Cloud Service Models

Module 2

Contents

- Cloud Service Delivery Models: The Cloud Service Provider Perspective
- Cloud Service Delivery Models: The Cloud Consumer Perspective
- Case Study Examples

Can you name some cloud services which you use?

Cloud Services

- There are three types of services offered by cloud service providers
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

The CSP Perspective

- Explores the architecture and administration of IaaS, PaaS, SaaS cloud delivery models from CSP perspective.
- The integration and management of these cloud-based environments and how they can relate to different technologies.

Building IaaS Environments

- The virtual server and cloud storage device mechanisms represents the two most fundamental that are delivered as part of a rapid provisioning architecture within IaaS environment.
- They are offered by the following properties:
    a. operating system
    b. primary memory capacity
    c. processing capacity
    d. virtualized storage capacity

Contd...

- Memory and virtualized storage capacity is usually allocated with increments of 1GB to simplify the provisioning of underlying physical IT resources.
- When limiting cloud consumer access to virtualized environments, IaaS offerings are preemptively assembled by CSPs via virtual server images that capture the pre-defined configurations.
- Some CSPs may offer cloud consumers direct administrative access to physical IT resources in which case bare-metal provisioning architecture may come into play.

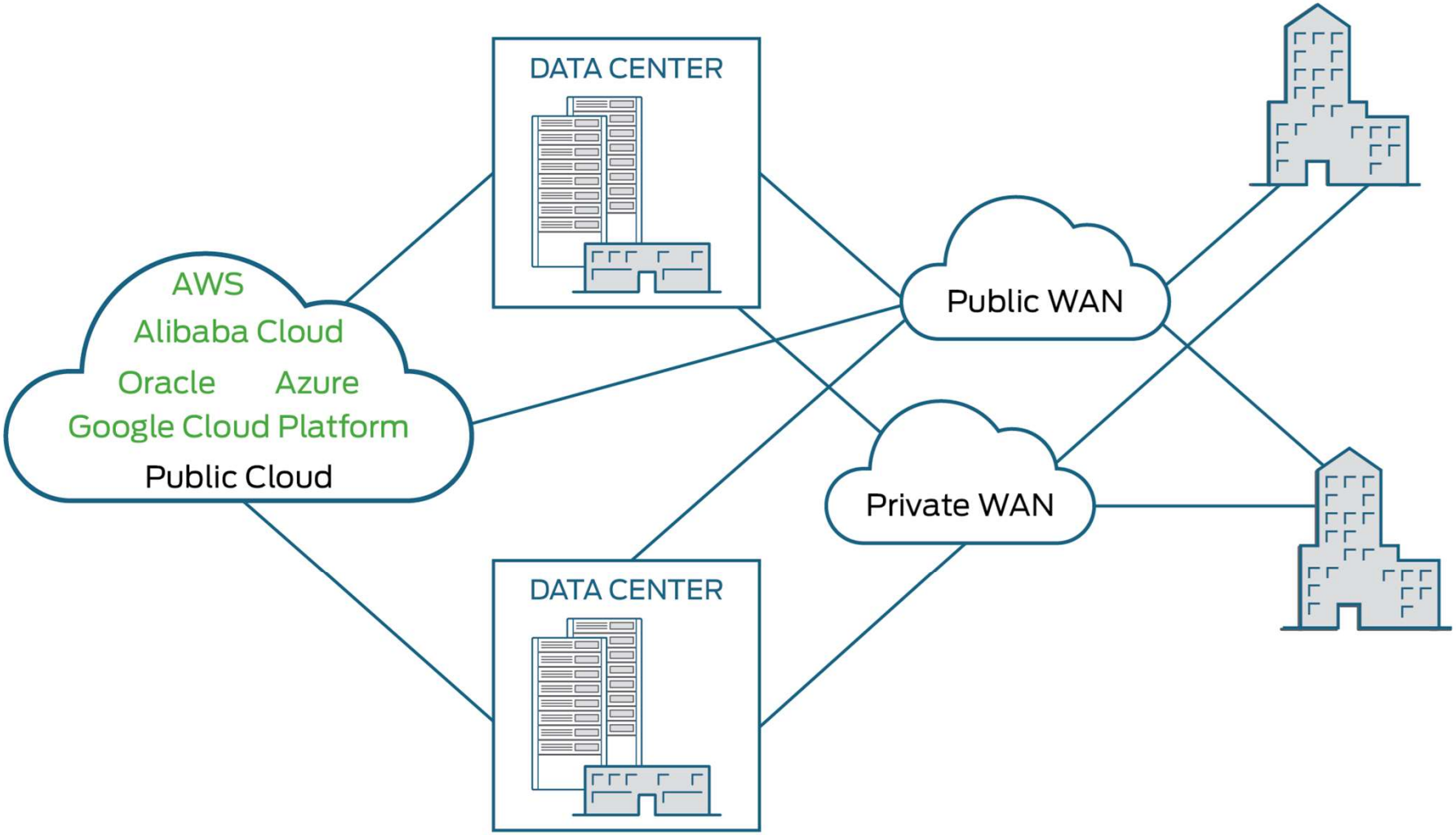
Contd...

