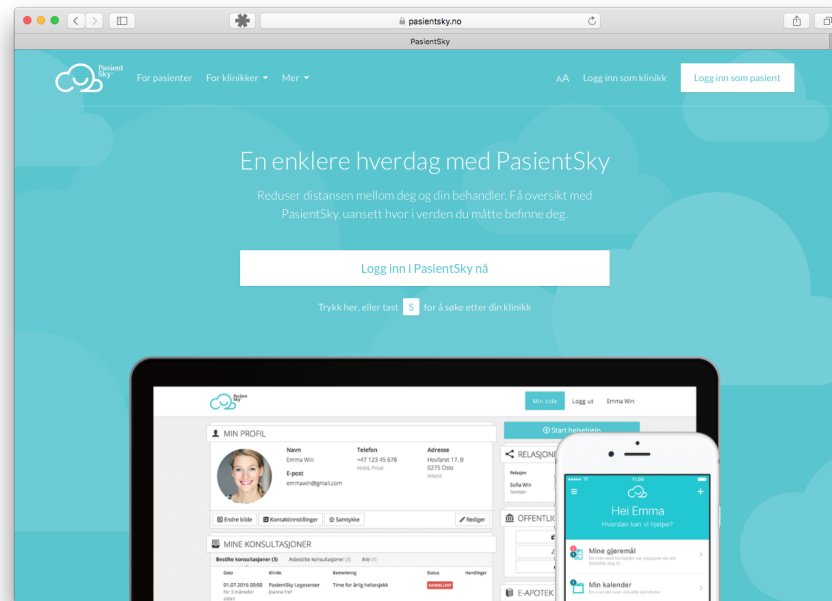
Ansible targets: Linux hosts, ESXi, network devices

Ansible examples, and workshop

Keywords: Ansible, YAML, automating boring stuff

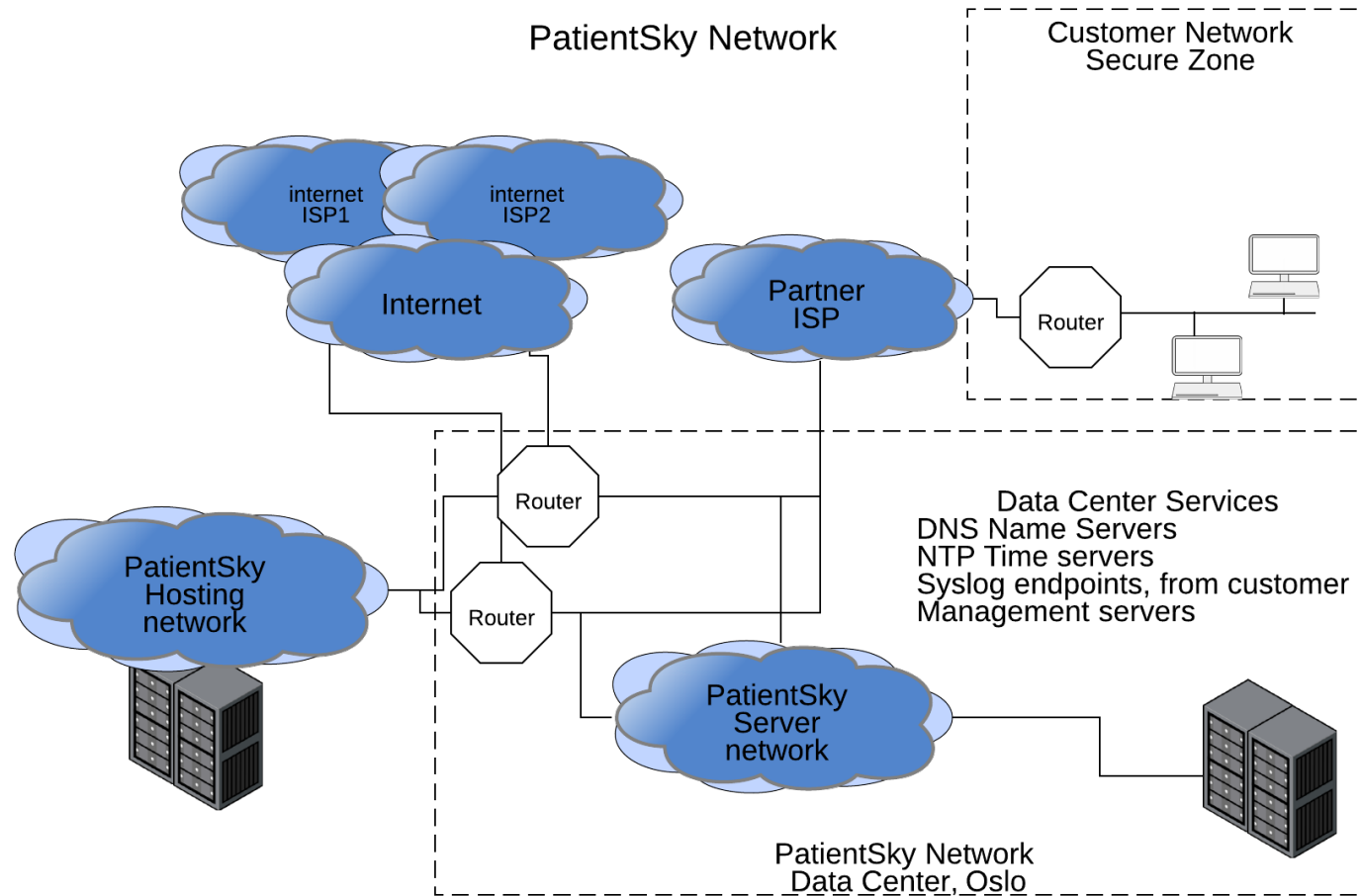
For optimal fun, use your laptop, fetch it in next break!

