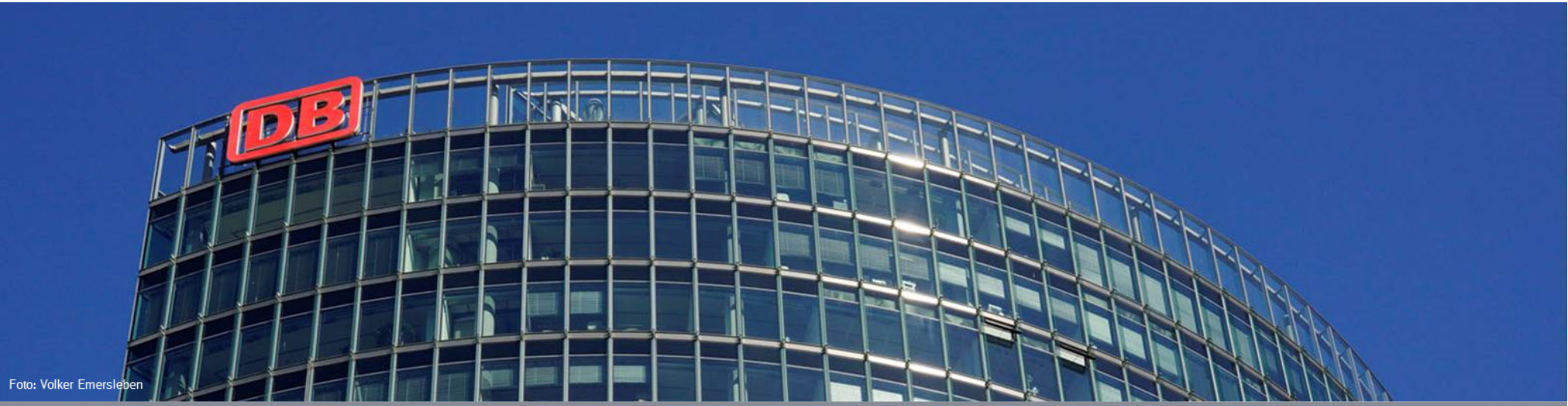


OpenShift auf AWS

Ein Erfahrungsbericht

DB Systel GmbH | Holger Koch | I.LVD83 | 18.09.2017

DB Systel
Digital bewegen. Gemeinsam.

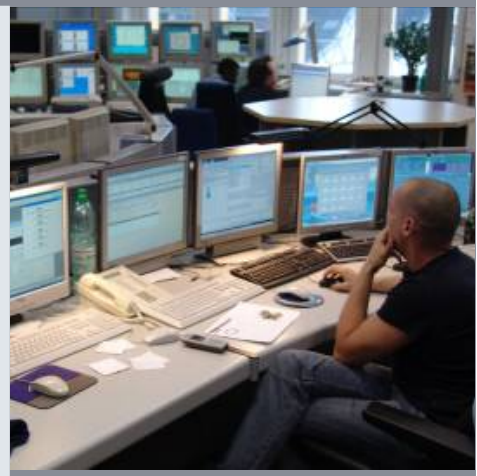
Der Vortragende

Über mich:

- Holger Koch
  „Innovation and Community Manager“
- Mitarbeiter DB Systel – D.IDP 62
- Meine Aufgabengebiete
  - Automatisierung
  - Cloud und Container
  - Open Source Evangelist

DB Systel – Das Unternehmen

Daten & Fakten



Wir sind:

- 4000 Mitarbeiter an den drei Standorten Frankfurt/Main, Berlin und Erfurt

Wir betreiben:

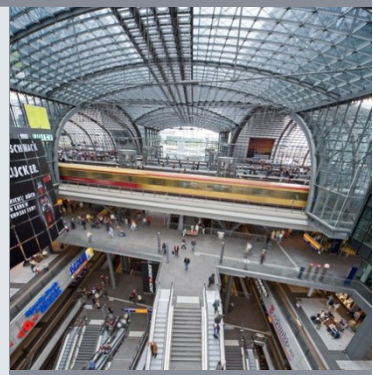
- 3 Rechenzentren mit über 3.800 Servern
- Datennetz mit rund 342.000 IP-Anschlüssen von DSL bis Breitband-Glasfaser
- Rund 600 produktive IT-Verfahren
- 3 Petabyte Plattenspeicher / 7 Petabyte Backup-Kapazität
- 500 IT-Anwendungen für den DB Konzern