- Snapshots can be taken of a virtual server to record its current state, memory, and configuration of a virtualized IaaS environment.
- This is done for backup and replication purposes in support of horizontal and vertical scaling requirements.

  The snapshot can alternatively be used to duplicate a virtual server.

Data Centers

- CSP offers IaaS-based IT resources from multiple geographically diverse data-centers which provides the following benefits:
    a. Multiple data-centers can be linked together for increased resiliency.
    b. Connected through high-speed communication networks with low latency.


DATA CENTER
AWS
Alibaba Cloud
Oracle
Azure
Google Cloud Platform
Public Cloud
Public WAN
Private WAN
DATA CENTER

Scalability and Reliability

- CSP can automatically provision virtual servers via dynamic vertical scaling.
- This can be performed through Virtualized Infrastructure Manager (VIM) as long as the host physical servers have sufficient capacity.
- If a given physical server has insufficient capacity to support vertical scaling, manual scalability requires the cloud consumer to manually request IT resource scaling.

Monitoring

- Cloud usage monitors in IaaS can be implemented using VIM or specialized monitoring tools.
- Several common capabilities:
  a) Virtual server lifecycles
  b) Data storage
  c) Network traffic
  d) Failure conditions
  e) Event triggers

Security

Cloud security mechanisms relevant for securing IaaS environment include:

- Encryption, hashing, and digital signature - data security
- Firewall and access control mechanisms
- Tracking of virtual IT resources to detect abnormal usage patterns

PaaS Environment

- CSP offers application development and deployment platform in order to accommodate different programming models, languages, and frameworks.
- A separate ready-made environment is usually created for each programming stack.
- Customers can create and control customized virtualized server images with ready-made environment.
- Features like managing and deploying applications, and configuring multi-tenancy.

