BlueSilverShift

Navigating the Cloud:

An Introduction to Cloud Language

Table of Contents

Introduction

Getting your mind around cloud language can seem onerous. The terms and acronyms which pepper IT-speak can make cloud phrases seem out of reach.

At BlueSilverShift, we believe that semantics shouldn't be a hurdle.

To help you navigate the language of the cloud, we will take you through common cloud phrases and concepts. Let's start at the very beginning.

1

The Cloud

What is **the cloud**, anyway?

Types of Cloud

What is the cloud, anyway?

To some people, it's DropBox. To others, iTunes, and to yet others, Google Drive or Microsoft OneDrive. All these assumptions are correct; however, none alone is the complete answer.

Effectively, the cloud is a non-physical data repository that includes anything stored, processed or running in the Internet. Fun fact: The cloud takes its name from old architectural drawings, where a cloud represented the Internet.

Types of Cloud

Having defined the cloud, we now look at its different types. Each presents its own considerations and benefits:

- The **private cloud** offers Internet- or private network-based computing to select users. A private server, hosted off-site, is managed by the host or by remote. It is scalable and elastic like the public cloud, but with greater security and privacy. By extension, its cost and management fall back on a company's IT department.
- The **public cloud** is perhaps the most common, and the most familiar. Anyone can use the public cloud, and many rely on Azure, AWS or Google to do so. Data is stored in a provider's data centres, and the provider takes care of management and maintenance. Its services and scalability are vast.
- The **hybrid cloud** combines elements of public and private clouds, allowing data and applications to be shared between them. The scalability of the public cloud combines with the security of the private cloud. In other words, it combines cost efficiency with increased security.

Types of Cloud

Finally, there is "**multi-cloud**," which is not actually a cloud type at all. Rather, it refers to a strategy of storing identical data in multiple clouds. Why would someone go to this trouble? In short, fear that choosing one provider may lead to future complications.

It may seem wise to avoid **vendor lock-in,** which is an inability to change providers because of an existing strong commitment. However, maintaining multiple environments can add to costs and complications. For instance, solutions may have to be customized for each, and synchronization is difficult to ensure.

Costs such as egress network charges and cloud management make this a strategy of diminishing returns

Book a Call With a Cloud Specialist

If someone asks me what cloud computing is, I try not to get bogged down with definitions. I tell them that, simply put, cloud computing is a better way to run your business.

Marc Benioff, Founder, CEO and Chair of Salesforce

2

Managing the Cloud

Why does **cloud management** matter?

Managing the Cloud

Establishing cloud management best practices at the outset is essential to ensuring a successful and smooth cloud migration. But what does this mean in principle and in practice? Here are some tips for getting started.

Developing a **cloud governance** strategy sets you up for early and ongoing success. Defined policies and procedures ensure that your file structures are logical and tidy, and that the lines of accountability for them are clear. Naming conventions, security, workload optimization, and spend are key factors to plan for from the beginning.

Getting these items into place early on can reap dividends over time. As your resources grow, your system has clear management parameters to follow. This saves both money and frustration as you effectively manage sprawl.

To be sure, **sprawl** is as it sounds: the uncontrolled creation of assets and consumption of resources to support them. This spans virtual machines, files, systems, servers, and networks, at a minimum. Deciding who owns which resources, and allocating specific permissions, can nip early sprawl in the bud. Conversely, without controls in place, it can be impossible to know who created resources, why, and whether they can safely be removed.

Managing the Cloud

That said, a **cloud custodian** can oversee cloud health at a high level. This role is responsible for monitoring, maintaining, and enforcing cloud governance standards and practices. The custodian ensures your environment is optimal, tracking costs and looking for workload optimization opportunities.

> *Fill your brain with cloud phrases – you'll be computing in no time.*

The technical nuts and bolts

Data is moved to the cloud in what is called a **migration**. There are different ways that this can happen, and each scenario must be considered for its constituent parts. Here are a few migration factors to consider.

One common migration technique is **lift and shift**, which is the process of taking data and applications from one repository and moving them to another, usually in the cloud. This is a quick solution which does not require re-architecting, but it can be short-sighted. The cloud offers unprecedented power and potential, and failing to re-architect may result in opportunity costs and lost cost-optimization alike.

Computers, cell phones, video game consoles, web servers and generally any device containing a computer will have an **operating system (OS)**. The OS supports basic computer functions across hardware and software resources. Programs such as Microsoft Windows, macOS and Linux manage the computer's memory and processes, allowing you to communicate with the computer without having to know its language. In cloud terms, OS compatibility is important; legacy systems may not be coded for modern applications and may lack security patches which keep your system safe.

