

EE 4215

Security Technology

Lecture 10: Cloud Computing Security
2018/19 Semester B

Course Structure

- Week 1: Security Fundamental
- Week 2: Classical Cryptography
- Week 3: Number Theory &
- Week 4: DES
- Week 5: Secret-key Cryptography
- Week 6: Public-key Cryptography
- Week 7: Quiz 1
- Week 8: Hashing, Digital Signature, PKI
- Week 9: SSL/TLS, Web Security
- Week 10: Wi-Fi & P2P Security, Blockchain Security
- Week 11: Smart-card Security
- Week 12: Cloud Computing Security
- Week 13: Quiz 2
- Week 13: Secure-code, Trusted Hardware, Review

Lecture 10: Cloud Computing Security

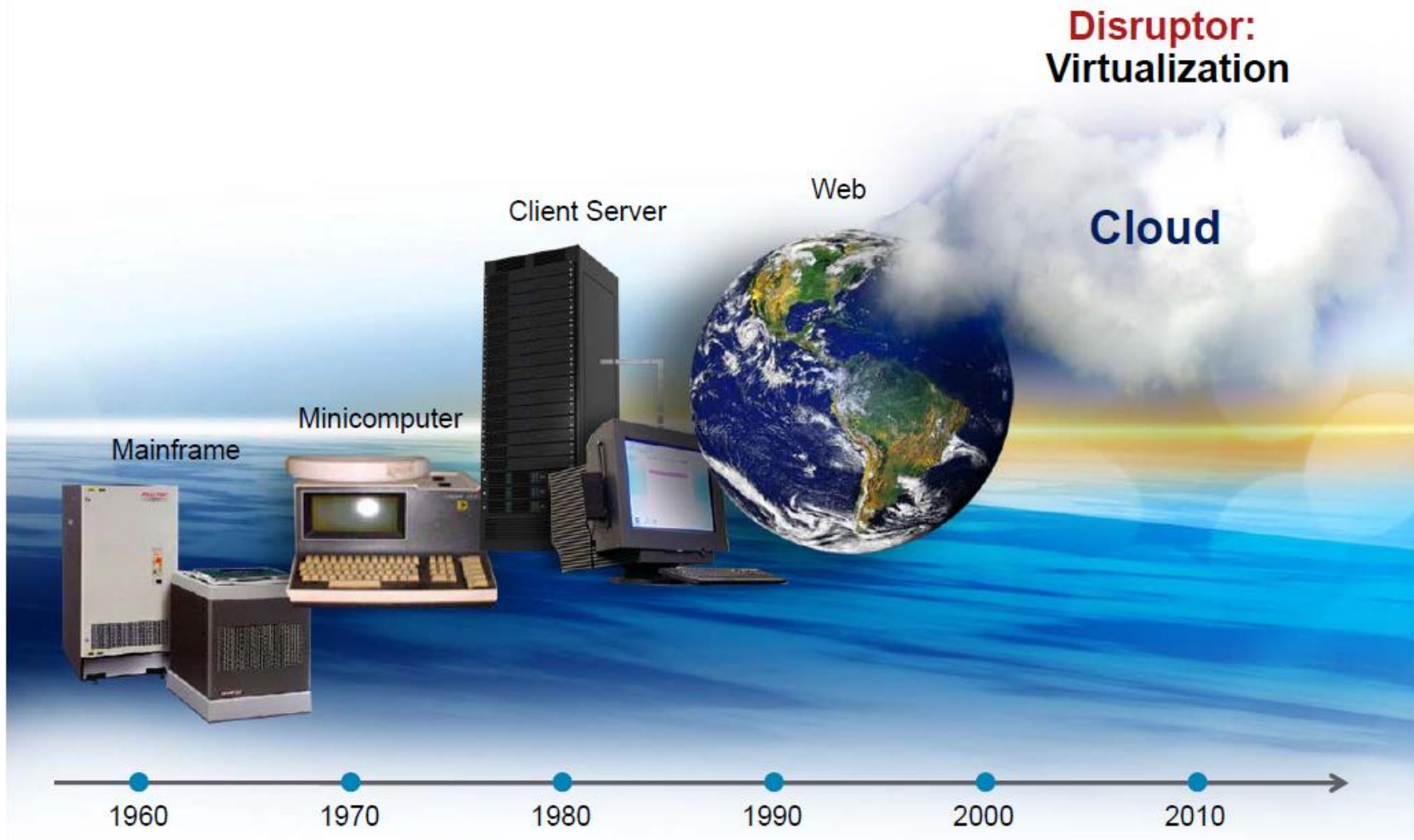
- Definitions
- Examples
- Cloud Security



What is a Cloud?



Development of Cloud Computing



Drivers

- Technology Drivers
 - fast wide-area networks
 - powerful, inexpensive server computers
 - high-performance virtualization for commodity hardware
 - Business Drivers: extend the outsourcing model
 - headache of business management to deal with the complexity of in-house IT operations
 - Less cost, and faster to get the IT service
 - Scalability
- ▶ http://www.youtube.com/watch?v=ae_DKNwK_ms

Definition

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model promotes availability and is composed of
 - five essential **characteristics**,
 - three **service models**, and
 - four **deployment models**.

