IAM in the hybrid cloud

Platform voor Informatiebeveiliging

13 September 2018

Jaap Hoekstra

CISA, CISM, CISSP, CCSP

Introduction

From:

- Project Manager System Development (8 years)
- IT auditor (5 years)
- E-commerce project leader (3 years)

- IT Risk advisor (6 years)
- IAM Governance (6 years)

- Cloud: Domain spoc CISO (1½ year)

Introduction

From:

- Project Manager System Development (8 years)
- IT auditor (5 years)
- E-commerce project leader (3 years)

To:

- IT Risk advisor (6 years)
- IAM Governance (6 years)
- Cloud: Domain spoc CISO (1½ year)

IAM in the hybrid cloud

1. Cloud & DevOps
2. IAM Governance
3. IAM for Cloud
4. Implementation
5. Conclusions

Cloud & DevOps

From:	To:
On-premise own IT-infrastructures	On-premise Private Cloud Dedicated private clouds in public clouds
Self build applications	SaaS solutions Continuous Integration / Delivery DevOps
Coordination - manual actions	Orchestration – fully automated
Security risk advice and assesments	Inherent security

IT (and CISO) will be fully automated

IAM in the hybrid cloud

1. Cloud & DevOps
2. IAM Governance
3. IAM for Cloud
4. Implementation
5. Conclusions

1. Identity & Access Management goals

1. **One IAM Governance, worldwide.**
2. **Be able to demonstrate “in control”.**
3. **Effective and efficient processes for Identity and Access Management.**

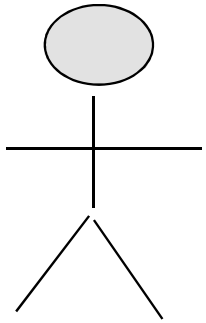
Cloud Control Consultancy

1. IAM principles

1. Business is accountable
2. Role Based Access
3. One IAM governance for ABN AMRO*
4. Conceptual models, to be able to support tailored implementations
5. Risk based, Business driven
6. Reuse of systems and processes when possible

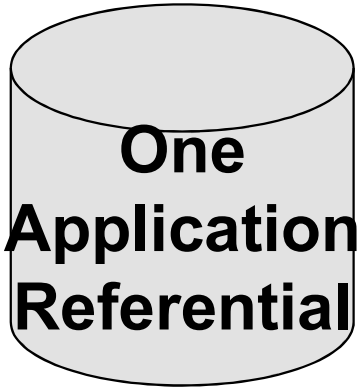
*	**ABN AMRO**	**Subsidiaries**	**Partners/ Suppliers**	**Joint ventures**
	Internally + externally hired employees in NL + foreign countries	e.g. ABN AMRO Lease, ICS	e.g IBM, TCS, Infosys, Stater	e.g. ABN AMRO Insurance, Geld Services Nederland

1. IAM: two referentials:



Identity Management

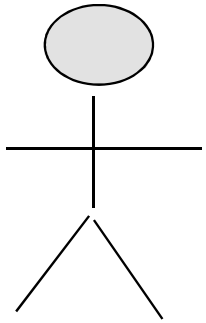
Each employee is screened
and has an unique Corporate ID.



Applications

Each application has
an unique Application ID

1. Dealing with 8 IAM events:



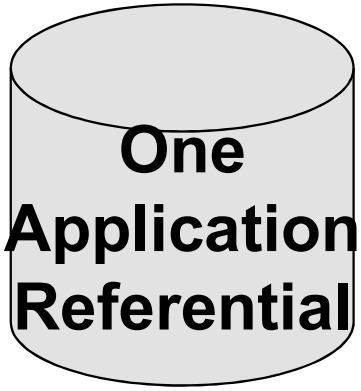
Identity Management

Corporate ID

Identity:
1.Joiner
2.Mover (change job)
3.Leaver

Application:
4.New
5.Change
6.Remove (Decommision)

