Cloud competing Pricing Model:

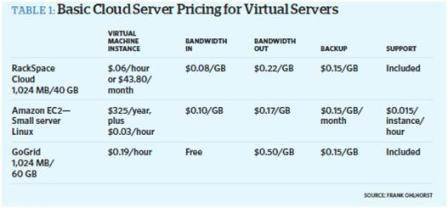
Pricing structures are [based on a multitude of factors](https://searchcloudcomputing.techtarget.com/news/450427235/Cloud-pricing-models-reignite-IaaS-provider-feud), from storage space needed to clock cycles used to monthly traffic allotments, and that's not all. Some service providers have additional charges hidden deep within their service-level agreements (SLAs).

To determine total pricing for a cloud service, users need to understand the individual service elements that [a provider bills for](https://searchitchannel.techtarget.com/news/2240181152/Cloud-pricing-and-sales-in-spotlight-at-Ingram-Micro-Cloud-Summit-2013) and how those charges are calculated. Does the provider, for example, bill based on traffic, storage space needed, server CPU time or a combination of these factors along with other elements?

**Costs stem from services**  
Another critical factor in determining true costs comes down to the type of service needed. For some, that service may be little more than a hosted, dedicated server to run applications in the cloud. For others, the service may be cloud-based backup or business continuity or basic hosted storage.

Perhaps, the easiest way to break down pricing is to focus on the primary services offered. The majority of cloud service providers break down their services into three primary areas: servers in the cloud, storage in the cloud, and sites and applications in the cloud. Each is governed by its own formula for pricing.

Servers in the cloud come in two forms: virtual and physical. In other words, you can purchase time on a virtual server (where the physical hardware may be shared with others) or time on a dedicated server (where you are the only "tenant" on that server). Table 1 shows the pricing breakdowns:

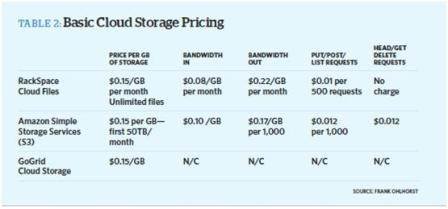
[](https://cdn.ttgtmedia.com/rms/misc/ebookTable1.JPG)  
**Table 1:** *Click to enlarge*

The pricing comparisons are only part of the overall picture; each vendor listed above includes extra services and features for an additional charge. What's more, prices can change depending on length of commitment, total bandwidth needs or total size of storage required, and in most cases, prices and packages are negotiable with a vendor's sales staff.

**Different providers, different services provided**  
Not all cloud service providers are created equal, and that becomes evident when you look more closely at the differences between providers and how they address customer needs. For the purposes of comparison, we picked three of the well-known cloud infrastructure providers:

* GoGrid includes load balancing at no extra charge on some of its server offerings and also includes the first 20 GB of storage for free.
* Rackspace uses a different billing mechanism and reduces per-gigabyte bandwidth charges as volume increases; the company also offers backup services at no charge on some of its virtual server bundles.
* Amazon offers sliding scales for rates on most of its services but charges for gets and puts to its storage services.

When you look at the simpler concept of cloud-based storage services, the differences in pricing structures and in how providers build bundles for dent (see Table 2). Once again, the pricing comparisons are only part of the picture. And like other cloud services, prices are affected by length of commitment, total bandwidth needs or total size of storage required. And as with other cloud services, there is plenty of room for negotiation.

[](https://cdn.ttgtmedia.com/rms/misc/ebookTable2.JPG)  
**Table 2:** *Click to enlarge*

Once you take a closer look, the differences between service providers take shape:

* GoGrid offers the first 20 GB of storage at no charge to customers using its hosted server services and offers its storage services only to hosted server customers. Typical of the market segment, GoGrid offers discounted per-gigabyte pricing as customers buy larger storage amounts. GoGrid's storage service is offered as a mountable volume and does not yet offer a Web services application programming interface for gets and puts and other commands.
* Rackspace tries to keep its storage services billing model as simple as possible. The company offers a sliding scale for storage purchases, where the price per-gigabyte decreases as total amounts ordered increases. What's more, if the file is more than 250 KB in size, the company doesn't charge for gets and puts.
* Amazon S3 does not charge for deletes and offers discounts as transaction volume and storage needs increase. The company also offers contract-based fixed pricing for those looking to stabilize their prices. For larger file transfers, the company recommends using its import and export services, which can reduce costs.

