



# Requirements for Securing Cross Cloud Deployments

3rd CIRRUS workshop, Vienna, 19/11/2013

Philippe Massonet

CETIC

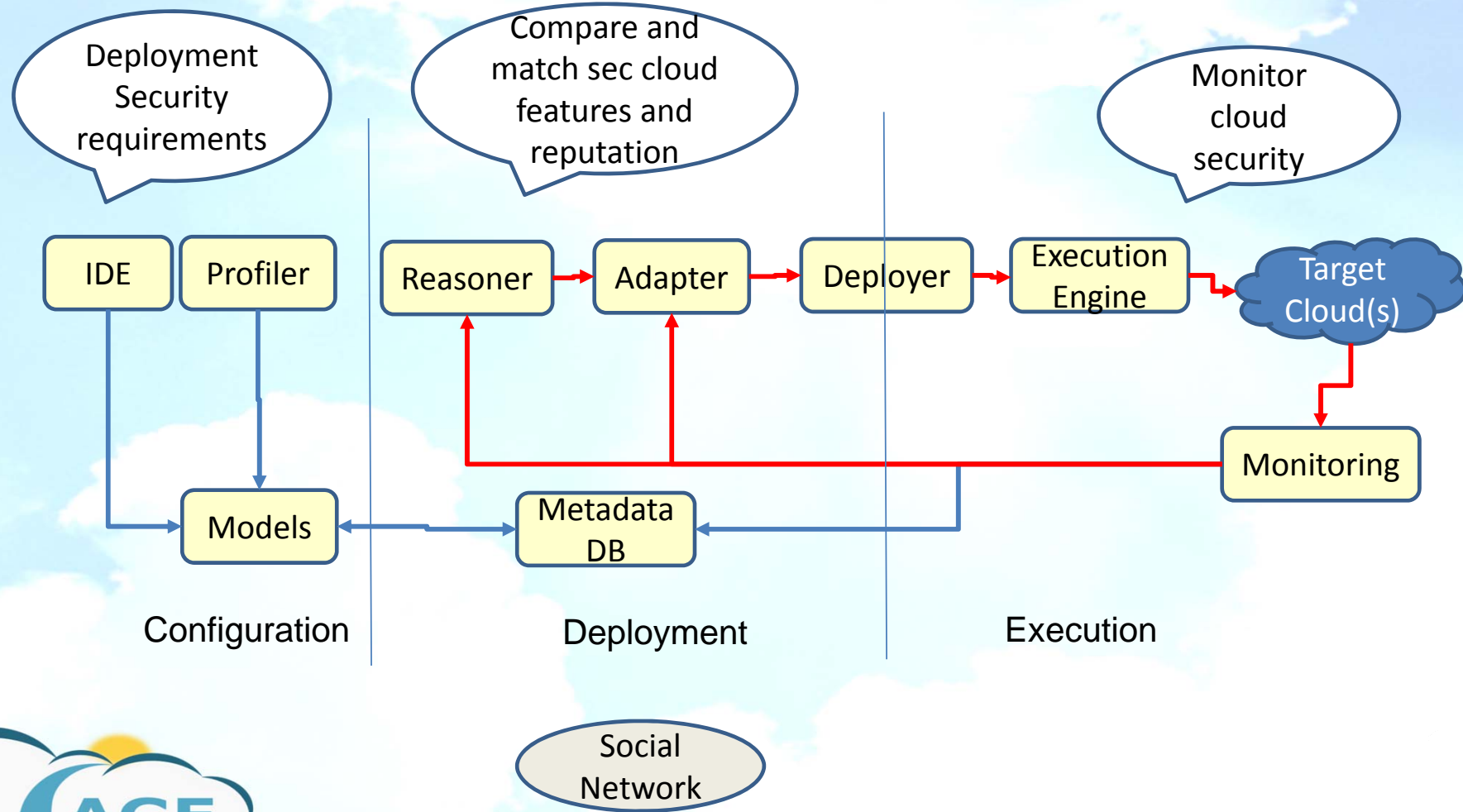
[Philippe.massonet@cetic.be](mailto:Philippe.massonet@cetic.be)