Access rights:
7.Assign Role*
8.Remove Role*



Applications

Application ID

Cloud Control Consultancy

* When Roles are made by the Role Manager first

IAM in the hybrid cloud

1. Cloud & DevOps
2. IAM Governance
3. IAM for Cloud
4. Implementation
5. Conclusions

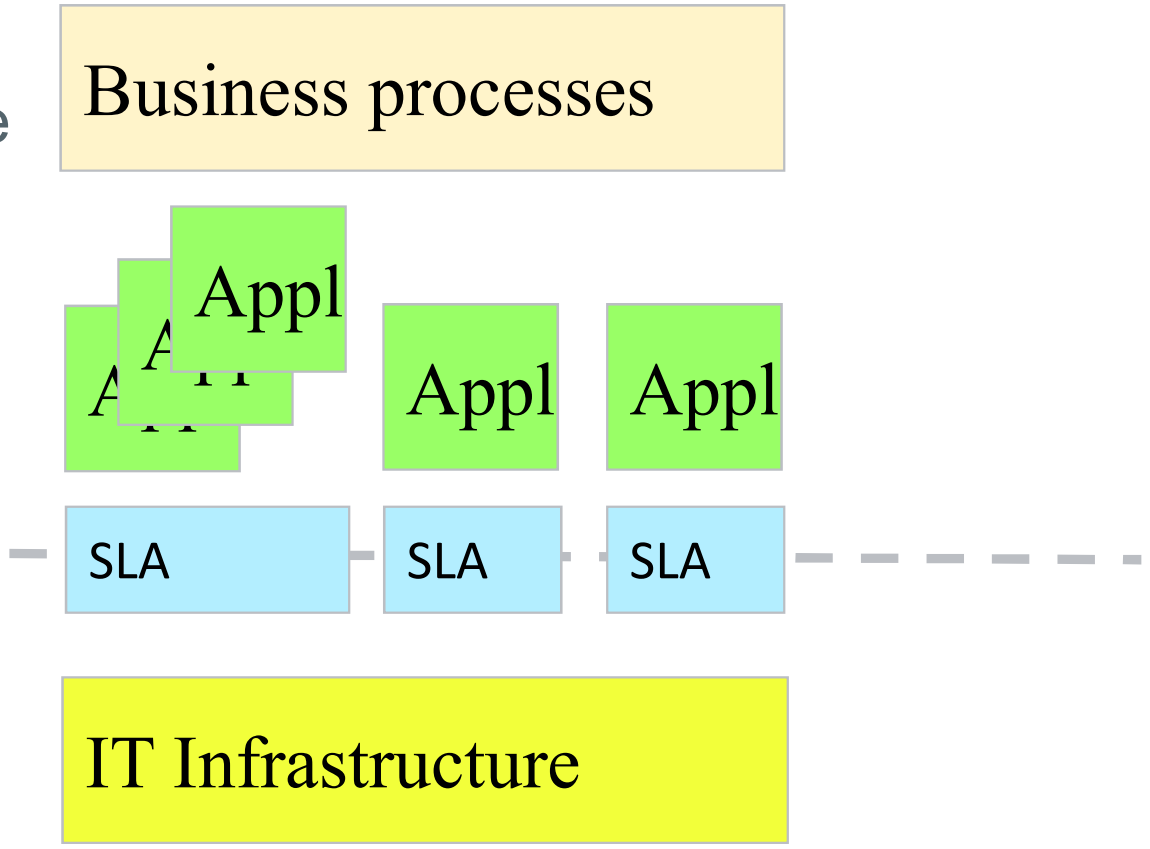
Scope: IT access rights

Three domains:

Business: here out-of-scope
(End-users using the applications)

IT Development
(Develops applications, DTAP)

IT Services
(Runs the applications + infrastructure)



Cloud Control Consultancy

IT Development organisation

Approx. 50 Grids
with 400 scrumteams

Accountability:

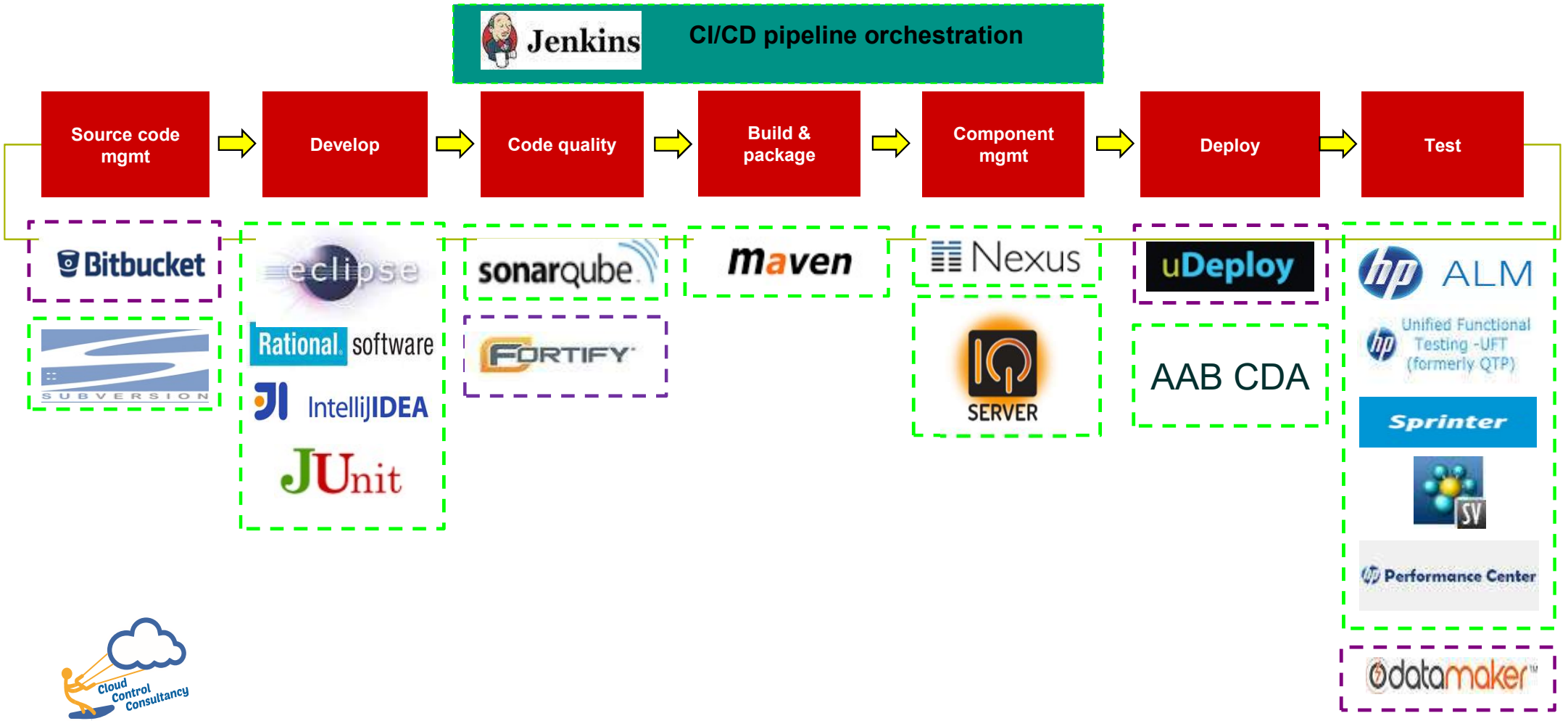
- Each application is the accountability of (only) one Grid owner.
- One of the scrumteams will be responsible for the application.

