YGT presentation

Kristoffer Dalby

About me

- Kristoffer Dalby
- 26 years old
- Norwegian
- Master in Informatics from NTNU

At ESA

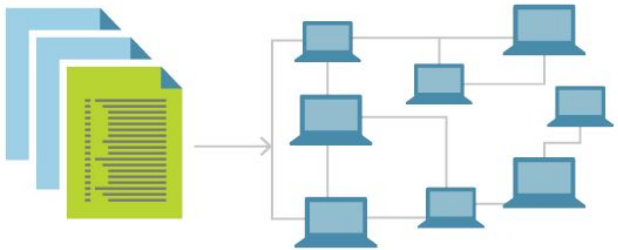
- 2 years as a YGT working with Jan Demey
- Been a part of the COMINF team
  - Working with Alberto, John, Jose and Juan
- Infrastructure as Code
  - Terraform
  - Packer
  - Ansible
  - Kubernetes
- Side projects

Infrastructure as Code

- Define how you want your infrastructure to look like
- Validate that the infrastructure can be implemented
- Automatically create the infrastructure
- Allow small team manage a large amount of infrastructure

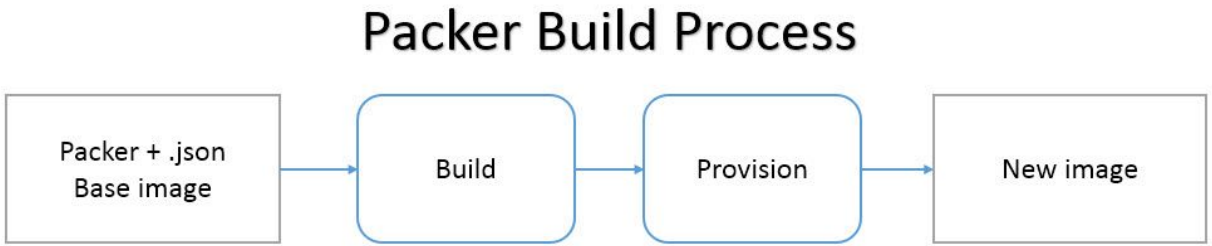
A IaS provider typically integrate many platforms which allows system to be tied together.

For example, when creating a virtual machine, automatically update the DNS server when the IP address is available.



Packer

- Automatically create virtual machine templates
- Programatically create official templates with ESA settings, security software and licenses.
  - Windows Server
  - Ubuntu
  - Red Hat
- Periodically recreate the images with security updates



Terraform

- Open source IaS platform
- Implements infrastructure vendors as “providers”
- Over a 100+ providers officially listed.
- Major cloud (GCP, AWS), Networking (Cisco, Fortinet), On-premise (VMware, Nutanix)
- Validate before run
- Collaborate and share
- Version control

```
resource "dns_a_record_set" "single_instance_dns" {
  zone = "${var.zone_name}."
  name = "${var.name}"

  addresses = [
    "${vcd_vm.single_instance.network.0.ip}",
  ]

  ttl = 10
}
resource "vcd_vm" "single_instance" {
  vapp_href                 = "${var.vapp_href}"
  name                      = "${var.name}"
  catalog_name              = "${var.catalog_name}"
  template_name             = "${var.template_name}"
  memory                    = "${var.memory}"
  cpus                      = "${var.cpu_count}"
  power_on                  = 1
  initscript                = "${file("${path.module}/../initscript.sh")} ${var.initscript}"
  nested_hypervisor_enabled = "${var.nested_hypervisor_enabled}"
  storage_profile           = "${var.storage_profile}"

  #  admin_password_auto       = "${var.admin_password_auto}"
  #  admin_password            = "${var.admin_password}"

  network = {
    name              = "${var.network}"
    ip_allocation_mode = "POOL"
    is_primary        = true
    adapter_type      = "VMXNET3"
  }
}

