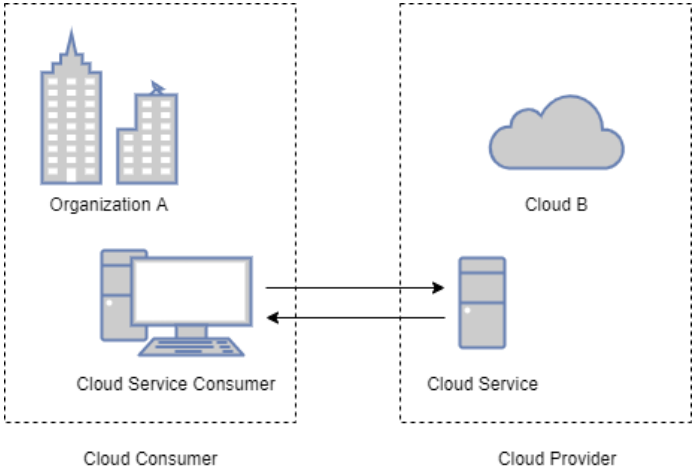
CS4650 Topic 19:
Cloud Computing Roles and Models

Roles and Models

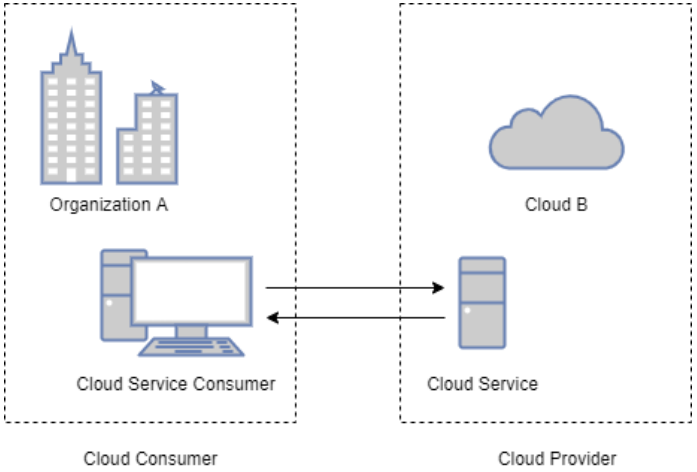
- Organizations and humans can assume various roles when dealing with cloud-based resources and services.
- Understanding these roles clarifies the responsibilities and their main interactions.

Cloud Provider



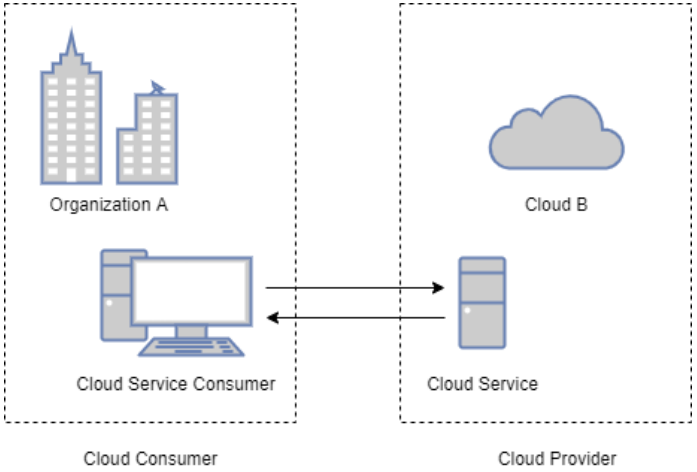
- A *cloud provider* is an organization that provides cloud-based IT resources.
- In this diagram, the cloud-based IT resource is a *cloud service*.
- This service is available on Cloud 'B', and as we will see, the organization that owns and manages Cloud B is also the entity that owns the cloud service.
- The role that this organization assumes is *cloud provider*.
- The cloud provider makes the services available, as stated in its SLA, and administers the service to ensure its on-going operation.