Responsiblities of the scrumteam:

- Development & maintenance of the application
- Correct registration in the CMDB
- Access rights of members scrumteam

Cloud Control Consultancy

Continuous Integration / Continuous Delivery



IAM for Cloud - requirements

1. Zero-touch platforms
   - With CI/ CD you do not want anybody having access on OS-level anymore
   - Only the CI/CD tools need access to OS-level

2. IAM needs to be fully automated (cloud is very dynamic)

3. In practice not all CI/CD tools are ready to use
   and not all applications can be deployed with CI/CD tools yet

IAM for Cloud - solution

1. Use RBAC to have access to CI/CD tools with normal user id

2. Integrate Identity Access Management with the CMDB
   - Before you request any VM you need the Application ID
   - Application ID is used to label all CI's
   - Maintain the organisation structure of Grids and scrumteams in CMDB
   - With the Application ID all ITIL processes are directly effective for the VM

3. Use sudo rights for access rights on OS-level with special user id

IAM in the hybrid cloud

1. Cloud & DevOps
2. IAM Governance
3. IAM for Cloud
4. Implementation
5. Conclusions

IAM for Cloud - solution

1. Use RBAC to have access to CI/CD tools with normal user id

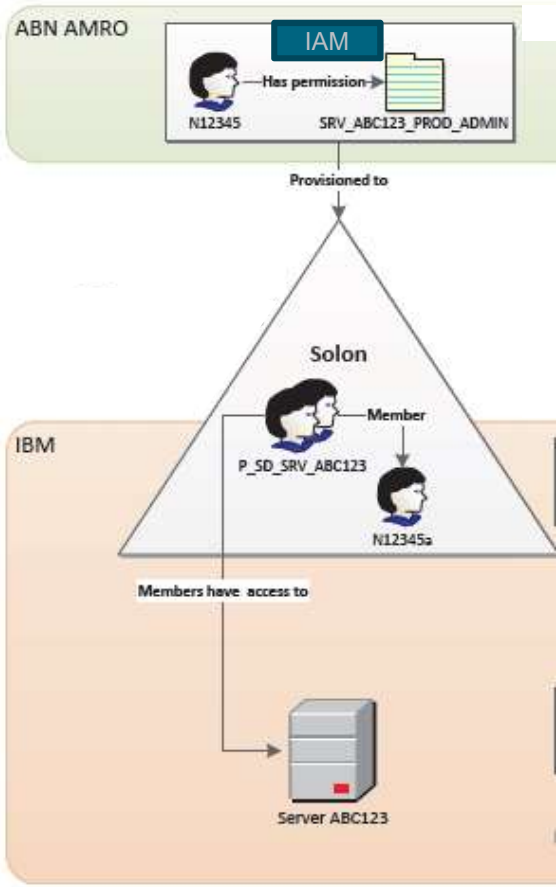
2. Integrate Identity Access Management with the CMDB
   - Before you request any VM you need the Application ID
   - Application ID is used to label all CI's
   - Maintain the organisation structure of Grids and scrumteams in CMDB
   - With the Application ID all ITIL processes are directly effective for the VM

