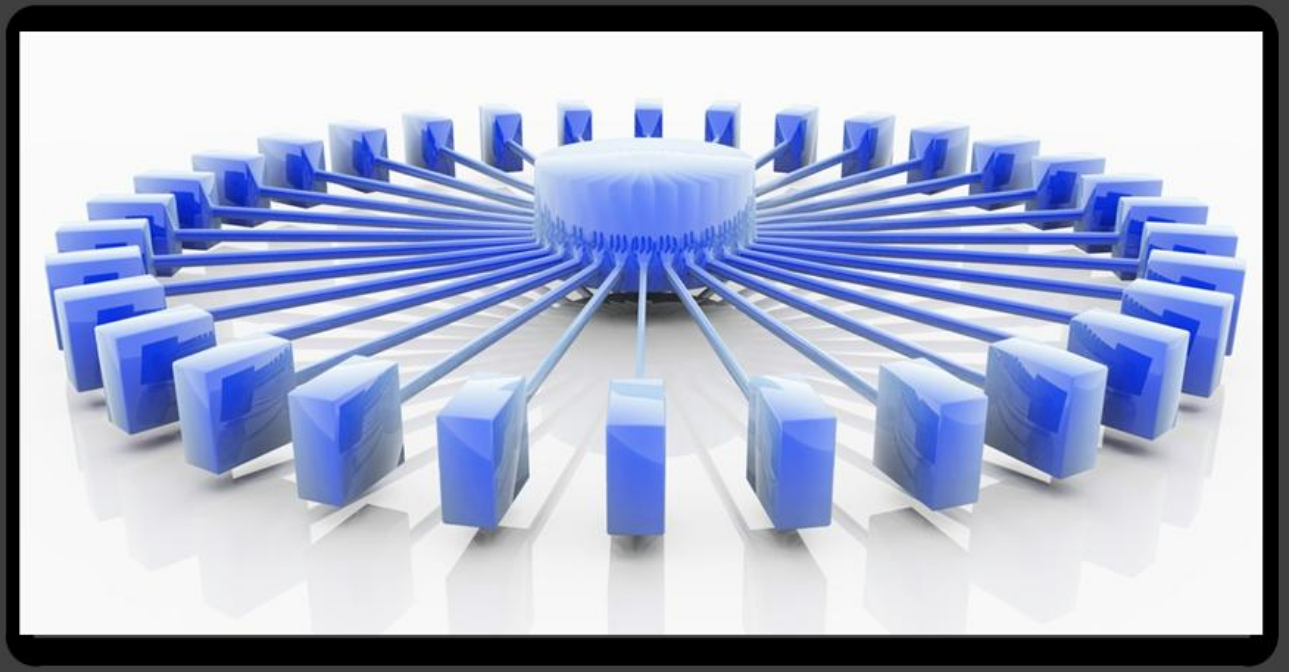
Community Cloud

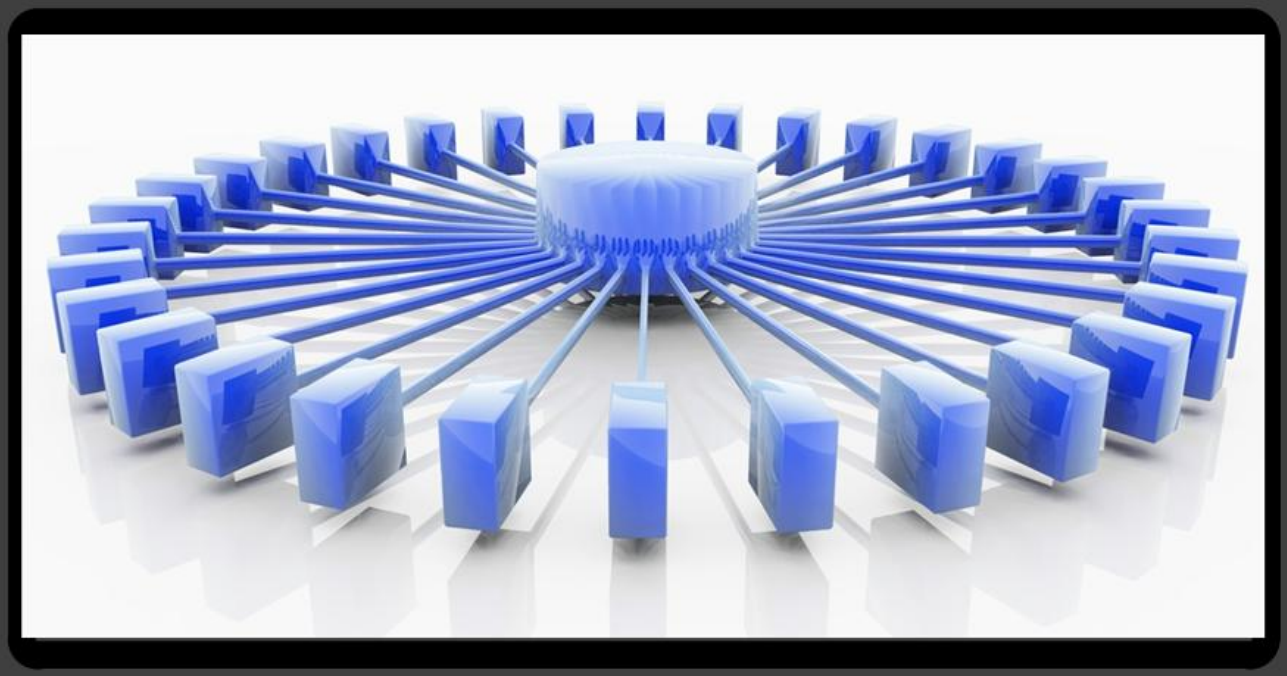


D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

Prof Bill Buchanan, Edinburgh Napier University

Author: Prof Bill Buchanan

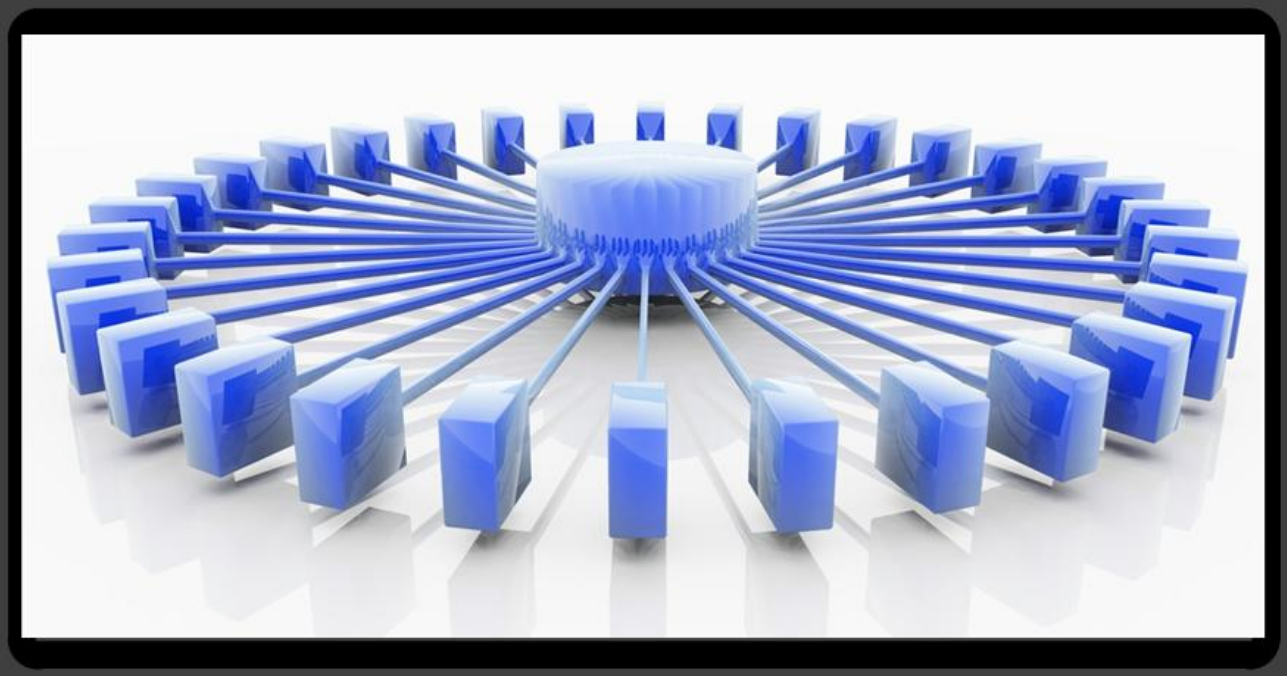
Community Cloud



- Overview for Cloud Computing.
- How Cloud Infrastructures could be used for teaching to enhanced skills.
- D-FET – A Community Cloud.
- Example used within teaching.

Author: Prof Bill Buchanan

Community Cloud



D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> Overview of Cloud Computing

Author: Prof Bill Buchanan

Terminals

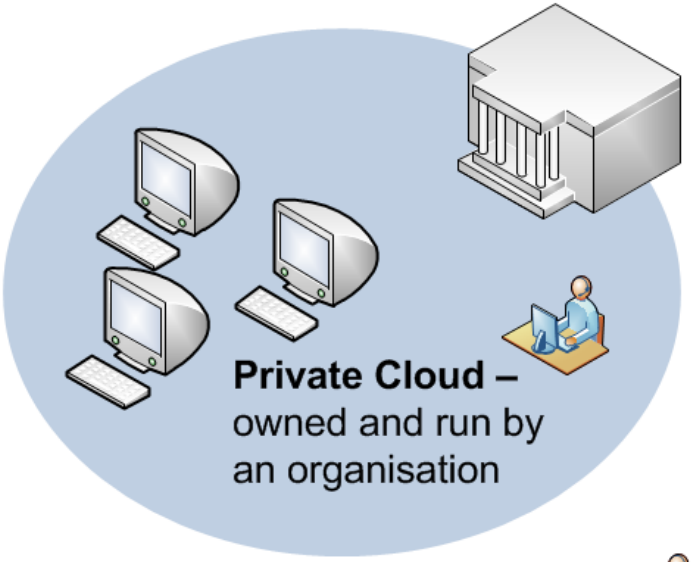
Mainframe

Stand-alone computers

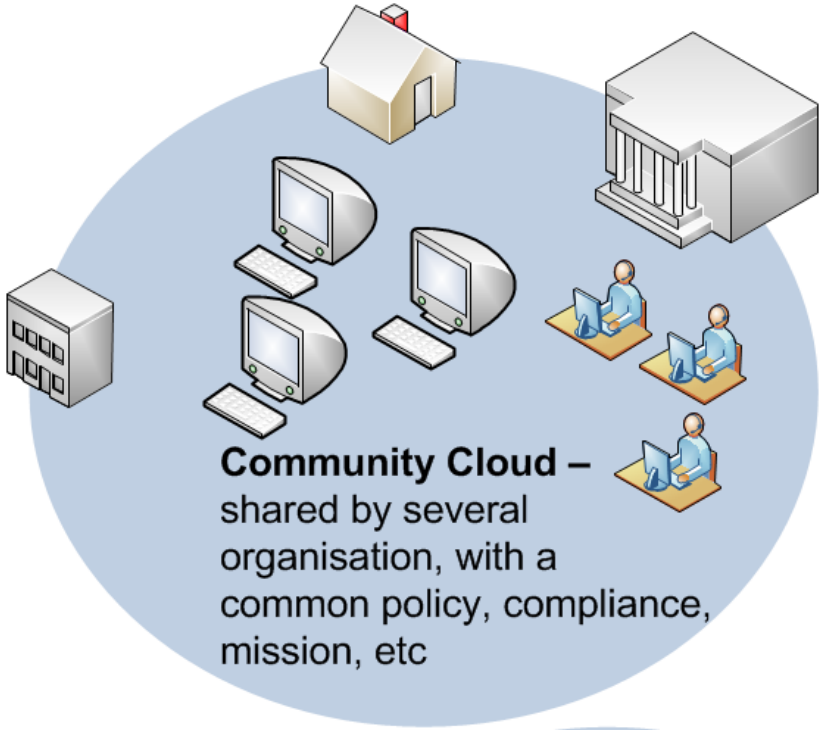
Computers connect to services (SoA)