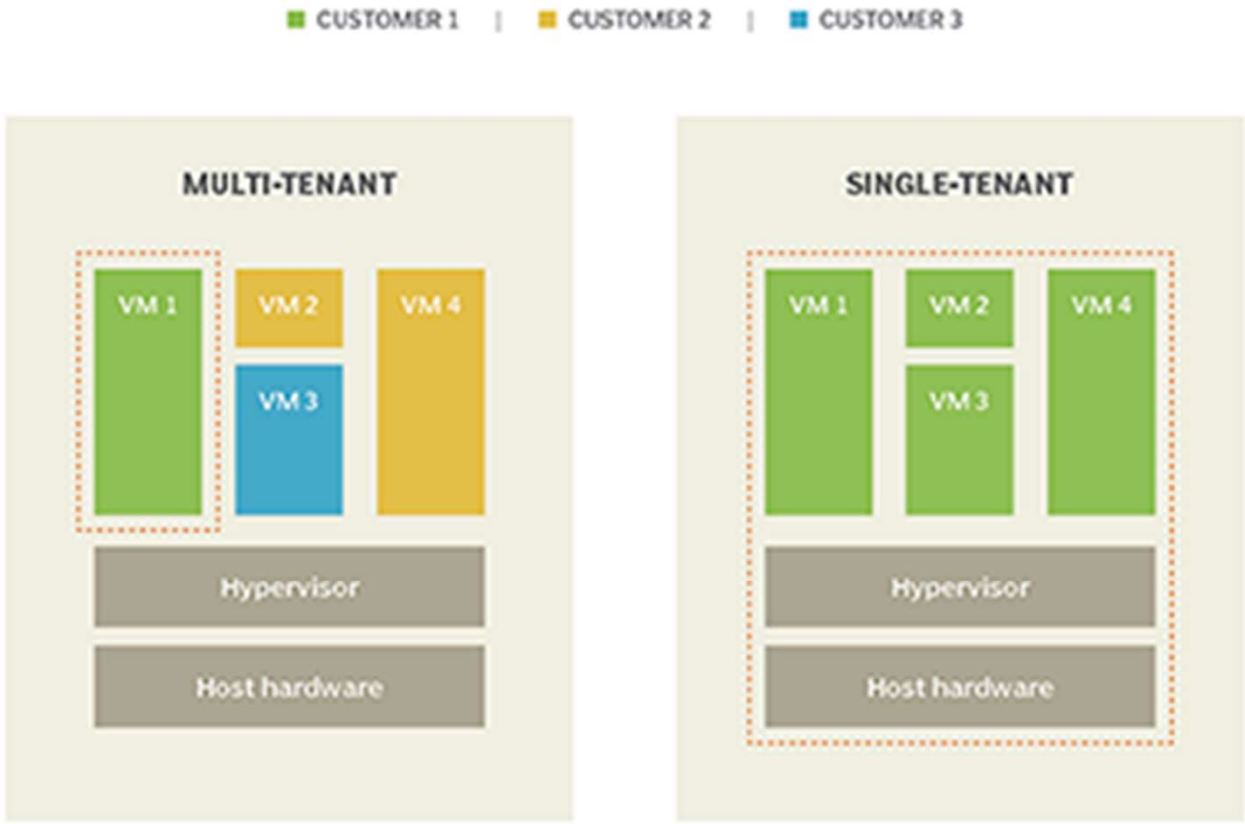
Monitoring

- Ready-made environment instances
- Data persistence
- Network usage
- Failure conditions
- Event triggers

SaaS Enviornment

- Cloud service architectures are generally based on **multi-tenant environment** that enable concurrent customer access.

Multi-tenant vs. single-tenant



SOURCE: GOOGLE

IaaS Environment - Customer Perspective

- Virtual servers are accessed at the operating system level through the use of remote terminal applications.
- Two accessing options:

1. Remote Desktop (or Remote Desktop Connection) client - for Windows-based environment
2. SSH client - for Mac and Linux based environments

Eg: Amazon Web Services etc.

Features of IaaS

- Web Access to resources
- Centralized management
- Elasticity and dynamic scaling
- Shared infrastructure
- Preconfigured VMs
- Metered Services

IaaS – Pros and Cons

Pros

- Pay as you use
- Reduced operational cost
- Elastic resources
- Better resource utilization
- Green IT

Cons

- Security
- Interoperability / Vendor Lock-In
- Network performance

PaaS Environment

- Offers a wide-range of tools and programming resources such as software libraries, class libraries, frameworks, API, and various runtime capabilities.
- Allows developers to create, test, and run application code.
- PaaS also allows applications to use cloud storage devices as independent data storing systems for holding development-specific data.
- Eg: Google App Engine, Microsoft Azure etc.

Features of PaaS

- All-in-one (dev+test+deploy+host+maintain)
- Web Access
- Built in Scalability
- Collaborative
- Diverse tools available

When to use PaaS?

- PaaS is a good option if:
  - Collaborative development
  - Automated testing and deployment
  - Less time to market

- PaaS might not be a good option if:
  - Frequent migration
  - Infrastructure customization
  - Platform flexibility
  - On-premise integration

PaaS – Pros and Cons

Pros

- Quick development and deployment
- Reduces ownership cost
- Agile software development
- Collaboration
- Ease of use
- Less maintenance
- Scalability

Cons

- Vendor Lock-In
- Security
- Less flexibility
- Depends on network connection

SaaS Environment

- Cloud consumers using SaaS products supplied by cloud provides are relieved of the responsibilities of implementing and administering their underlying hosting environment. For example:
  - Managing security related configurations
  - Managing availability and reliability options
  - Managing usage costs
  - Managing user accounts, profiles, and access authorization
  - Managing SLA

Contd…

- Provides access to applications running on a cloud infrastructure.
- Accessible from client devices via a browser or program interface.
- Customer does not manage or control underlying infrastructure or applications – limited customization.
- Eg: Google Documents, Sharepoint etc.

SaaS Features

- Multi-tenancy Model
- Web Access
- Centralized Management
- Multi-device support
- Scalability
- Availability
- API integration

When to use SaaS?

- You should use SaaS for:
  - On demand software
  - Software for startups
  - Software compatibility
  - Varying loads

- SaaS might not be a good option if:
  - Unreliable network connection
  - Confidential data

SaaS - Pros and Cons

Pros

- No installation
- Cost savings
- Less maintenance
- Ease of Access
- Dynamic scalability
- Disaster Recovery
- Multitenancy

Cons

- Security
- Connectivity
- Loss of Control

Comparison of Cloud Services

Traditional Setup	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Runtime Environment	Runtime Environment	Runtime Environment	Runtime Environment
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Network	Network	Network	Network

Under user's control Under common control Under provider's control

Future of Cloud - XaaS

- Network as a Service (NaaS)
- Desktop as a Service (DEaaS)
- Storage as a Service (STaaS)
- DB as a Service (DBaaS)
- Data as a Service (DaaS)
- Security as a Service (SECaaS)
- Identity as a Service (IDaaS)

Open Challenges

- Cost
- Service Provider Reliability
- Downtime
- Password Security
- Data Privacy
- Vendor lock-in
- Portability
- Availability