```

Ansible

- Provisioning
- Configuration management
- Application deployment

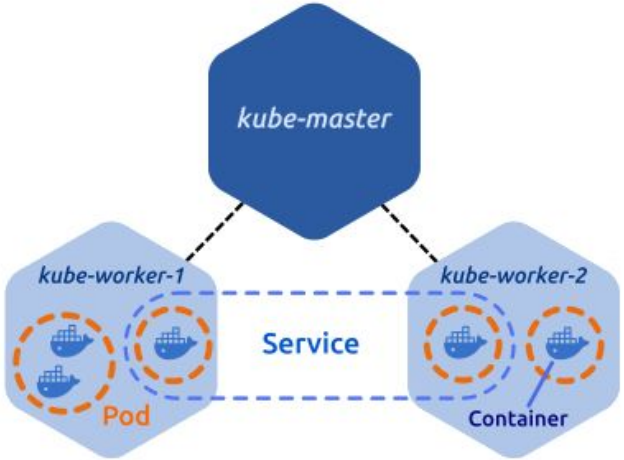
```yaml
---
- name: 'Install docker and role dependencies'
  become: yes
  apt:
    name: "{{ packages }}"
    state: present
    install_recommends: false
  vars:
    packages:
      - "apt-transport-https"
      - "ca-certificates"
      - "software-properties-common"
      - "curl"

- name: Add docker repository key
  apt_key:
    url: https://download.docker.com/linux/ubuntu/gpg
    state: present

- name: Add docker repository
  apt_repository:
    repo: 'deb [arch=amd64] https://download.docker.com/linux/ubuntu {{ ansible_distribution_release }} stable'
    state: present

- name: Install docker engine
  apt:
    name: "docker-ce={{ docker_version }}"
    update_cache: yes
    state: present
  notify: start docker

- name: hold docker
  dpkg_selections:
    name: docker-ce
    selection: hold
```

What can esait do with this?

- We can offer it as a part of our services, allowing customers to automate
- We could make our service providers use this technology to save costs
- If service providers use this, the code could be shared with ESA
  - Allowing greater insight, (e.g. for auditing)
  - Get involved with how our infrastructure is configured
  - Allow easier handover (between ESA, service providers, etc)
- To promote allover time saving, we could go in front with a good example :)

Kubernetes

- Container orchestration
- Microservice friendly
- Scaling applications
- Zero downtime upgrades
- Describe your application in code
- Standardized
- Very “pluggable”

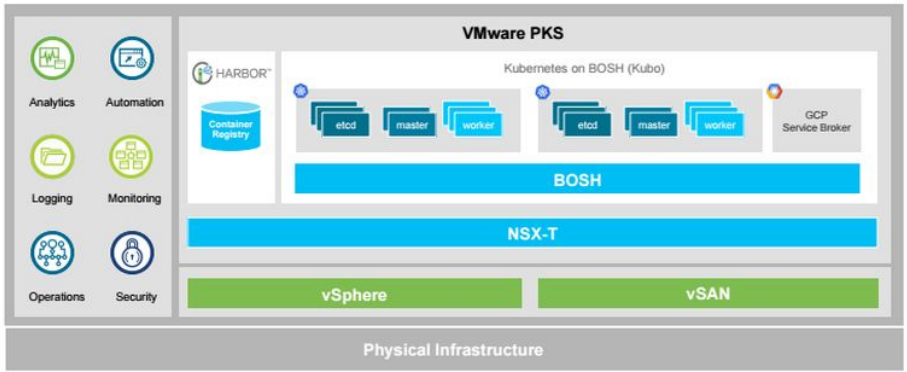


Pivotal Container Service (PKS)

- Enterprise Kubernetes platform
- Based on VMware
- Handles cluster creation, high availability and networking
- Support

- Proof of Concept
- Together with OBS
- Learned a lot
  - Very fast moving
  - More hands on
  - ESA need to have competence

VMware PKS in SDDC Portfolio

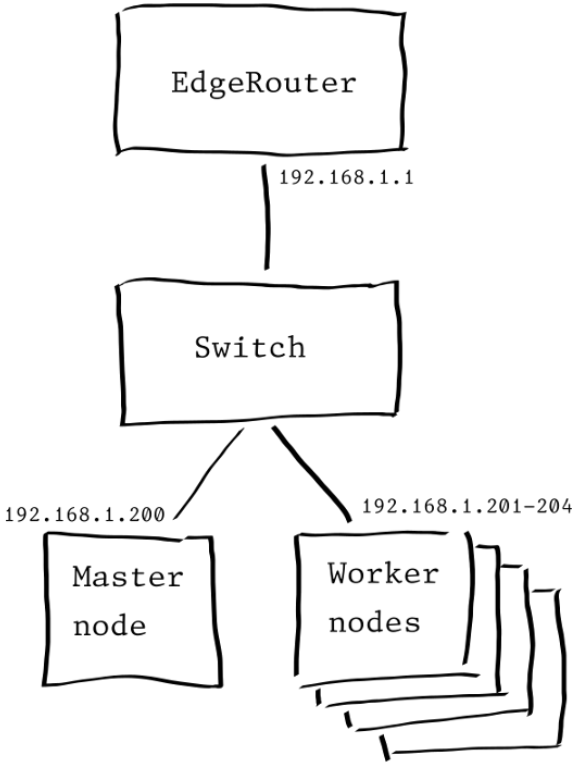


Kubernetes on-premise alternatives

- Red Hat OpenShift
  - Custom version of Kubernetes
  - Enterprise ready
- Rancher 2.0 Kubernetes
  - Deploy to Major cloud and VMware
  - User management and creation
  - Lacks networking/load balancer
- VMware vCloud Container Service Extensions
  - Deploy clusters within ESAcloud organizations
  - Quite simplistic, but seems sufficient for our current state
  - Lacks networking/load balancer