# Introduction to the PaaSage Project

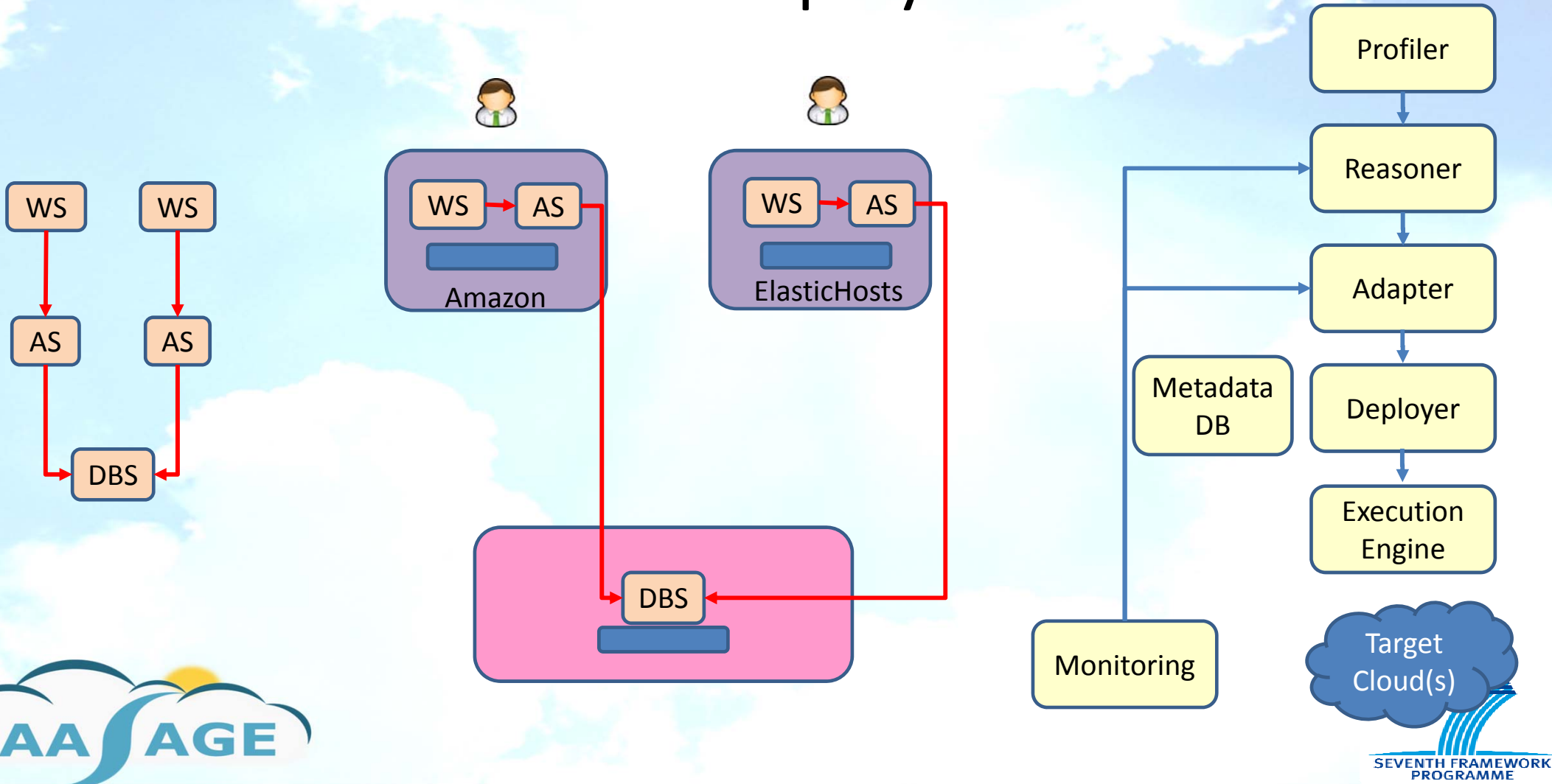
- PaaSage aims at creating a development and deployment platform together with an appropriate methodology for helping software engineers creating new applications and migrating old applications that can run on multiple Cloud platforms.
- Main concepts
  - Model based approach
  - Cross-cloud deployments
  - Optimisation of deployments
  - Security is taken into consideration via a security model
- Result will be an open source Eclipse based platform + cloud deployment language