Computers connected to servers

Servers

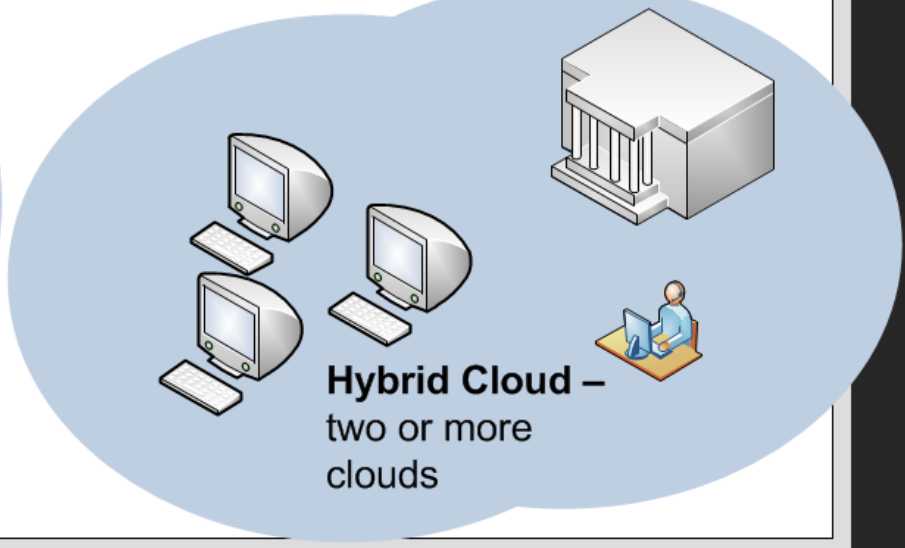


Private Cloud – owned and run by an organisation

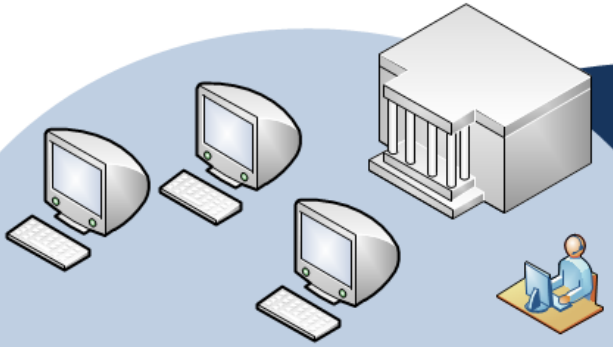


Community Cloud – shared by several organisation, with a common policy, compliance, mission, etc

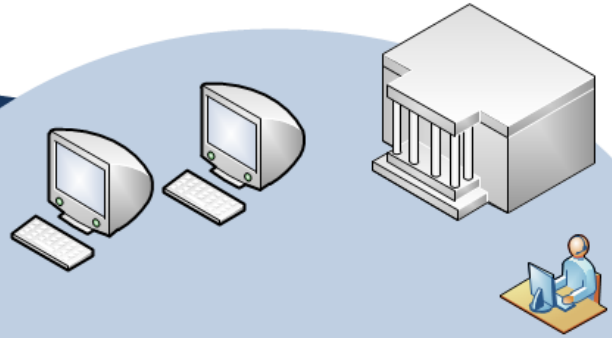
Public Cloud – owned by an organisation selling a cloud infrastructure



Hybrid Cloud – two or more clouds

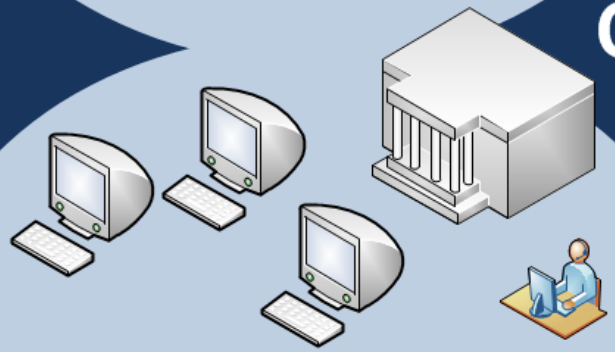


On-demand self-service. Consumers get server CPU, memory, bandwidth and storage resources whenever required.

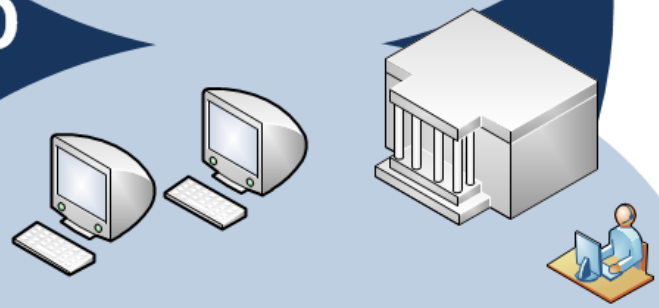


Location independent resource pooling. Multiple customers use shared resources within the provider, without actually knowing where the exact location of these are.

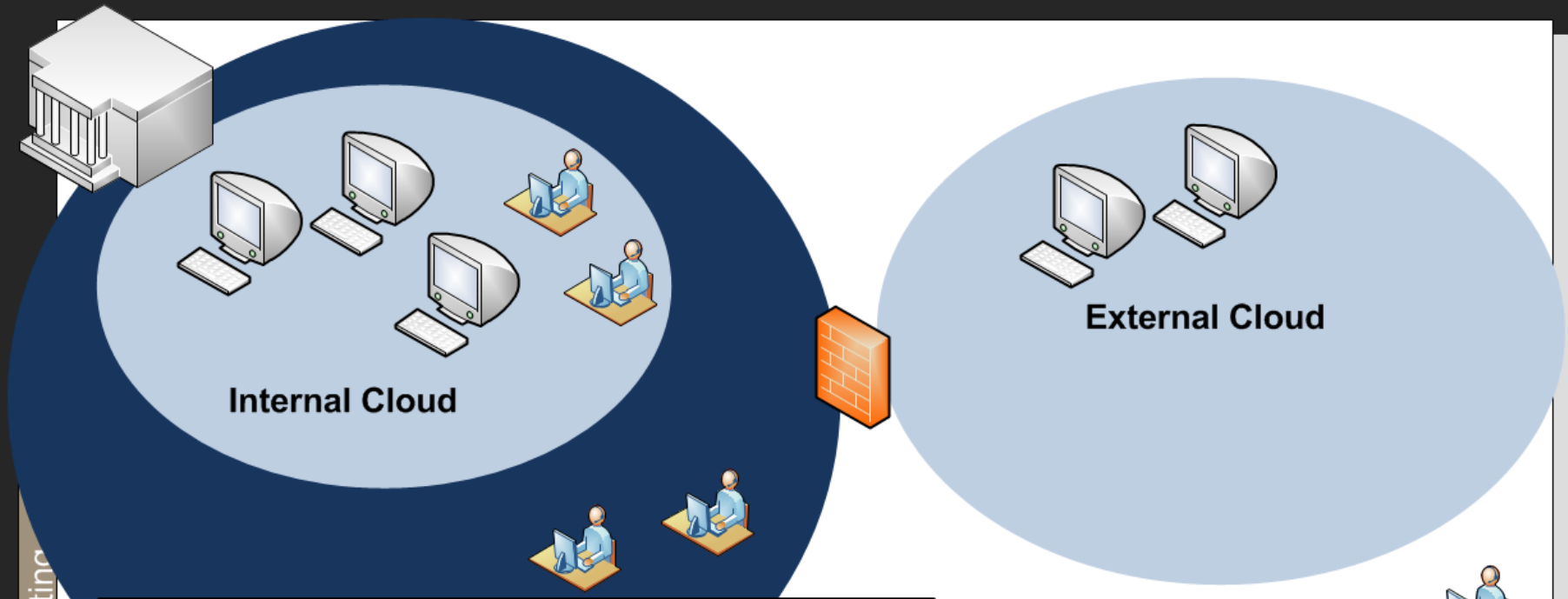
CLOUD

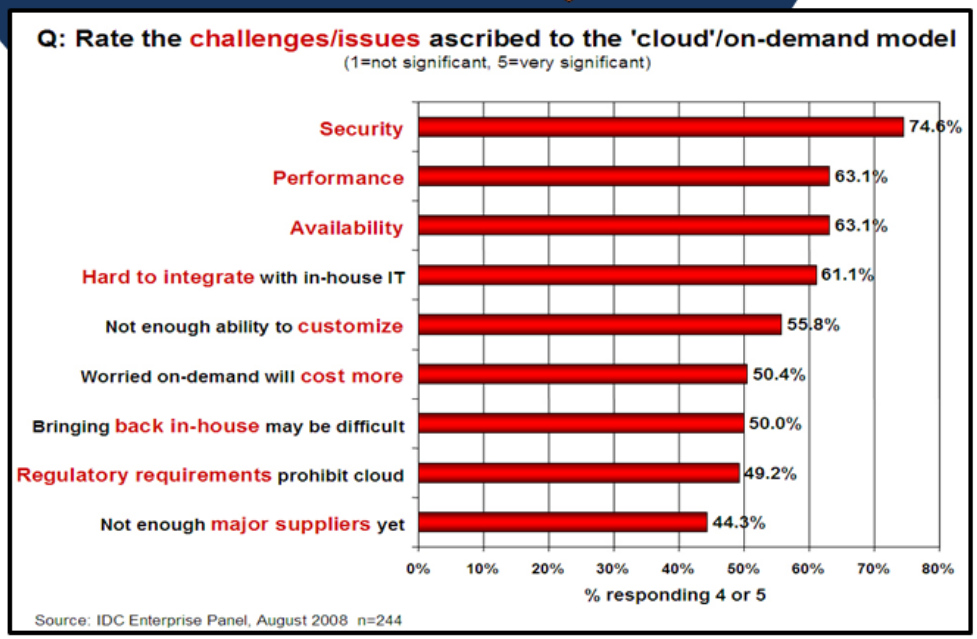


Rapid elasticity. Consumers can easily scale-up and scale-down, whenever required.



Pay per use. All access to resources is monitored, and paid for either by advertising or usage. Payment methods: per users created, per hour usage (service), etc.





Audit/compliance

Can I be compliant with statutory and regulatory requirements?

- Where is my data stored?
- Who handles breach notifications?
- How long is my data stored for?
- How is eDiscovery handled?

Cloud Computing

Cloud

Client

amazon web services

Pay-per-usage

Amazon SimpleDB
This produces a mixture of structured data storage with the reliability of a traditional database.

Amazon CloudFront
This allows content to be placed close to the places where it is to be consumed, the content thus gets moved to the edge of the cloud to support rapid delivery of content.

Amazon Elastic Cloud Compute (Amazon EC2)
This is the core of the Amazon Cloud, and provides a Web services API to create, manage and delete virtual servers within the Amazon Cloud. This includes US, Asia (Japan and Singapore) and European data centres (Ireland), and uses the Xen hypervisor for the management of the servers.

Amazon Simple Storage Service (Amazon S3).
This provides data storage with web services through APIs. It differs from normal filesystems in that it does not have a hierarchal structure. Instead it uses buckets, which are unique namespaces across all of the Amazon customers. It is thus not a filesystem, and is a Web service, thus applications need to be written which specifically store data into the S3 Cloud.

