



SETTING UP DELTA IN A HETEROGENOUS TELCO SDN ENVIRONMENT

Sebastian Dittrich, Telekom Security



LIFE IS FOR SHARING.

AGENDA

01 Introduction

02 Network Transformation @ DT

03 Setting up DELTA

Used hard- and software

DELTA architecture

Issues encountered during installation

Demonstration

04 Future plans / next steps

01 INTRODUCTION

\$ whoami

Sebastian Dittrich

- Security Consultant @ T-Systems International GmbH, Telekom Security
 - Network and Infrastructure Security, Security of Access and Optical Networks
- Project Security Manager for CORD-driven project Access 4.0 @ Deutsche Telekom
- Bachelor of Engineering in Computer Science and Telecommunications @ University of Applied Sciences Leipzig
- Certified Cyber Security Professional (Cologne Chamber of Commerce and Industry)



Let's connect:

[LinkedIn](#)

[XING](#)

02 NETWORK TRANSFORMATION @ DT

SDN/NFV-ENABLED PROJECTS AT DEUTSCHE TELEKOM



Pan IP programme

- DT's Pan-European telco network for a centralised production of services
- Enabled by (Open)Contrail



Next Generation Enterprise Network Alliance

- A new global business network that enables Industry 4.0
- Enabled by SDN technologies from Cisco



ACCESS 4.0

Access 4.0: Innovation project @ DT

- Reduce complexity in DT's access networks (fixed, mobile and hybrid)
- Following CORD-approach
- Enabled by ONOS

03 SETTING UP DELTA

WHAT IS DELTA?



DELTA IS A PENETRATION TESTING FRAMEWORK THAT REGENERATES KNOWN ATTACK SCENARIOS FOR DIVERSE TEST CASES. THIS FRAMEWORK ALSO PROVIDES THE CAPABILITY OF DISCOVERING UNKNOWN SECURITY PROBLEMS IN SDN BY EMPLOYING A FUZZING TECHNIQUE.

[PROJECT'S GITHUB](#)