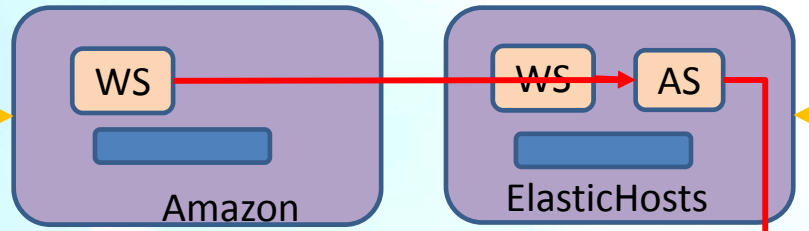
# PaaSage Components, Life Cycle and Security



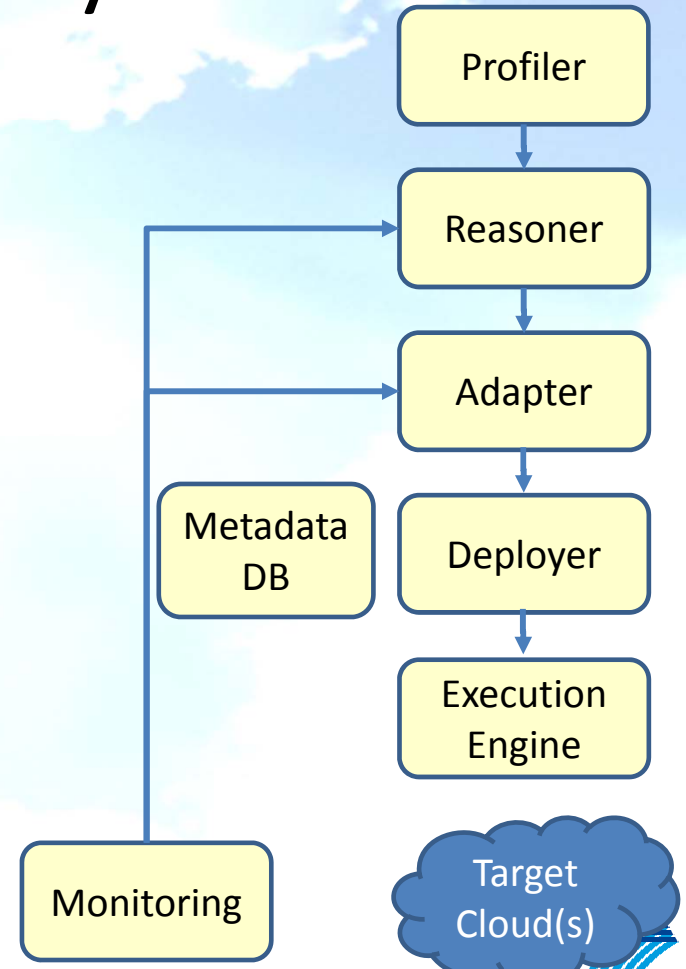
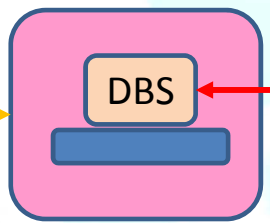
# Cross cloud deployments



