Radical Agility with Autonomous Teams and Microservices

jan.loeffler@zalando.de / @jlsoft2 GOTO Copenhagen 2015-10-06

Zalando



We shape our buildings; thereafter they shape us



Conway's Law

"organizations which design systems ... are constrained to produce designs which are copies of the communication structures of these organizations"



AN ARCHITECTURE FOR INNOVATION





STREET STYLES >

1 TREND, 2 LOOKS>





A BRIEF HISTORY OF ZALANDO TECHNOLOGY











li.











DELIVER AMAZING PRODUCTS **EFFICIENTLY AT** SCALE, AND **FEELING GREAT** ABOUT IT.

PURPOSE - AUTONOMY - MASTERY



AUTONOMY THE DESIRE TO BE SELF DIRECTED



You want to know *the difference* between a master & a beginner?



The master has failed more times than the beginner has even tried.



The Surprising Truth About What Motivates Us

DRIVE

The Surprising Truth About What Motivates Us

Daniel Pink



FROM **CONTROL** & COMMAND **TO PURPOSE** AND TRUST









OKR



API FIRST

REST



MICRO SERVICES

CLOUD

OPEN SOURCE










Inumethod JalseSwap. x:

and and the of the sector of

falseSwap(int x, int y)

C.J. method falseSwap. ns.a:"+a+"b:"+

+ a +

the make improve public class PrimitiveParameters

Thin metrical public static void ac

moreParametecenter void manusuum(+marga)-("Intme@id (dornePararDeters and a series of a Sent a frank to be a

Replace and excelled for real

public class PrintiveParameters

photo pratic, voic main (Setting] arge)

++ a. Ity - 2 b: in method spaceRacameters a amount and bar TalseSwap(x,y): * System.out.printing "in method go PROFINED IN THE R. 4 moreParameters (k,y): 1 Interferent E.A.T.: Second address in method more administration, p. 7, Aug. 7, b. 7 - 6 bit.

static void main (String[] args) public static void falseSwap(int x, int y) (System.out.println("in method faiseSwap, x: *** int temp = x;

 Y: static void go(v = temp: pairs wats with branding the is the gift Donan automatical maked tetraheap, a 7 a 4 a 7 a

68.83.

pairs wate out waterwaters in a, in \$1. Design and printing the implication of the printing of the state of the State State Separate protection method monthstanders, at " + a + " b. " + b."

old...main

Manufacture and and service and and

printer("in method most interfectors reprinter in method of a \$5,000 " or " a site

static wold got 3

state (Star Weld (String () args) System as protection method manufactures a " + a + " b " + b"

explains in method ge. o * -Contractor in the set of

> taxadiment in the up d falseDeep, x: " + x + " y; " + y);

IN SHITE 2.5.86 System.out.printin("in method go. s. * . 92 falseSwap(x,y); System.out.printin("in method go, au moreParameters (x,y); System.out.printin("in method po.

the cost of world main [String]] (rgs)

public static void talesSwapp(int x, int y) (System.out.printin ("in method fall and all a int temp + 1 x - y₁ y - temp; System out printe ["in inte

public static gold morePagements(int a, int System out printing in a good in



STUPS.io

STUPS To Unleash Penguin Swarms

STUPS COMPONENTS







Deployment with Docker



Managed SSH Access

REST / OAuth 2.0 mandatory

















Pier One Docker Registry









https://github.com/zalando/spilo



Highly available open-source PostgreSQL appliance

Spilo



STUPS COMPONENTS



Try STUPS.io https://stups.io https://docs.stups.io



All components are **Open Source** https://github.com/zalando https://github.com/zalando-stups



Jan Löffler

- Head of Platform Engineering
- Twitter: @jlsoft2
- jan.loeffler@zalando.de
- http://www.slideshare.net/jlsoft/

We shape our buildings; thereafter they shape us

STUPS website & docs https://stups.io https://docs.stups.io



All components are **Open Source** https://github.com/zalando https://github.com/zalando-stups

BACKUP

MILLIARDEN EURO Nettoumsatz 2014 50%

Retourenquote

und Kategorien

über alle Märkte



Besuche der Website pro Monat

ÜBER über 150.000 6 Artikel ^{ÜBER} 1.500 9.000+ aktive Marken Mitarbeiter in Kunden Deutschland 15 Länder





FROM zalando/openjdk:8u40-b09-4

EXPOSE 8080

COPY target/hello-world.jar /
COPY target/scm-source.json /

DOCKER BUILD & PUSH

```
$ docker build -t √
```

pierone.example.org/myteam/hello-world:0.2 .