3. Use sudo rights for access rights on OS-level with special user id

Basic principle

Access Management systeem

Active Directory

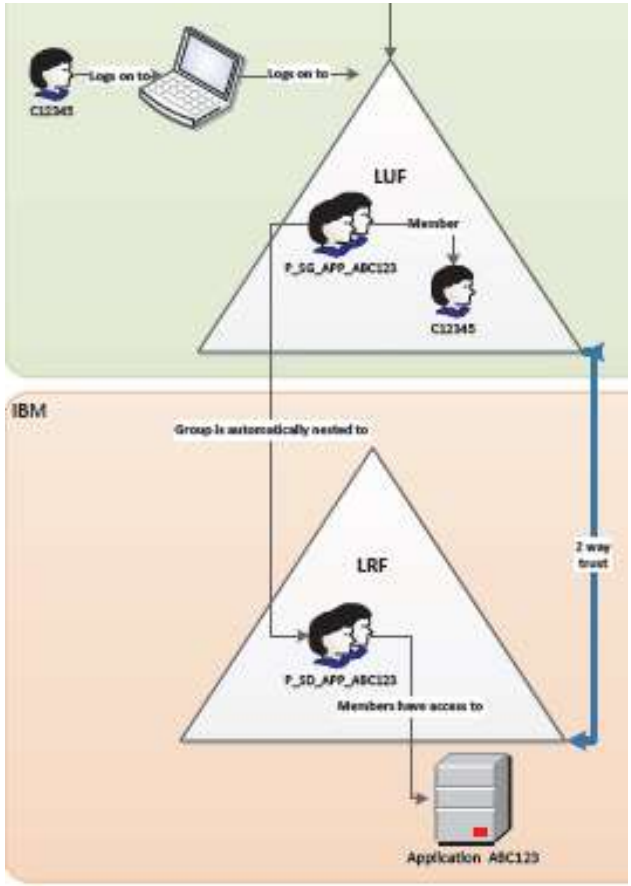


Cloud Control Consultancy

Physical separation between Resources and Users

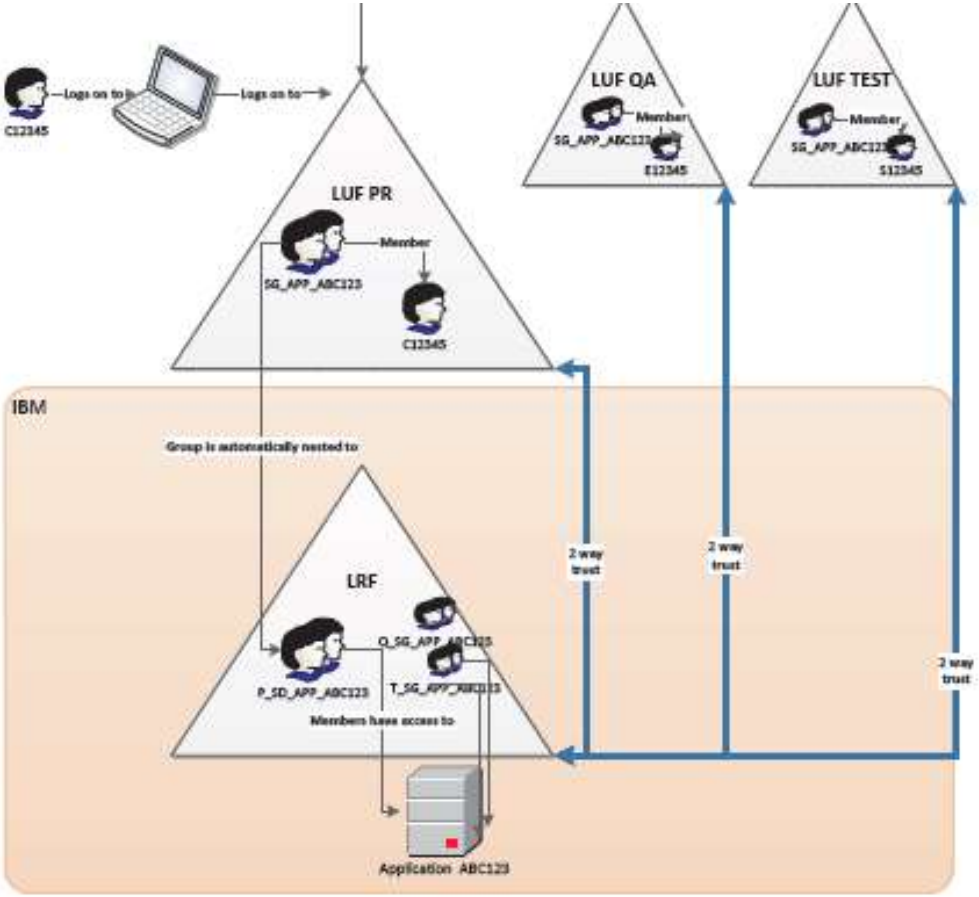
Launcher User Forest

Launcher Resource Forest



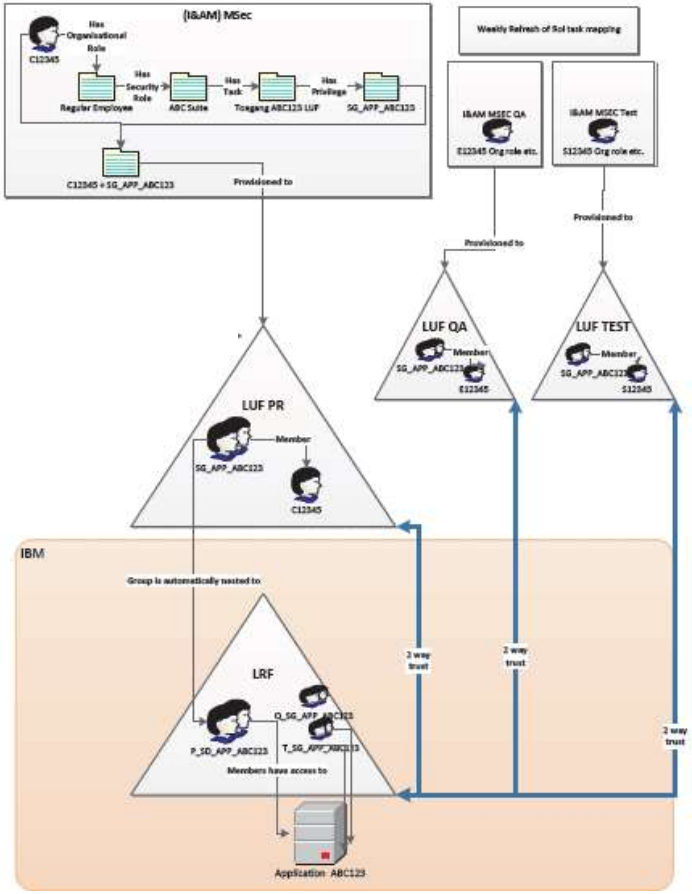
Cloud Control Consultancy

Physical separation between PR, QA and ST