Wir betreuen bei der Bahn:

- 96.000 Nutzer des Bürokommunikationssystems der Bahn
- 93.000 VoIP-Anschlüsse

Die Deutsche Bahn AG – Daten und Fakten

Geschäftsfelder in Zahlen



Personenverkehr

- 25.000 Personenzüge pro Tag, 2,7 Milliarden Reisende pro Jahr
- 260 ICE Züge / jeder fährt rechnerisch pro Monat einmal um die Welt
- 9 Nachbarländer sind mit der DB ohne Umsteigen erreichbar

Netze

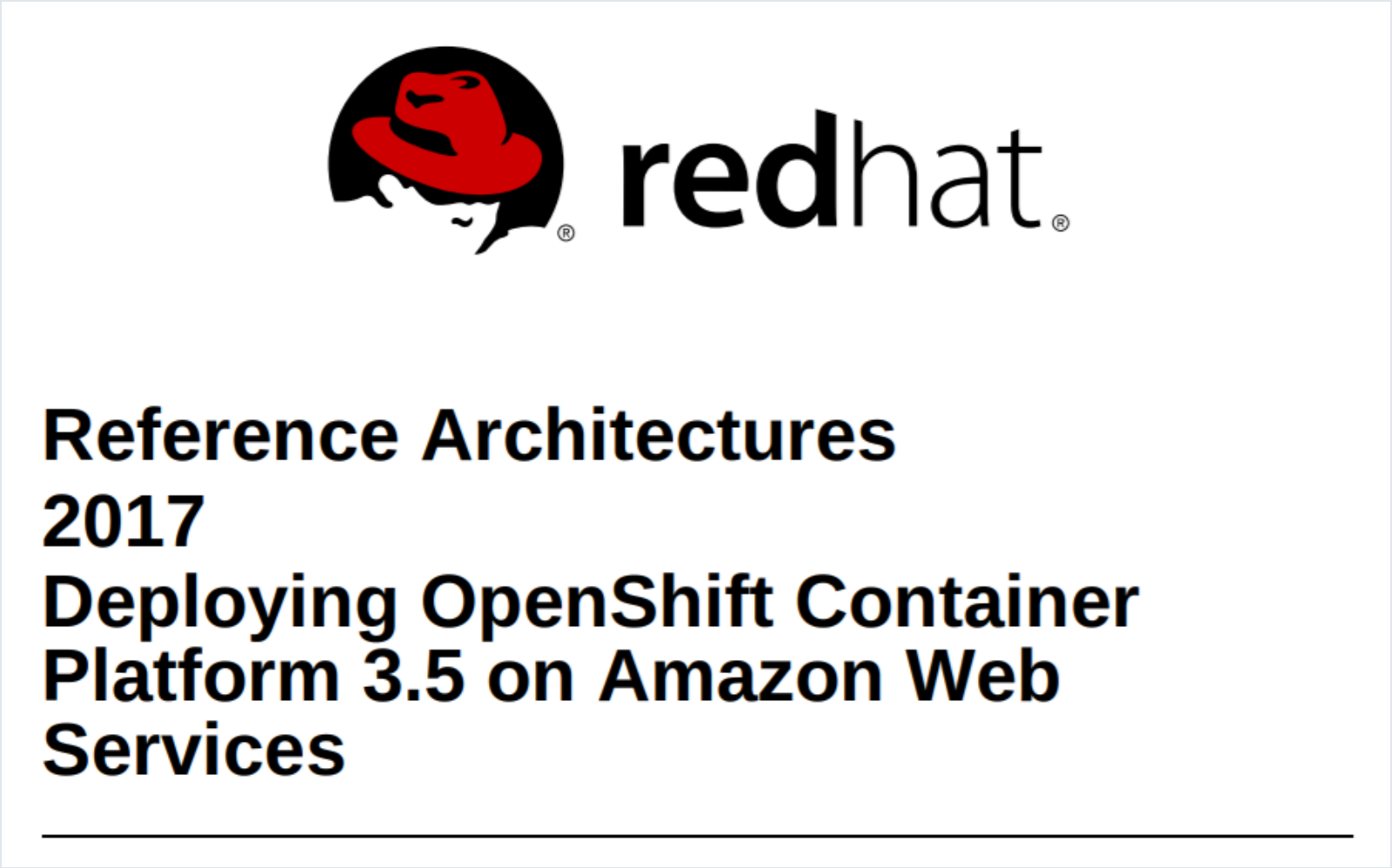
- 5.700 Bahnhöfe
- 33.300 km Streckennetz / dreimal so lang wie die deutschen Autobahnen
- 48.800 beheizte Weichen von insgesamt 70.000
- 5. größter Energieversorger in Deutschland

