



# (Centralised) Elasticsearch Service

- A bit of History
- Project goals
- Security model
- Cluster management
- Experiences
- Summary

# Elasticsearch at CERN in the past

- ES in use for the last years, also in IT (eg for monitoring)
- Many small clusters around
- Privately run, not always very well managed or secured
- Project to upgrade and **consolidate ES instances** launched in Jan 2016
  - Production status planned for Q1 2017

# Centralised Elasticsearch Service

## Goals:

- Consolidation of various use cases in a single place
  - Spare hardware resources by sharing where possible
- Setup of a reliable service covering as many use cases as possible
- Provide Elasticsearch and Kibana access

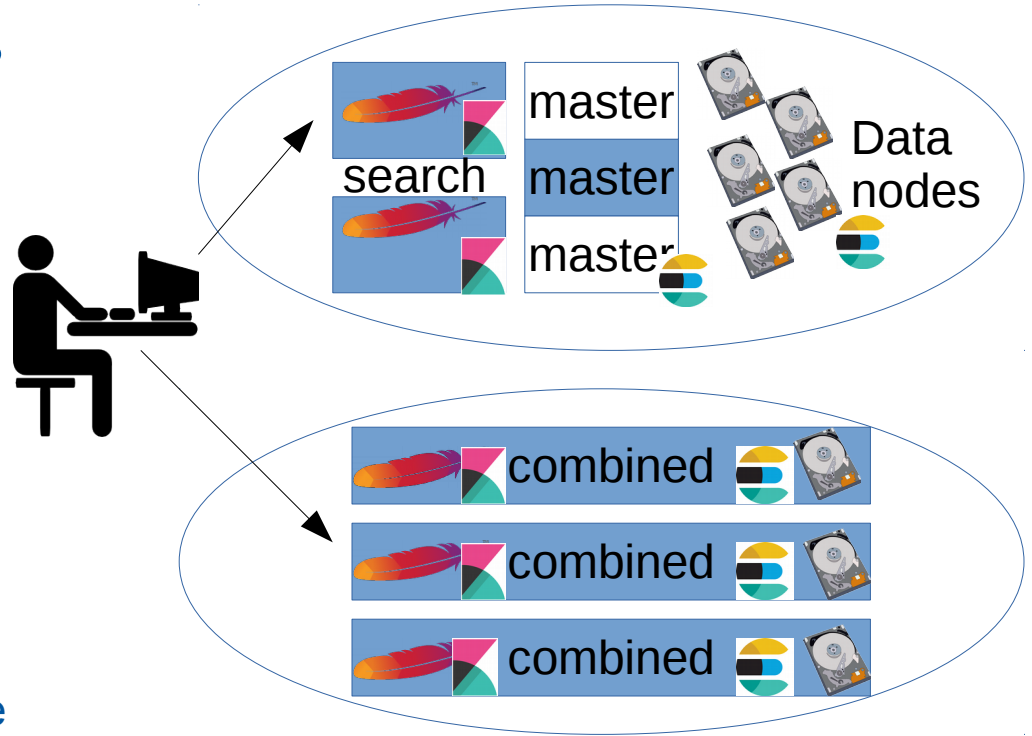
# Centralised ES service: management

## Architecture:

- Full integration into the existing infrastructure
- Puppet managed and monitored as any other cluster
- Shared and dedicated cluster
  - Preferred way is to go via the central monitoring
  - Offer shared clusters for users with public data
  - Dedicated clusters for use cases with sensitive data
- No commercial plugins (including security)

# Node organisation: models in use

- Made to spare resources
- 4 node types:
  - ES Master nodes (3)
  - Search nodes (2+)
    - Http proxy (apache)
    - Kibana services
  - Data nodes (3+)
  - Combined nodes:
    - Master, search and data node
    - For small installations



# Current status, numbers

- Currently **21** independent ES clusters, **30** use cases
- Up to **5** use cases on a single cluster
- Elasticsearch versions ranging from **2.3.3** to **5.1.1**
- Kibana versions **4.5.1** to **5.1.1**
  - Plugins and version configurable by cluster
  - Allows to upgrade at different speed, as needed by the users

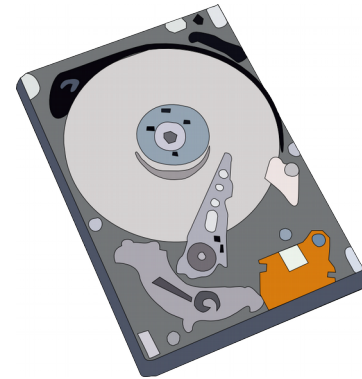
# Hardware

## Virtualized hardware

- Higher flexibility and better resource consolidation
- Allows to give smaller nodes to small use cases
- Allows for rapid access and replacement
- **114** VMs for search, master and combined nodes

## Work horse for data nodes:

- Virtualised data nodes on special hypervisors
- Spinning disks with SSD cache (b-cache)
- 630GB/60GB RAM per full node
- Use full or half nodes (315GB/30GB RAM), **115** nodes in use





# Security model and access

## Access SSL only

- 443 Kibana, via CERN SSO
- Possibility to have read-only Kibana access  
(ES 2.X only, via readonlyrest plugin)
- Port 9103 REST access with basic authentication
- Java API is in general closed
- For shared clusters no access to ES plugins (head, ...)
- Firewall rules to separate clusters from each other
- Different access pattern rules for different entry points into the same cluster

# Cluster management

## Automation and monitoring:

### – Automated work flows

- Cluster restart, Kernel upgrades
- ES updates
- Adding/removing data nodes
- ...