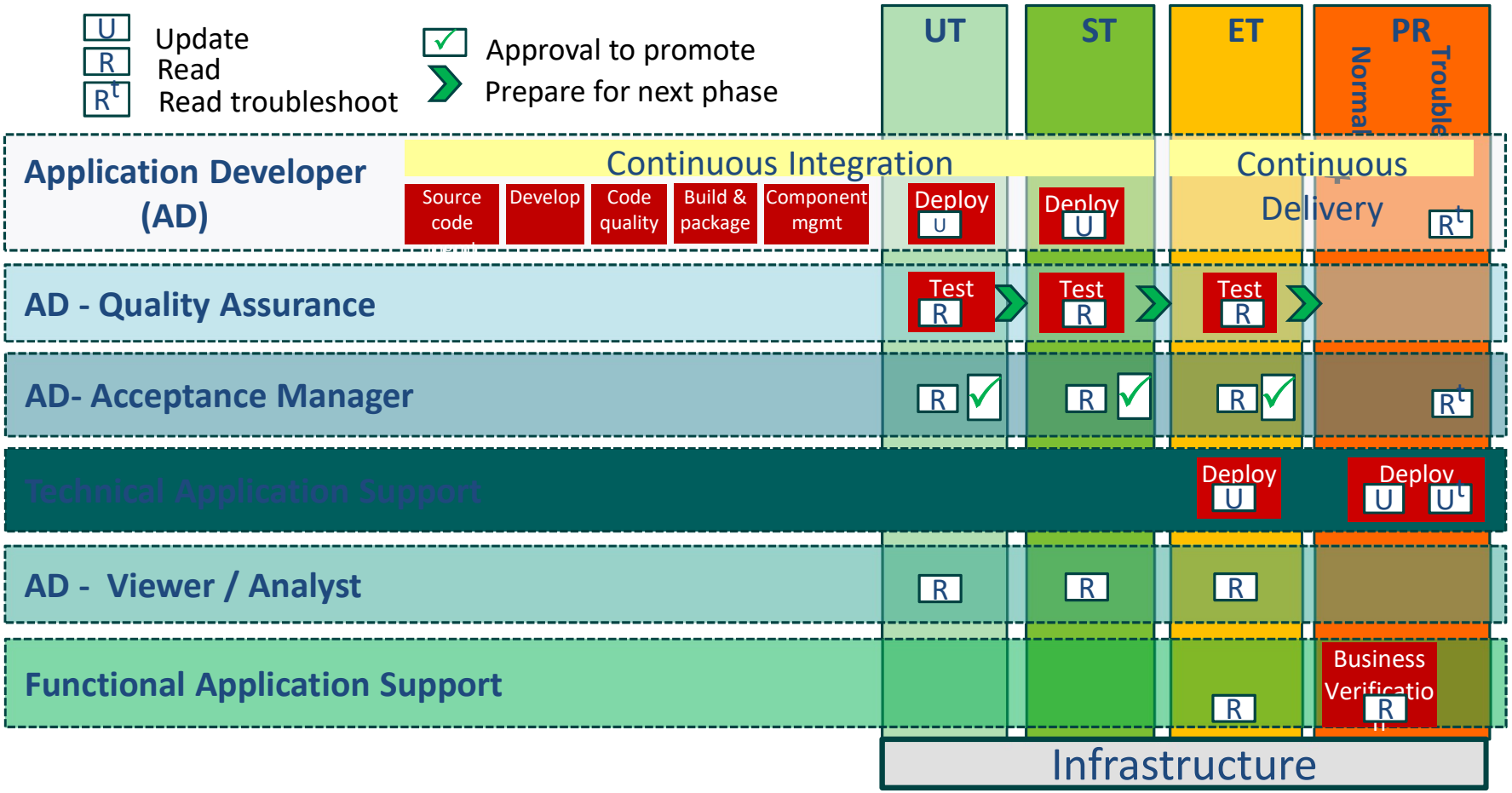
Cloud Control Consultancy

Full scheme of the 4 Launcher AD's



Cloud Control Consultancy

High level authorisation matrix



Cloud Control Consultancy

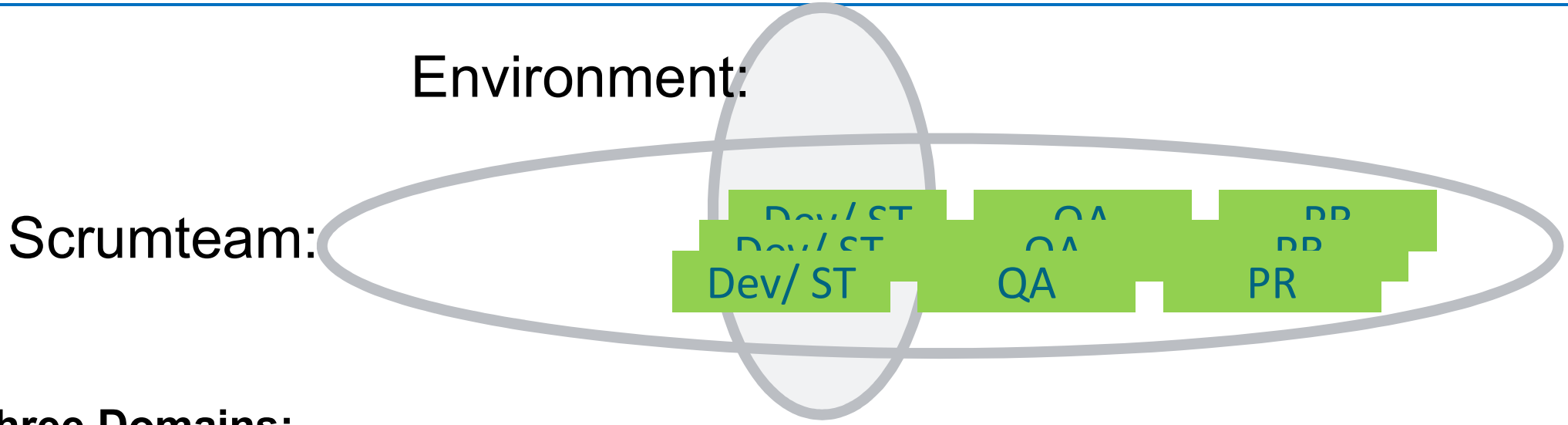
IAM for Cloud - solution

1. Use RBAC to have access to CI/CD tools with normal user id

2. Integrate Identity Access Management with the CMDB
   - Before you request any VM you need the Application ID
   - Application ID is used to label all CI's
   - Maintain the organisation structure of Grids and scrumteams in CMDB
   - With the Application ID all ITIL processes are directly effective for the VM

3. Use sudo rights for access rights on OS-level with special user id

Owners and environments



Three Domains:

Consumer: **Business domains: Business chains of processes (not in scope)**

Grids/scrumteams: Channels, Markets, Functions, Transactions, etc.