Ideally, [pricing out cloud-based services](https://searchcloudcomputing.techtarget.com/tip/Five-overlooked-costs-that-add-to-a-public-cloud-bill) should take little more than selecting features and determining storage and server computing needed. In reality, most IT managers will find that ideals don't apply here and will have to carefully consider the "hidden extras" as well as the standard charges to determine the cost for services.

The bigger challenge is converting the "technospeak" of cloud services pricing into something that those holding the purse strings can understand and to bring those individuals into the loop to negotiate pricing and contract terms as well as SLAs.

The trick is to get all estimates in writing with clear, concise language that explains what the total charges will be per contracted period: Written confirmation is the only way to see an apples-to-apples comparison of pricing models and determine true budget amounts.

**The future of IaaS**  
A recent study by the University of New South Wales in Australia, in collaboration with researchers at NICTA (National ICT Australia) and the Smart Services Cooperative Research Centre, spent seven months stress testing Amazon's EC2, Google's App Engine and Microsoft's Azure cloud computing services.

The analysis simulated 2,000 concurrent users connecting to services from each of the three providers, with researchers measuring response times and other performance metrics. The results were less than stellar, with response times varying widely depending on the time of day in which services were accessed. In addition, the study revealed a lack of monitoring tools to enable organizations to check whether the service has met their SLA.

It's obvious that cloud providers have their work cut out in terms of simplifying pricing models, beefing up security and providing SLAs that guarantee better reliability. The market is evolving fast, and today's dominant players could be history in two years. Just one catastrophic data privacy breach could extinguish a brand and potentially slow the market down for a decade.

Link: <https://searchcloudcomputing.techtarget.com/tutorial/Understanding-cloud-computing-pricing>

**Cloud SLA:**

A cloud infrastructure can span geographies, networks and systems that are both physical and virtual. While the exact metrics of a cloud SLA can vary by service provider, the areas covered are uniform: volume and quality of work -- including precision and accuracy -- speed, responsiveness and efficiency. The document aims to establish a mutual understanding of the services, prioritized areas, responsibilities, guarantees and warranties provided by the service provider.

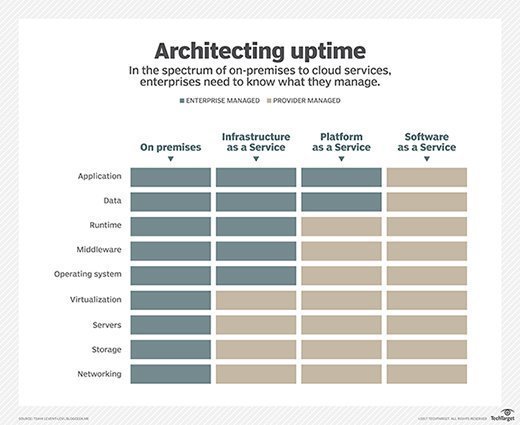
Metrics and responsibilities among the parties involved in cloud configurations are clearly outlined, such as the specific amount of response time for reporting or addressing system failures.

Financial penalties a provider must pay for failing to live up to the guaranteed terms are also included. These penalties are often in the form of credits for service time.

**What to look for in a cloud SLA**

Service-level agreements have become more important as organizations move their systems, applications and data to the cloud. A cloud SLA ensures that cloud providers meet certain enterprise-level requirements and provide customers with a clearly defined set of deliverables.

The defined level of services should be specific and measureable in each area. This allows the quality of service ([QoS](https://searchunifiedcommunications.techtarget.com/definition/QoS-Quality-of-Service)) to be benchmarked and, if stipulated by the agreement, rewarded or penalized accordingly.



An SLA will commonly use technical definitions that quantify the level of service, such as mean time between failures ([MTBF](https://whatis.techtarget.com/definition/MTBF-mean-time-between-failures)) or mean time to repair ([MTTR](https://searchstorage.techtarget.com/definition/mean-time-to-repair-MTTR)), which specifies a target or minimum value for service-level performance.