5 Essential Cloud Characteristics

- On-demand self-service
- Broad network access
 - promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)
- Resource pooling
 - serve multiple consumers with different physical and virtual resources dynamically assigned
- Rapid elasticity
- Measured service

3 Cloud Service Models

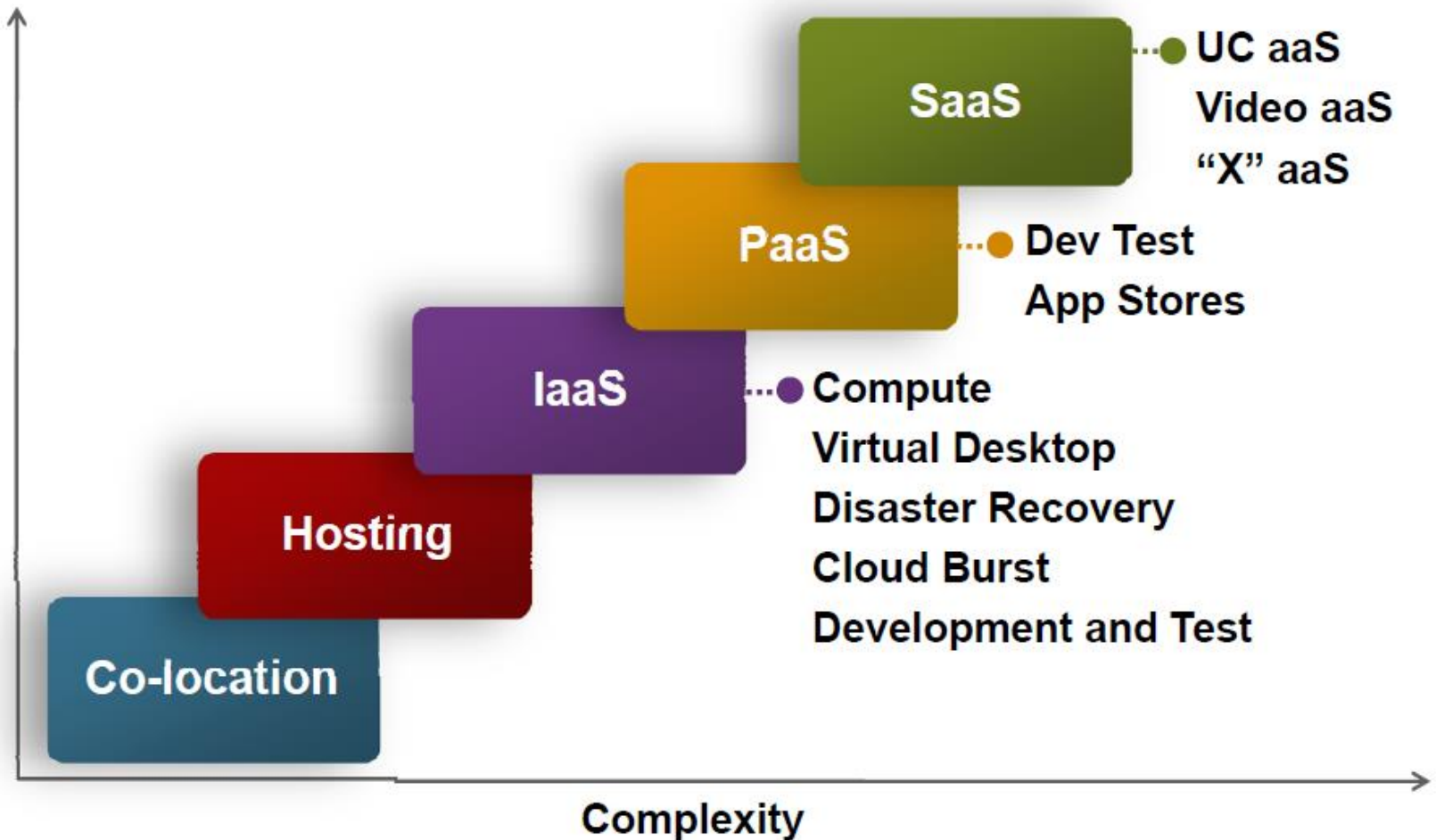
- Cloud Software as a Service (SaaS)
 - Use provider's applications over a network
- Cloud Platform as a Service (PaaS)
 - Deploy customer-created applications to a cloud
- Cloud Infrastructure as a Service (IaaS)
 - Rent processing, storage, network capacity, and other fundamental computing resources
- To be considered “cloud” they must be deployed on top of cloud infrastructure that has the 5 essential cloud characteristics

Service Model

Service Class	Main Access & Management Tool	Service content
 SaaS	Web Browser	Cloud Applications Social networks, Office suites, CRM, Video processing
 PaaS	Cloud Development Environment	Cloud Platform Programming languages, Frameworks, Mashups editors, Structured data
 IaaS	Virtual Infrastructure Manager	Cloud Infrastructure Compute Servers, Data Storage, Firewall, Load Balancer