Provider: **Operating system**

Environments: **ST = System test**

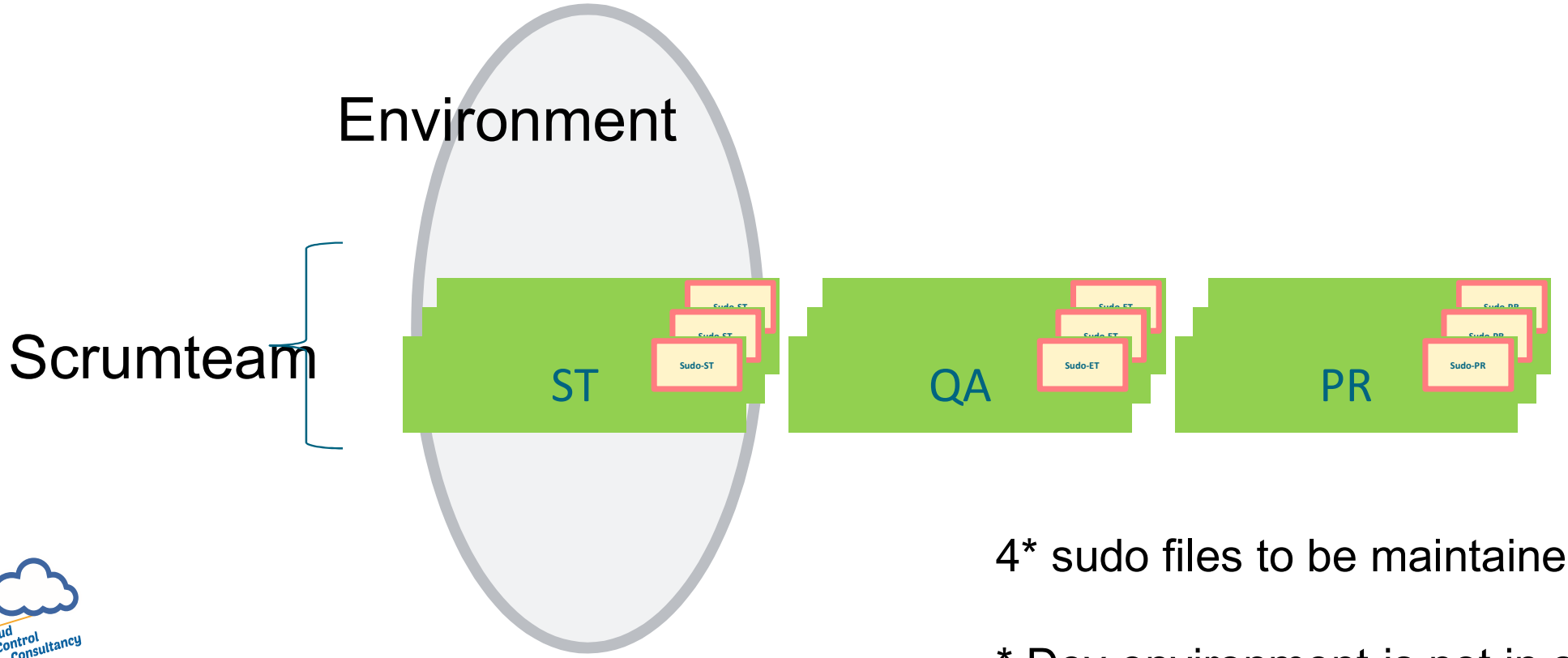
QA = Quality Acceptance

PR = Production

Cloud Control Consultancy

Cloud: New Sudo files - one for each environment!

Linux is used by approx. 75 – 80 % of the applications



4* sudo files to be maintained

* Dev environment is not in scope

Cloud Control Consultancy

Sudo file characteristics + Design principles 1 - 3

Group (for each actor)	**sudo commands**
Consumer:	
Developer:	sudo command 1
	sudo command 2
	sudo command 3
Application Support:	sudo command 9
	sudo command 11
Functioneel Beheer:	sudo command 27

Design principles:

Sudo file: 1. unique per environment (ST of QA of PR
2. standard for each Cloud VM