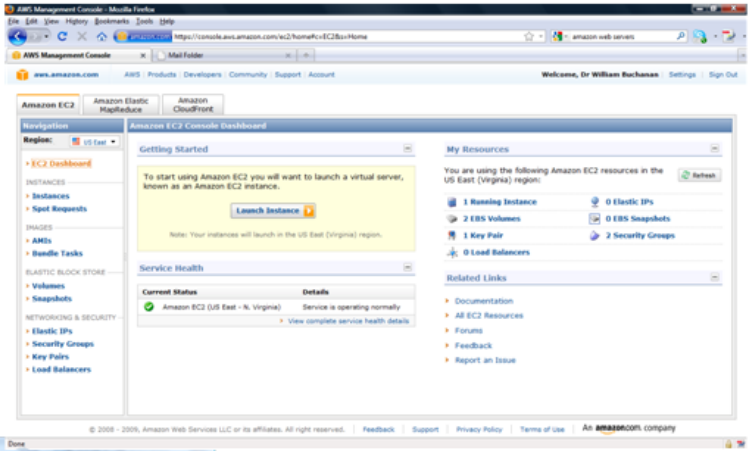
Amazon Simple Queue Service (Amazon SQS).
This supports a grid infrastructure, where message can be passed to a queue, and then consumed by any subscribers.

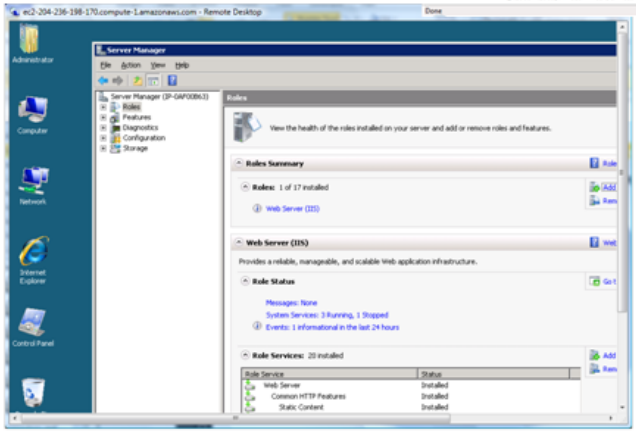
Amazon Virtual Private Cloud (VPC) This allows for complete network infrastructures to be built, which are isolated from other network infrastructures

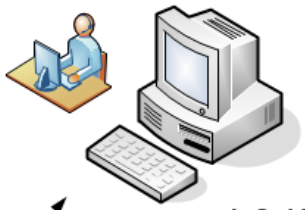
AWS Cloud

Amazon Web Services

Amazon Machine Images (AMI)



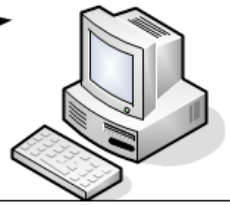




i-0d895567

Machine Instances

- Command line tools
- Web Service Console



i-0d895566

```
$ ec2-describe-images -o AKIAIWUMTTAZYST2I2AA
$ ec2-describe-images
IMAGE ami-45c22e2c powerdns/image.manifest.xml 495219933132 available private
$ ec2-run-instances i-0d895566
```

Client

amazon web services

Pay-per-usage

Amazon Simple Storage Service (Amazon S3).

This provides data storage with web services through APIs. It differs from normal filesystems in that it does not have a hierarchal structure. Instead it uses buckets, which are unique namespaces across all of the Amazon customers. It is thus not a filesystem, and is a Web service, thus applications need to be written which specifically store data into the S3 Cloud.

bill.bucket

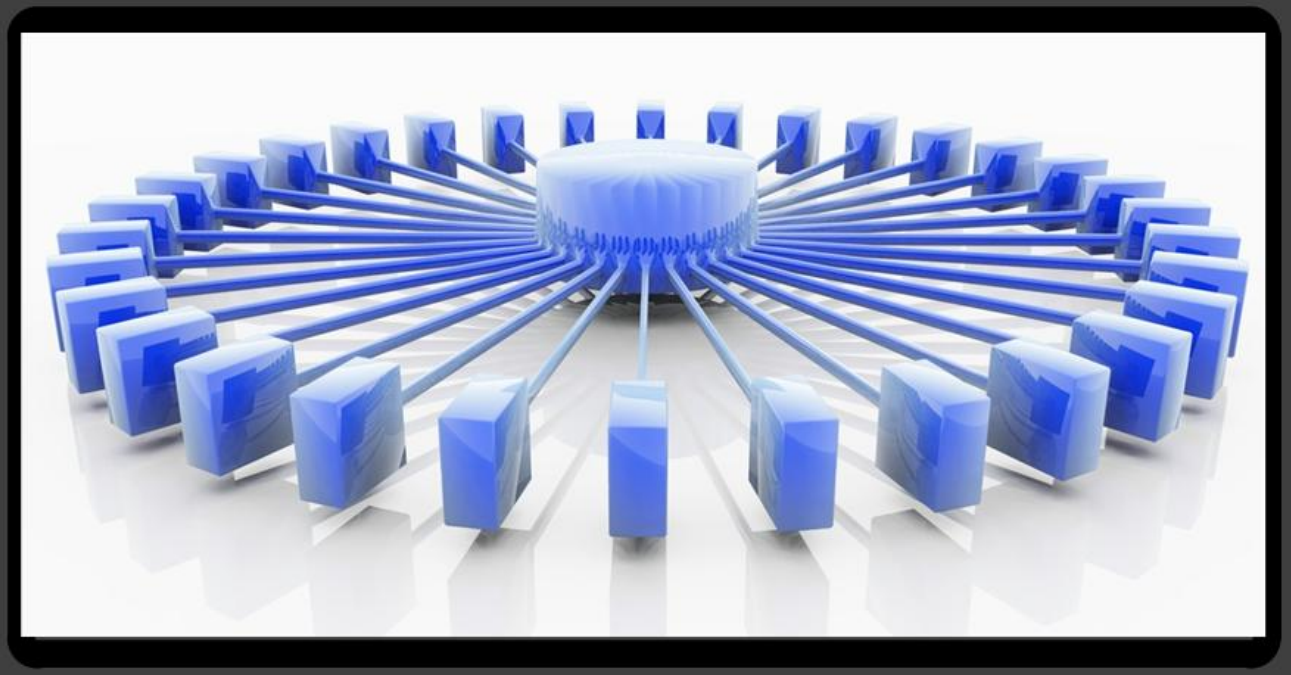
- Data storage: $0.125 per GB per month.
- Windows desktop: $0.12 per hour.
- Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year – less than one hour per year.

```
s3cmd mb s3://bill.bucket
s3cmd put myfile.mp3 s3://bill.bucket/myfile.mp3
s3cmd get s3://bill.bucket/myfile.mp3 myfile.mp3

s3cmd ls
s3cmd ls s3://bill.bucket/

s3cmd delete s3://bill.bucket/myfile.mp3
s3cmd rb s3://bill.bucket
```