The technical nuts and bolts

Like its non-cloud counterpart, **legacy** simply refers to an old technology, system or application. Outdated but still in use, the “legacy” moniker often implies that it broke ground for systems that would follow. However, the business impact of legacy systems can be detrimental in lost productivity and opportunity cost. Conversion to a new system can be complex, though, and adequate time should be allowed for planning and migration.

> *You, too, can love cloud language!*

I don't need a hard disk in my computer if I can get to the server faster... carrying around these non-connected computers is byzantine by comparison.

Steve Jobs, late CEO of Apple

3

Life in the Cloud

Where does my **stuff live** and it safe there?

Where does my stuff live?

In the public cloud, a certain number of resources are shared across users, bringing down costs and allowing for efficiency of provision. But what does this mean for security and privacy? How is the cloud segmented, exactly? Tenants and subscriptions are two of the high-level delineations.

A **tenant** is a dedicated space with a secure boundary. This space exists within a larger space offered by a cloud provider but is used exclusively by an entity for business or personal purposes. The resource sharing aspect reduces the cost of provision, akin to private houses which share roads and water lines.

Alternately, the tenant can be thought of as a suite in an apartment. The suite's walls provide a security boundary, and although those walls might be shared with neighbours, they are themselves impassable. Similarly, in the cloud, one must have the key to be able to enter a tenant. Certain entry rules can be applied, and within that space, specific areas may be further secured.

If the tenant is a directory, the **subscription** can be thought of as the “folders” one organizes resources in. Subscriptions are tied to a tenant: a tenant can have multiple subscriptions, but the subscription belongs to only one tenant.

Within your home, to extend the metaphor, rooms represent areas for specific purposes. Sleep takes place in the bedroom, showering in the bathroom. Different strategies apply for resourcing within subscriptions – for instance, subscriptions can be segmented internally based on cost accountability, and interact internally with no extra egress charges – but subscription strategy is a topic for another book.

> *It’s a whole other world in the cloud – but we can help you navigate.*

What about security?

While tenant and subscription boundaries are important for containing and organizing your personal data, they alone are not enough to ensure the best possible security for your information. Additional layers of protection, such as Network Security Groups (NSGs) and firewalls are integral. These two concepts are not synonymous.

NSGs are a universal concept although the name is Azure specific. It is a security boundary and helps to protect your virtual network. However, it is not a firewall, and does not provide the same level or type of protection.

NSG can be a useful tool to partition the network. For instance, a front-end network with customer-facing web servers might only “talk” to a back-end database using a strict port limited to one server. This provides a control point that protects the system. This kind of control can also be outward facing, controlling entry at the port level or IP address level.

However, with up to 200 rules allowed in an NSG, and some of those with multiple IP addresses and ports associated, it can quickly become unmanageable. There is no logging capability, so mistakes can be difficult to see. A mistake within those rules without a firewall in place opens the virtual network to vulnerabilities.

The **firewall** is a necessary backstop, adding another protective layer behind NSGs. It provides a barrier between internal trusted networks and external untrusted ones. It also monitors, logs, and controls traffic based on predetermined security rules.

Firewalls can provide further capabilities such as machine learning. Behind the scenes, for instance, Microsoft is looking for common threats across the world, recognizing things that are coming into their data centers, and triggering responses based on what they observe. This helps the firewall to stay ahead of trends and developments as much as possible.

Check Your Cloud Security

"Cloud computing is often far more secure than traditional computing."

Vivek Kundra, Executive Vice President, Salesforce.com

4

Cloud Costs

How do I **pay for** the cloud?