Kubernetes on-premise networking issue

- To get network packets from the external network to pods/services in Kubernetes is a bit hard
- Most development for the “load balancer” plugin happens only for major cloud providers
- Two alternatives:
  - Integrating with on premise SDN (VMware NSX-T)
  - Integrating with a routed network (BGP)
- We have tried to research a foundation on how BGP could work for ESA with CSE.



Kubernetes demo

- Demo a DevOps setup with
  - Version control (git and GitLab)
  - Continuous integration (GitLab CI)
  - Automatic deployment (GitLab CD)
  - Running on Kubernetes with no downtime

What can esait do with this?

- Offer it as a service to users.
  - Perfect for users who just run applications
  - Can free up VMs
  - Less maintenance for users (and security), less VM to keep up
  - Built with automation in mind
  - OPS is very interested
- This is not for everything, but it can be an evaluation for new software projects

Side projects

- DNS
- ESA bootstrap and typefaces
- cloud.esa.int
- bork and kubespace
- Mobile Directory
- Staff Survey Search
- Flexiday

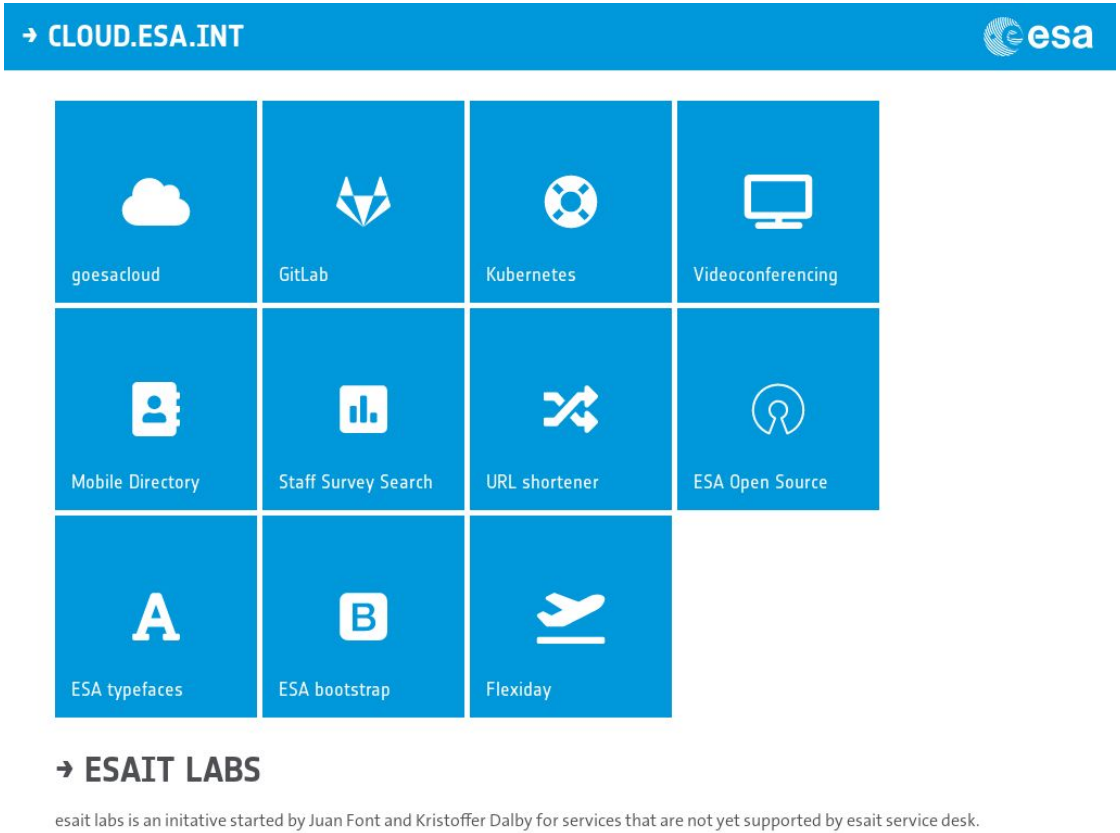
DNS management: cloud.esa.int and it.esa.int