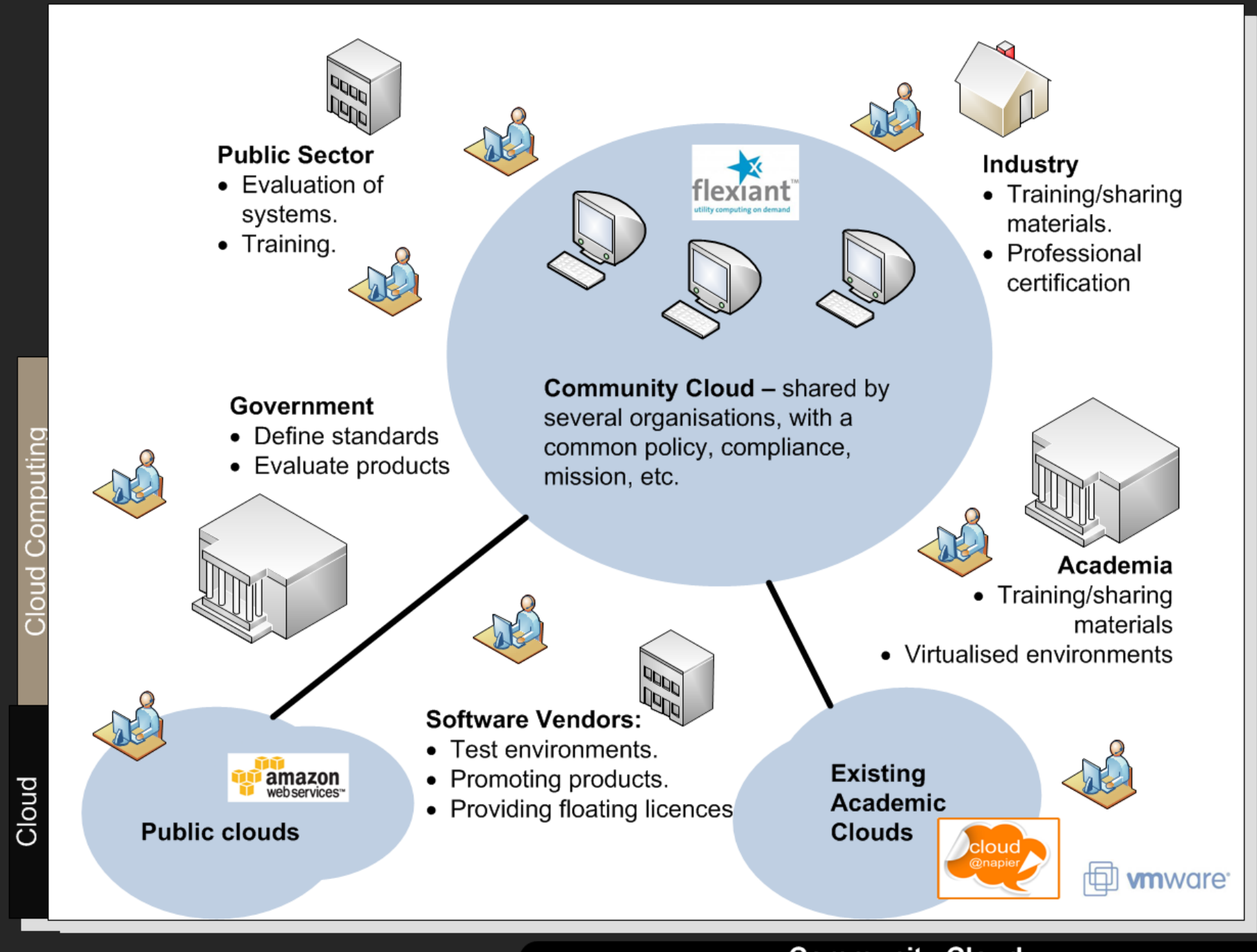
Community Cloud



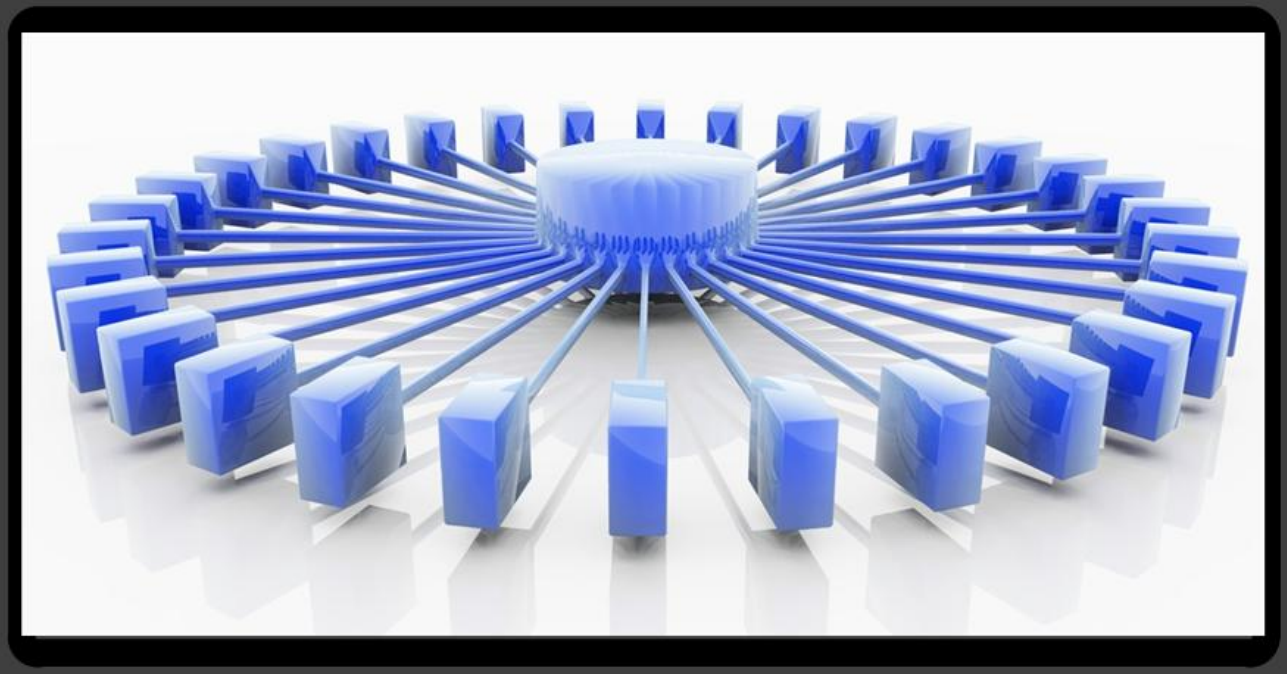
D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> How Cloud Computing could be used to enhance skills

Author: Prof Bill Buchanan


Cloud Computing
Cloud
Public Sector
• Evaluation of systems.
• Training.
Industry
• Training/sharing materials.
• Professional certification
flexiant
utility computing on demand
Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc.
Government
• Define standards
• Evaluate products
Academia
• Training/sharing materials
• Virtualised environments
Software Vendors:
• Test environments.
• Promoting products.
• Providing floating licences
amazon web services
Public clouds
Existing Academic Clouds
cloud @napier
vmware
Community Cloud

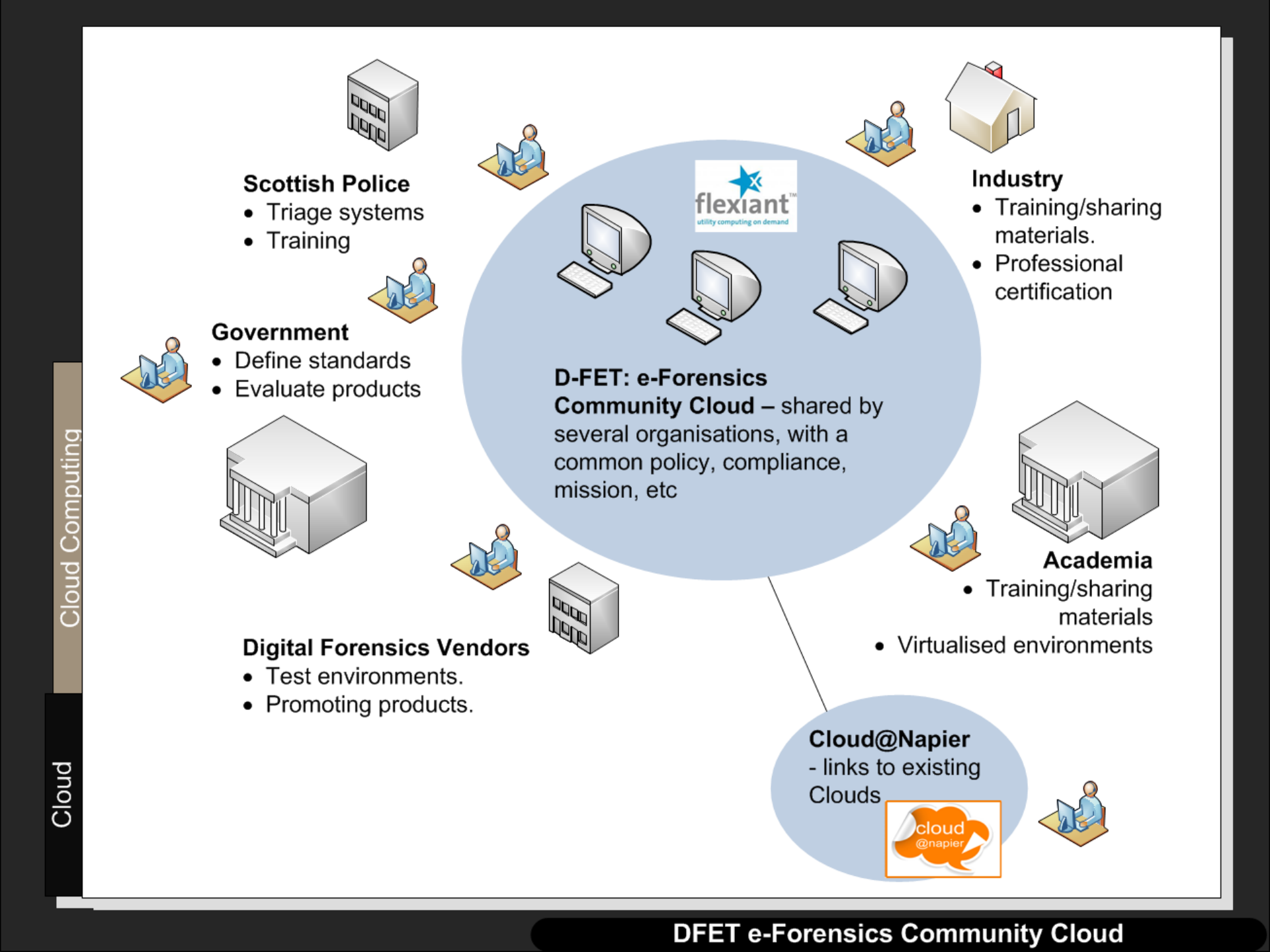
Community Cloud



D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> D-FET – A Community Cloud

Author: Prof Bill Buchanan


Cloud Computing
Cloud
Scottish Police
• Triage systems
• Training
Government
• Define standards
• Evaluate products
flexiant
utility computing on demand
D-FET: e-Forensics Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc
Industry
• Training/sharing materials.
• Professional certification
Academia
• Training/sharing materials
• Virtualised environments
Digital Forensics Vendors
• Test environments.
• Promoting products.
Cloud@Napier
- links to existing Clouds
cloud @napier
DFET e-Forensics Community Cloud

Distance learners
- Exact environments as face-to-face students.
- Blended learners have greater choice and flexibility.

Industry
- Adding evaluation infrastructures.
- Post project work/ interesting areas of work.
- Ability to review materials presented to students.
- Ability to study within the workplace.

Enhancing skills
- Supports a wide range of pre-built enviroments within a sandboxed infrastructure

Working across institutions
- Cloud environments allow for working across traditional boundaries.

Project work
- Students can start from existing well-tested environments.

Engaging students
- State-of-the-art infrastructures

Community Cloud – shared by several organisations, with a common policy, compliance, mission, etc

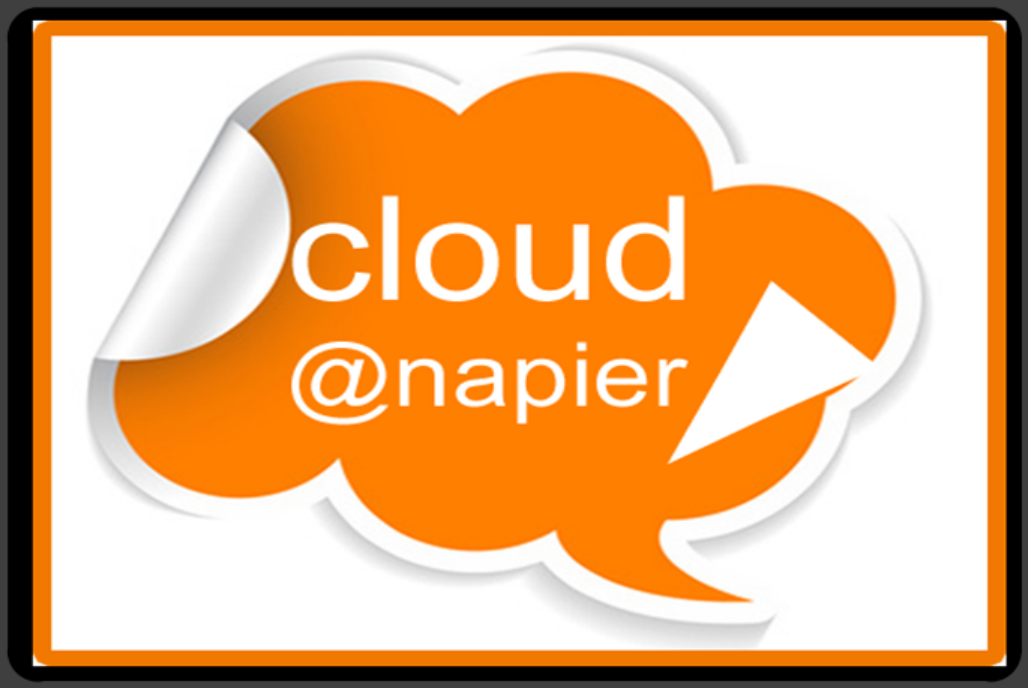
Continuation of work
- Students can carry their infrastructures throughout modules/ years.

Group working
- Students can integrate their systems in an isolated environment.

Robust infrastructures
- No more 9-5pm, Mon-Friday environments.

Snap-shots of work
- Student can create snap-shots, and move back and forward amoungst them.

Community Cloud



D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

> Example used in teaching

Author: Prof Bill Buchanan

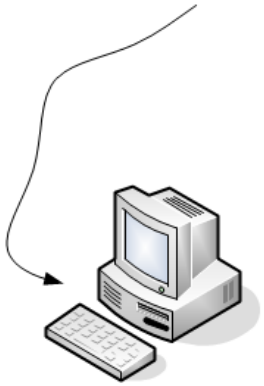
White Hat

Good...