Service Providers

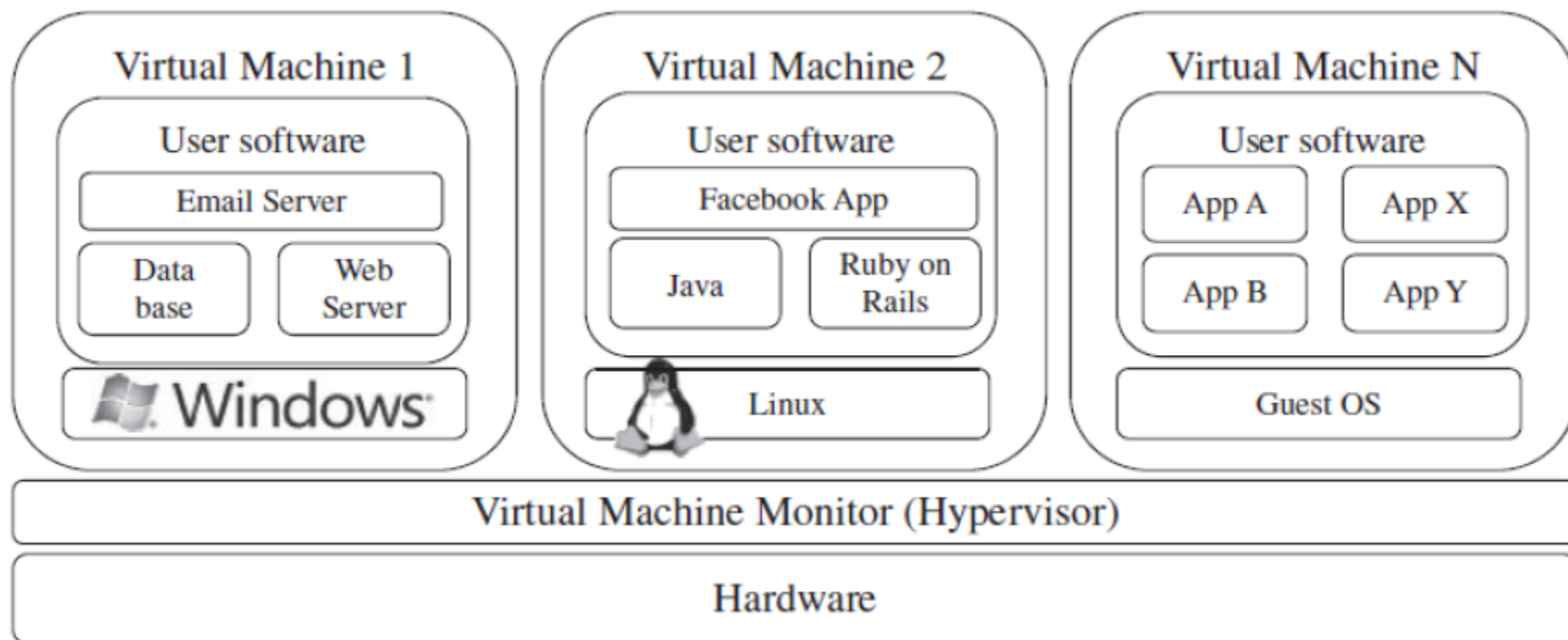
Revenue & Revenue/Sq. Ft.



Virtualisation

- In the IaaS model, cloud consumers directly use infrastructure components (storage, firewalls, networks, and other computing resources) provided by the cloud provider.
 - Virtualization is widely used in order to provide physical resources in an ad-hoc manner to meet current resource demand of cloud consumers