# Optimising Cross cloud deployments



Cross Cloud  
Monitoring  
Infrastructure



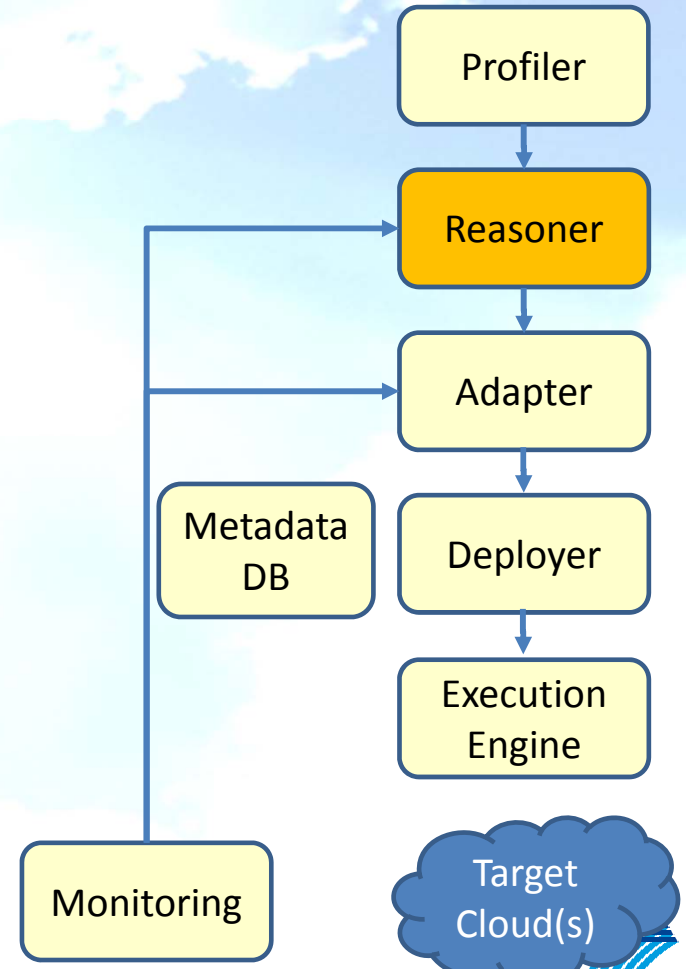
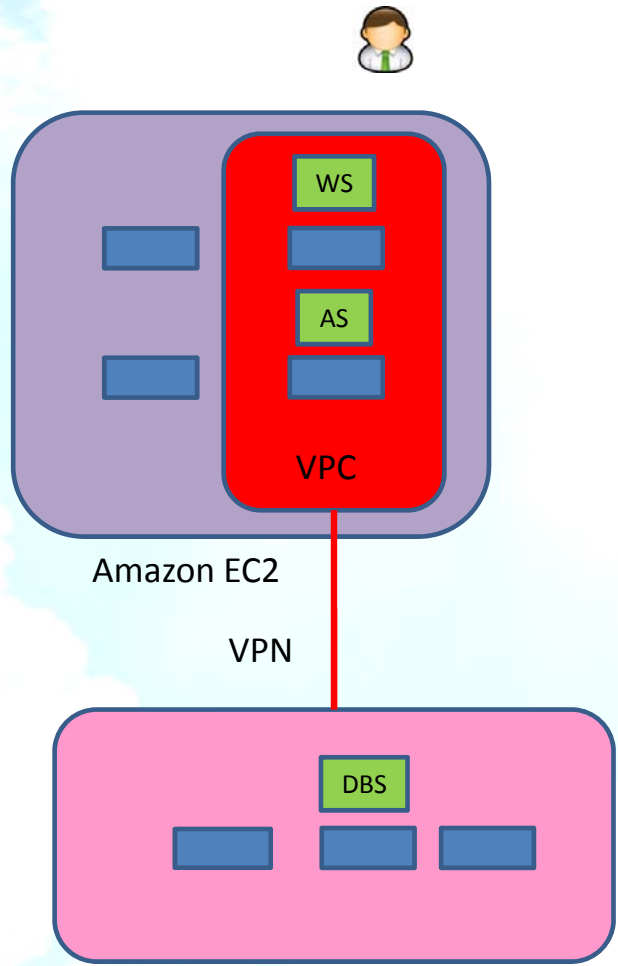
# A Security Deployment Scenario

