Material and some slide content from:
- Atif Kahn

SERVICES

COMPONENTS

OBJECTS

MODULES

Cloud Computing and Service-Oriented Architectures

Reid Holmes

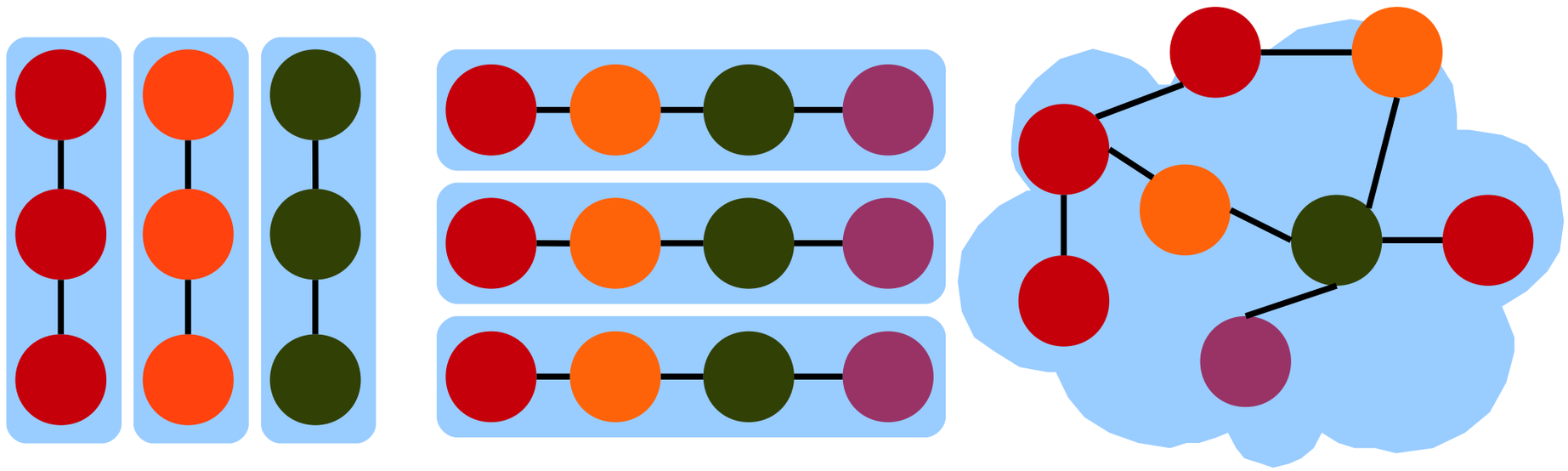
Lecture 20 - Tuesday November 23 2010.

SOA

- “Service-oriented architectures are a way of developing distributed systems where components are stand-alone services executing on geographically distributed computers” [Sommerville]
- “The policies, practices, frameworks that enable application functionality to be provided and consumed as sets of services published at a granularity relevant to the service consumer. Services can be invoked, published and discovered, and are abstracted away from the implementation using a single, standards-based form of interface.” [CBDI]

SOA Characteristics

- Applications comprise of a “mesh-up” of services.
- Services are narrowly focused.
  - Tradeoff between ?
- Focus on loose coupling and reusability.
- Challenges (2): ?



Architectural Perspectives

- Application architecture
  - Business facing, service consuming.
- Service architecture
  - Bridges implementations and applications.
- Component architecture
  - Service implementations.
- Consumers are dependent on service architectures and are oblivious of the ?

Discovery

- Services are published and can be found by:
  - search
  - UDDI [Universal Description Discovery and Integration]

Potential Service Domains

- Identity management
- Asset management
- Publishing & discovery
- Security infrastructure
- Certification
- Middleware

Sample SOA Application

Transitioning to Services

Cloud precursors

- Grid Computing:
  - Combination of computing resources from multiple administrative domains applied to common tasks.
    - Usually used to ?
- 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:
  - ?
  - ?

NIST Essential Characteristics

- Rapid elasticity
  - ?
- Measured service [services and/or resources]
  - Metering of storage, processing, bandwidth, etc.

Benefits

- Agility
  - ?
- Scalability
  - ?
- Cost
- Reliability
  - ?
- Security
  - ?

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)
  - Paravirtualization (Xen)
  - Full (VMWare)
  - Memory
  - Storage
  - Data
  - Network

Cloud Layers

- SaaS (e.g., Google Docs)
  - 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 Layer Diagram

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 Grid

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
  - Integrity
  - Authenticity
  - Anonymity
  - Privacy
- Data remanence is problematic:
  - ?