Understanding subscription costs

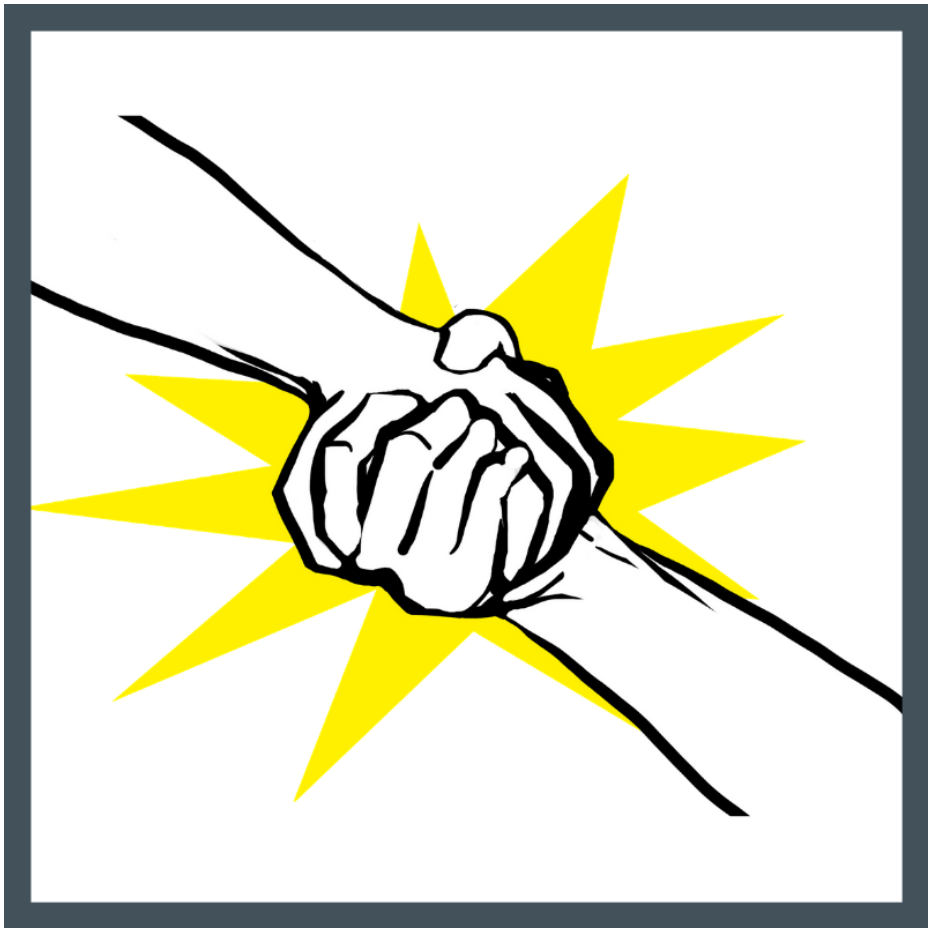
Of course, any service comes with a cost. An on-site server has an upfront cost, along with maintenance and repairs, electricity, and eventual obsolescence. While the cloud is conceptually simpler, having no physical components to maintain, pricing can be taken in different ways.

The **pay as you go** model is just as it sounds, allowing cloud resources to be purchased at the retail price, or MSRP (manufacturer's suggested retail pricing). Every public cloud vendor has retail price lists and pricing calculators, which can be used to understand the cost to run a specific resource with certain inputs. This is based on a 'per minute, per second' cost, where usage is monitored to the second.

With pay as you go, there is no commitment, and no heady upfront cost. It is more palatable, in this sense, than buying a $50,000 server and depreciating that over its useful life. There is no risk in testing different levels of use, because it can be stopped or changed at any time. With pay as you go, you only purchase – and pay for – what you need.

Conversely, **reserved instances** offer the ability to reserve a SQL database for one- or three-years' consumption, with substantial cost savings in exchange for prepayment. On the provider's side, this reservation of space reduces their model costs enough to offer the savings to the consumer.

Recently, Microsoft announced the ability to purchase reserved instances one or three years yet pay monthly. A 12% penalty on the balance of a contract is incurred in case of early cancellation. For some, this is a manageable cost to absorb in case of needing to scale up the environment.



Working with a trusted partner helps to ensure a successful cloud journey

Planning for two-way traffic

It is also important to understand how traffic affects costs, and why elasticity and scalability are important in responding to fluctuating needs, whether short or long term.

Elasticity refers to a system's ability to adapt to workload changes by automatically adjusting resources. To use Black Friday sales as an example, the old days would require the purchase of numerous servers that would sit idle most of the year. When a traffic spike occurs in an event like Black Friday, there is enough capacity to handle demand – after which, the servers return to being idle.

Elasticity in the cloud allows for scaling on demand. There are two ways in which this occurs:

1. Vertically – scaling out, adding more of the same compute systems or virtual systems. This adds power (CPU, RAM) as a resource.
2. Horizontally – going to a larger instance size to meet the demand. This adds more machines as resources.

Scalability is literally the ability to scale, referring to the ability of a system to add resources in response to an increase in work.

In the cloud, scalability is infinite; on-premises is constrained by the physical limitations of the server.

Inbound traffic is known as **ingress**. Ingress has many variations, such as a web server on the front end of a system, or people connecting to a network through a remote desktop connection and an inbound public service point. Appropriate ingress style solutions should be developed in each case.

It is important to protect ingress traffic. Left open to the world, ingress is an easy target for hacking. Solutions can include a firewall, web application, and network security groups.