Requirements

- WS** Confidential
- AS** Confidential
- DBS** Personal data, keep in PC

Amazon Sec Features

- Normal EC2
- VPC + VPN



# But How to Choose between different Cloud providers?

**Requirements**

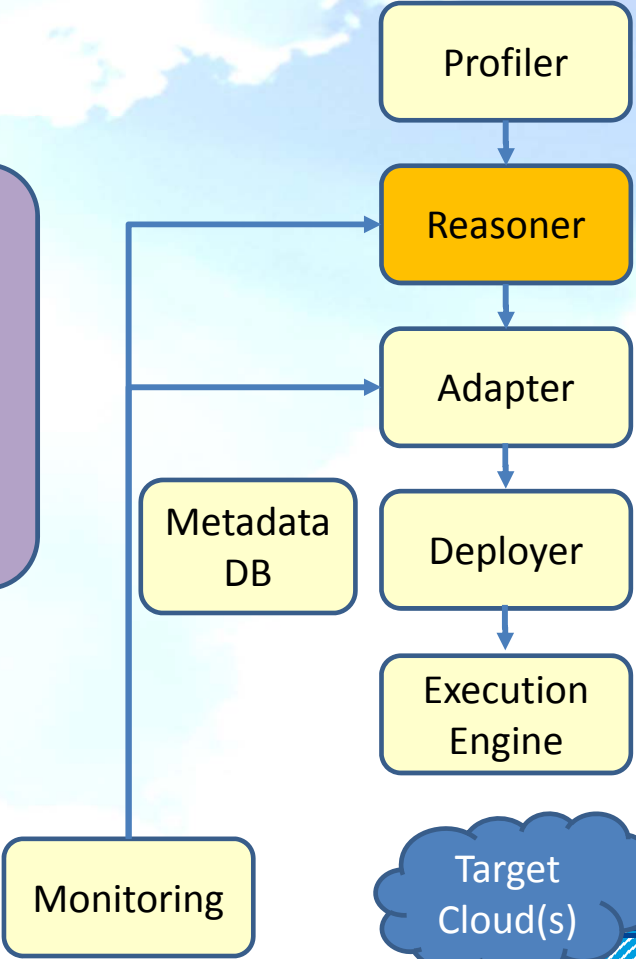
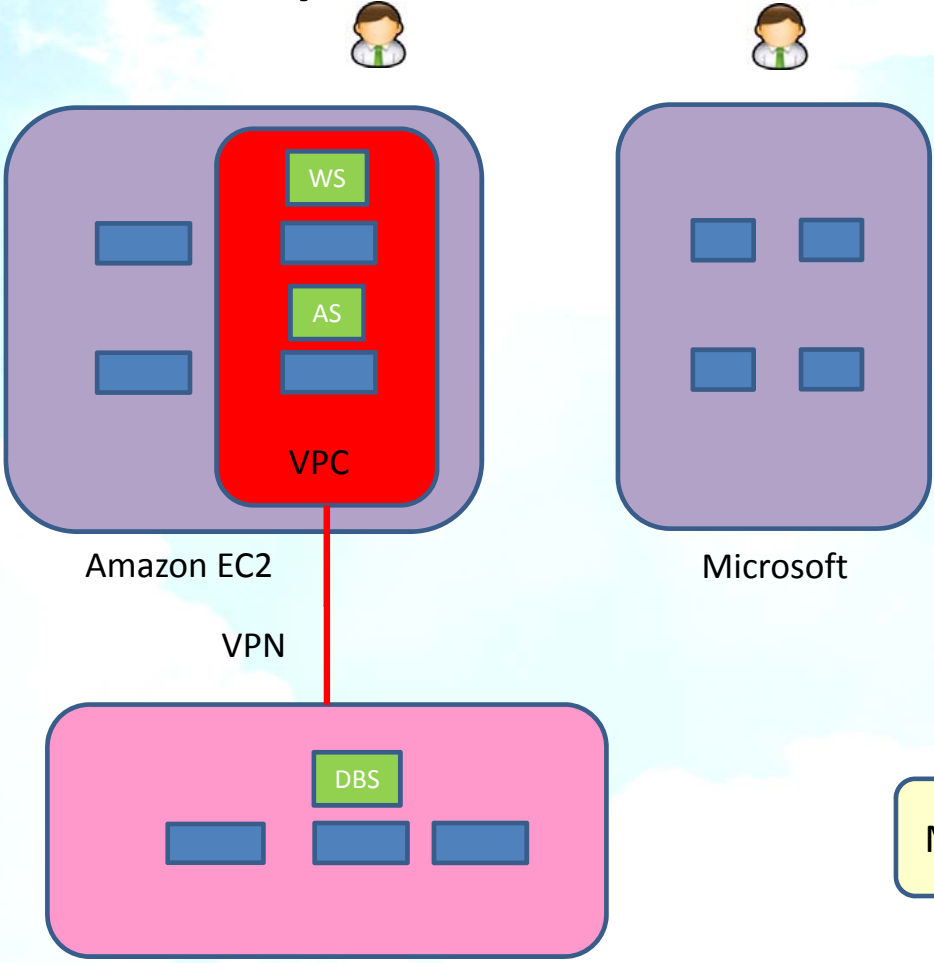
- WS** Confidential
- AS** Confidential
- DBS** Personal data, keep in PC