\$ pierone login
Getting OAuth2 token "pierone".. OK
Storing Docker client configuration in ~/.dockercfg.. OK

\$ docker push pierone.example.org/myteam/hello-world:0.2

VERIFY IMAGE UPLOAD

\$ pierone tags myteam hello-world

Team	Artifact	Тад	Created By
myteam	hello-world	0.1-andre-test	13d ago ahartmann
myteam	hello-world	0.1	3d ago ahartmann
myteam	hello-world	0.2	3m ago hjacobs

SENZA: DEFINITION YAML

SenzaInfo:

StackName: hello-world

Parameters:

- ImageVersion:

Description: "Docker image version of Hello World."

SenzaComponents:

- Configuration:

Type: Senza::StupsAutoConfiguration # auto-detect network setup

- AppServer: # will create a launch configuration and ASG with scaling triggers

```
Type: Senza::TaupageAutoScalingGroup
InstanceType: t2.micro
SecurityGroups: [app-hello-world]
ElasticLoadBalancer: AppLoadBalancer
TaupageConfig:
runtime: Docker
source: "stups/hello-world:{{Arguments.ImageVersion}}"
ports:
8080: 8080
```

\$ senza create hello-world.yaml 1 0.2 Generating Cloud Formation template.. OK Creating Cloud Formation stack hello-world-1.. OK

\$ senza events hello-world.yaml 1

Stack M	Name Ver	. F	Resource Type	Resource ID	Status	Status	Reason	Event	
Time									
hello-v	world 1	1	CloudFormation::Stack	hello-world-1	CREATE_IN_PROGRESS	User Ir	nitiated	10 m	ago
• • •									
hello-v	world 1	1	CloudFormation::Stack	hello-world-1	CREATE_COMPLETE			6 m	ago

- docker run -d --log-driver=**syslog** 🚽
 - --restart=on-failure:10 🚽
 - -e DB_SUBNAME=.. 🚽
 - -v /meta:/meta:ro 🚽
 - -e CREDENTIALS_DIR=/meta/credentials 4
 - -p 8080:8080 -p 7979:7979 🗸
 - -u 999 🗸

pierone.example.org/stups/pierone:0.5

SENZA: MANAGE STACKS

∼ \$ senza list						
Stack Name	Ver.	Status		Crea	ated	Description
essentials	b10	CREATE	COMPLETE	3d	ago	Essentials (ImageVersion: 0.1.0-SNAPSHOT)
even	b29	CREATE	COMPLETE	10d	ago	Even (ImageVersion: 0.3-SNAPSHOT)
fullstop	b8	CREATE	COMPLETE	2h	ago	Fullstop version 0.6
hello-world	1	CREATE	COMPLETE	47h	ago	Hello World ()
kio	b35	CREATE	COMPLETE	47h	ago	Kio (ImageVersion: 0.1.0-SNAPSHOT)
mint-storage	b12	CREATE	COMPLETE	8d	ago	Mint Storage (ImageVersion: 0.1.0-SNAPSHOT)
pierone	b19oauth	CREATE	COMPLETE	27h	ago	Pierone (ImageVersion: 0.2-SNAPSHOT)
pierone	b20	CREATE	COMPLETE	3h	ago	Pierone (ImageVersion: 0.1-SNAPSHOT)
swagger	b6	CREATE	COMPLETE	10d	ago	Swagger (ImageVersion: 0.4-SNAPSHOT)
twintip-crawler	b9	CREATE	COMPLETE	8d	ago	Twintip Crawler (ImageVersion: 0.1.0-SNAPSHOT)
twintip-storage	b15	CREATE	COMPLETE	8d	ago	Twintip Storage (ImageVersion: 0.1.0-SNAPSHOT)
vivi	2	CREATE	COMPLETE	24h	ago	Vivi version 0.1
yourturn	b51	CREATE	COMPLETE	3h	ago	YourTurn version 0.24-SNAPSHOT
zmon-agent	1	CREATE	COMPLETE	15m	ago	Zmon Agent (AgentVersion: 0.5)
zmon-appliance	22	ROLLBAC	K_COMPLETE	40m	ago	Zmon Appliance (AgentVersion: 0.5, WorkerVersion: 0.8, SchedulerVersion: 0.2
zmon-appliance	23	CREATE_	COMPLETE	18m	ago	Zmon Appliance (WorkerVersion: 0.8, SchedulerVersion: 0.2)
~ \$ senza insta	nces pier	one				
Stack Name Ver.	Reso	urce ID	Instance I	D Pub	olic	IP Private IP State LB Status Launched
pierone b20	AppS	erver	i-cb242e2d			172.31.160.20 RUNNING IN_SERVICE 3h ago
pierone b20	AppS	erver	i-db18023c			172.31.159.168 RUNNING IN_SERVICE 3h ago
pierone b190	auth AppS	erver	i-dfd6de39			172.31.168.182 RUNNING IN_SERVICE 27h ago
pierone b190	auth AppS	erver	i-fe649654			172.31.134.149 RUNNING IN_SERVICE 27h ago
~ \$ senza statu	s pierone			_		
Stack Name Ver.	Stat	us	Inst.#	Runn	ning	Healthy LB Status HTTP Main DNS
pierone b190	auth CREA	TE_COMPL	ETE 2		2	2 IN_SERVICE OK no
pierone b20	CREA	TE COMPL	ETE 2		2	2 IN SERVICE OK yes