Cloud Provider



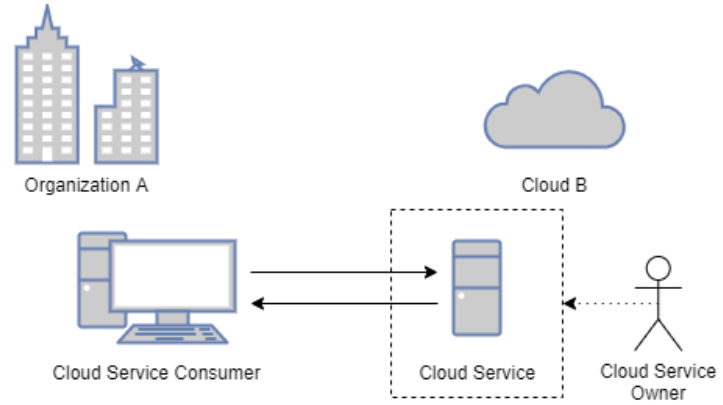
- As previously stated, the cloud provider 'owns' the service.
- However, the cloud provider could 'resell' IT resources leased from other cloud providers. This is merely a detail, however, as the SLA is between this cloud provider and its consumers, and the consumers typically are not even aware of the other provider in the background.

Cloud Consumer



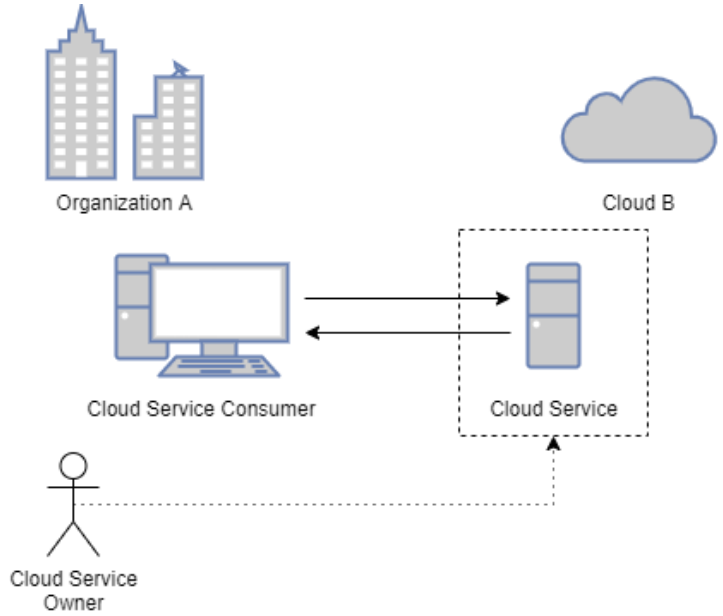
- A *cloud consumer* is an organization or an individual that has a formal contract or arrangement with the cloud provider.
- In this case, the consumer is more specifically a *cloud service consumer*, because in relationship to this cloud service, this entity is a consumer of that service.

Cloud Service Owner



- The *cloud service owner* is the person or organization that legally owns a cloud service.
- In this case, the cloud service owner is the cloud provider.
- In this case, the cloud service consumers are dealing with the cloud provider, but in the role as the cloud service owner. The SLA specifies the arrangement for this specific service, not for use of the cloud in general.

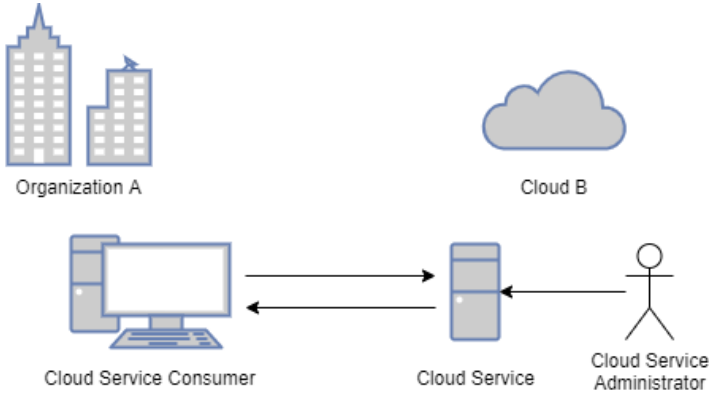
Cloud Service Owner



- In this example, the cloud service owner is in fact the cloud consumer.
- In this case, the cloud provider is providing the hosting and underlying resources.
- In essence, the cloud consumer is just leasing the underlying computing or storage resources from the cloud provider.
- A related example would have one cloud consumer being the owner of the cloud service while other cloud consumers use that resource.