Transport & Logistik

- Zweitgrößter Transport- und Logistikanbieter der Welt
- über 2.000 Standorte in über 140 Ländern
- 400 Millionen Tonnen beförderte Güter auf der Schiene pro Jahr
- 99 Millionen Sendungen im europäischen Landverkehr pro Jahr
- 7 Millionen Quadratmeter Lagerfläche weltweit

OpenShift auf AWS?

OpenShift auf AWS - Standardinstallation



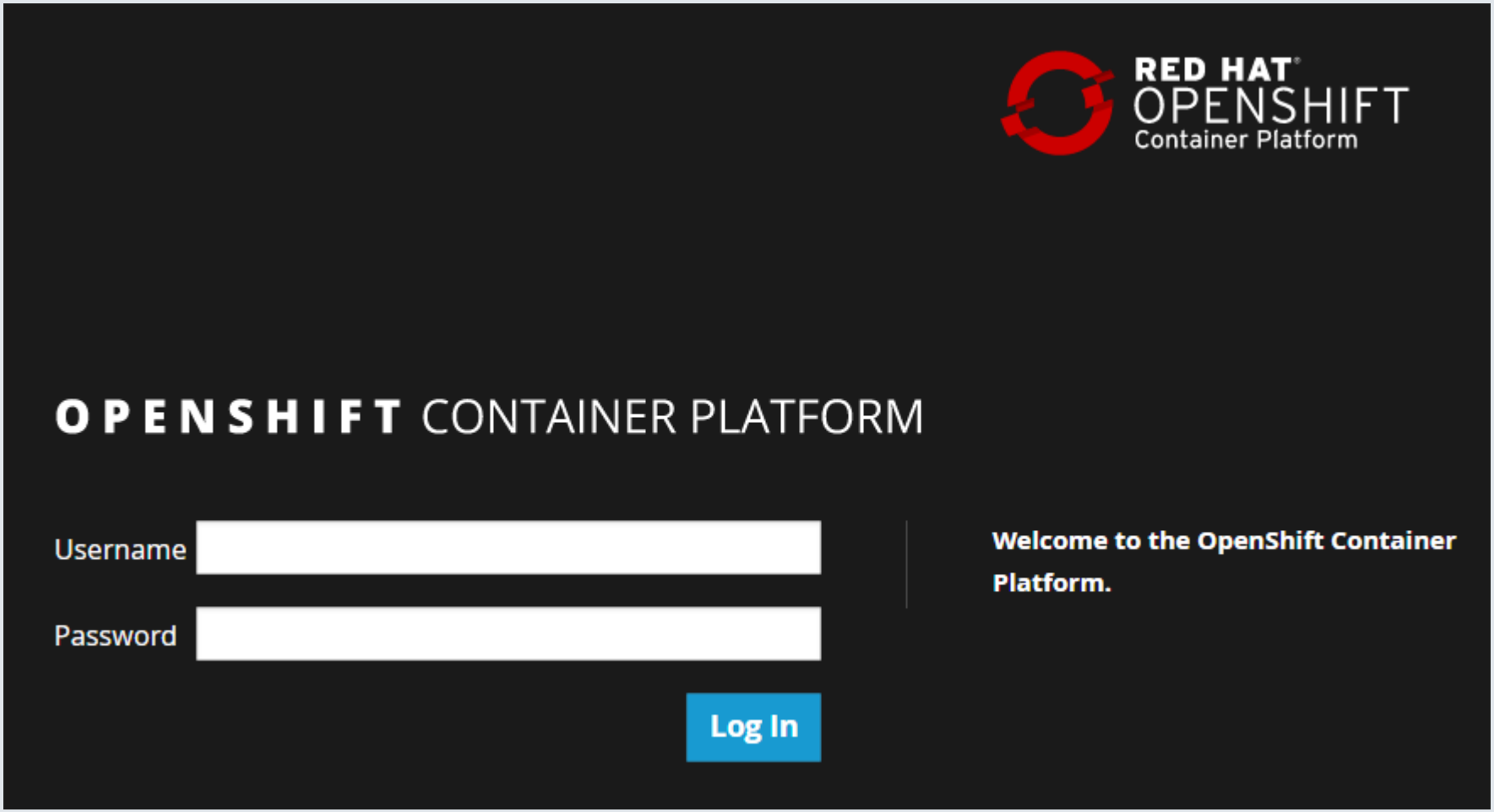
OpenShift auf AWS - Standardinstallation

```
$ git clone https://github.com/openshift/openshift-ansible-contrib.git
$ export AWS_ACCESS_KEY_ID= ...
$ export AWS_SECRET_ACCESS_KEY= ...
$ openshift-ansible-contrib/reference-architecture/aws-ansible/ose-on-aws.py --create-vpc=no --vpc-id=123 --deployment-type=openshift-enterprise ....ganz viele weitere Parameter
```