Virtualisation

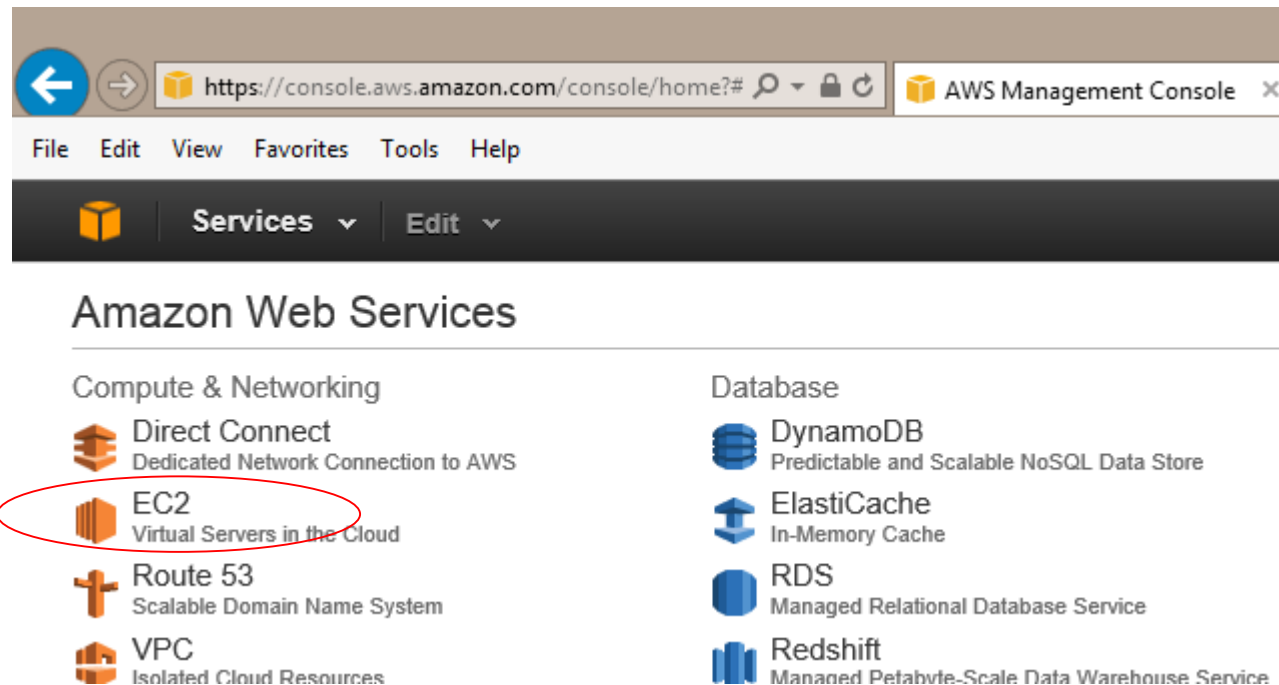


Example IaaS Providers

Provider	Geographic distribution of data centers	User interfaces and APIs	Hardware capacity	Guest operating systems	Smallest billing unit
Amazon E2C	US Europe	CLI, WS, Portal	CPU: 1_20 EC2 compute units Memory: 1.7-15 GB Storage: 160-1690 GB, 1 GB – 1 TB (per ESB units)	Linux Windows	Hour
Flexiscale	UK	Web console	CPU: 1-4 Memory: 0.5-16 GB Storage: 20-270 GB	Linux, Windows	Hour
GoGrid		REST, Java, PHP, Python, Ruby	CPU: 1-6 Memory: 0.5-8 GB Storage: 30-480 GB	Linux, Windows	Hour
Joyent	US		CPU: 1/16-8 Memory: 0.25-32.5 GB Storage: 5-100GB	OpenSolaris	Month
RackSpace	US	Portal, REST, Python, PHP, Java, .NET	CPU: Quad-core Memory: 0.25-16 GB Storage: 10-620 GB	Linux	Hour

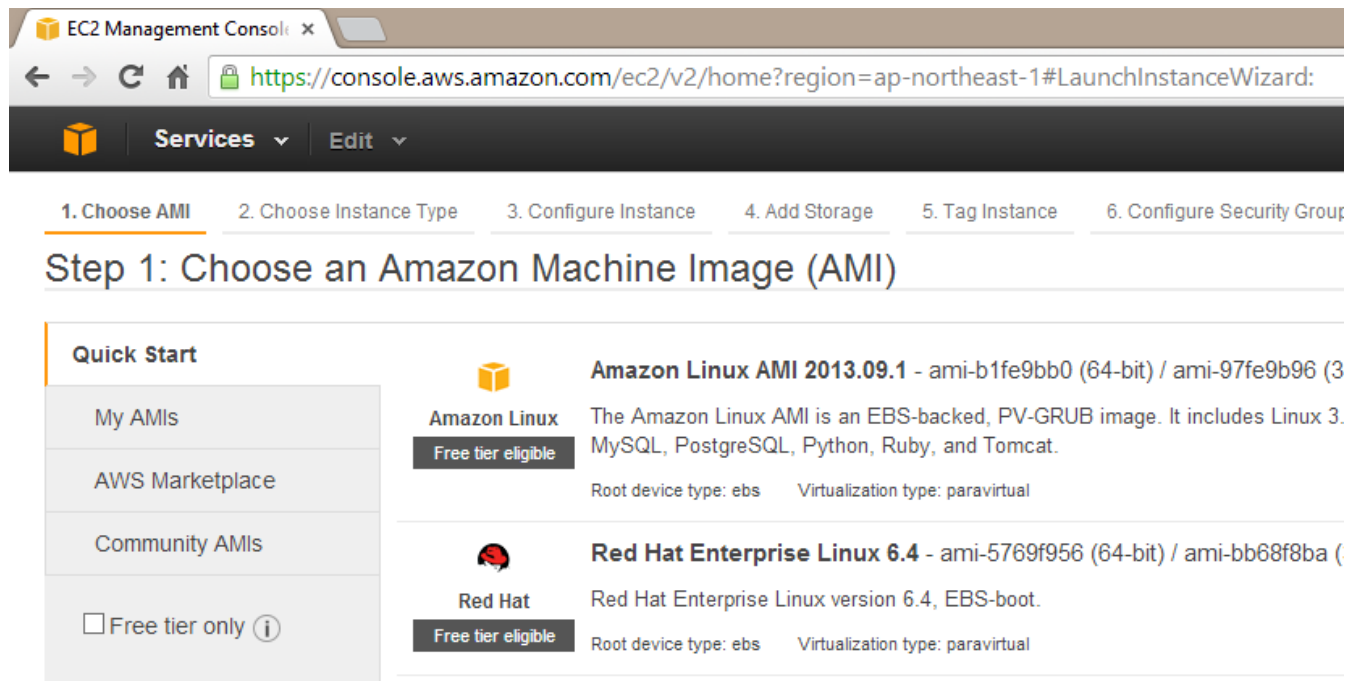
Exercise

- Sign up an account at Amazon Web Service
 - <http://aws.amazon.com/>
- After sign-in, choose the EC2 service



Exercise

- Choose and create a server that you like
 - N.B. Only choose those machines under “Free tier eligible”



EC2 Management Console x

← → ↺ 🏠 <https://console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#LaunchInstanceWizard:>

 Services ▾ Edit ▾

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group

Step 1: Choose an Amazon Machine Image (AMI)

Quick Start

- My AMIs
- AWS Marketplace
- Community AMIs
- ☐ Free tier only ⓘ



Amazon Linux

Free tier eligible

Amazon Linux AMI 2013.09.1 - ami-b1fe9bb0 (64-bit) / ami-97fe9b96 (32-bit)

The Amazon Linux AMI is an EBS-backed, PV-GRUB image. It includes Linux 3.10, MySQL, PostgreSQL, Python, Ruby, and Tomcat.

