Investigation of the Infrastructure Level of Cloud Computing

Realising a Basis for Privacy and Security of Software Services

Ina Schiering, Jan Kretschmer

Ostfalia University of Applied Sciences

IFIP Summerschool: Privacy and Identity Management for Life,
Trento, September 6th, 2011



Outline

- **Introduction**
- **Requirements**
- **Prototype**
- **Administration of the prototype**
- **Risks**
- **Conclusion**



Cloud Services

- **SaaS - Software as a Service**
  - Application Services
- **PaaS - Platform as a Service**
  - Programming Environments
  - Execution Environments
- **IaaS - Infrastructure as a Service**
  - Resource Sets (Virtual Resource Sets, Physical Resource Sets)
  - Infrastructure Services (Network, Storage, Higher Infrastructure Services e.g. Database)
- **Hardware**

1

[1] A. Lenk , M. Klems , J. Nimis , S. Tai , T. Sandholm, What's inside the Cloud? An architectural map of the Cloud landscape, Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, p.23-31, May 23-23, 2009.



Cloud Services

Interacting Partners

- Cloud User - Organisation using a Cloud Service
- Cloud Provider - Organisation providing a cloud service

Cloud Deployment Models

- Public Cloud
- Private Cloud
- Hybrid Cloud
- Community Cloud



Cloud Services

Cloud services are an important trend

- Perspective Cloud Provider
  - Economy of scale
  - Standardisation of IT services
  - Industrialisation
- Perspective Cloud User
  - Risks: Security, privacy, availability, legal compliance
  - Benefits: flexibility, no investment in data center and hardware

Despite of the risk the use of cloud services is increasing



Szenario

Aim: Building an SaaS-Prototype with security and privacy in mind

- Build an SaaS cloud service
- Based on an IaaS cloud service providing virtual resource sets

Possible assumptions about the IaaS cloud service

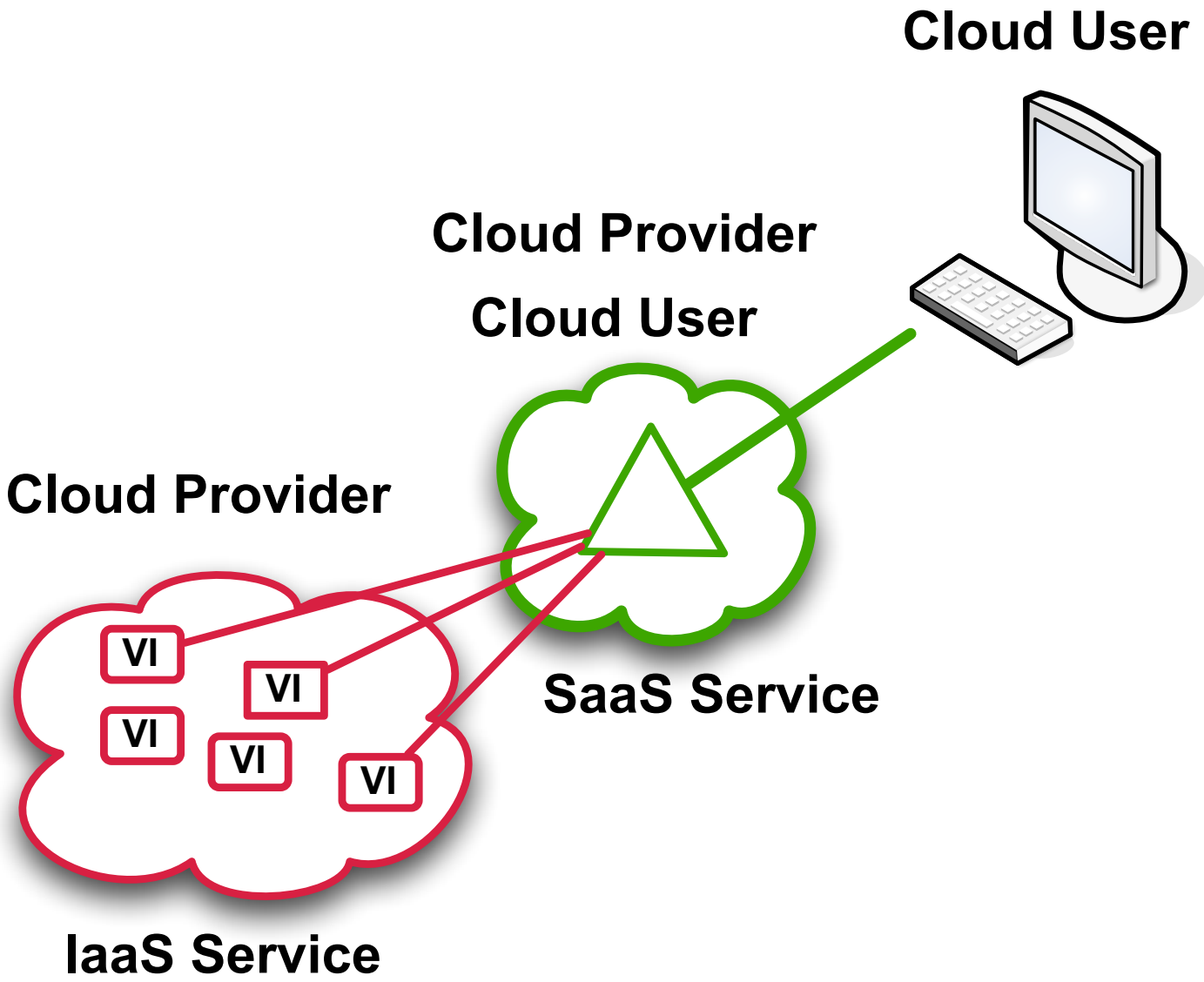
- Make no assumptions
- Approaches for trusted cloud computing (e.g. Merlin)