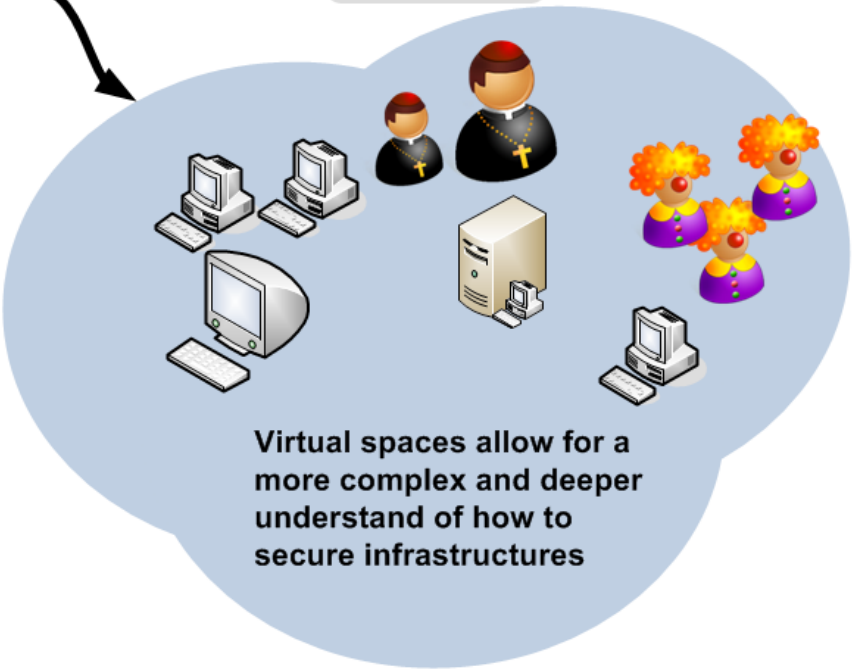
... Bad

Black Hat

Grey Hat



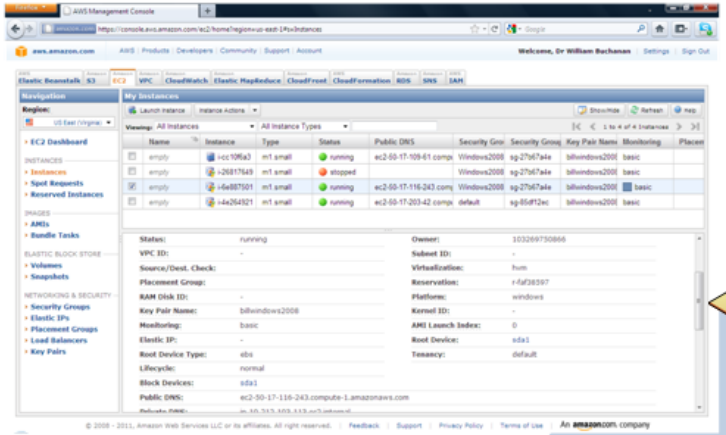
Difficult to use many of the techniques within a real-life space



Virtual spaces allow for a more complex and deeper understand of how to secure infrastructures

Demands on professional certification

Employers now require in-depth knowledge and a range of skills



Virtualised and Cloud-based labs (AWS):

- Range of state-of-the-art operating systems and tools.
- Evaluation of Public Cloud resources.

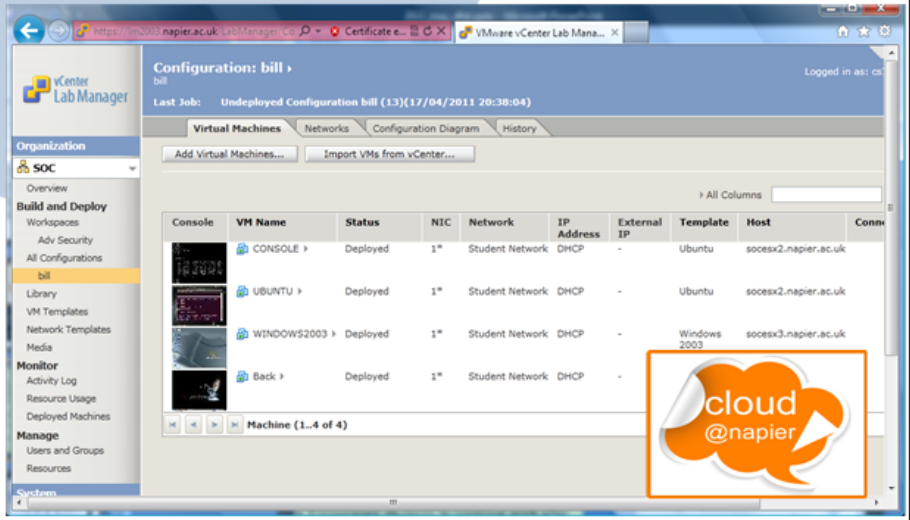
amazon web services™

Teaching of four modules in computer security, digital forensics and database systems for 2010/2011 (inc. CSN09102/CSN10102/CSN11112) - BEng/BEng (Hons)/MSc

vmware

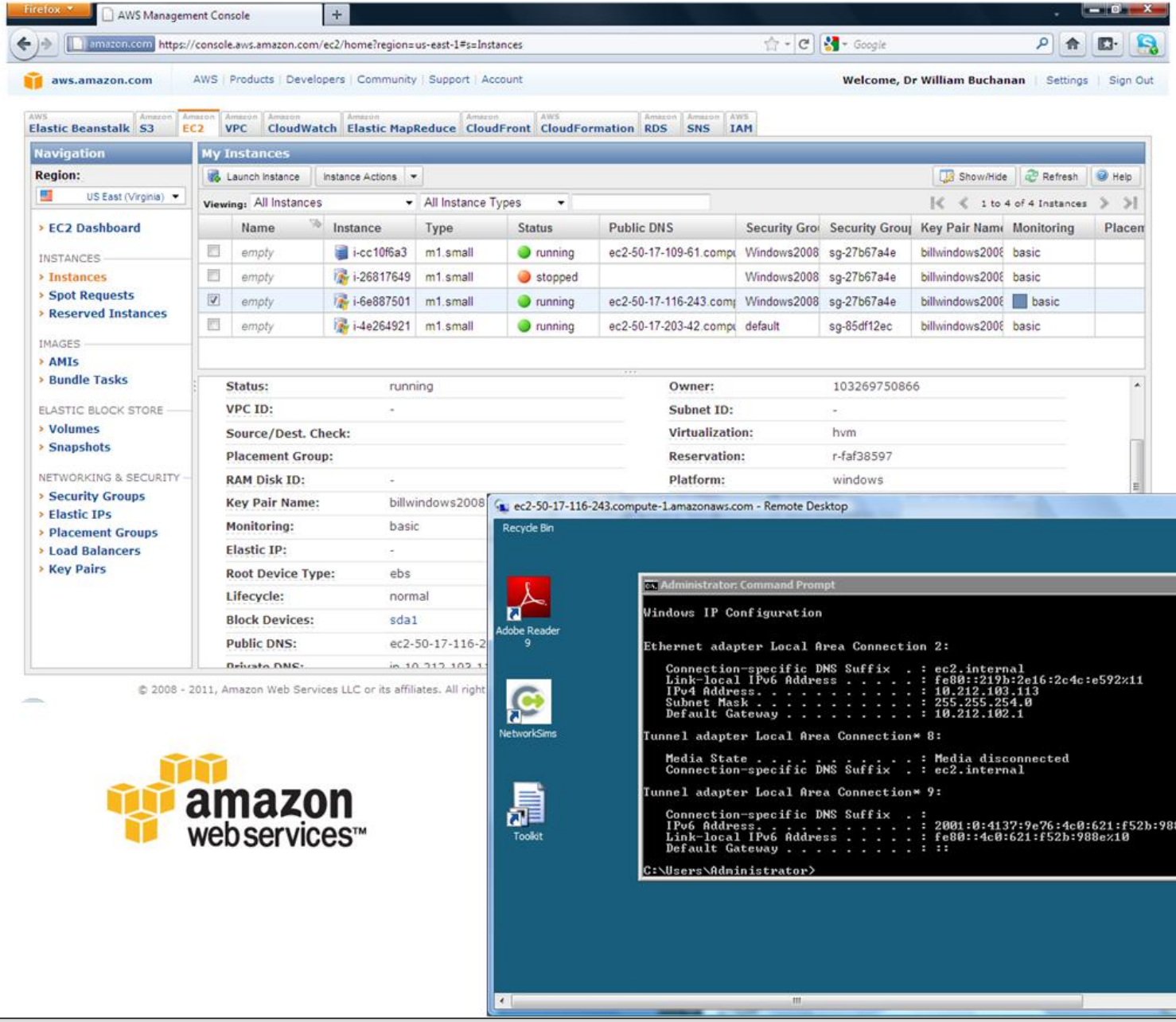
Virtualised and Cloud-based labs:

- Complex infrastructures for evaluation for students.
- Deep analysis of security and digital forensics in an isolated environment.
- Industry standard tools and methods.