**Amazon Sec Features**

- Normal EC2
- VPC + VPN

**Microsoft Azure Features**

- Normal



# Choosing an initial Deployment: Matching Security Features



Requirements

- WS Confidential
- AS Confidential
- DBS Personal data, keep in PC

Amazon Sec Features

- Normal EC2
- VPC + VPN

Amazon Sec Controls

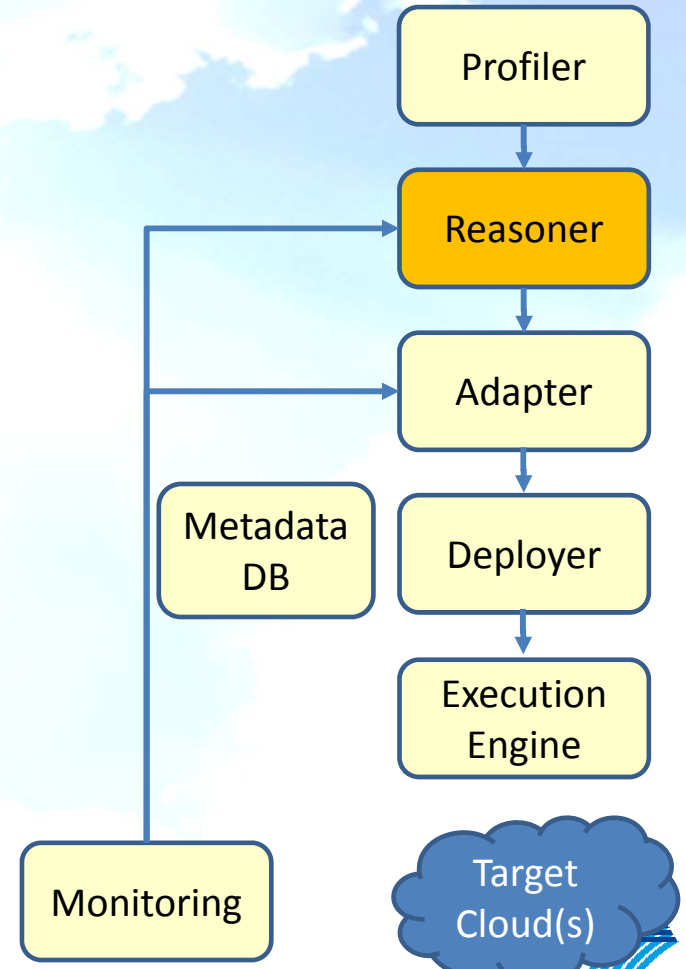
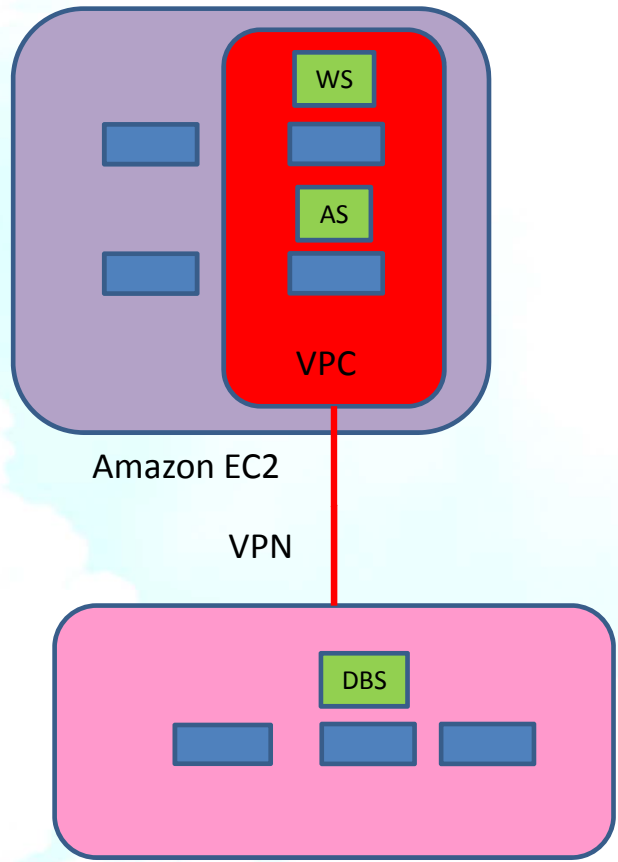
- auditability
- ...