Cloud Service Administrator

- Another role is the *cloud service administrator*. This is the person or organization responsible for administrating the cloud service.
- The cloud service administrator can be, or belong to, the cloud provider, the cloud consumer or to a third-party organization.



Other Roles

In addition to the roles mentioned before, these additional roles may also be present:

- *Cloud Auditor* -- A third-party that conducts independent assessments of the cloud service, typically evaluating the securing, privacy impacts, and performance of the service. The main purpose is to strengthen the trust relationship between the provider and consumers.
- *Cloud Broker* -- This is the party that assumes responsibility of managing and negotiating the relationship between the cloud provider and the cloud consumers.

Trust Boundary

- When an organization assumes the role of a cloud consumer to access an cloud-based IT resource, it needs to extend its trust beyond the physical boundary of the organization to include parts of the cloud environment.
- The *trust boundary* is the perimeter that encloses all of the resources that the organization must trust.
- Issues exist when entities that cannot be trusted can encroach upon a portion of the resources within the trust boundary, or when resources that are within the trust boundary 'leak outside' of the boundary.
- The organization may not have enough information to determine how far this boundary reaches, who else might be within that boundary, and how secure is the boundary.

Key Points

- Common roles associated with cloud-based interactions include cloud provider, cloud consumer, cloud service owner, and cloud resource administrator.
- An organizational boundary represents the physical scope of IT resources owned and governed by an organization.
- A trust boundary is the logical perimeter that encompasses the IT resources trusted by an organization.

Cloud Characteristics

An IT environment requires a specific set of characteristics to enable it to be an effective cloud:

1. On-demand usage
2. Ubiquitous access
3. Multitenancy (and resource pooling)
4. Elasticity
5. Measured usage
6. Resiliency

On-Demand Usage

- A cloud consumer can unilaterally access cloud-based IT resources.
- The cloud consumer has the freedom to self-provision these IT resources.
- Once configured, usage of the IT resource can be automated, requiring no further human involvement by the cloud consumer or cloud provider.
- This environment is known as an *on-demand usage* environment.

Ubiquitous Access

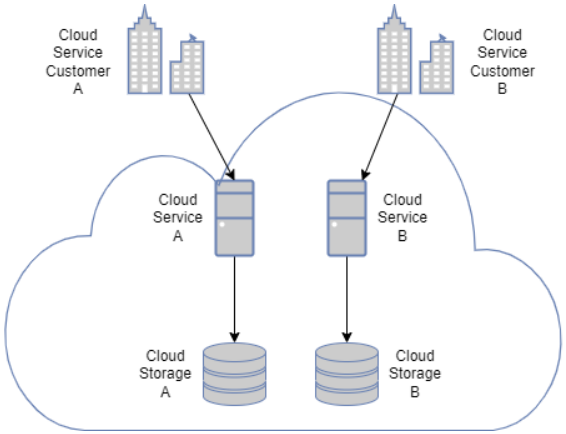
- *Ubiquitous access* represents the ability for a cloud service to be widely accessible.
- This may require support for a range of devices, transport protocols, interfaces, and security protocols.
- This generally requires that the architecture support a variety of consumer types.

Multitenancy (and Resource Pooling)

- The characteristic of a software program that enables an instance of the program serve different consumers (tenants) where each is isolated from the others is called *multitenancy*.
- This is frequently done through virtualization, allowing IT resources to be dynamically assigned and reassigned.
- Resource Pooling allows cloud providers to pool large-scale IT resources to serve multiple cloud consumers.

