Material and some slide content from:
- Atif Kahn

SERVICES

COMPONENTS

OBJECTS

MODULES

Cloud Computing and Service-Oriented Architectures

Reid Holmes

Lecture 29 - Friday March 22 2013.

Cloud precursors

- Grid Computing:
  - Combination of computing resources from multiple administrative domains applied to common tasks.
    - Usually used to create ‘super computers’ that can work on specific parallel computation tasks.
- Utility Computing:
  - Combining computation, storage, and services metered like utilities.

Cloud Computing

- “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.” [NIST]

NIST Essential Characteristics

- On-demand self-service:
  - Consumers can provision computing capabilities without human interaction.
- Broad network access:
  - Capabilities are available over the network through standard mechanisms.
- Resource pooling:
  - Computing resources are pooled to serve multiple consumers.
  - Location independence. [perfomance/security]

NIST Essential Characteristics

- Rapid elasticity
  - Resources can be easily added and removed.
- Measured service [services and/or resources]
  - Metering of storage, processing, bandwidth, etc.

Benefits

- Agility [quickly respond to changes]
- Scalability [resources can be added, peak load]
- Cost [resources can be released; multi-tenancy (amortization)]
- Reliability [different sites, experts in control]
- Security [works both ways]

Technology

- Thick and thin clients
- Broadband
- Data centres
  - Large capacity
  - Globally distributed
- APIs
  - Administration
  - Development
  - Resource migration