Amazon Sec Certifications

- ...

Amazon Sec Reputation

- Monitored QoS
- Social network





# Monitoring (Observable) CIA Variables

## Requirements

- WS Confidential
- AS Confidential
- DBS Personal data, keep in PC

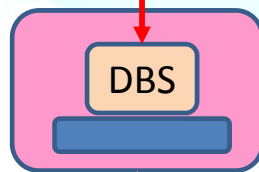
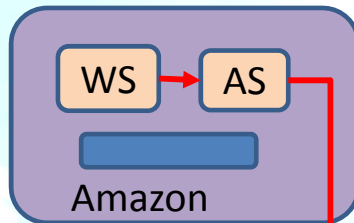
## Security reputation



## Availability

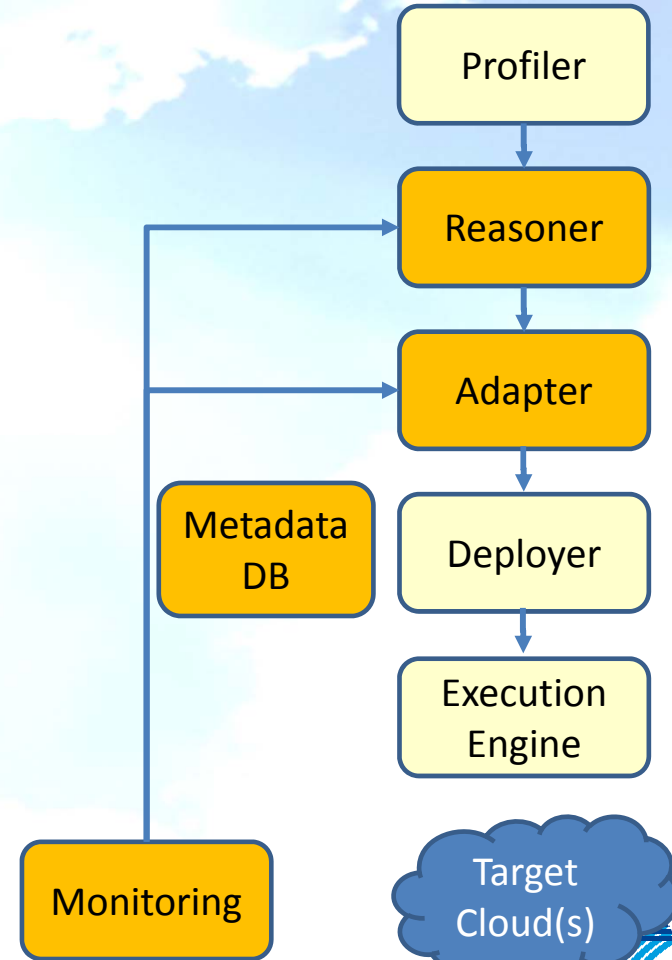


## Auditability



Cross Cloud Monitoring Infrastructure

PaaSage Platform



# Towards risk based management for Cloud Security

- Integrate security risk in optimised deployment selection
  - Minimise  $f(x)$  such that
    - $G(x) > 0$
    - $H(x) = 0$
    - ...
  - Maximise availability(x), Minimise cost(x) such that
    - CommunicationsSecured(x)
    - SecurityAuditsPerformedRegularly(x)
    - ...

# Conclusions and Cloud Security Standards

- Walkthrough of model based cloud deployment with security requirements: configuration, deployment, execution
- Cloud security standards in the deployment lifecycle:
  - Configuration: describing application security requirements (standard Protection level agreements?)
  - Deployment:
    - Cloud security features (via a standard security ontology?)
    - Specifying and reasoning on security controls (standard controls? Standard ontology to describe and compare controls?)
    - Reasoning on deployments (using standard cloud security ontologies?)
    - Risk based assessment of cloud security (standard cloud security risk assessment guidelines?)
  - Execution
    - Monitoring compliance to SLA/PLA (using standard PLA language?)
    - Measuring reputation (using standard controls)