### – Self-monitoring

- Kibana dashboard with health and account information

The screenshot displays the Rundeck web interface. At the top, the 'RUNDECK' logo is visible. Below it, there's a navigation bar with 'Jobs (6) Filter' and 'Expand All Collapse All' options. A 'Job Actions' button is on the right. The main content area shows a list of job steps under a 'steps' folder:

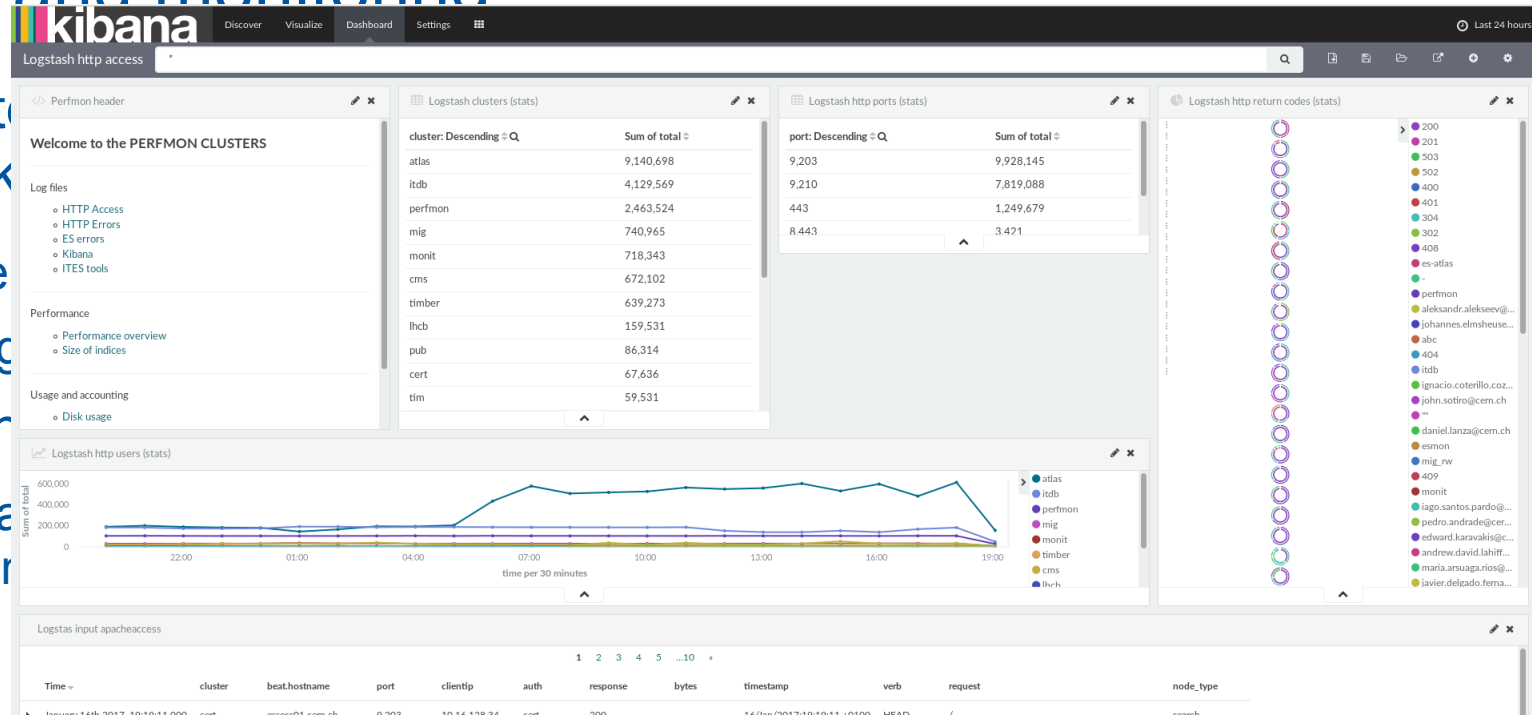
- [Get esmon Kerb ticket for rundeck](#)
- [Kill or reboot VM](#) - Use 'ai-kill-vm' or 'openstack server reboot' on the selected nodes after setting the OpenStack environmental variables.
- [Refresh firewall rules on selected cluster](#) - Run Puppet on the selected cluster limited to the firewall tagged resources. [More >](#)
- [Restart elasticsearch](#) - Run Puppet on the selected cluster and restart elasticsearch. [More >](#)
- [Add node to cluster](#) - Moves selected nodes from spare to the target subhostgroup based on cluster name and node type. [More >](#)
- [Drain and freboot/removel node](#) - Drains and removed node