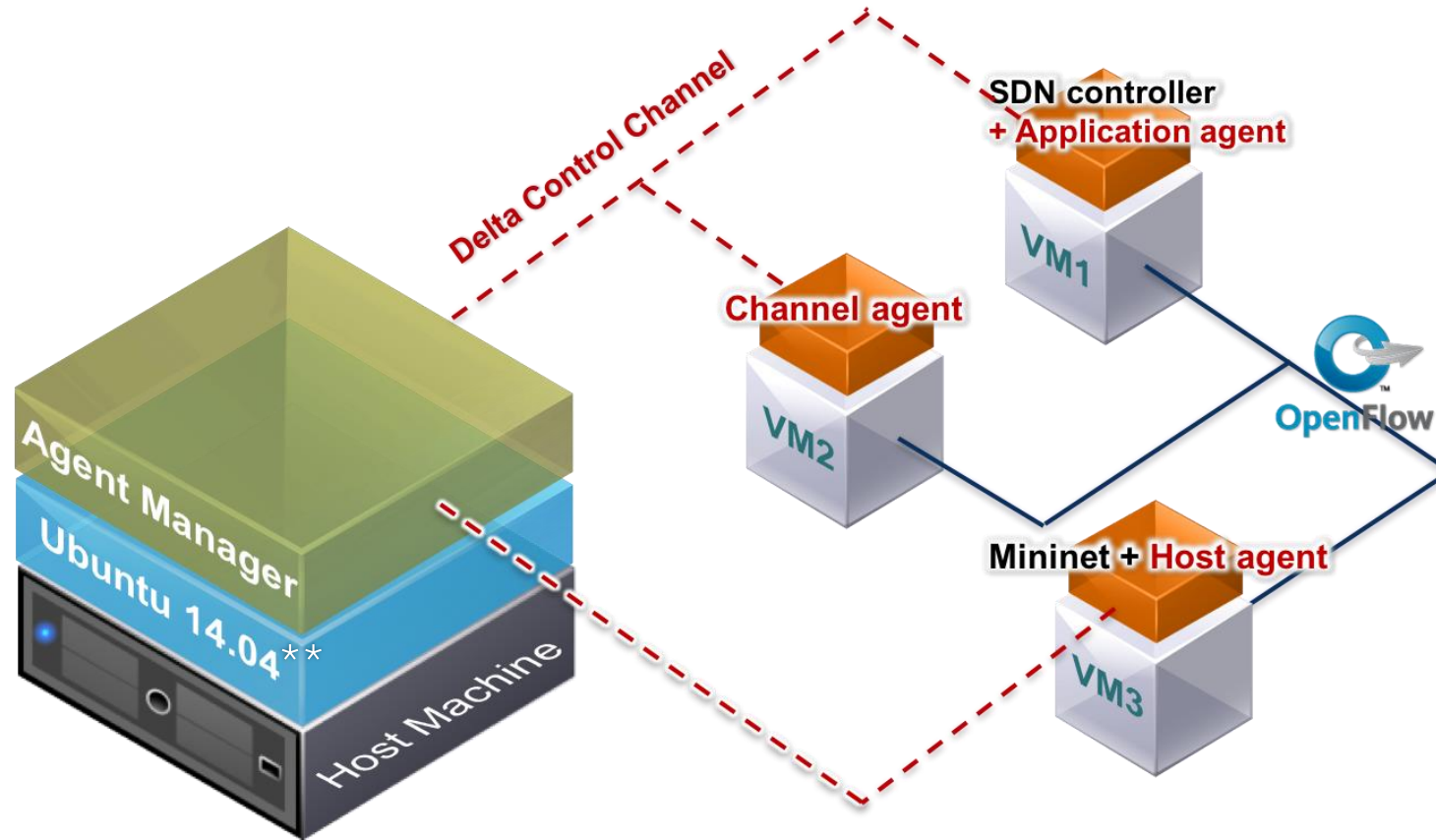
03 SETTING UP DELTA

USED HARD- AND SOFTWARE

Hardware		Software	
HP ProLiant DL360 G6 (single machine)		Mostly according to documentation on GitHub	
CPU	2x Intel Xeon-Prozessor X5560 @ 2,8 GHz	OS	Ubuntu 16.04.4 LTS (Kernel 4.4.0-116)
RAM	6x 8 GB DDR3-1333	Agent manager	Vagrant (2.0.2) + VirtualBox (5.0.40)