OpenShift auf AWS - Standardinstallation

Nach einer Stunde...

OpenShift auf AWS - Standardinstallation



OpenShift auf AWS - Standardinstallation

OpenShift auf AWS - Standardinstallation

Ja, das war wirklich alles...

...wenn man einen Standard AWS Account hat.

Und wer hat das schon!!!

OpenShift auf AWS – Warum die Standardinstallation nicht funktionierte

- vorgegebenes VPC Design
- kein Route53, sondern eigenes DB DNS
- der Installer fragt direkt Configitems bei AWS ab
- kein direkter Internetzugriff möglich, alles nur per Proxy
- Subscriptions, Subscriptions, Subscriptions
- …

OpenShift auf AWS – Lösungsansatz

Installation wird aufgesplittet in:

1. Bereitstellung der Infrastruktur mit openshift-ansible-contrib (Brownfield)
2. Advanced Installation mit ansible und Inventory

OpenShift auf AWS - Lösungsansatz

```
$ vi reference-architecture/aws-ansible/playbooks/openshift-install.yaml


- include: ../../../playbooks/prerequisite.yaml
# - include: openshift-setup.yaml
```

Bereitstellung Infrastruktur – vorgegebenes VPC Design

- Freischaltung „Golden Image“ für dieses VPC
- manuelles Anlegen der Netze (3 private, 3 public)
- Routing konfigurieren
- Route53 Private Hosted Zone anlegen
- Anpassen DHCP Option Set
- IAM User anlegen

Bereitstellung Infrastruktur – Anpassen openshift-ansible-contrib

Problem: Route53 darf nicht verwendet werden

- Einträge aus Route53 mit cli53 auslesen
- mit dns-soap-api im DB DNS einzupflegen
- ansible Rolle erstellen und konfigurieren

Bereitstellung Infrastruktur – Anpassen openshift-ansible-contrib

Problem: kein direkter Zugriff auf das Internet

- ansible Rolle um Proxy in diversen Konfigdateien zu setzten

Bereitstellung Infrastruktur – Anpassen openshift-ansible-contrib

anpassen brownfield.json.j2

- ELB auf „internal“
- verwenden des „richtigen“ Hostnamen

  „CanonicalHostedZoneNameID“ <-> „DNSName“
- „PrivateIp“ anstelle „PublicIp“
- …

Bereitstellung Infrastruktur – Anpassen openshift-ansible-contrib

anpassen playbooks/vars/main.yaml

- cidr_block
- subnet_blocks
- Proxy setzen

Bereitstellung Infrastruktur – Wie viele Server und welche?

kleines Quiz:

1. Aus wie vielen Servern, besteht der kleinste, sinnhafte OpenShift Cluster?

14! Ansible Host, Bastion Host, 3xMaster, 3xInfra, 6xWorker

2. Wie viel Speicher und CPU sollten die Worker haben?

r4.2xlarge: 8 CPU, 61 GB RAM

Bereitstellung Infrastruktur - Brownfield

```
$ export AWS_ACCESS_KEY_ID= ...
$ export AWS_SECRET_ACCESS_KEY= ...
$ openshift-ansible-contrib/reference-architecture/aws-ansible/ose-on-aws.py --create-vpc=no --vpc-id=123 --deployment-type=openshift-enterprise ....noch viel, viel mehr Parameter
```

30 Minuten später...

Bereitstellung Infrastruktur – Brownfield

Ergebnis:

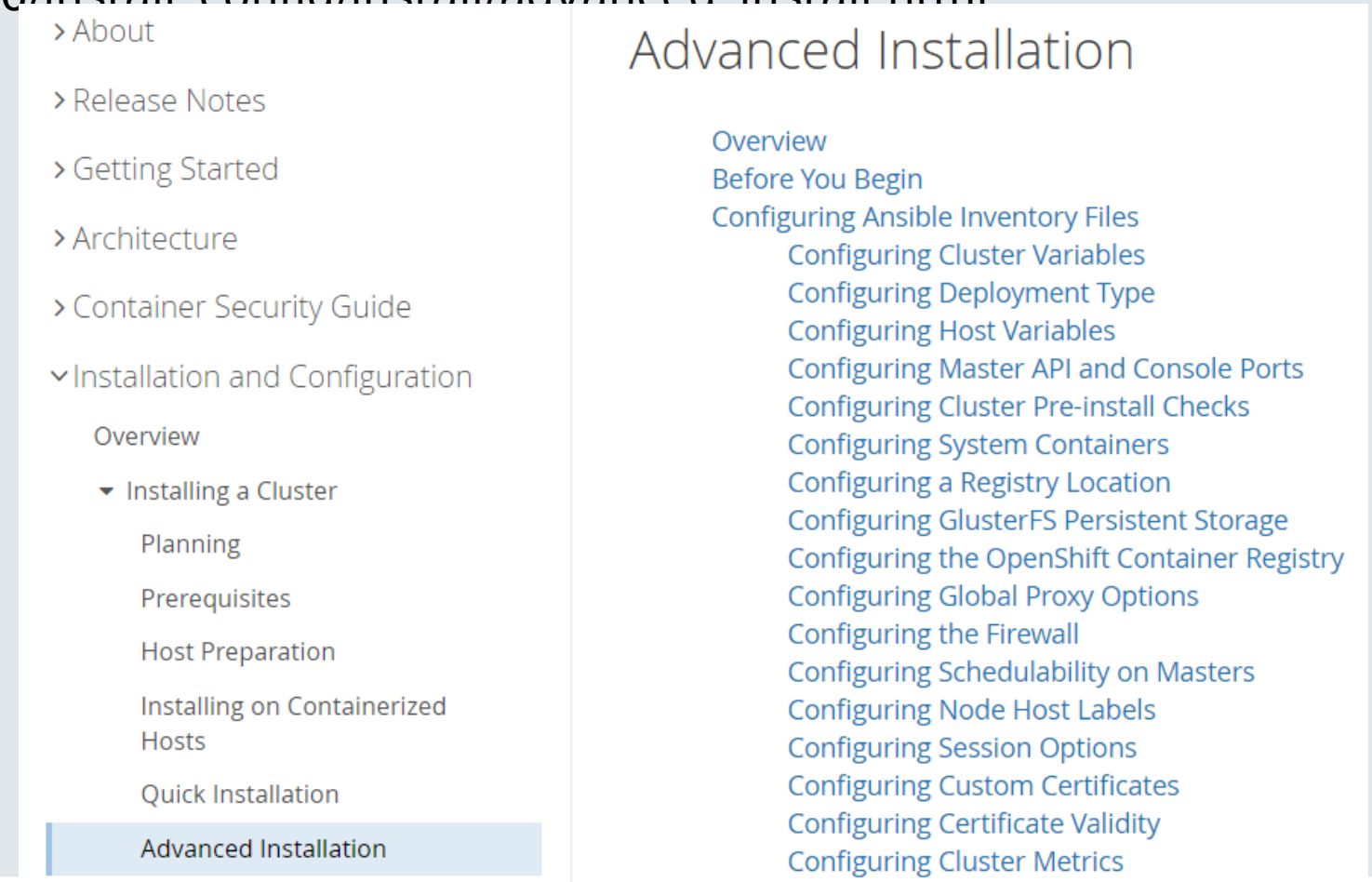
- Security Groups angelegt
- Storage angelegt
- EC2 Server bereitgestellt
- Server bei Redhat subscripiert

2. Teil

Advanced Installation

Advanced Installation

https://docs.openshift.com/container-platform/3.6/install_config/install/advanced_install.html