Below the steps, there's an 'Activity for Jobs' section with filters for 'running', 'recent', 'failed', and 'by you'. At the bottom, there's a footer with the text: 'esops001.cern.ch 18', 'Rundeck 2.7.1-1 "cafecito steelblue leaf" 2016-12-03', and '© Copyright 2016 #SimplifyOps. All rights reserved. Licenses'.

# Cluster management

## Automation and monitoring:

- Automate
- Rundeck
- Cluste
- Adding
- Self-mor
- Kibana
- accour



# Automation and

## Automated Rundeck

- Clusters
- Adding

## Self-monitoring

- Kibana  
accounts



Logstash http access

Perfmon header

Welcome to the PE

Log files

- HTTP Access
- HTTP Errors
- ES errors
- Kibana
- ITES tools

Performance management

- Performance overview
- Size of indices

Usage and accounting

- Disk usage

Logstash http users



Logstash input apache

Time

information > Navigate Catalog

Overview 16 Jan, 2017 19:1

graded ⊘ Service Unavailable ✔

### Desktop Services

✔ Windows

### Development

✔ Git

✔ JIRA

✔ SVN

### Documentation

✔ CDS

### Engineering

✔ Electri

✔ Mathe

✔ Mecha

### GRID Services

✔ File Tr

✔ GRID

✔ GRID

✔ GRID

✔ MyPro

✔ VOMS

Normal since: 14 Jan 2017 00:20

[Link to availability history](#)

### Details:

acron:https://es-acron.cern.ch: green  
alice:https://es-alice.cern.ch: green  
atlas:https://es-atlas.cern.ch: green  
cert:https://es-cert.cern.ch: green  
cms:https://es-cms.cern.ch: green  
cms:https://es-cmsdt.cern.ch: green  
gitlab:https://es-gitlab.cern.ch: green  
itdb:https://es-itdb.cern.ch: green  
landb:https://es-landb.cern.ch: green  
lhcb:https://es-lhcb.cern.ch: green  
licmon:https://es-licmon.cern.ch: green  
mig:https://es-mig.cern.ch: green  
monit5:https://es-monit5.cern.ch: green  
monit:https://es-monit.cern.ch: green  
perfmon:https://es-perfmon.cern.ch: green  
pub5:https://es-pub5.cern.ch: green  
pub5:https://es-teigi.cern.ch: green  
pub5:https://es-es-lhcb5.cern.ch: green  
pub:https://es-bmkgw.cern.ch: green  
pub:https://es-vc.cern.ch: green  
pub:https://es-inspire.cern.ch: green  
pub:https://es-puppetdb.cern.ch: green  
pub:https://es-patstat.cern.ch: green  
scada:https://es-scadastats.cern.ch: green  
scada:https://es-anodet.cern.ch: green  
timber:https://es-timber.cern.ch: green  
tim:https://es-tim.cern.ch: green  
tim:https://es-diamon.cern.ch: green  
wslogs:https://es-wslogs.cern.ch: green

### Infrastructure Application Services

✔ Indico Event Application Support

### Interactive Services

✔ LXPLUS

✔ Windows Terminal Servers

### IT Infrastructure Services

✔ ACRON

✔ Centralised Elasticsearch

✔ Configuration Management

✔ Linux Operating System

✔ Load Balancing

✔ Messaging

✔ Monitoring

✔ Server Provisioning

### Network Services

✔ Campus Network

✔ CIXP

✔ Datacenter Network

✔ Network Database and Registration

✔ Network for Projects and Experiments

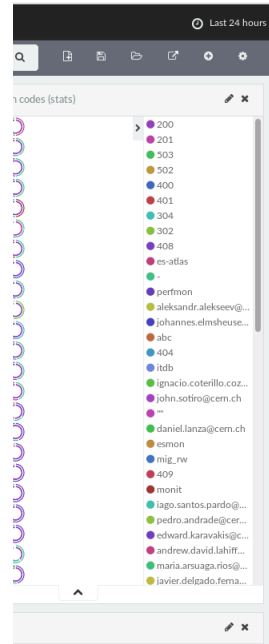
✔ Technical Network

✔ WIFI

✔ WLCG Network

### Printing Services

✔ Printing and Copying



# Experiences so far

- ES is very flexible and dynamic
- User expectations follow that pattern closely ...
- Hard to fit everybody with a single solution
  - Hence split into independent clusters
  - Also for performance reasons
- Resource consolidation tricky
  - Requires good control of ACLs
  - Work in progress



[www.cern.ch](http://www.cern.ch)