ixia
A Keysight Business

Ixia's Guide to Cloud Computing

TERMS AND ACRONYMS

Cloud Terms & Acronyms

Spending on cloud computing is growing faster than ever before and virtually all organizations have workloads running in one or more clouds. The agility and cost savings of cloud technology has helped our digital economy grow and thrive. Adopting cloud technology is mainstream, but also still a work in progress for many organizations. Even those who are well versed in cloud migration are still learning new practices for securing and optimizing workloads in the cloud. This guide to Cloud Computing Terms & Acronyms is designed to clarify concepts you will encounter as you move forward in your journey to the cloud.

Automation and Orchestration

Automation refers to a task or function that is performed without requiring human intervention.

Orchestration refers to the coordination or sequencing of automated tasks and/or functions to accomplish a defined process or workflow. Both automation and orchestration are critical technologies in the cloud, enabling day-to-day tasks, such as provisioning, patching, and resource management to be performed at a massive scale—across hundreds of thousands (even millions) of servers and other cloud components.

Backhaul

In cloud computing, backhaul refers to the transfer of data and transactions in the cloud back to an on-premises data center for further processing, typically security inspection and performance monitoring. Most cloud providers charge a substantial fee for moving data out of their physical domain, which discourages customers from readily switching cloud providers. If there is a large volume of data to transfer, the network pipe needed to bring the data back in-house may also need to be upgraded, resulting in additional backhaul costs. Read more about backhaul in the white paper: Security and Performance Monitoring in the Cloud.

Blind Spots

Areas in the network where there is not access to data packets flowing between network devices. The two best examples of this are: data that flows between virtual machines on a single server (common in private cloud environments) and data that flows between two public cloud instances. Packet-level data is required for many types of threat detection and security analysis, as well as for performance monitoring and application optimization.

Cloud Access Security Broker (CASB)

A software tool or service that sits between an organization's on-premise infrastructure and a cloud provider's infrastructure; allowing the organization to extend the reach of their security policies beyond their owned infrastructure.

Cloud-based Security Tools

Some vendors of popular security solutions such as next generation firewalls and intrusion detection systems are migrating their technology to cloud platforms to offer their customers more flexibility, faster scalability, and easier maintenance. Cloud-based security services can be purchased on a pay-as-you-go basis and fewer trained staff are generally required. Vendors of solutions that have been in the market for many years have little incentive to migrate

915-8274-01-5081 Rev A

their solutions to cloud, since new development is required and overall revenues may end up being lower. This is one of the reasons that some companies still find it necessary to backhaul data from the cloud to the data center for processing.

Cloud Bursting

Cloud bursting relates to hybrid clouds. The idea is that a given application normally runs in a private cloud or a local computing environment. If a situation arises where the application needs additional resources (computing power, storage, etc.), it can "burst" into the public cloud and use cloud computing for those additional resources.

Cloud Maturity Model

Model used to segment organizations according to their adoption and use of cloud computing.

- **Cloud Beginners:** Organizations (~22%) that have started working on initial cloud projects, but are still gaining comfort and experience in the cloud.
- **Cloud Explorers:** Organizations (~25%) that have deployed multiple applications to the cloud and are exploring opportunities to improve and expand their cloud strategies.
- **Cloud Focused:** Organizations (~33%) that have adopted a "cloud first" strategy, and are looking for opportunities to further optimize their cloud environments while reducing costs.
- **Cloud Watchers:** Organizations (~14%) that are developing their cloud strategies and evaluating cloud options, but currently do not have any applications deployed to the cloud.

Cloud-Native

To take advantage of the cloud, organizations must design their applications and services so they are decoupled from physical resources and capable of moving easily between virtual machines or cloud instances. This is referred to as being cloud-native (Read more at Cloud-Native Visibility for Public Cloud). Cloud-native computing uses an open source software stack to be:

- **Containerized:** Each part (applications, processes, etc.) is packaged in its own container. This facilitates reproducibility, transparency, and resource isolation.
- **Dynamically orchestrated:** Containers are actively scheduled and managed to optimize resource utilization.
- **Microservices oriented:** Applications are segmented into microservices. This significantly increases the overall agility and maintainability of applications.

Cloud Computing

National Institute of Standards and Technology (NIST) defines the following five essential characteristics of cloud computing:

- **On-demand self-service:** Services can be unilaterally and automatically provisioned.
- **Broad network access:** Services are available over the network through various platforms and devices.
- **Resource pooling:** Compute, storage, and networking resources are pooled to serve various tenants and demand levels, and are dynamically assigned and reassigned, as needed.
- **Rapid elasticity:** Services can be provisioned and released, in some cases automatically, to scale (up/down and in/out) with demand.
- **Measured service:** Resource usage can be transparently monitored, controlled, optimized, and reported.