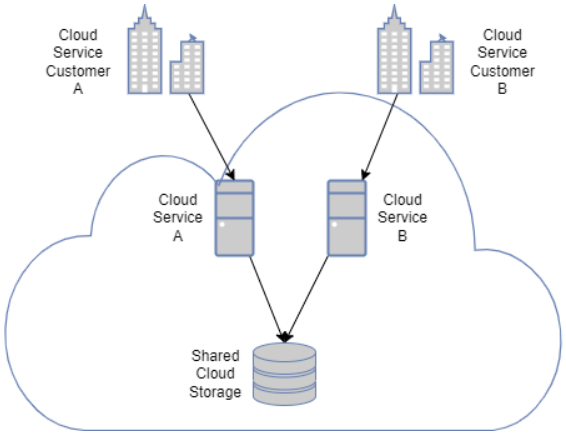
Multitenancy (and Resource Pooling)

- This diagram shows a single-tenancy environment.
- Each cloud service consumer has its own service and its own resources.
- There is no sharing of the resources (although the interconnecting network may be shared).



Multitenancy (and Resource Pooling)

- This diagram shows a multiple-tenancy environment.
- In this instance, each consumer has its own cloud-based service, but these are both sharing a common resource: storage.
- In an alternate configuration, the consumers may also be sharing a single instance of the service.
- The consumers are unaware that the service or resource might be shared.



Elasticity

- *Elasticity* is the automated ability of a cloud to transparently scale its IT resources:
  - Possibly in response to runtime conditions (such as load)
  - As pre-determined by the cloud consumer, or
  - As pre-determined by the cloud provider.
- Elasticity is one of the core justifications for the adoption of cloud computing.

Measured Usage

- The *measured usage* characteristic represents the ability of a cloud platform to keep track of the usage of its IT resources by cloud consumers.
- Based on these measurements, the cloud provider can charge the cloud consumers based on the IT resources actually used.
- This also gives the cloud consumer the ability to control its spending.

Resiliency

- Resilient computing is a form of failover that distributes redundant implementations of IT resources across physical locations.
- IT resources can be pre-configured so that if one becomes deficient, processing is automatically handed over to another redundant implementation.
- Redundancy may be in the same cloud (but at different physical locations), or across different clouds.
- In some cases, the cloud consumer can select (and pay for) the desired degree of redundancy.

Key Points

- On-demand usage is the ability of a cloud consumer to self-provision and use necessary cloud-based services without requiring cloud provider interaction.
- Ubiquitous access allows cloud-based services to be accessed by diverse cloud service consumers.
- Multitenancy is the ability of a single instance of an IT resource to transparently serve multiple cloud consumers simultaneously.
- Elasticity represents the ability of a cloud to transparently and automatically scale IT resources out or in.
- Resiliency pertains to a cloud's failover features.

Cloud Delivery Models

- A *cloud delivery model* represents a specific, pre-packaged combination of IT resources offered by a cloud provider.
- Three common cloud delivery models have become widely established:
  - Software-as-a-Service (SaaS)
  - Platform-as-a-Service (PaaS)
  - Infrastructure-as-a-Service (IaaS)
- Variations of these models have emerged, and others have latched onto the term '...as-a-Service', but are sort of doing a disservice to the term.

Software-as-a-Service

- A software program is positioned as a shared cloud served and is made available as a product.
- The SaaS delivery model is typically used to make software available, often commercially, to a range of cloud consumers.
- A cloud consumer is generally granted very limited administrative control over an SaaS implementation.
- It is most often provisioned by the cloud provider.
- In other cases, a cloud consumer may make the service available to others, thus being a consumer and a provider simultaneously.

Software-as-a-Service

- Many software companies find the SaaS concept attractive:
  - When an update or upgrade of the software is available, all users are automatically migrated to the new version, since the software is in the provider's cloud.
  - Because of this, the producer does not have to support older versions of the software. Prior to this:
    - The company makes new versions of the software to offer new features, but customers are not required to upgrade to the new version.
    - As bugs or security holes are discovered, patch releases of the software become necessary.
    - This means that the company needs to provide patches not only for the current version of the software, but also for several previous versions.