First step: Building an IaaS cloud using a standard cloud software

- Adversary: administrators of operating system and virtualisation resp. cloud software
- Apply technical measures and processes

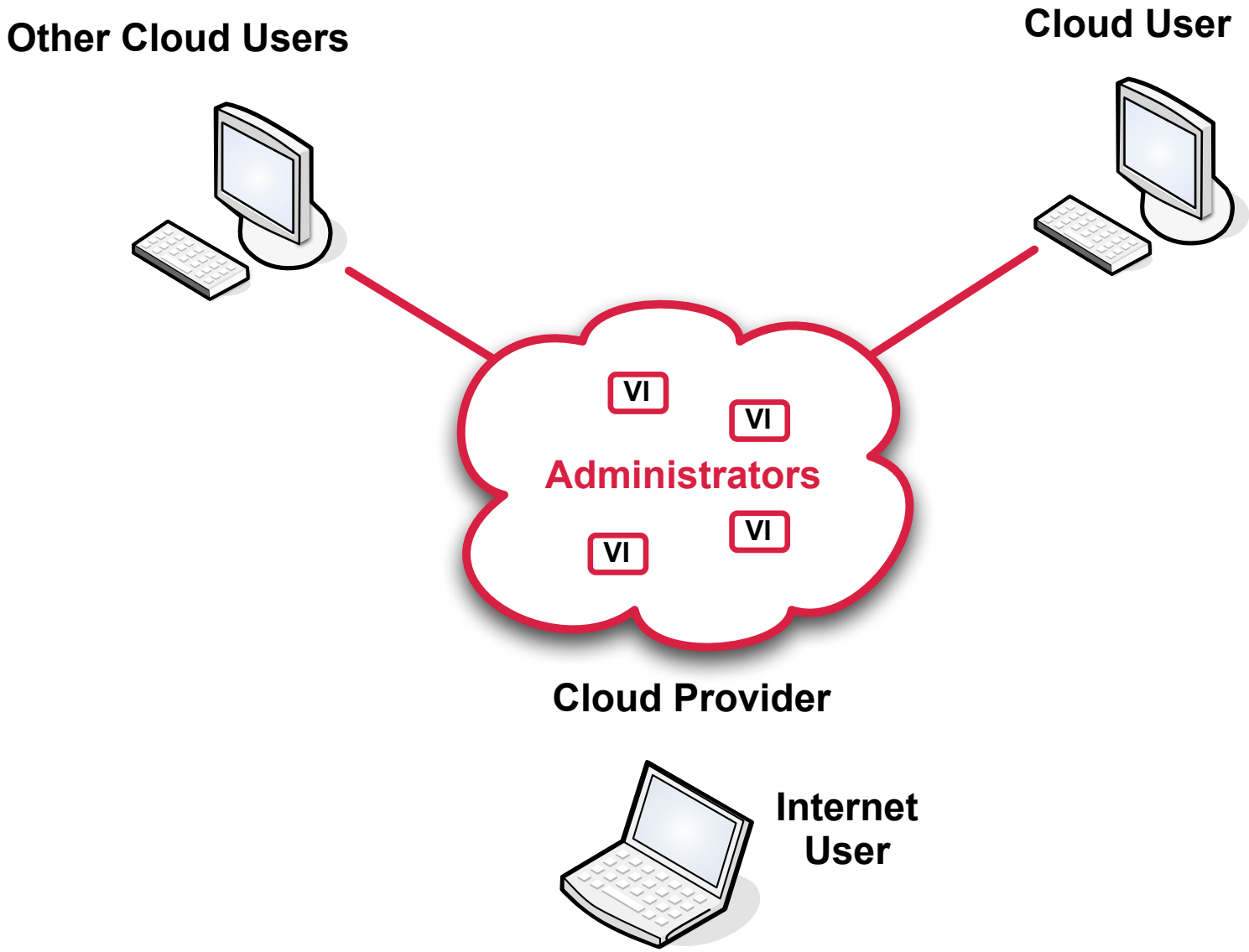


Szenario


Cloud User
Cloud Provider
Cloud User
Cloud Provider
VI
VI
VI
VI
VI
SaaS Service
IaaS Service

First Step - IaaS Cloud Service

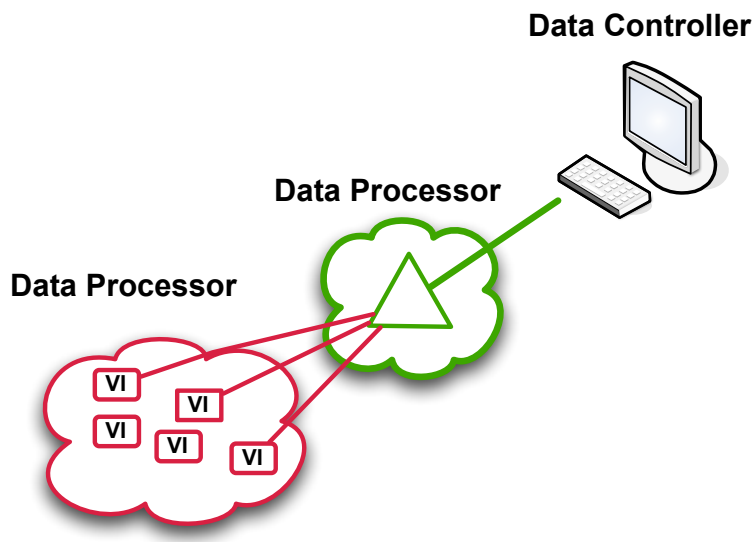
Adversary Model



Requirements - Data Protection Directive

Assumption: No processing of sensitive data (Article 8).

- Article 12 (b) Erasure of data (SaaS: rectification, blocking)
- Article 16 Confidentiality of processing
- Article 17 Security of processing: "the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access"
- Article 25, 26 transfer of personal data to third countries