Cloud Computing

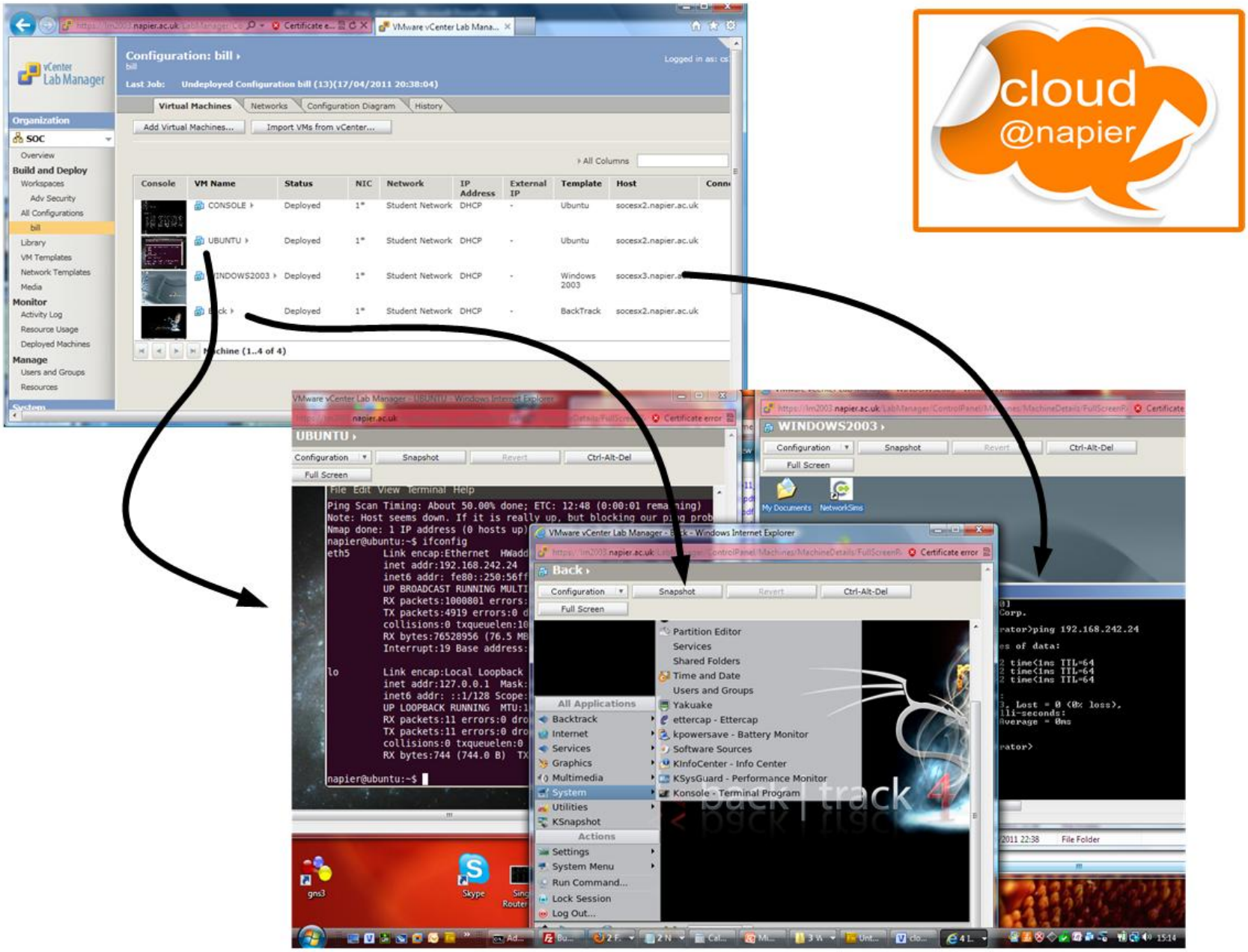
Cloud



amazon web services™

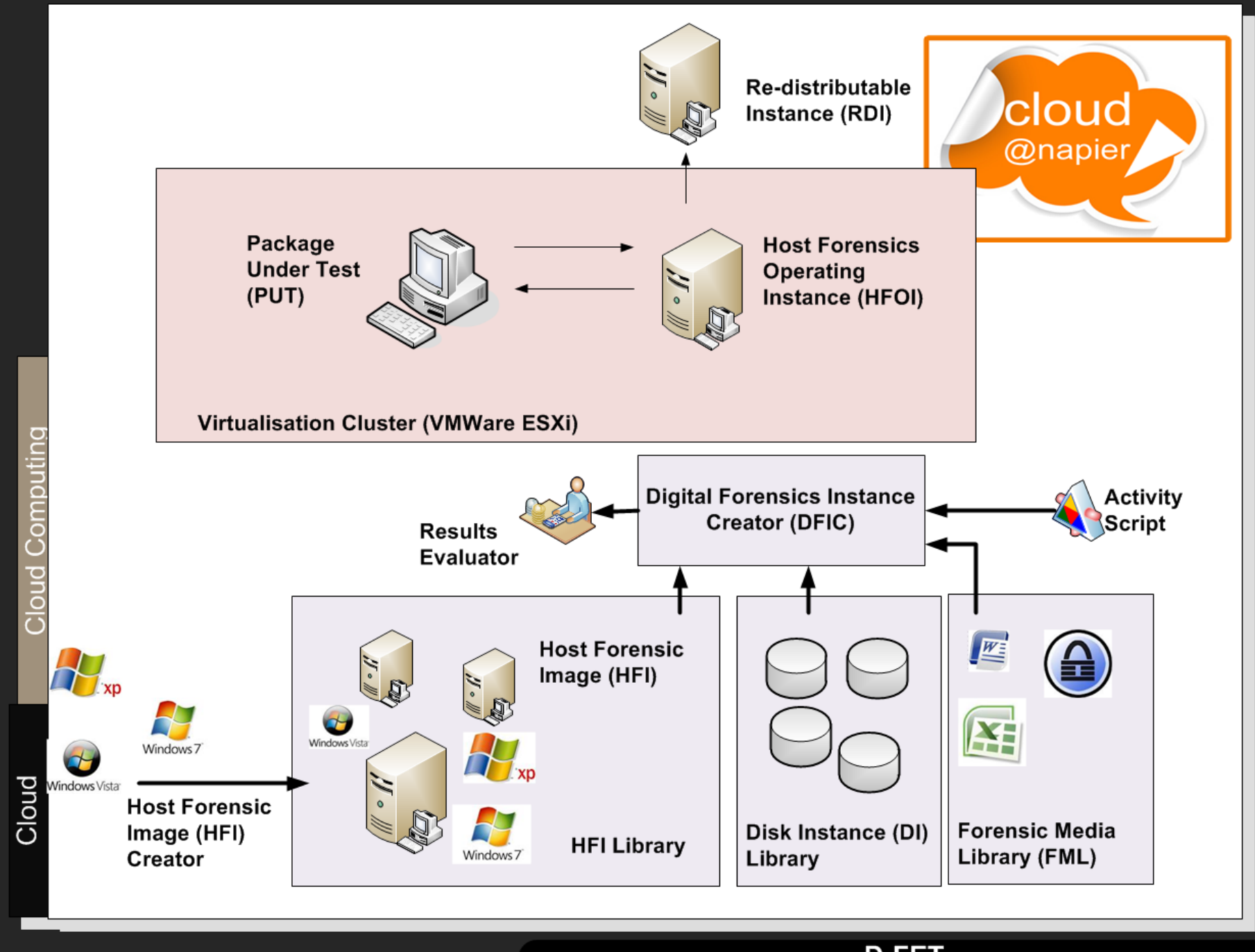
Cloud Computing

Cloud

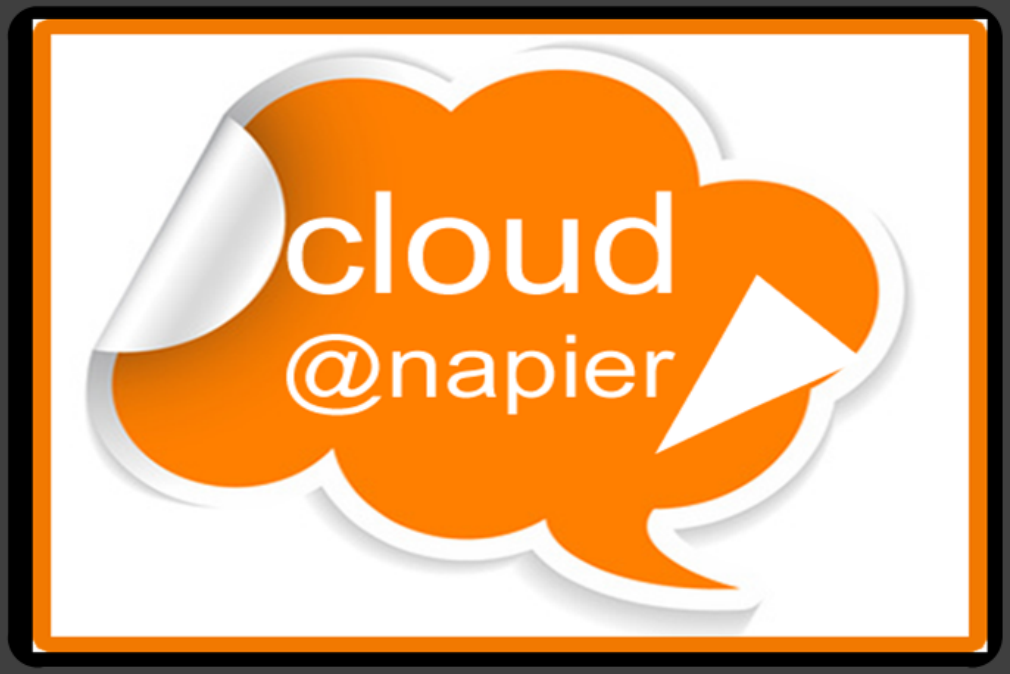


Cloud Computing

Cloud


Re-distributable Instance (RDI)
cloud @napier
Package Under Test (PUT)
Host Forensics Operating Instance (HFOI)
Virtualisation Cluster (VMWare ESXi)
Cloud Computing
Results Evaluator
Digital Forensics Instance Creator (DFIC)
Activity Script
Host Forensic Image (HFI)
Windows Vista
xp
Windows 7
Windows Vista
Host Forensic Image (HFI) Creator
HFI Library
Disk Instance (DI) Library
Forensic Media Library (FML)
Cloud
D-FET

Community Cloud

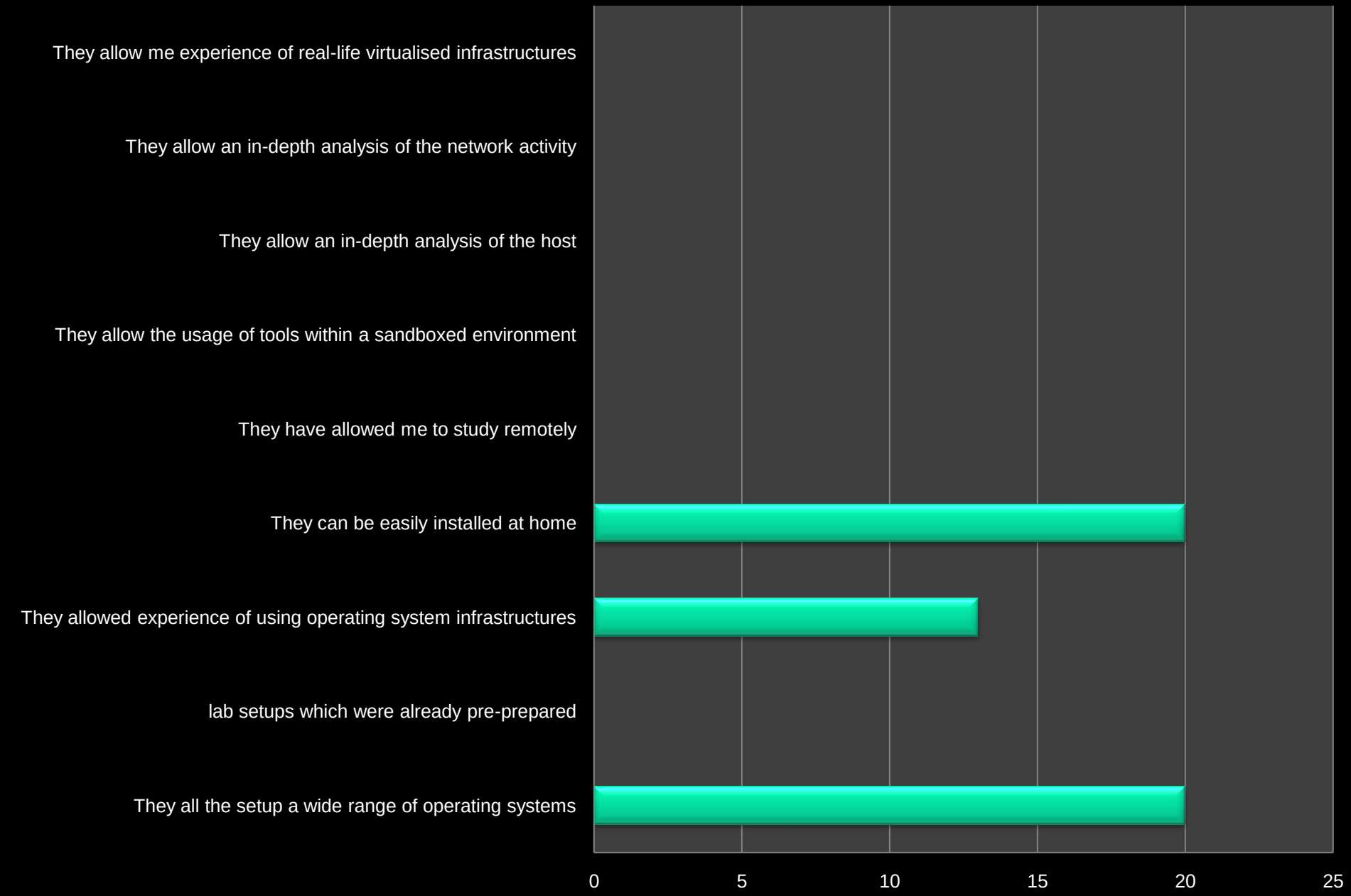


D-FET – A Community Cloud for Enhancing Skills using Virtualised Environments and Cloud-based Infrastructures