03 SETTING UP DELTA

DELTA ARCHITECTURE*

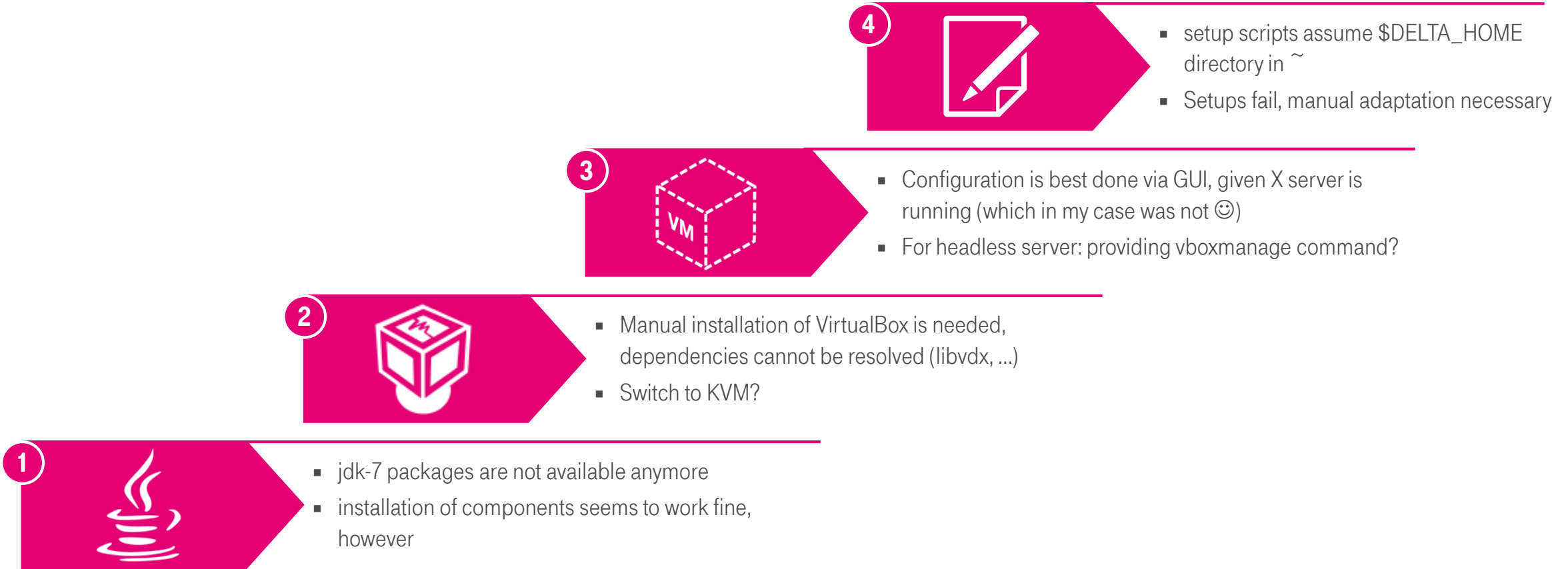


* As documented on GitHub

** Ubuntu 16.04

03 SETTING UP DELTA

ISSUES ENCOUNTERED DURING INSTALLATION




```

sdittrich@dmz-sditt:~/git/DELTA$ ./tools/dev/delta-setup/delta-agents-scp
- for application agent...
agent.cfg
- for channel agent...
delta-agent-channel-1.0-SNAPSHOT-jar-with-dependencies.jar
libjpcap.so
test-controller-topo.py
- for host agent...
delta-agent-host-1.0-SNAPSHOT.jar
test-advanced-topo.py
test-controller-topo.py
test-fuzzing-topo.py
test-switch-topo.py
sdittrich@dmz-sditt:~/git/DELTA$ bin/run-delta tools/config/manager_vm.cfg

```

100%	38	0.0KB/s	00:00
100%	25MB	25.3MB/s	00:01
100%	63KB	62.6KB/s	00:00
100%	978	1.0KB/s	00:00
100%	7607	7.4KB/s	00:00
100%	1982	1.9KB/s	00:00
100%	978	1.0KB/s	00:00
100%	1582	1.5KB/s	00:00
100%	1049	1.0KB/s	00:00



DELTA: A Penetration Testing Framework for Software-Defined Networks

- [pP] - Show all known attacks
- [cC] - Show configuration info
- [kK] - Replaying known attack(s)
- [uU] - Finding an unknown attack
- [hH] - Show Menu
- [qQ] - Quit

Command>

```

ssh tunnel seclab: ssh2secl \
portmapping Berlin: seclpm \
ssh Berlin: ssh2b \

```



```

[sebastian@satya ~]$ seclpm
Enter passphrase for key '/home/
/sebastian/.ssh/seclab':
Welcome to Ubuntu 16.04.3 LTS (
GNU/Linux 4.4.0-103-generic x86
64)
sdittrich@jh-ext-01:~$

```

03 SETTING UP DELTA DEMONSTRATION

04 FUTURE PLANS / NEXT STEPS

OBJECTIVES FOR FURTHER EVALUATION



But why?!

Currently, Deutsche Telekom tests every single network component manually

- Heavy on resources for testers, testing equipment, testing period, ...

Centralised testing frameworks leverage productivity

- Software bits can be tested almost automatically in real-time (little to no preparation required), sophisticated security tests can be done on the things that cannot be done automatically

Currently, there are no best practices for scope, test cases (specific to SDN), tools etc.

DELTA has the potential to become the de facto standard at DT for pen-testing multiple SDN controllers



CONTACT

SEBASTIAN DITTRICH

S.DITTRICH@TELEKOM.DE