Prototype

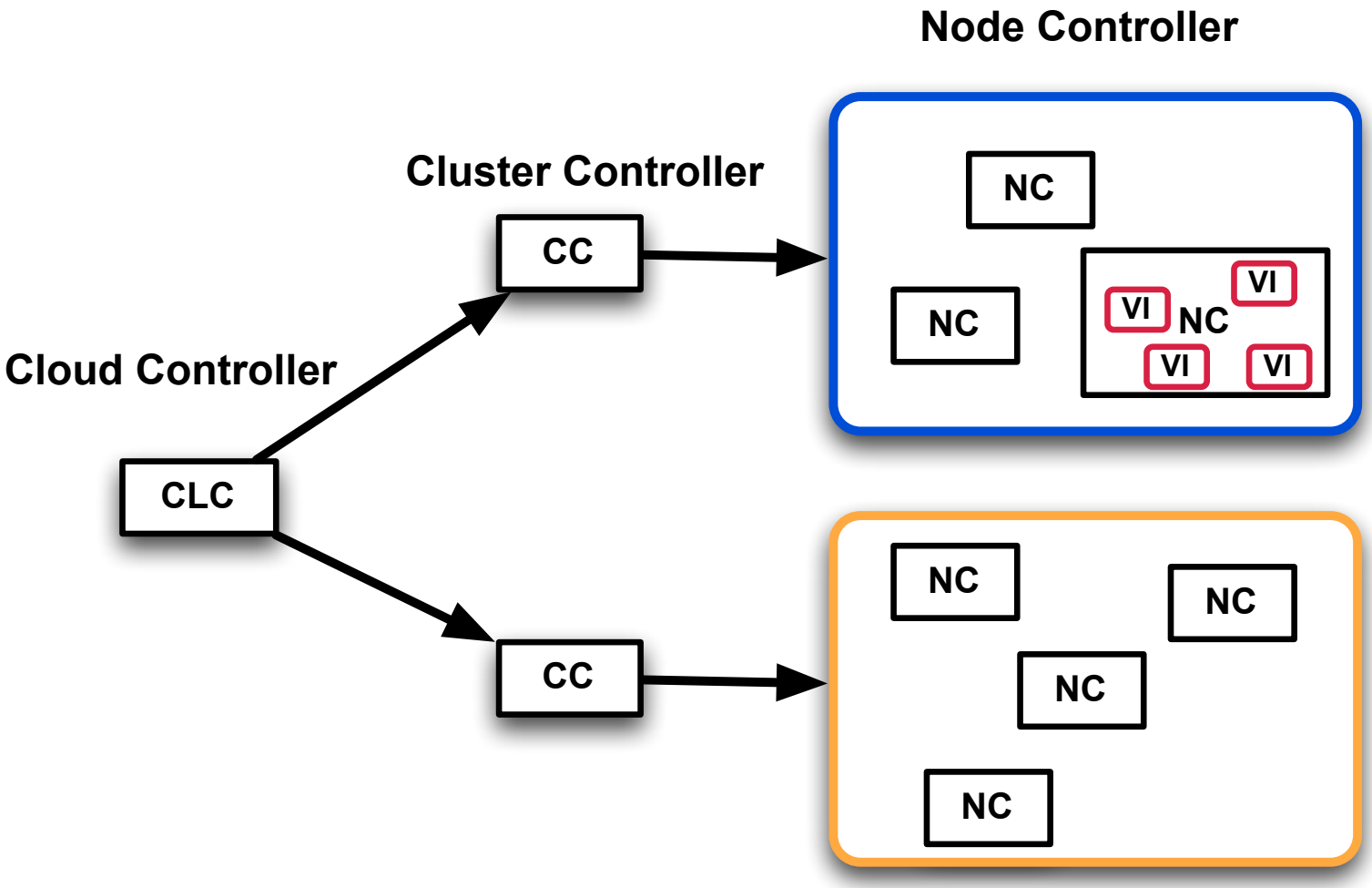
Public IaaS cloud service for virtual resource sets

- Several software stacks available (Eucalyptus, OpenNebula, OpenStack, VmWare)
- Criteria:
  - Open Source
  - Sufficiently stable at the start of the realisation (January 2011)
  - Concept of division of the cloud into separate "parts"(Amazon regions, Eucalyptus clusters)