docker run .. --log-driver=syslog ..

/etc/logrotate.d/.. Don't forget log rotation..

APPLICATION LOGS: TAUPAGE SUPPORTS LOGENTRIES AND SCALYR



May 21 11:58:39 ip-172-31-160-20 docker/800488d94562[781]: INF0 [qtp676538195-May 21 11:58:40 ip-172-31-160-20 docker/800488d94562[781]: INF0 [qtp676538195-May 21 11:58:40 ip-172-31-160-20 docker/800488d94562[781]: INF0 [qtp676538195-

0 [qtp676538195-38] [PUT /v1/images/73d7a3416ad5d82fa704fa1e744a7cf27bd429b9b0c622c9aa9f05e9833b99f4/layer <- 94.13 0 [qtp676538195-31] [PUT /v1/images/095e2250b67a92908ce0802a9738cd75427f16de64128f48dbeb0b6f20fa5ccd/layer <- 94.13 0 [qtp676538195-71] [PUT /v1/images/b3b59818883e859bcf55eaaedf657b02cbc75eb0df0a15127bfb2de39b695b3/layer <- 94.13



SSH ACCESS: TIME-LIMITED ACCESS TO ANY TEAM SERVER

∼ \$ senza instances pierone b20					
Stack Name Ver. Resource ID Instance ID Public IP	Private IP	State LB	Status L	aunched	
pierone b20 AppServer i-cb242e2d	172.31.160.20	RUNNING IN	SERVICE	4h ago	
pierone b20 AppServer i-db18023c	172.31.159.168	RUNNING IN	SERVICE	4h ago	
~ \$ piu 172.31.160.20 "debug my instance"					
Please enter password for encrypted keyring:					
Requesting access to host 172.31.160.20 via odd-e	u-west-1.	for	^r hjacobs.		
Access to host odd-eu-west-1.	for use	er hjacobs v	vas grante	d.	
You can now access your server with the following	command:				
ssh -tA hjacobs@odd-eu-west-1. ssh	 o StrictHostKey 	Checking=no	o hjacobs@	172.31.160.20	
~ \$ ssh -tA hjacobs@odd-eu-west-1.	ssh -o StrictHos	tKeyCheckir	ng=no hjac	obs@172.31.160.	20
<pre>Welcome /</pre>	31-21-47.eu-west ranting service)	-1.compute on 2015-05	.internal 5-21 13:13	:21	
CONTAINER ID IMAGE	COMMAND	CREA	ATED	STATUS	PORTS
800488d94562 stups/pierone:0.1-SNAPSHOT hjacobs@ip-172-31-160-20:~\$	"/bin/sh -c 'jav	/a\$(3 ho	ours ago	Up 3 hou	rs 0.0.0



ZMON





HYSTRIX TURBINE





RECAP: DOCKER IN STUPS



- Ubuntu & OpenJDK base image
- Log to **STDOUT**
- Config via environ. vars (+ KMS decryption)
- Non-root execution
- **Persistence** via EBS mounts
- Immutable stacks, no orchestration
- **DNS endpoints**, etcd e.g. for Hystrix streams

Securing REST based Microservices

Lock all doors



- Open only ports that you need permanently
- Grant SSH access only temporary
- Use a firewall for each app container

Authenticate & Authorize



- Make sure you talk to the right guy
- Check if access is permitted
- Use OAuth 2.0

Isolate your apps



Only one app per container / server Use Docker or CoreOS Rkt

Encrypt all channels

- Keep all tranferred data confidential
- Use TLS

Monitor & Limit your API calls

- Control who accesses your API how often, when and from where
 - Use Rate Limiting against fraud
 - Use external Security Services against DDoS

OAuth 2.0 explained