Root device type: ebs Virtualization type: paravirtual



Red Hat

Free tier eligible

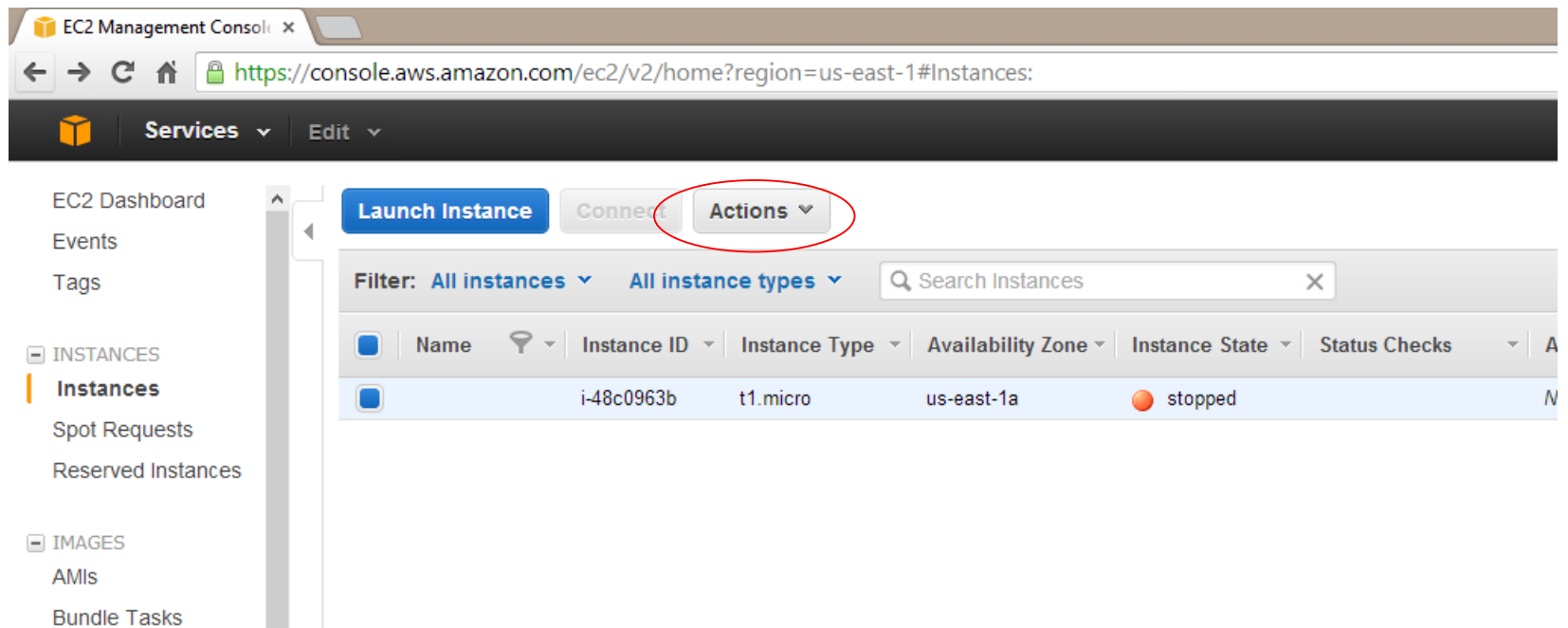
Red Hat Enterprise Linux 6.4 - ami-5769f956 (64-bit) / ami-bb68f8ba (32-bit)

Red Hat Enterprise Linux version 6.4, EBS-boot.