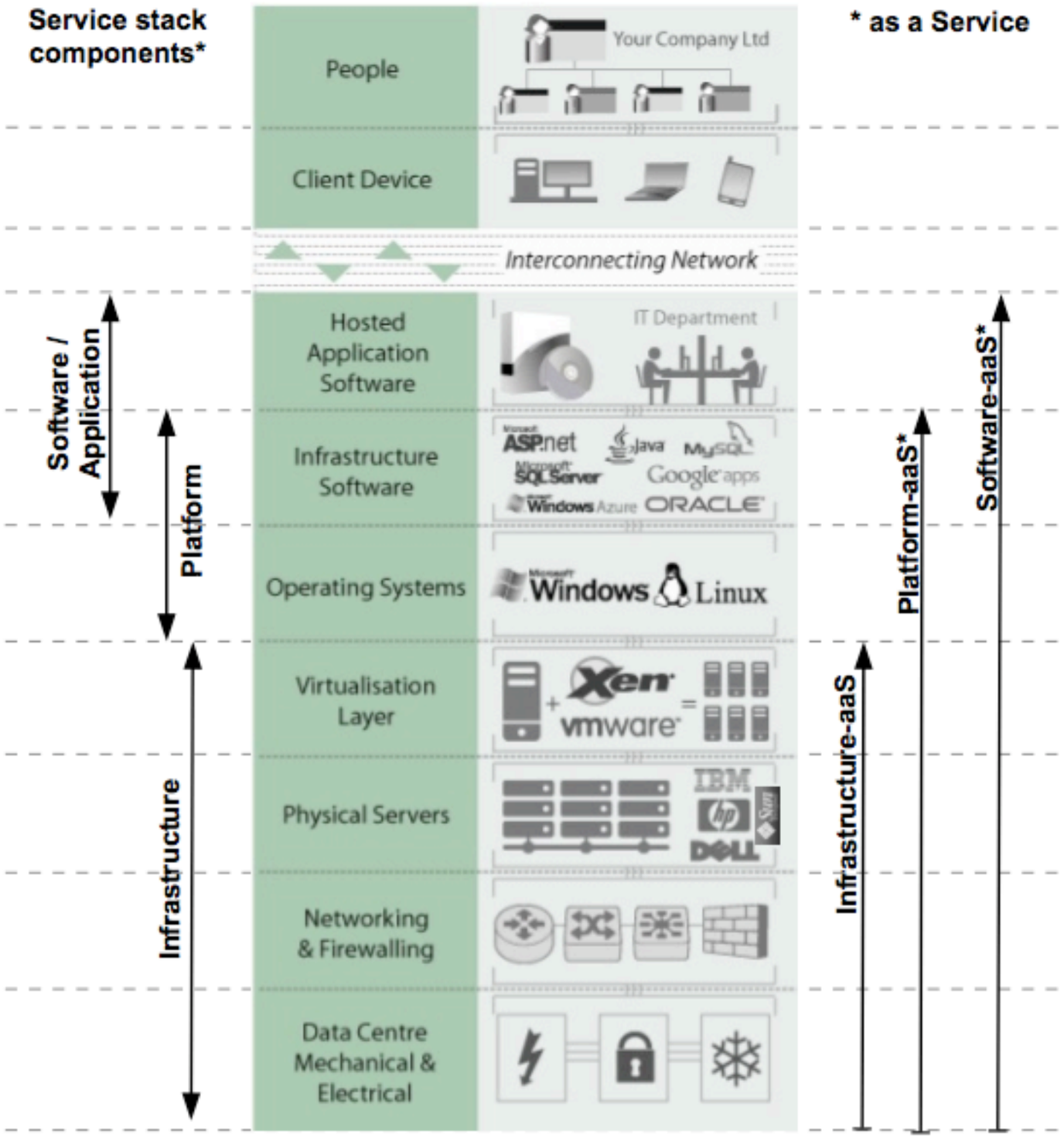
Virtualization

- Virtualization [decoupling physical & computing resources]
  - Emulation (QEMU) [VM simulates partial HW]
  - Paravirtualization (Xen) [SW int to VM]
  - Full (VMWare) [complete sim of HW]
  - Memory [decouple RAM from sys]
  - Storage [abstract logical & phys storage]
  - Data [abstract database / storage]
  - Network [abstract network e.g., VPNs]

Cloud Layers

- SaaS (e.g., Google Docs) [multi-tenancy, single release for all users]
  - Vendor-controlled remote applications.
  - Concerns: control, performance, security, privacy.
- PaaS (e.g., AppEngine)
  - Vendor-controlled environment.
  - Concerns: as for SaaS w/ limited technology choices.
- IaaS (e.g., Amazon EC2)
  - Vendor-provided resources; consumer provisions VM.
  - Concerns: more expertise needed to leverage flexibility.

Service Layers Definition



***Notes**:*
Brand names for illustrative / example purposes only, and examples are not exhaustive.

** Assumed to incorporate subordinate layers.*

Cloud Spectrum

less flexible
more constrained
less effort

more flexible
less constrained
more effort

Google docs

salesforce.com

TurboTax

Windows Azure

amazon web services

Eucalyptus

the rackspace cloud

Layers of Control

In-house Deployment	Hosted Deployment	IaaS Cloud	PaaS Cloud	SaaS Cloud
Data	Data	Data	Data	Data
APP	APP	APP	APP	APP
VM	VM	VM	Services	Services
Server	Server	Server	Server	Server
Storage	Storage	Storage	Storage	Storage
Network	Network	Network	Network	Network

Organization controlled

Organization & service provider share control

Service Provider controlled

[1] **Visualizing the Boundaries of Control in the Cloud. Dec 2009.**
http://kscottmorrison.com/2009/12/01/visualizing-the-boundaries-of-control-in-the-cloud/

NIST Deployment Models

- Private cloud:
  - Infrastructure runs for single organization.
- Community cloud:
  - Infrastructure supports specific community.
- Public cloud:
  - Infrastructure is available to everyone.
- Hybrid cloud:
  - Infrastructure combines two or more clouds.

Cloud Security

- Users want assurances of:
  - Confidentiality [keep unauthorized users out]
  - Integrity [data has not altered]
  - Authenticity [data provenance]
  - Anonymity [users are unidentifiable]
  - Privacy [user data is properly controlled]
- Data remanence is problematic:
  - How can you purge data from the cloud?