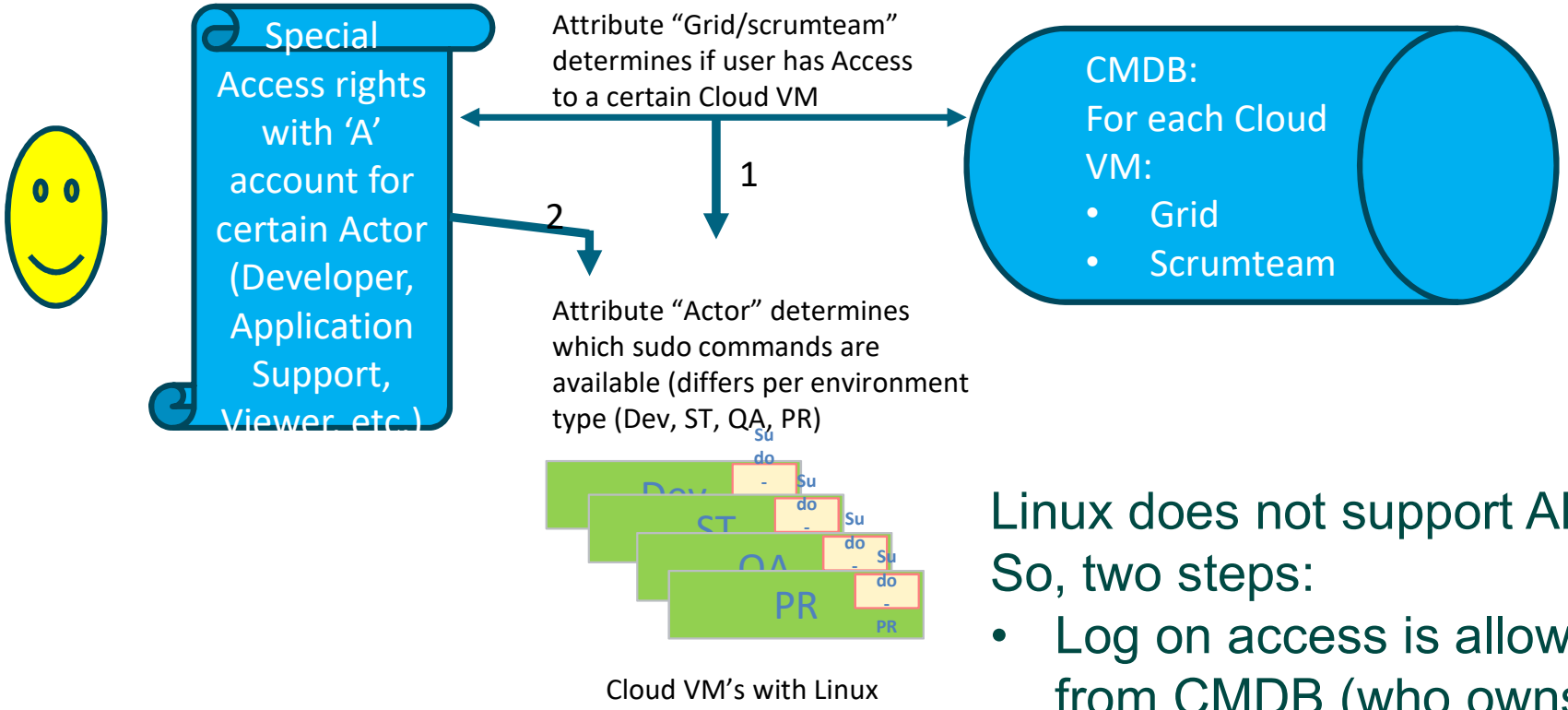
Sudo rules: 3. sudo commands per actor (Consumer)

Sudo file example

```
# FOR CMS Linux VMs
User_Alias OPER = %P_SD_SYS_LinuxOperators, %P_SD_SYS_WASOper
User_Alias SYSMAN = %P_SD_SYS_LinuxAdmins
User_Alias MWAMAN = %P_SD_SYS_WASAdmin
User_Alias SUPPORT = %P_SD_SYS_WASSupport
User_Alias READONLY = %P_SD_SYS_LinuxDeveloper, %P_SD_SYS_WASReadOnly
User_Alias MQAMAN = %P_SD_SYS_MQAdmins

# ORIGINAL - HVE
#User_Alias OPER = %oper
#User_Alias CONTROL = %control, %secadmin
#User_Alias SDDMAN = %sddman
#User_Alias SYSMAN = %sysman
#User_Alias MWAMAN = %mwaman, %dbsysman, %webman
#User_Alias SUPPORT = %support
#User_Alias SECDESK = %secadmin, %security
#User_Alias READONLY = %readonly, %sysdev, %appldev
```

IAM for Cloud – sudo access (Exception)



Linux does not support AD groupnesting
So, two steps:

- Log on access is allowed by attribute from CMDB (who owns the VM)
- The AD-group determines what sudo commands are available (standard for all VM's)

Cloud Control Consultancy

Identity & Access Management

IAM for Cloud

One logical model; **implementations per native Cloud**:

1. **Happy flow**: personal user id and RBAC role (LUF AD)
2. **Admin flow**: ‘A’ user id (like N12345A) in LRF AD:
   - ApplDev for Developer (Dev & ST)
   - ApplMan for Maintenance (QA & PR)

IAM in the hybrid cloud

1. Cloud & DevOps
2. IAM Governance
3. IAM for Cloud
4. Implementation
5. Conclusions

Conclusions and last additions

IAM is key for managing access in the hybrid cloud:

- Centralise, Standardise, Automate
- Integrate with CMDB
- Data quality is key
- One logical model for all Cloud environments (AWS, Azure, IBM, bare metal, RACF on mainframe)
- Use Application ID’s everywhere to label everything

Thanks for your attention

“It's not about having an idea, but making it happen”