Pasientsky.no - the environment and services



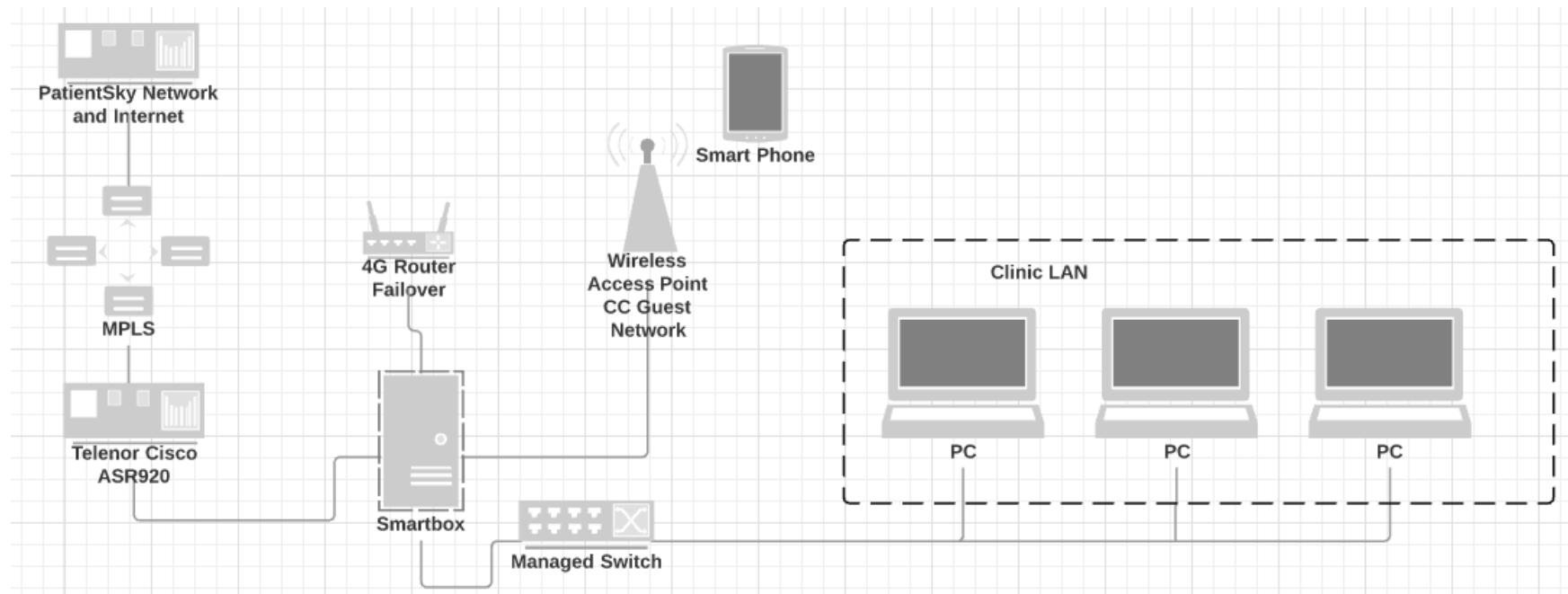
Connected Clinic from PasientSky provides modern and revolutionary solutions meeting the special communication needs in the health sector. A small and smart box provides quick and stable internet connection with integrated telephony and time book.