Cloud Security

Security of data and applications is often cited as a reason organizations are hesitant to migrate to public cloud platforms. However, most security analysts believe public cloud is not inherently less secure than the data center, rather both environments are vulnerable to cyberattacks in our highly-connected digital world. Visibility to all the data flowing through cloud platforms is the first step, combined with the use of proven security solutions that can isolate suspicious traffic and quickly contain any attacks that get past perimeter defenses. Read more in the white paper: What You Can Do to Strengthen Cloud Security.

Cloud Sandbox

In general, sandboxes provide an environment to validate untested or unknown code. Sandboxes protect production systems and their data from code that is yet unproven or coming from unknown sources. Cloud sandboxes differ from traditional sandboxes in that they do not sit on-premise in the data center, but on the internet between users and applications, analyzing unknown code for threats and malware. A cloud sandbox can be operated offline or inline, without backhauling traffic to the data center. This reduces the cost of operation.

Cloud Service Providers (CSP)

A cloud provider is a company that offers some component of cloud computing—Infrastructure as a Service (IaaS), Software as a Service (SaaS), or Platform as a Service (PaaS)—to other businesses or individuals.

Cloud Visibility

While using network taps and packet brokers to access network traffic is well-established, it is not as straight-forward to access traffic in cloud environments. Users do not have control over, or access to, the underlying physical infrastructure. Ensuring strong security and efficient performance, therefore, requires the ability to access to packet-level data on the traffic flowing from, to, or between an organization's clouds. Sensor and container technology have made it possible to make copies of cloud traffic to perform traffic inspection and analysis. This is referred to as cloud visibility. Read more in the brief: Get Visibility into Your Clouds.

Compliance

Standards and regulations, such as PCI-DSS, SOX and HIPAA, require organizations to take specific action to protect sensitive customer data. In the cloud, however, providers do not generally track or disclose exactly where data is stored and workloads are processed, thus impacting the ability to prove and document compliance. This means IT teams must proactively identify processes and solutions to ensure compliance when using public cloud.

Containers

A software technology that allows application components to be paired with the operating system components necessary to run them in a single package (known as a container). Containers, such as Docker, allow applications to be deployed in seconds and booted up in fractions of a second. The desire for hybrid cloud or cross-cloud integration is a key driver for container adoption.

Continuous Security Testing

A fast-growing approach to validating security in environments with a high degree of change and variability. Continuous security testing relies on threat simulations to expose gaps in security architecture and gives organizations a chance to strengthen their defenses before an intruder causes damage. Read more in the brief: Validate Security Resilience in Cloud Environments.

DevOps

DevOps and cloud computing work together to help organizations bring new services and applications to market more quickly, at less cost. DevOps is about streamlining development, while cloud offers on-demand resources, automated provisioning, and easy scaling, to accommodate application changes. Many DevOps tools can be acquired on-demand in the cloud or as part of a larger cloud platform. To support hybrid cloud deployment (workloads with an ability to move between clouds), enterprises should select DevOps platforms with an interface to the cloud providers they will use.

Docker

Docker is the technology responsible for driving the container movement and is still the market leader. Docker is open source with several vendors offering enhancements and support. Depending on the specific use case, alternatives to Docker are CoreOS rkt, LXD (for Ubuntu Linux), Kubernetes, Cloud Foundry Garden, and other container services offered by the major cloud providers (e.g. Azure Container Service).

East-West Traffic

Originally defined as traffic that never left the data center—moving from server to server Now, with the prevalence of virtualization and cloud computing, the term has expanded to include traffic that moves from one virtual machine (VM) or application to another. Cisco estimates that 76% of network traffic is of the east-west type.

Generic Routing Encapsulation (GRE) Tunnel

Tunneling protocol developed by Cisco that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an internet protocol network.

Governance

Refers to the rules for cloud usage, specifically for defining, continuously monitoring, and auditing the rules, policies and processes that allocate, coordinate and control the use of cloud resources. Governance is distinct from cloud management, which refers to the operation of cloud environments.

Horizontal Scale

Ability to connect multiple hardware or software entities, such as servers, so they work as a single logical unit. This is what software-defined networking (SDN) and other such technologies enables. It is also what creates the public cloud structure and makes it unique.

Hybrid Cloud and Hybrid IT

Hybrid cloud infrastructure refers to the simultaneous use of both public and private cloud environments, with applications and data sometimes moving between them. Hybrid IT generally refers to a mix of an on-premises data center with public and private clouds.

Hyperscale

Hyperscale generally refers to the architecture necessary for companies like Amazon, Apple, Facebook, and Google to provide digital services on a massive scale, and the same concepts increasingly apply to other organizations. Synergy Research found 390 web-scale data centers operating worldwide in 2017, up from 300 in 2016, with no sign of slowing down in 2018. The majority are in the US with 44 percent of total. Chinese companies like Tencent and Baidu also operate hyperscale data centers, as well as companies in Japan, the UK, Australia, and Germany.