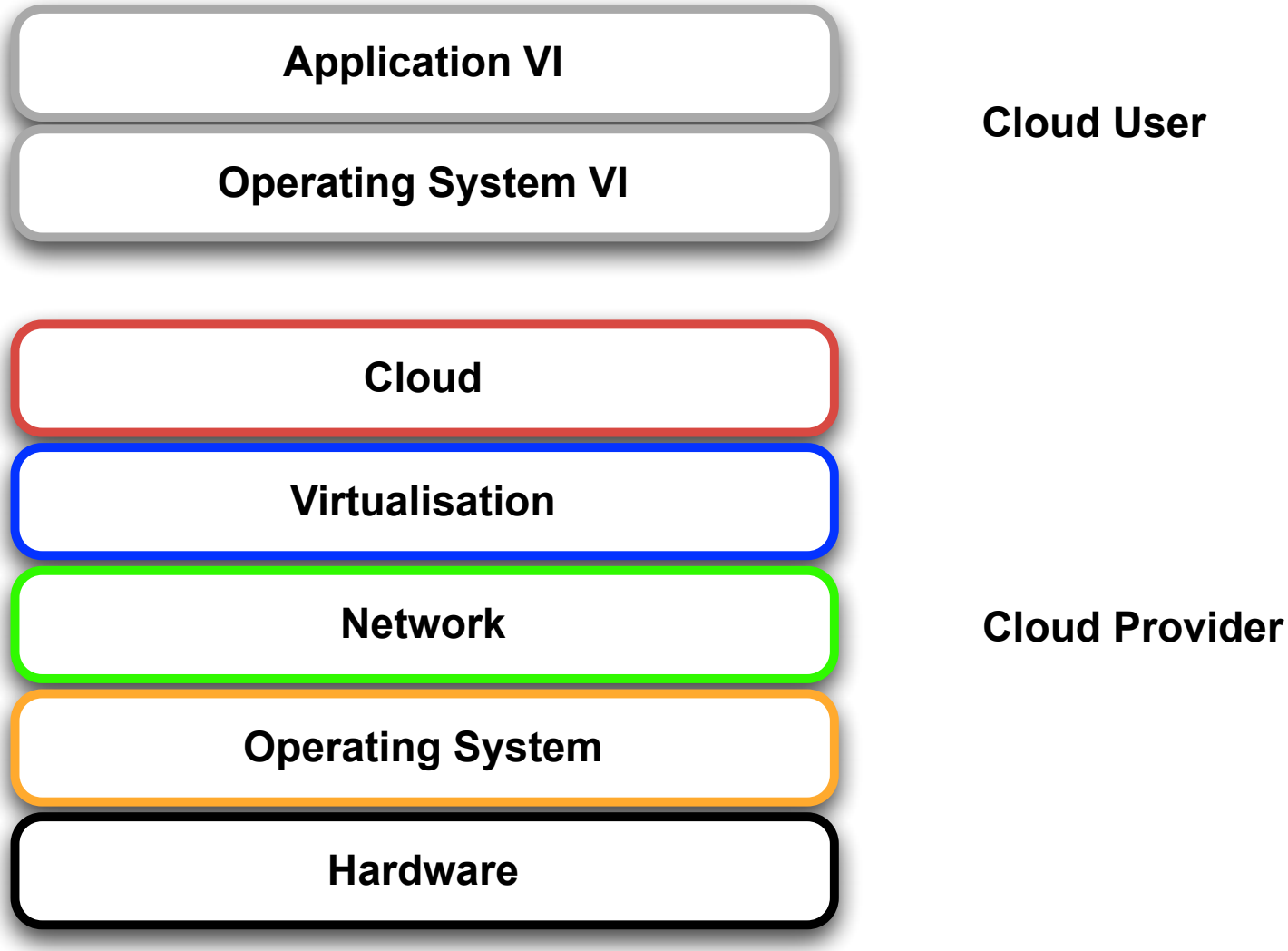
Use of Eucalyptus as cloud software



Prototype


Node Controller
Cluster Controller
Cloud Controller
CC
CLC
CC
NC
NC
VI
VI
NC
VI
VI
NC
NC
NC
NC