Software-as-a-Service

- One reason why customers might want to keep an older version of the software is that the provider might charge for upgraded versions.
- The provider has some responsibility to provide bug fixes and security updates, even on older versions, up to some point (usually a few years).
- Hard as it might be to imagine, some people work off-line. Perhaps they don't have a solid internet connection every place they work, or it could be a cost issue, or a privacy/security issue.
- Software is faster when it is installed on the machine, it doesn't have to be downloaded each time it is used.
- On the other hand, SaaS software does not take (as much) space on the user's machine.

Platform-as-a-Service

- The PaaS delivery model represents a pre-defined 'ready-to-use' environment of configured IT resources.
- One example is a virtual machine which has:
  - A specific operating system (and in fact a specific version of that operating system)
  - A database server configured with a database that has been initialized with some data.
  - One or more software packages pre-installed.
  - All of the above are 'connected'.

Platform-as-a-Service

- One company I tangentially worked with had a complex program.
- This program was designed and tested for a particular version of the OS.
- In the past, whenever there was a patch or upgrade to the OS, they needed to reverify that their software worked.
- In some cases, they needed to upgrade their software to work with the new OS. This involved writing new code, but then doing a lot of verification to make sure the software worked properly with the new configuration.
- They also connected to a database. Sometimes it can be a very detailed and tedious process to establish the database connection.
- When the database had an upgrade, they had to re-test and probably modify their software.

Platform-as-a-Service

- The alternative for this company was to build a complete virtual environment that they established one time.
- They completely tested their system with this known configuration of the OS and this known version of the database server.
- Once the package was complete, they simply replicated the package for each installation.
- Since this was using virtualization technology, if the OS was modified, it wouldn't affect their product, since their product was using a frozen version of the OS. Similar for the database.

Platform-as-a-Service

- One place where this virtualization fell apart was security upgrades.
- As hackers find bugs and security holes in operating systems (or even in database packages or other software), new viruses and other malware are developed.
- To combat this, the operating system is patched.
- In addition, virus protection software is upgraded with new rules.
- With a freeze-dried version of the complete environment, the environment is vulnerable to these new security threats.
- One approach to deal with this is to simply discard an infected virtual image, creating a fresh new copy. However, a mechanism is required to migrate the database data from the old to the new version.

Infrastructure-as-a-Service

- The IaaS delivery model represents a self-contained IT environment that includes infrastructure, such as hardware, networks, connectivity, and operating systems.
- These are usually all virtualized.
- The IaaS customer has a high level of control, and responsibility, over the configuration and utilization of the environment.
- The administrative responsibility is placed directly upon the cloud consumer.
- This model is used by consumers that require a high level of control over the cloud-based environment they intent to create.
- Sometimes a cloud provider will contract IaaS offerings from other cloud providers to scale their own cloud environments.

IaaS + PaaS

- In some cases, a combined IaaS + PaaS model is used. Why?
- A company may offer a PaaS product, but then leases a IaaS from another cloud provider.
  - The motivation for this might be economics -- it is cheaper to lease IaaS from another provider rather than expand this company's infrastructure.
  - Maybe this is a temporary solution until a more permanent arrangement can be built.
  - This might also be a time-of-day or seasonal requirement, when the expanded capability is not needed on a permanent basis, but on a temporary or a recurring temporary basis.
  - Perhaps a cloud consumer imposes a legal requirement that the data be physically stored in a specific region.

Summary of Key Points

- The IaaS cloud delivery model offers cloud consumers a high level of administrative control over infrastructural-based IT resources.
- The PaaS cloud delivery model enables a cloud provider to offer a pre-configured environment that cloud consumers can use to build and deploy cloud services and solutions, with decreased administrative control/responsibility.
- SaaS is a cloud delivery model for shared cloud services that can be positioned as commercialized products hosted by clouds.