- To support the IaS initiative, we control the whole zones
- Integrated with Terraform for management
- Using RFC2136 for automatic updates
  - Used by Kubernetes
  - Let’s Encrypt
  - Terraform

ESA bootstrap and typefaces

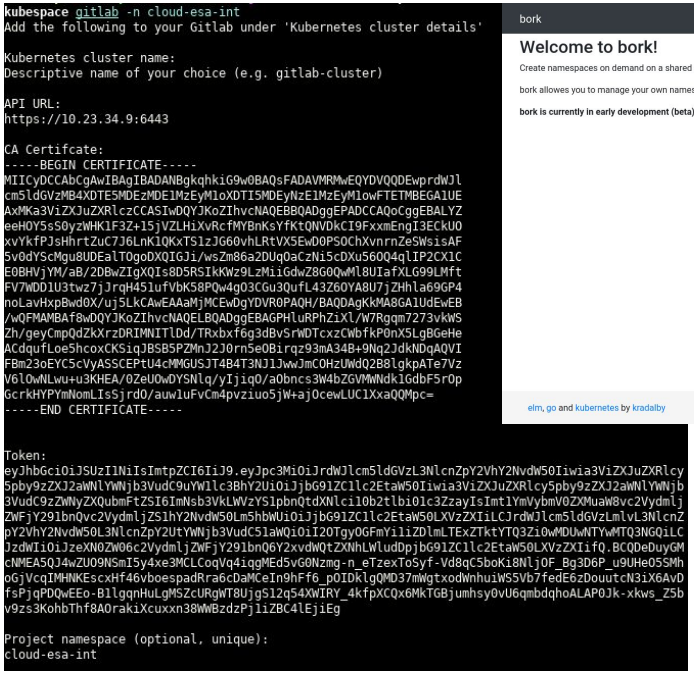
- Follow the ESA Corporate Identity (esa.int/identity)
- Make the “right way” easier than the “half assed way”
- Promote consistent user experience across applications
- Open to the ESA community
- Allow and promote contributions
- Based upon popular frameworks (Bootstrap and NodeJS)

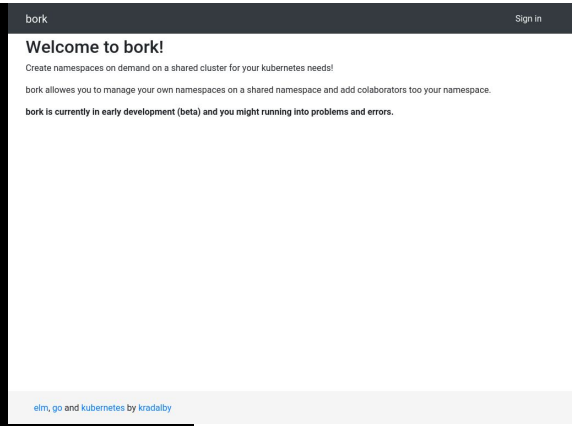
cloud.esa.int landing page



bork and kubespace

- Allow users to share cluster
- Restrict user access
- Automate user management
- Help the user set up DevOps
  - GitLab
  - Drone CI



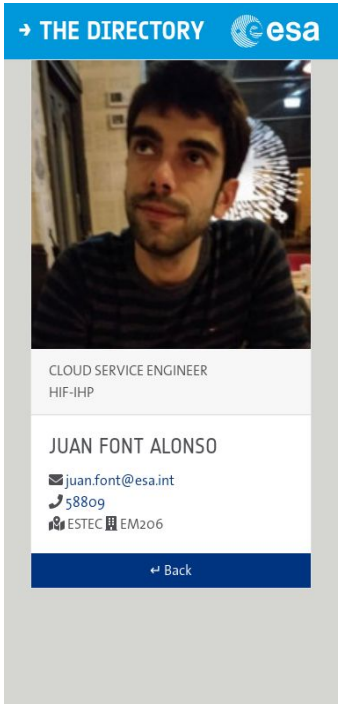


Mobile Directory - d.cloud.esa.int

Mobile friendly version of the ESA Directory

Made by Juan Font

Migrated to ESA Bootstrap for corporate feel



Staff Survey Search - staffsurvey.cloud.esa.int

→ STAFF SURVEY WORDCLOUD

→ STAFF SURVEY WORDCLOUD

one esa

the One-ESA mindset is clearly not there. The tone-at-the-top on this issue should be ensured.