Overview



Most servers are Linux, percentage is OpenBSD, running on VMware ESXi

OpenBSD CPE: BGP, PF and service daemons



- Soekris Net6501-50 1 Ghz CPU, 1024 Mbyte DDR2-SDRAM, 4 x 1Gbit Ethernet
- OpenBSD operating system
- We install new Smartboxes every week

Important processes and components



- Setup hardware
- Connect cables
- Setup development environment
- Setup staging environment - like development
- Setup production environment - like staging
- Setup firewalls, security, LDAP servers
- Setup other surrounding infrastructure

Top parts hard to automate, bottom easier 😊

What is Ansible



AUTOMATION FOR EVERYONE

Ansible is designed around the way people work and the way people work together.

Ansible has thousands of users, hundreds of customers and over 2,400 community contributors.

750+ Ansible modules

`https://www.ansible.com/`

We have been using Ansible for about 2 years

Alternatives: (cfengine), Chef, Puppet or Salt

Who uses Ansible



- PatientSky Danmark Aps
- Bornhack - Thomas Tykling Rasmussen

How Ansible Works: inventory files



List your hosts in one or multiple text files:

```
[all:vars]
ansible_ssh_port=34443
```

```
[office]
fw-01 ansible_ssh_host=192.168.1.1 ansible_ssh_port=22
ansible_python_interpreter=/usr/local/bin/python
```

```
[infrastructure]
smtp-01      ansible_ssh_host=185.60.160.37 ansible_python_interpreter=/usr/local/bin/python
vpnmon-01    ansible_ssh_host=10.50.22.18
```

- Inventory files specify the hosts we work with
- Linux and OpenBSD servers shown here
- Real inventory for the site with development and staging approx 500 lines
- office and infradstructure are group names

How Ansible Works: ad hoc parallel execution



Using the inventory file you can run commands with Ansible:

```
ansible -m ping new-server
ansible -a "date" new-server
ansible -m shell -a "grep a /etc/something" new-server
```

- Running commands on multiple servers is easy now

How Ansible Works: Playbooks



The benefit comes with tasks - do something:

```
- hosts: smartbox-*
  become: yes
  tasks:
    - name: Create a template pf.conf
      template:
        src=pf/pf.conf.j2
        dest=/etc/pf.conf owner=root group=wheel mode=0600
      notify:
        - reload pf
      tags:
        - firewall
        - pf.conf
```

- Specify the end result, more than the steps, also restarts daemons
- Use the modules from https://docs.ansible.com/ansible/modules_by_category.html
- Jinja templates - ooooooh so great!

How Ansible Works: typical execution



```
ansible-playbook -i hosts.odn1 -K infrastructure-firewalls.yml -t pf.conf --check --diff
```

```
ansible-playbook -i hosts.odn1 -K infrastructure-firewalls.yml -t pf.conf
```

```
ansible-playbook -i hosts.odn1 -K infrastructure-nagios.yml -t config-only
```

```
ansible-playbook -i smartboxes -K create-pf-conf.yml -l smartbox-xxx-01
```

- Pro tip: check before you push out changes to production networks ☺
- Diff will show the changes about to be made

How Ansible Works: atypical execution / gotchas



```
ansible -i ../smartboxes.osl1 --become --ask-become-pass -m shell  
-a "pfctl -s rules" -l smartbox01
```

```
ansible -i ../smartboxes.osl1 --become --ask-become-pass -m shell  
-a "nmap -sP 185.161.1xx.123-124 2> /dev/null| grep done" all
```

- Sometimes you need a trick or persistence
- Ansible moving from *sudo* to *become*
- The normal -K did not work, but the above does for ad hoc commands

Stop: discussion benefits of Ansible



Do we even need to run the same command on multiple servers?

What are the benefits of Ansible?

- Central configuration management - git repo
- Same playbook - different inventory file, what happens
- Already using Ansible, tell us why and how

Life of a server



- Create VM
- Network install - with pxeboot
- Standard settings: hostname, LDAP, SSH, timezone, ...
- Configure this server: application installation, settings, etc.
- Configure monitoring: like Smokeping

Up and running with Ansible



Prerequisites for Ansible:

- python language - Ansible uses this
- ssh keys - remote login without passwords
- Sudo - allow regular users to do superuser tasks
- Recommended tool: `ssh-copy-id` for getting your key on new server
- Recommended Change: `sshd_config` - no passwords allowed, no brute force
- Recommended to use: `jump hosts/ProxyCommand` in `ssh_config`

Install python on servers



- Ubuntu server: `apt install python`
- OpenBSD: `pkg_add python`
Requires `PKG_PATH` set, see below