Root device type: ebs Virtualization type: paravirtual

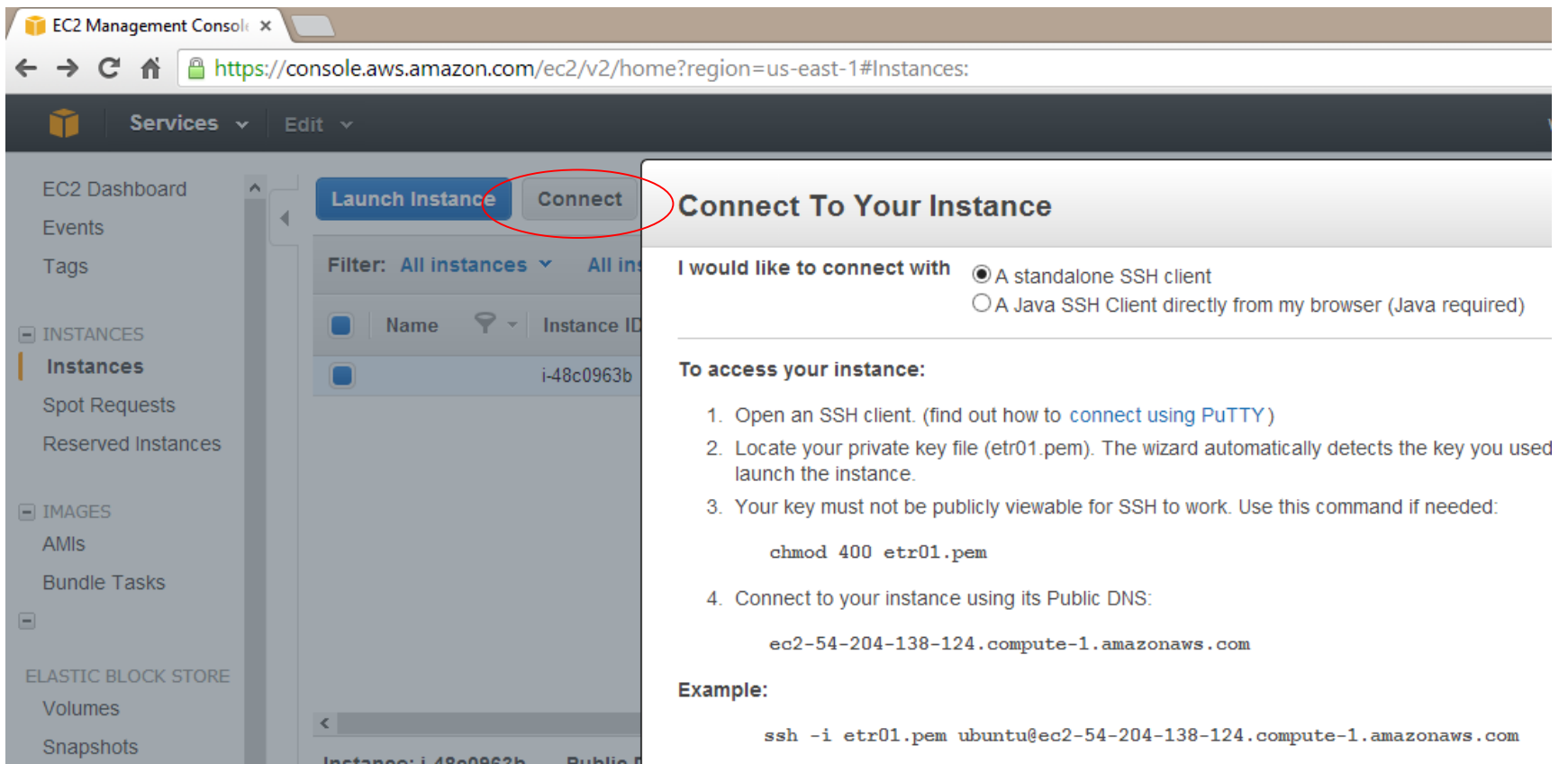
Exercise

- After successful creation, you can select your server and launch it by running **Actions** → **Start**



Exercise

- You can ssh to your Amazon server from your notebook
 - Press **Connect** to get the help window



The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, INSTANCES, Spot Requests, Reserved Instances, IMAGES, AMIs, Bundle Tasks, ELASTIC BLOCK STORE, Volumes, and Snapshots. The main content area displays a table of EC2 instances with columns for Name and Instance ID. A red circle highlights the 'Connect' button next to the 'Launch Instance' button. To the right of the table, a panel titled 'Connect To Your Instance' provides instructions on how to connect to the instance using an SSH client or a Java SSH client. It includes a list of steps to access the instance, a command to set permissions on the private key file, and an example SSH command.

EC2 Management Console x

← → ↻ 🏠 <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:>

Services ▾ Edit ▾

EC2 Dashboard
Events
Tags

INSTANCES
Instances
Spot Requests
Reserved Instances

IMAGES
AMIs
Bundle Tasks

ELASTIC BLOCK STORE
Volumes
Snapshots

Launch Instance Connect

Filter: All instances ▾ All instances

	Name	Instance ID
☐		i-48c0963b

Connect To Your Instance

I would like to connect with ☒ A standalone SSH client
☐ A Java SSH Client directly from my browser (Java required)

To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))
2. Locate your private key file (etr01.pem). The wizard automatically detects the key you used launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

```
chmod 400 etr01.pem
```
4. Connect to your instance using its Public DNS:

```
ec2-54-204-138-124.compute-1.amazonaws.com
```

Example:

```
ssh -i etr01.pem ubuntu@ec2-54-204-138-124.compute-1.amazonaws.com
```

Exercise

- After selecting the instance
 - **Actions** → **Stop** to halt the machine
 - **Actions** → **Terminate** to remove the machine

PaaS

- PaaS offers a faster, more cost-effective model for application development and delivery



Example PaaS Providers

Provider	Target to Use	Programming language, Frameworks	Programming Models	Persistence options
Aneka	.NET enterprise applications, Web applications	.NET	Threads, Task, MapReduce	Flat files, RDBMS
AppEngine	Web applications	Python, Java	Request-based Web programming	BigTable
Force.com	Enterprise applications	Apex	Workflow, Request-based Web programming, Excel-like formula language	Own object database
Azure	Enterprise applications, Web applications	.NET	Unrestricted	Table/BLOB/queue storage, SQL Services

Example SaaS Providers

Provider	Software	Pricing model
Salesforce.com	CRM	Pay per use
Google Gmail	Email	Free
Process Maker Live	Business process management	Pay per use
XDrive	Storage	Subscription
SmugMug	Data sharing	Subscription
OpSource	Billing	Subscription
Appian Anywhere	Business process management	Pay per use
Box.net	Storage	Pay per use
MuxCloud	Data processing	Pay per use

4 Cloud Deployment Models

- Private cloud
 - enterprise owned or leased
- Community cloud
 - shared infrastructure for specific community
- Public cloud
 - Sold to the public, mega-scale infrastructure
- Hybrid cloud
 - composition of two or more clouds

Possible Effects of Cloud Computing



- Small companies might use public SaaS / public clouds and minimize growth of data centers
- Large enterprise data centers may evolve to act as private clouds
 - may also use hybrid cloud infrastructure to leverage both internal and public clouds