Conversely, **egress** is outbound traffic. It, too, should be controlled, but for a different reason than ingress. There are two main reasons why:

1. In the public cloud, ingress traffic is free. The cloud provider is happy to accept your data. However, outbound traffic to the Internet has a cost attached, and this can escalate quickly left unattended.
2. Egress control is important to protect your system against being compromised. Without restraints in place, a server may 'talk' to information that is detrimental and bring that traffic into your system.

Some people call this artificial intelligence, but the reality is this technology will enhance us. So instead of artificial intelligence, I think we'll augment our intelligence.

Ginni Rometty, CEO of IBM

5

Next Level Cloud

I get the cloud basics. **What's next**?

Intelligent data and operations

The power and capacity of machines to both analyze and learn is both awesome and just getting started. While this often provides fodder for imagining myriad futuristic scenarios, there are a few key pieces at play today.

A **Virtual Machine (VM)** is just as it sounds, emulating a physical machine in structure and functionality. There are two kinds:

- **System VMs** substitute for a real machine, allowing a full OS to operate.
- **Process VMs** execute programs in a platform-independent environment.

SQL, or **Structured Query Language** is a standardized programming language for managing relational databases and performing operations on the data within them. It is the most widely used database language, but its code may require adjustments between systems.

Machine learning is a branch of artificial intelligence that applies data analysis to systems. These systems learn from the data and patterns they observe, then make decisions with minimal human interference. It is closely related to (the rather less futuristic sounding) **computational statistics**, where computers make predictions. Applied to business problems, machine learning is also referred to as **predictive analysis.**

Ahh, the aaS: "As a Service"

The 'aaS' list is long, as this small compilation shows. Here are a common few:

- **IaaS – Infrastructure as a Service** includes services like Microsoft Azure, GCP or AWS, which allow users to host VMs in the cloud. Users don't have to worry about hardware or infrastructure maintenance, and can run various OSs.
- **SaaS – Software as a Service** in practice has been around some time. Often cloud-based, it includes email, accounting, CRM, and other on-demand services. Traditionally, customers would purchase software out-of-the-box and run it on their own machines. With SaaS, you skip the ownership part and access the service as you need it.
- **PaaS – Platform as a Service** provides a platform on which software can be created. Applications can be written much more quickly than building them from scratch, but they are in turn trickier to scale. With PaaS, organizations can write their own software without worrying about the back-end infrastructure.
- **DRaaS – Disaster Recovery as a Service** replicates and hosts physical or virtual servers as a failsafe in case of a catastrophic event. A function of business continuity planning, DRaaS provides timely operational recovery in case of an outage. The **Recovery Point Objective (RPO)** is the age of the files that must be recovered for regular business operations to resume. Whether measured in minutes or hours, DRaaS requires off-site mirrored backups to be maintained. The old process of backing up data at the end of the day is insufficient.

Ahh, the aaS: “As a Service”

- **XaaS – Anything as a Service**. Virtually anything can be a service through the Internet, and many defy traditional categorization. Storage, function, desktop, security, database…the list goes on. Even malware on the dark web is viewed as a service to prospective cyber criminals.

> *Don't be the dinosaur of the future. Move to the cloud.*

Speaking of semantics

Lastly, a cloud linguistic point that we at BlueSilverShift are sticklers about: **On-premises.** Industry often abbreviates this to "**on prem**," and these both refer to the server at your premises. However, many mistakenly say, "on premise." But that would make it a conclusion inferred or following from a previous statement of proposition, rather than part of a building.

In fact, you could say that our premise is to get you off premises and realizing your full cloud potential.

Cloud is just emerging,
but it's high growth.

Satya Nadella, CEO of Microsoft

6

Your Cloud Journey

This is all very interesting and I am not a dinosaur. **How do I get me some cloud?**

Get your head in the cloud

The cloud is increasingly pervasive. Eventually, unless you are a dinosaur, you will engage with the cloud, if not be tasked with making business decisions about it. As a result, it is ever more important to understand the basic concepts and ideas.

Technology for its own sake is not an end, and the cloud is no exception. But harnessing technology wisely can help unlock value in your business, and the cloud is a powerful tool. Its security, flexibility, and scalability are unprecedented, and it is worth understanding, even in basic terms.

This is a brief entrée into the world of the cloud. While perhaps heady, its terms and concepts need not be a barrier. With a trusted partner like BlueSilverShift to guide you, harnessing the power of the cloud is well within your reach.

Get me to the cloud

BlueSilverShift

Ready to Learn More?

BlueSilverShift is your trusted cloud partner.

We are here to help you on your cloud journey, whether you are taking your first steps or well on the path.

Get in touch today to learn how the cloud can empower you and your business.

TELL ME MORE ABOUT THE CLOUD