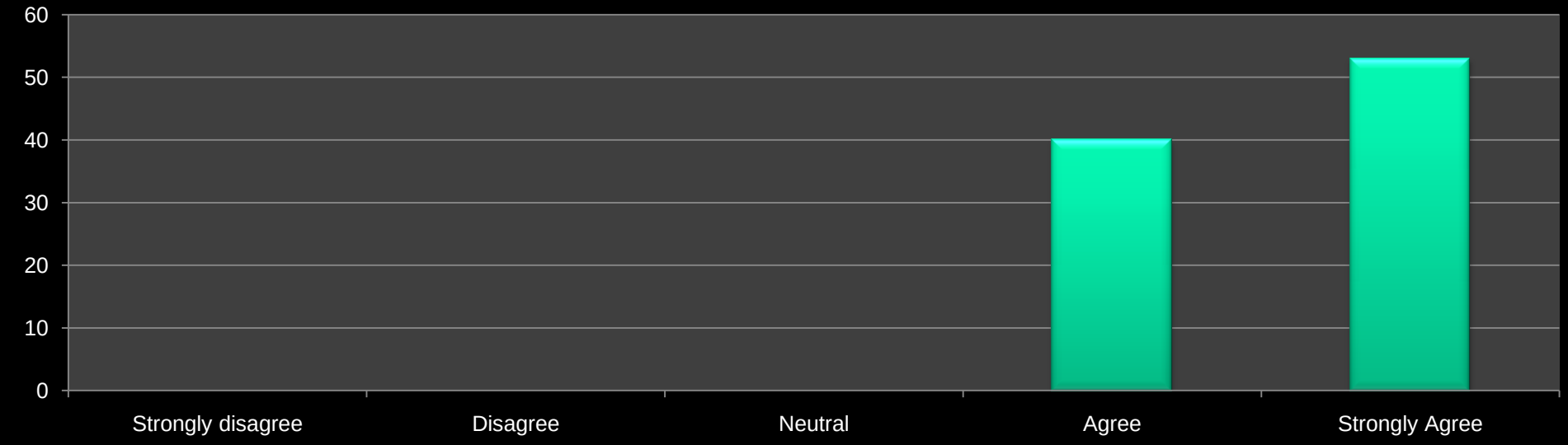
> Some results

Author: Prof Bill Buchanan

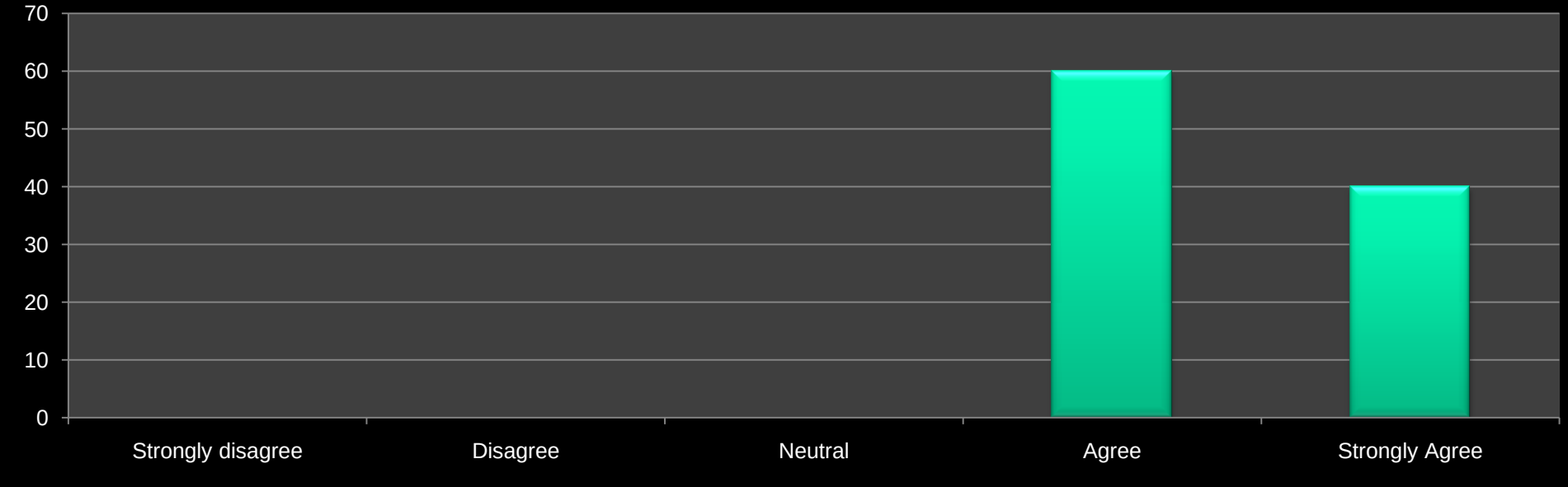
17. Within a computing module, which is the main advantage of using VMWare images:



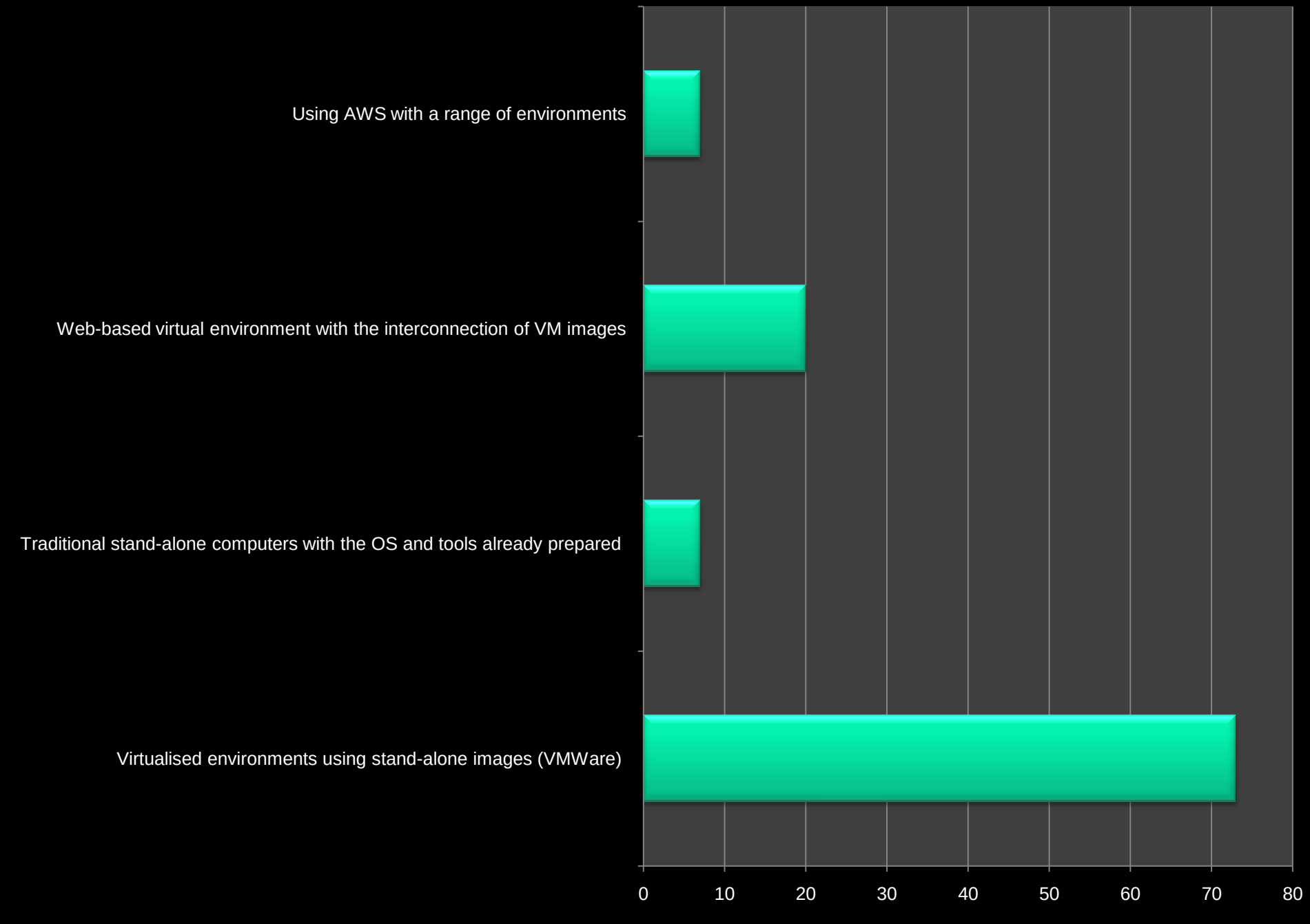
3. For VMWare images, they allowed you to setup a wide range of operating systems.



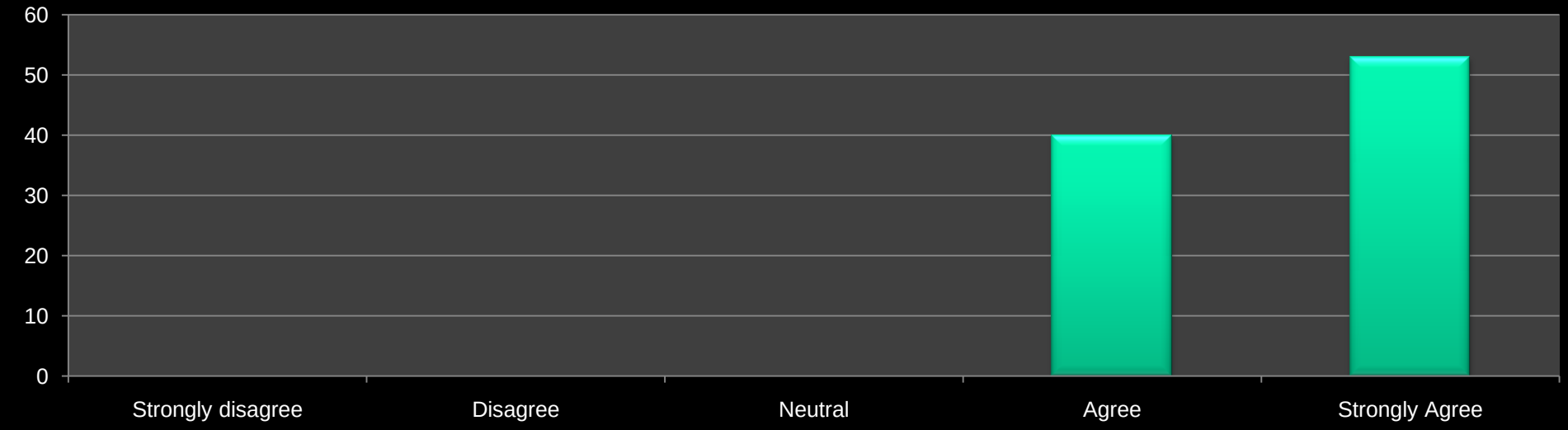
4. For VMWare images, they supported lab setups which were already pre-prepared.



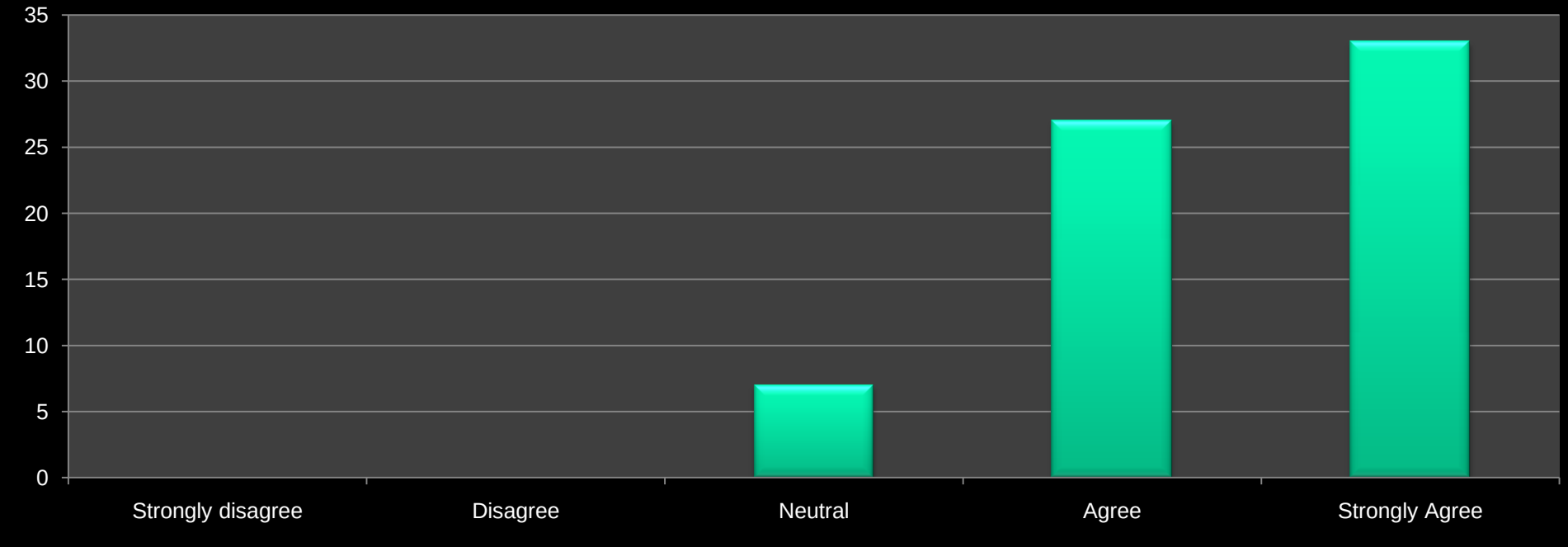
13. In labs, which environment do you prefer:



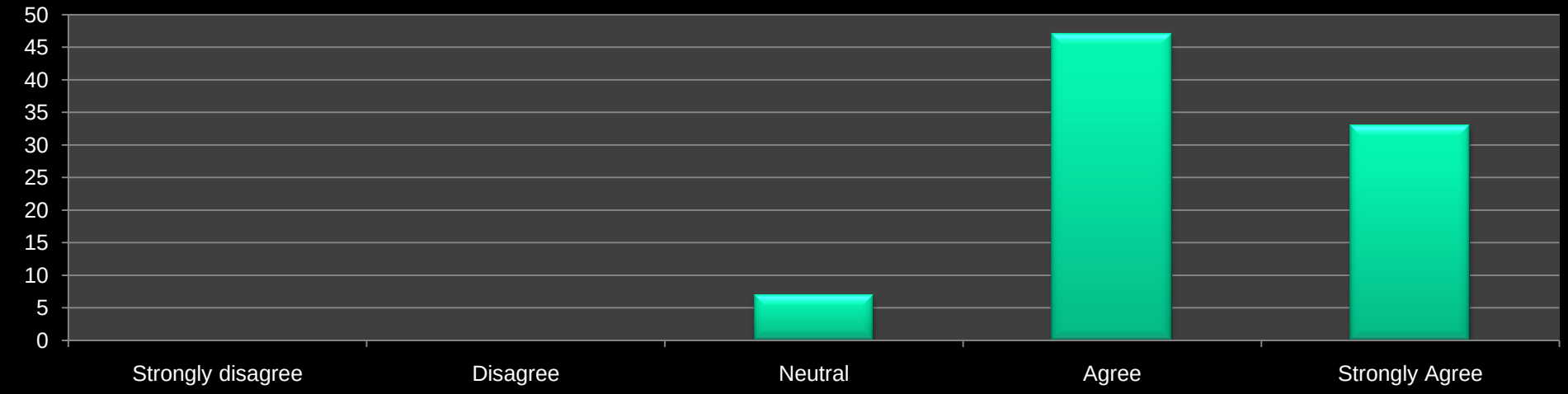
10. For AWS, they allowed experience of using real-life cloud infrastructures.



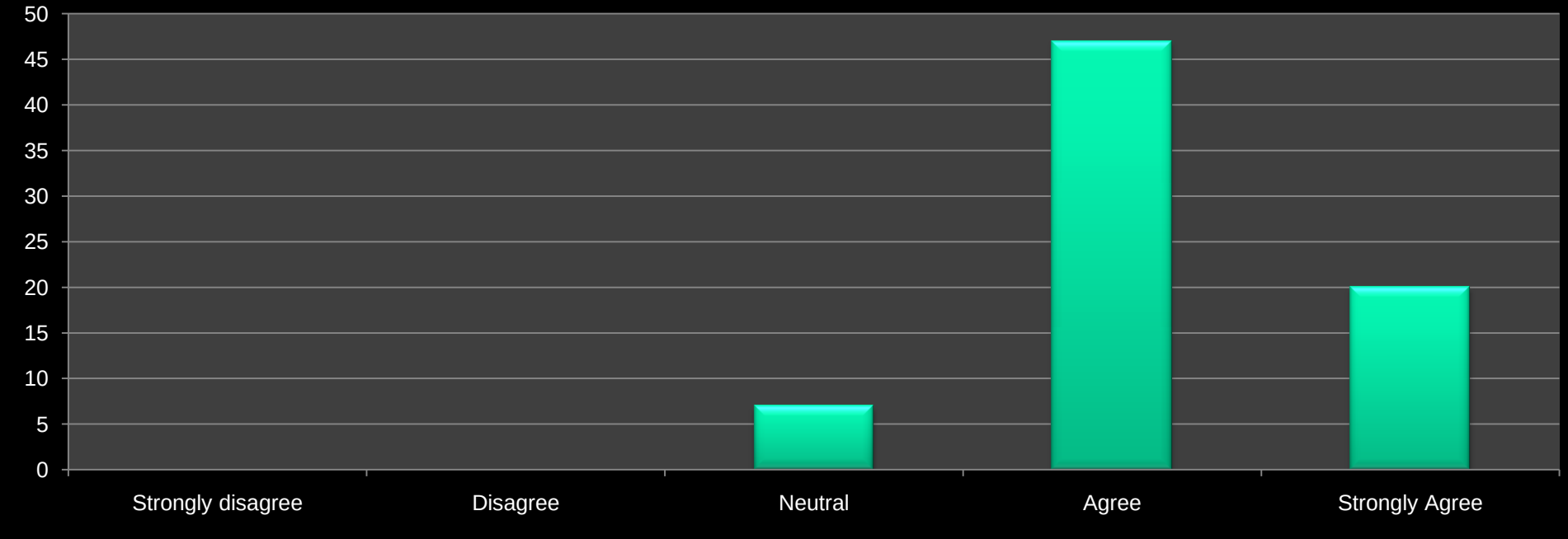
11. For AWS, they have allowed me to study remotely.



8. For AWS, they allowed me to setup a wide range of operating systems.

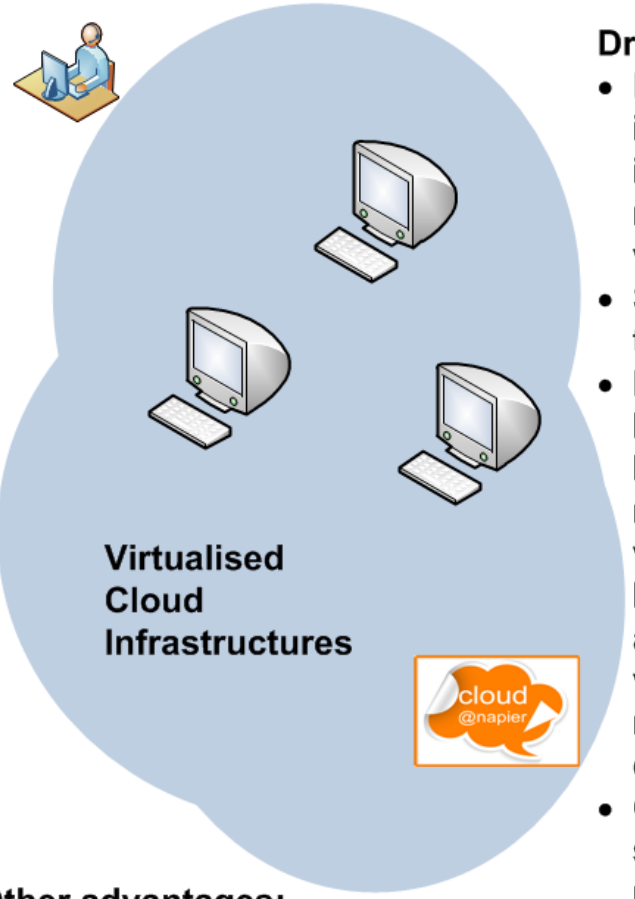


9. For AWS, they supported lab setups which were already pre-prepared.



Skills:

- Allows students to remotely complete labs.
- Students training on state-of-the-art infrastructures.
- Different labs can be created for different situations (Linux/Oracle/Windows IIS/etc).
- Supports remote/distance learning.
- Infrastructure can be ring-fenced.
- Supports group work in an isolated environment.
- In-depth analysis of infrastructures.
- Students can build systems from scratch.
- Students can update their own infrastructure/tools, as required.
- Seems to engage the students, and show them a wide potential.
- Encourages students to continue work after the lab/tutorial.
- Time windows of labs/tutorials can be carefully controlled.
- Extensive and complex infrastructures assessed within a sandboxed environments.



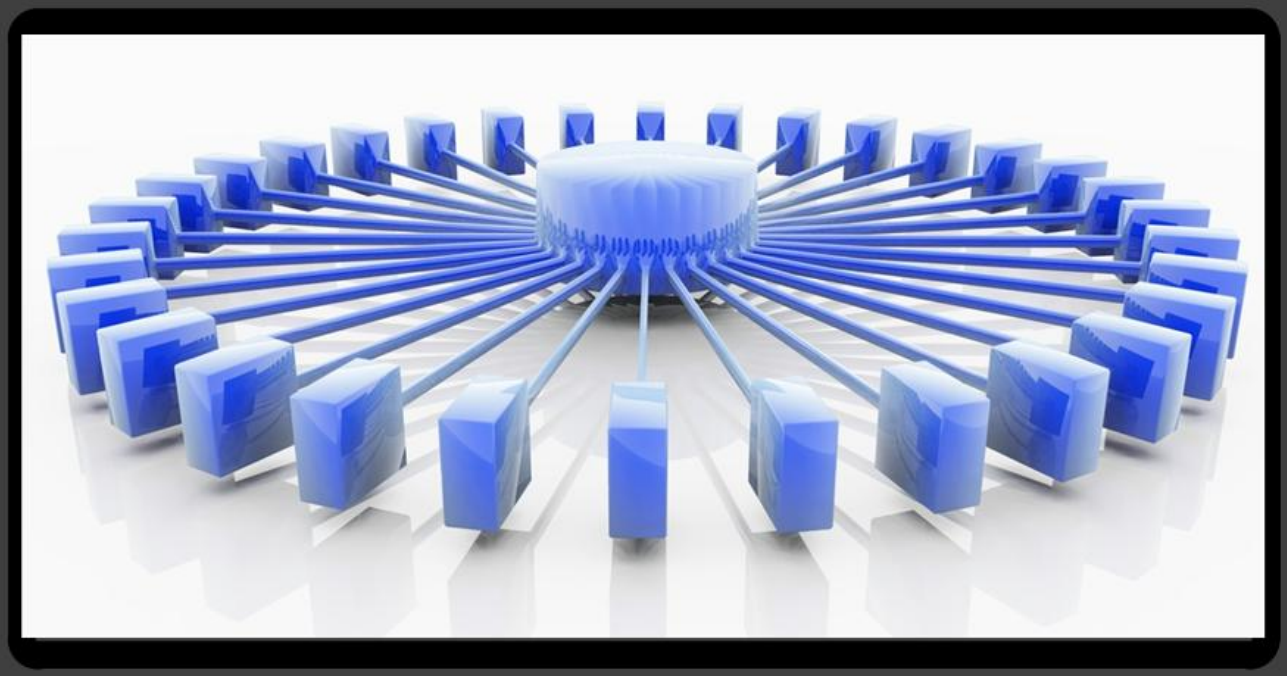
Drawbacks:

- Requires an investment in time in creating and maintaining the virtual image.
- Students can avoid the lab situation.
- Possibly requires a backup strategy for labs (if using network-based virtualisation – but has advantages that a standalone version does not need a network connection).
- Goes against the stand-alone machine philosophy.

Other advantages:

- Easy for teaching team to update.
- Helps with franchised colleges.
- Easy setup for classroom demonstrations.
- Infrastructure can be ring-fenced.
- Produces repeatable labs.
- Not dependent on Napier/network infrastructure.
- Time windows of labs/tutorials can be carefully controlled.

Community Cloud



- Overview for Cloud Computing.
- How Cloud Infrastructures could be used for teaching to enhanced skills.
- D-FET – A Community Cloud.
- Example used within teaching.

Author: Prof Bill Buchanan