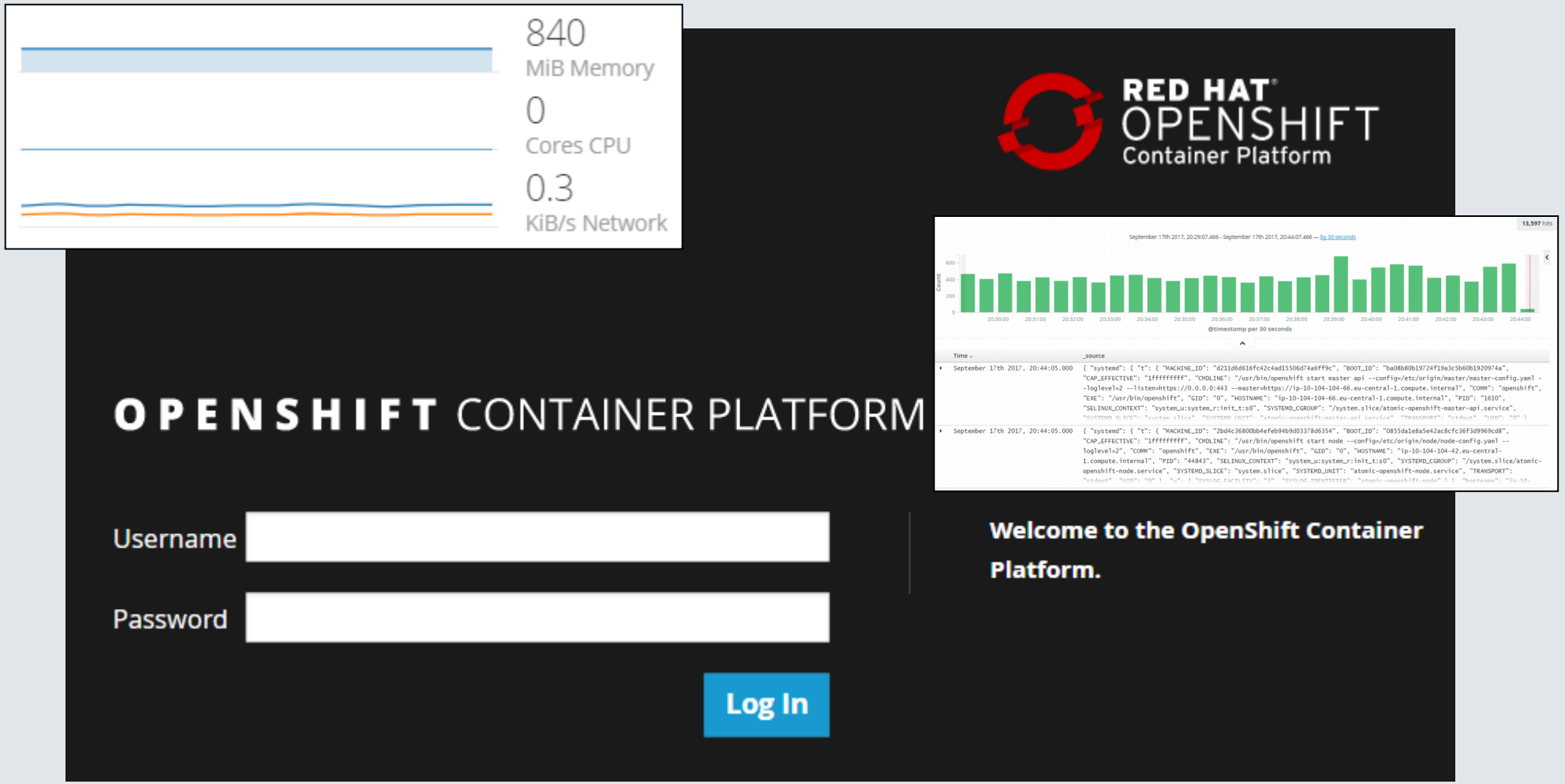
Advanced Installation – Inventory

- Shellskript und Template zur Generierung Inventory File
- [illegible] der Advanced Installation

```
$ ./generate_ansible_inventory
$ ansible-playbook /usr/share/ansible/openshift-ansible/playbooks/byo/config.yml
```

45 Minuten später...

Advanced Installation



Advanced Installation

Offene Punkte:

- Subscription nach Pool ID
- Default Router Deployment
- persistent Storage mit EFS
- ...

Fragen?

Mobility Networks Logistics

Holger Koch

D.IPD62

Tel. +49 361 300 5957
Mobil +49 151 628 45 902
holger.koch@deutschebahn.com

DB Systel GmbH
Schlachthofstraße 80
99098 Erfurt
www.dbsystel.de