— Answering: *What improvement opportunities do you see in the category "Leadership"*

one esa intranet is very difficult to find information that was once easy to find

— Answering: *Further comments or improvement suggestions regarding the category "Information & Communication"*

Directorates collaborate little with each other. Not one ESA but many little ESAs

— Answering: *What improvement opportunities do you see in the category "Work Processes and Policies"*

We have done serious improvements to link, on the one esa intranet, documents that we couldn't possibly find previously. In addition to that, the fact that communication takes place on Facebook, twitter or Instagram has considerably improved the way esa communicates internally and externally. It is far more dynamic and interactive.

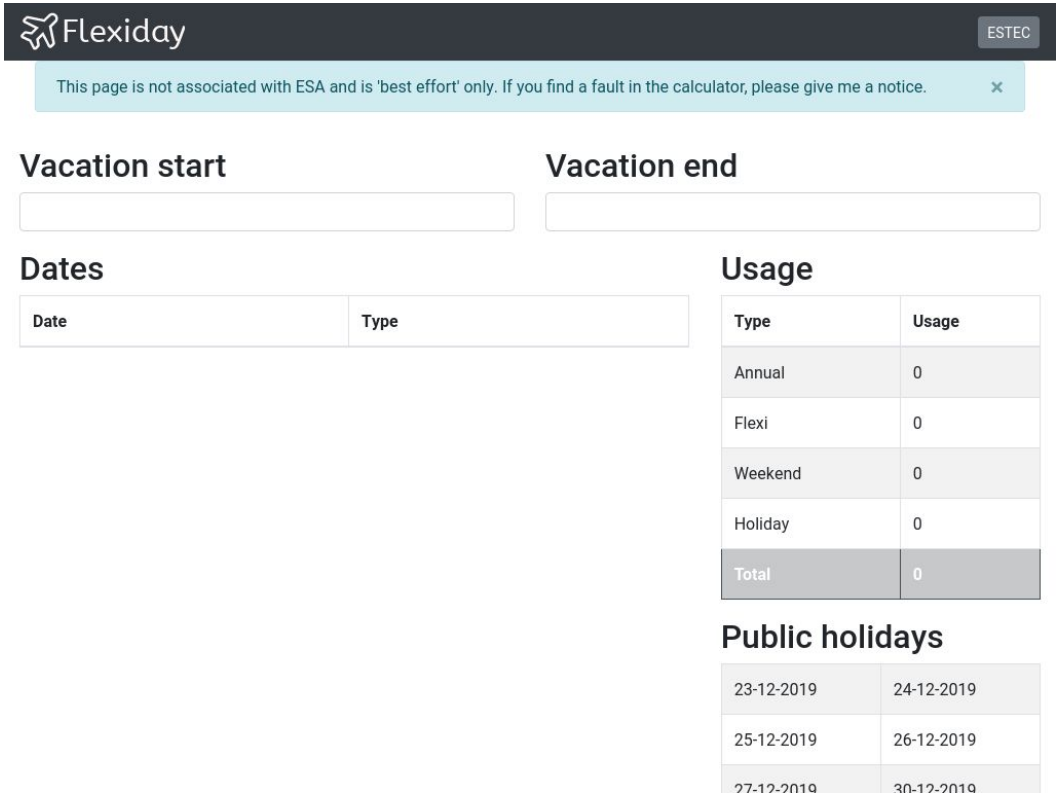
— Answering: *Further comments or improvement suggestions regarding the category "Information & Communication"*

Within ESA staff members are not rewarded equally simply because of their nationality, this does not foster the ONE-ESA approach. Rewards should be independent of once nationality.

ALL QUESTIONS:

WHAT IMPROVEMENT OPPORTUNITIES DO YOU SEE IN THE CATEGORY "MY JOB":

Flexiday - flexiday.kradalby.no



What I think ESA IT could improve?

- Outsourcing is not always the way
  - You cannot outsource the knowledge
  - There should be capacity to do small projects internally
  - R&D and evaluation should be done internally or internally with external support
  - Software development projects should be created on ESA's infrastructure
- Not all projects are suitable for writing all requirements up front
  - Look into doing incremental software projects
  - Possibly even infrastructure projects
  - It is hard to make a project perfect from the beginning
  - Think about Minimum Viable Product
- It does not help to try to avoid vendor lock-in if you look yourself in with many vendors that do not work together

Next move

- Site reliability engineer at G-Research
- SRE’s supports other IT staff with both infrastructure and development knowledge
- London

Keep contact: kradalby@kradalby.no

Questions?