IaaS Technology Stack

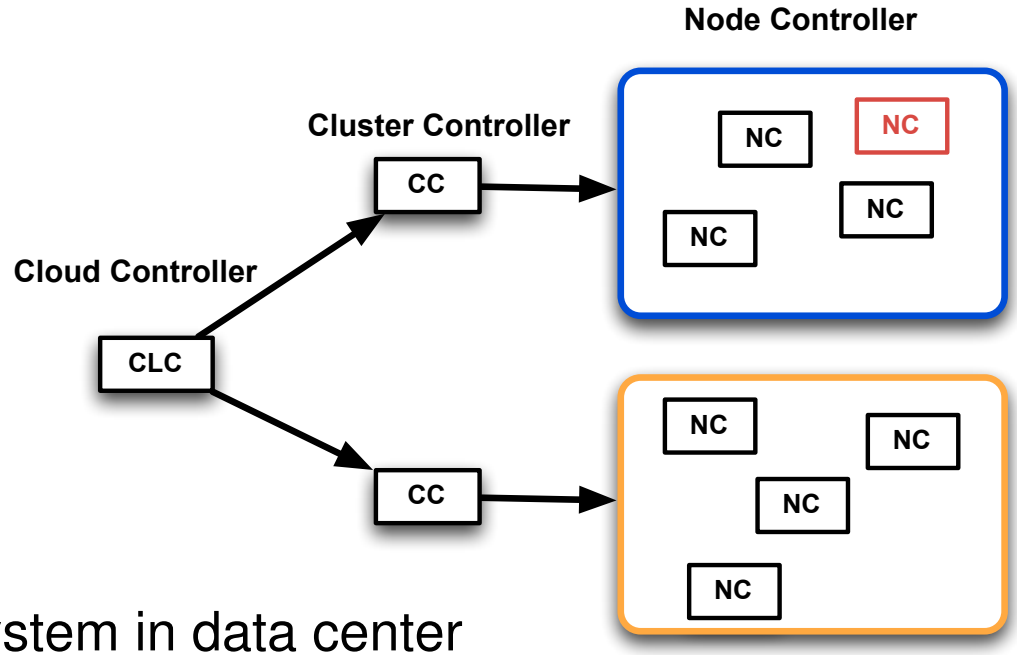


Administration of the Prototype

1. Add, remove system
2. Change system
3. Monitoring, Backup, Restore
4. Troubleshooting



1. Add, Remove System



- Place system in data center
  Segregation of duties: Data center access but no system access
- Install system
  Automated: Data added to configuration of boot server, **image** is booted
- Add system to cloud configuration
  Automated

Remove system is done in a similar way.



A. Create Image

Image is a collection of software packages and configuration changes

- Plan image: select **packages** and plan configuration changes, document image
- Build image
  Automated
- Test image with respect to documentation
  Process with tool support
- Create checksum
  Automated
- Deploy image on boot server
  Automated
- Regularly check integrity of image with checksum
  Automated

We need a special image to delete all data of a virtual instance after the image is deleted.



B. Create Package

- Plan package: document requirements, changes
- Implement package
  Manual process, risk can be reduced by applying rigid SE methodologies
- Test image
  Difficult
- Create checksum
  Automated
- Deploy package to repository
  Automated
- Regularly check integrity of package with checksum
  Automated

Automated procedures are also created in form of packages



2. Change System

Systems are just changed in form of updates

Minor updates realised as updates in form of updated packages (B)

Major updates new image (A)

- Plan update (see A, B)
- Test update (see A, B)
- Realise update (see , A, B)
  - Minor updates: updated packages (B)
  - Major updates: virtual instances are migrated, new image is booted (A)



Summary - Administration of the Prototype

1. Add, remove system
   Automated
2. Change system / Update System
   Automated
3. Monitoring, Backup, Restore
   Automated
4. **Troubleshooting**

A Create Image
Automated procedures and processes

B Create Package
Risk can only be reduced



Risk

Risk management strategies:
reduce, mitigate, prevent, accept, contingency plan

- Troubleshooting is the only administrative task where system access can be required, if it is not possible to reproduce the issue in test environment.
  Reduce risk: four-eyes principle, logging of actions, IT service management
- Create Packages
  Reduce Risk: SE methodologies, IT service management



Requirements - Data Protection Directive

Assumption: No processing of sensitive data (Article 8).

- Article 12 (b) Erasure of data (SaaS: rectification, blocking)
- Article 16 Confidentiality of processing
- Article 17 Security of processing: "the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access"
- Article 25, 26 transfer of personal data to third countries



Conclusion

- **Apply technical measurements:** automated procedures, encryption, access control, checksums
- **Where not possible apply processes:** IT service management frameworks (e.g. ITIL), SE methodologies, ...
- **Accompany both with automated auditing:** logging and automated evaluation of logs
- **Apply regular assessments** to assure the measurements and processes are in place

Future Work

- We have already implemented a very simple SaaS prototype and applied first technical measurements
- Start identifying gaps and balancing cost of additional technical measurements with gain related to privacy metrics