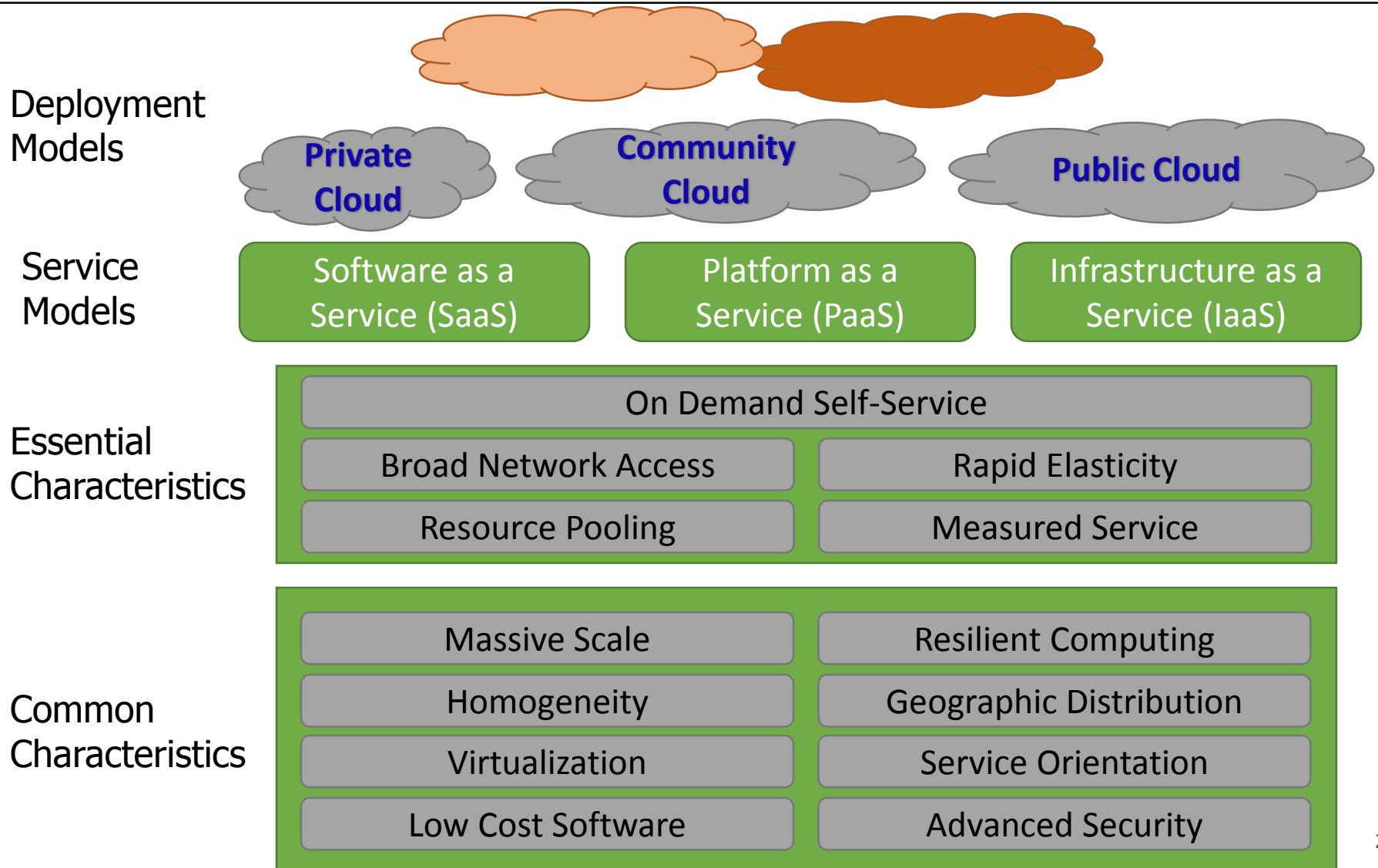
Security Considerations

- Clouds typically have a single security architecture but have many customers with different demands
- Organizations have more control over the security architecture of private clouds followed by community and then public clouds
- Highly sensitivity data is likely to be processed on clouds where organizations have control over the security model / operations

Balancing Threat Exposure and Cost Effectiveness

- Private clouds may have less **threat exposure** than community clouds which have less threat exposure than public clouds.
- Massive public clouds may be more **cost effective** than large community clouds which may be more cost effective than small private clouds
- *Doesn't strong security controls mean that I can adopt the most cost effective approach?*