OpenBSD package path can be set in `/root/.profile`

```
PKG_PATH=ftp://mirror.one.com/pub/OpenBSD/`uname -r`/packages/`uname -m`  
PKG_PATH=https://stable.mtier.org/updates/$(uname -r)/$(arch -s):$PKG_PATH  
export PKG_PATH
```

Exercise: trying Ansible



Create inventory file, and then:

```
ansible -m ping new-server
ansible -a "date" new-server
ansible -m shell -a "grep a /etc/something" new-server
```

- Lets try running Ansible!
- Hopefully there is a small getting started repo to clone from Github ☺
- Server to use should be shown on the whiteboard (or similar)
- Dont forget you can override user with `ansible -u`
very usefull if you are bringing up a server from PXE boot using `user manager`
- Trouble? Try running with `-vvv`, try manual ssh, is Python ready?

Exercise: try fetching facts



```
ansible -i hosts.odn1 -m setup $HOST | grep hostname  
    "ansible_hostname": "odn1-fw-odn1-01",
```

- Facts are fetched by default from servers
- Can be fetched / investigated using the setup module
- Returns JSON
-
-

Important notes about tasks



Ansible Tasks are **idempotent**. Without a lot of extra coding, bash scripts are usually not safely run again and again. Ansible uses "Facts", which is system and environment information it gathers ("context") before running Tasks.

Ansible uses these facts to check state and see if it needs to change anything in order to get **the desired outcome**. This makes it safe to run Ansible Tasks against a server over and over again.

Also not describing what to do, but what you want the result to be!

Quote from:

<https://serversforhackers.com/an-ansible-tutorial>

Exercise: try adding you own user



- Copy or edit the create-user.yml
- Run this task so your own user is created
-
-

Structure of Ansible repos



Listing of dirs

```
host_vars/  
group_vars/  
roles/  
library/  
tasks/  
handlers/  
tools/
```

Warning: we do not use the roles much, our fault, YMMV

Group vars basics



```
---  
# file: group_vars/osl1  
  
location_name : "osl1"  
country_code  : "no"  
city          : "Oslo"  
timezone      : "Europe/Oslo"
```

- Group variables get loaded automatically
- Can be used for site specific things, Odense or Oslo for us
- Host vars work the same way, we prefer groups
- **Note:** secrets can use Ansible vault, https://docs.ansible.com/ansible/playbooks_vault.html

Group vars - grouping hosts dynamically



```
# talk to all hosts just so we can learn about them,  
# and save dynamic group os_OpenBSD etc.  
- group_by: key=os_ ansible_os_family  
  tags:  
    - always
```

with group_vars files:

```
group_vars/os_Debian:service_sshd: ssh  
group_vars/os_FreeBSD:service_sshd: sshd  
group_vars/os_OpenBSD:service_sshd: sshd
```

Then the handler script can use:

```
- name: restart sshd  
  service: name= service_sshd  state=restarted
```


Exercise: which operating system



```
tasks/common.yml
```

```
tasks/common-ubuntu.yml - include: common.yml
```

```
tasks/common-openbsd.yml - include: common.yml
```

```
tasks/common-freebsd.yml - include: common.yml
```

- Service ssh vs sshd was just an example, we can add more to files
- Different operating systems have small differences

Templates



Go back to example with packet filter config

```
src=pf/pf.conf.j2 dest=/etc/pf.conf owner=root group=wheel mode=0600
```

Exercise: play with lineinfile



Try doing changes to your `.profile` using `lineinfile`

- Copy or edit the `edit-profile.yml`
- Run this task so your own user profile is updated
- Advanced users: copy a file like `/etc/services` to `$HOME` and try modifying that
-

Use the documentation:

https://docs.ansible.com/ansible/lineinfile_module.html

Special cases



Templates and the groups



if/endif, else etc. NRPE example with default part and specials

firewalls differences between dev and prod, things that are not ready yet

smokeping loops over the group vars smartboxes

the smartboxes custom files, with neat trick if file does not exist

Adopting a server



- Copy files from server: like relevant ones from `/etc/`
- Create basic playbook(s) to copy back to server
- Generalize by making it templates and moving stuff to `group_vars`

Use the check and diff a lot 😊

Bad stuff with Ansible



- Worst, slow speed - solved by running specific tags, but annoying
- Nasty problem with Notify on Macs - did not notify and restart services!

Other problems when using Ansible

- Log rotate - easy to install and configure a lot, and forget this
- Requires monitoring, especially if you have many servers *duuuuh*
- Central logging, also recommended for other reasons

Conclusion



Automation is cool - use it