A typical compute and cloud SLA articulates precise levels of service, as well as the recourse or compensation the user is entitled to should the provider fail to deliver the service as described. Another area to consider carefully is service availability, which specifies the maximum amount of time a read request can take; how many retries are allowed; and so on.

The SLA should also define compensation for users if the specifications aren't met. A cloud storage service provider usually offers a tiered service credit plan that gives users credits based on the discrepancy between SLA specifications and the actual service levels delivered.

Most [public cloud storage services](https://searchstorage.techtarget.com/definition/public-cloud-storage) provide details of the service levels that users can expect on their websites, and these will likely be the same for all users. However, an enterprise establishing a service with a [private cloud storage provider](https://searchstorage.techtarget.com/definition/private-cloud-storage-internal-cloud-storage) may be able to negotiate a more customized deal. In this case, the cloud SLA might include specifications for retention policies, the number of copies that will be retained, storage locations and so on.

Cloud service-level agreements may be more detailed to cover governance, security specifications, compliance, and performance and [uptime](https://searchdisasterrecovery.techtarget.com/definition/cloud-uptime) statistics. They should address security and encryption practices for data privacy, disaster recovery expectations, data location, as well as data access and portability.

**SLAs that scale**

Most SLAs are negotiated to meet the needs of the customer at the time of signing, but many businesses change dramatically in size over time. A solid cloud service-level agreement outlines intervals for reviewing a contract so that it meets the changing needs of an organization.

Some vendors even build in notification workflows that indicate when a cloud service-level agreement is close to being breached so new negotiations can be initiated based on the changes in scale. When entering any cloud SLA negotiation, it's important to protect the business by clarifying uptimes. A good SLA protects both the customer and supplier from missed expectations.

**Link:** [**https://searchstorage.techtarget.com/definition/cloud-storage-SLA**](https://searchstorage.techtarget.com/definition/cloud-storage-SLA)

**10 best SLA practics:**

1.Specify roles and responsibilities of all parties with respect to the SLA, and, at a minimum, include agency and cloud providers. These definitions would include, for example, the persons responsible for oversight of the contract, audit, performance management, maintenance, and security.  Define key terms, including activation date, performance, and identify any ambiguities in the definitions of cloud computing terms.

2.Define key terms, such as dates and performance. Define the performance measures of the cloud service, including who is responsible for measuring performance. These measures would include, among other things, the availability of the cloud service; the number of users that can access the cloud at any given time; and the response time for processing a customer transaction.

3.Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures would include:

•Level of service (e.g., service availability—duration the service is to be available to the agency).

•Capacity and capability of cloud service (e.g., maximum number of users that can access the cloud at one time and ability of provider to expand services to more users).

•Response time (e.g., how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages).

4. Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the SLA and transitioned back to the agency in case of exit/termination of service.

5.Specify the following service management requirements:

•How the cloud service provider will monitor performance and report results to the agency.

•When and how the agency, via an audit, is to confirm performance of the cloud service provider.

6. Provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency. In addition, how the provider will remediate such situations and mitigate the risks of such problems from recurring.

7. Describe any applicable exception criteria when the cloud provider’s performance measures do not apply (e.g., during scheduled maintenance or updates).

8. Specify metrics the cloud provider must meet in order to show it is meeting the agency’s security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency’s data). Specify the security performance requirements that the service provider is to meet. This would include describing security performance metrics for protecting data, such as data reliability, data preservation, and data privacy. Cleary define the access rights of the cloud service provider and the agency as well as their respective responsibilities for securing the data, applications, and processes to meet all federal requirements. Describe what would constitute a breach of security and how and when the service provider is to notify the agency when the requirements are not being met.

9. Specifies performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach).

10.Specify a range of enforceable consequences, such as penalties, for non-compliance with SLA performance measures. Identify how such enforcement mechanisms would be imposed or exercised by the agency.Without penalties and remedies, the agency may lack leverage to enforce compliance with contract terms when situations arise.

**Link:** [**https://www.networkworld.com/article/3053920/cloud-computing/10-best-cloud-sla-practices.html**](https://www.networkworld.com/article/3053920/cloud-computing/10-best-cloud-sla-practices.html)