The NIST Cloud Definition Framework



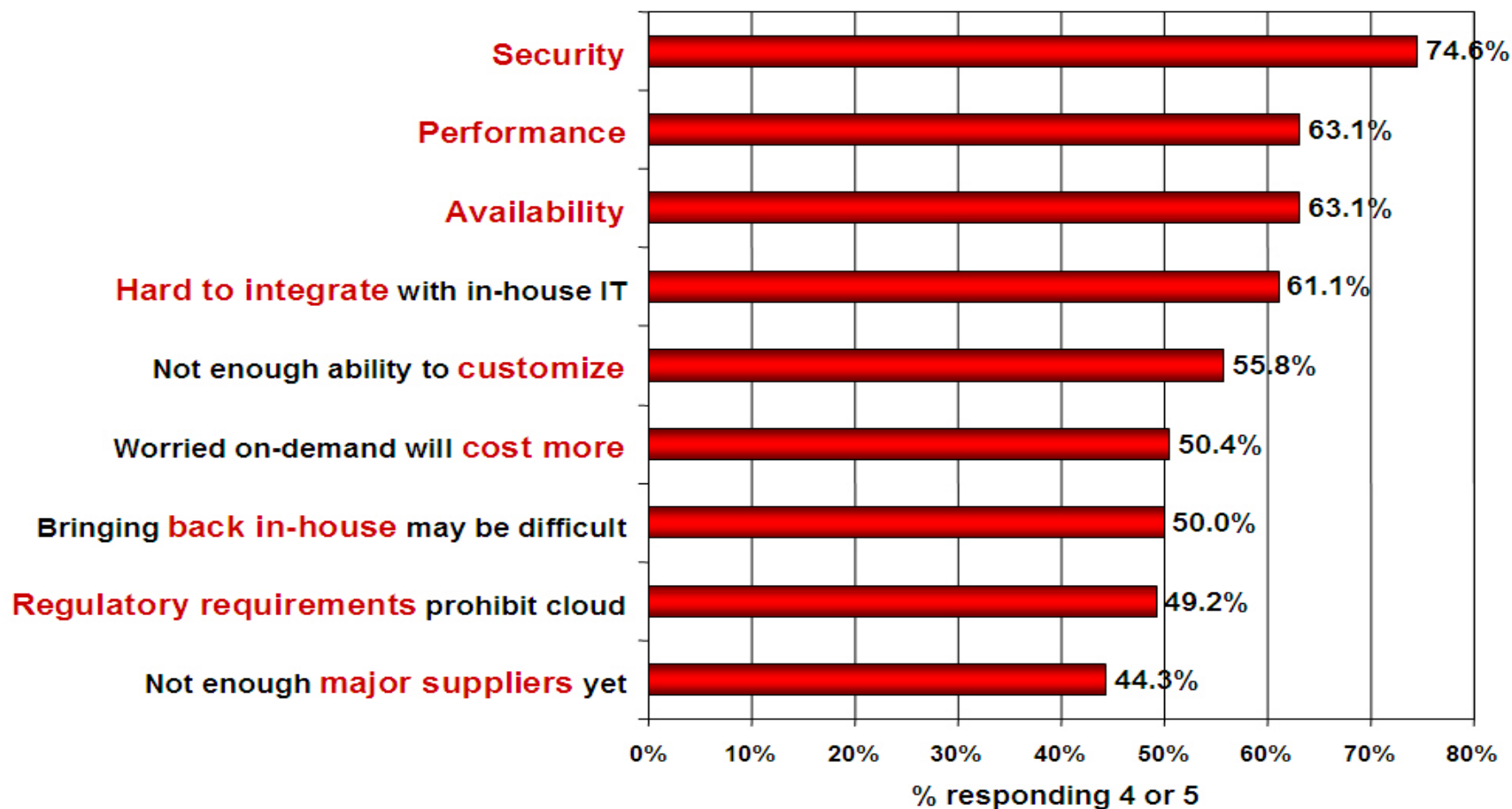
Cloud Computing Security



Security is the Major Issue

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model

(1=not significant, 5=very significant)



Analyzing Cloud Security

- Some key issues:
 - trust, multi-tenancy, data security, compliance
- Clouds are massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
 - There are both advantages and challenges



Advantages of using Cloud

- Shifting public data to an external cloud
 - Segregates the group of external users accessing to the public data from internal / authorised users
 - Reduces the exposure of the internal sensitive data
- Redundancy / Disaster Recovery
 - Dropbox as a backup storage (for non-sensitive data)
- Cloud vendors can recruit a dedicated security team and adhere to a stricter security protection



Cloud Security Challenges

- Loss of physical control
 - Where is my data now?
 - Who owns the data?
 - Customers' inability to know the audit findings
 - Vendor's proprietary implementations can't be examined
- Vendor lock-in
- Is the vendor's security model / operation trustworthy?
 - Who are the system administrators and what did they do?
 - Rely on international certification, e.g. ISO27001



Cloud Security Challenges

- Might be difficult to obtain support for investigations
 - Some vendors do not allow you to enter their data centres
- Data dispersal and international privacy legal requirements
 - Exposure of data to foreign government and data subpoenas?
- Need for isolation management for multi-tenancy
- Encryption needs for data stored in cloud

Service Level Agreements (SLAs)

- Contract between customers and service providers of the level of service to be provided
 - Documented roles and responsibilities
 - Service and security requirements
- Contains performance metrics (e.g., uptime, throughput, response time)
- Problem management details
- Penalties clauses for non-compliance

Moving Personal Data to Cloud

- An organisation intending to move personal data to the cloud may consider
 - Defining its security, privacy and compliance requirements;
 - Identifying what data, processes, or services it wants to move to the cloud;
 - Reviewing its own internal security and privacy policy and other restrictions on its use of personal data, such as pre-existing contracts, applicable laws and regulations, guidelines, and best practices;
 - Analyzing and assessing the risks of moving data to the cloud;

Moving Personal Data to Cloud

- Identifying what security controls (and certifications) are required or useful
 - to achieve adequate protection of personal data while being stored or processed in the cloud;
- Defining responsibilities and tasks for security controls implementation
 - i.e., understand which security controls are under the direct governance of the organization and which security controls would be under the responsibility of the CSP;
- Determining what obligations the entity has to monitor the activities of its service providers
 - e.g., are on-site visits required, or is it sufficient to rely on a certification or attestation from a third party?

Privacy Level Agreement (PLA)

- PLAs are intended to be used as an appendix to Cloud Services Agreements to describe the level of privacy protection that the cloud service provider (CSP) will maintain.
- PLAs will address information privacy and personal data protection practices.
- Reference:
 - *https://downloads.cloudsecurityalliance.org/initiatives/pla/Privacy_Level_Agreement_Outline.pdf*

Common Security Standards

- An organisation might be audited in accordance with:
 - ISO27001
 - An information security management system (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
 - Current version: ISO27001:2013
 - SSAE 16 (Statement on Standards for Attestation Engagements 16)
 - Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB)
 - Replacing SAS 70

Your Mission



- Understand Cloud Security
- Try various applications in cloud