Hypervisor

Also known as a virtual machine monitor (VMM); a hypervisor is computer software, firmware, or hardware that creates and runs virtual machines. A computer on which a hypervisor runs one or more virtual machines is called a host machine, and each virtual machine is called a guest machine.

Infrastructure as a Service (IaaS)

Infrastructure resources owned and operated by a third-party and made available to users over the internet. The user has no physical access to, or control over, the infrastructure and generally does not know where the infrastructure is located. Examples include: VMs, storage, load balancers, and networking.

Instance

Refers to a virtual server instance from a public or private cloud network.

Kubernetes

Kubernetes is a portable, open-source platform for automating the deployment, scaling and management of containerized applications. Kubernetes services, support, and tools are widely available. The platform provides the building blocks for creating a development environment that preserves user choice and flexibility.

Lift and Shift

Industry term for when something from a physical environment is migrated to the cloud (vs. a cloud-native design or a rebuild for cloud).

Metadata

In the context of cloud, metadata is information about cloud instances, such as operating systems, memory, cloud service provider, and geolocation, that can be used to configure or manage cloud workloads. Depending on the provider, metadata may not be automatically provided to cloud users. This lack of transparency can be a challenge for monitoring security and performance in the cloud.

Microservices

Like Service-Oriented Architecture (SOA), microservices are application building blocks comprised of small, independent processes and services.

Migration

Term used to describe the process of moving data, applications, or other business services processes from an organization's on-premises data center to a private or public cloud environment. The migration can be of the "lift and shift" variety or can be accomplished by redesigning the service to be more independent of the underlying processing technology, such as through the use of containers or microservices.

Multi-cloud

Industry term for using more than one cloud service provider. IDC predicts that by 2020, 90% of enterprise IT organizations will have multi-cloud architectures (IDC FutureScape, Worldwide 2018 Predictions).

Multilayer Cloud Security

Security in the cloud is governed by a "shared responsibility model" that spreads risks between the cloud provider and the cloud user. For that reason, cloud adopters need to consider security at three levels:

- **System level:** This is about protecting system-level components such as operating systems, networks, virtual machines, management services, and containers. Examples are keeping systems current with the latest patches and updates.
- **Application-level:** This is primarily about identity and access management. Examples are policies such as multifactor authentication.
- **Data-level:** No cloud provider is responsibility for protecting data, but some may offer encryption as an option.

Multitenancy

Commingles the data and processing for multiple clients in a single application instance.

Network Security Groups

Groups of cloud instances that are managed by applying the same rules and policies.

North-South Traffic

Refers to traffic moving from end-users (clients) to an organization's internal resources, once contained in the data center and now likely a distributed ecosystem including data centers, as well as private and public clouds. This type of traffic is primarily composed of queries, commands, and specific data requests. Cisco estimates that 17% of enterprise network traffic is north-south.

Open Cloud

An open cloud is not owned by any vendor, but is created using software that is freely available from a public-facing repository and built using open application programming interfaces (APIs). Open clouds provide cloud users the right to move data out of the cloud as they wish, without having to pay access fees (sometimes referred to as backhauling). OpenStack is the most popular open cloud environment and is associated with a large community of developers. Some cloud providers may use open cloud software, but sell differentiated tools, enhancements, or support.

OpenStack

A free and open source cloud platform that has become a de facto standard for building clouds that are not dependent on any one cloud platform provider. OpenStack enhancements, services, support, and tools are widely available.

Pay-as-You-Go

Payment model where customers are charged only for the application or service capacity they really use. As distinguished from an earlier model where organizations purchased software to run on specific hardware platforms in their data centers, generally sized with some 'headroom' to handle increasing demand. The result was often extra capacity waiting to be used, or delays in getting new capacity configured to keep up with growth in demand.

Platform as a Service (PaaS)

A category of cloud computing services that provides users with a platform for developing, running, and managing applications without the complexity of integrating and maintaining the components normally required.

Private Cloud

A cloud infrastructure that is used exclusively by a single organization and may be owned, managed, and operated by the organization or a third party (or a combination of both) either on or off premises. Key private cloud technology providers are:

- **VMware:** Virtualization and cloud computing software provider operated as a subsidiary of Dell Technologies. VMware bases its virtualization technologies on its bare metal hypervisor ESX/ESXi in x86 architecture.
- **OpenStack:** Free and open-source software platform for deploying cloud computing, mostly infrastructure as a service (IaaS). The platform consists of interrelated components that control diverse, multi-vendor hardware pools of processing, storage, and networking resources throughout a data center.
- **Hyper-V:** A native hypervisor from Microsoft; it can create virtual machines on systems running Windows. Hyper-V can be configured to expose individual virtual machines to one or more networks.

Public Cloud

A cloud infrastructure that is used by multiple organizations (multitenant) and is owned, managed, and operated by a third party (or parties) on the cloud provider's premises. Popular providers include:

- AWS—Amazon Web Services
- Microsoft Azure
- Google Cloud
- IBM Cloud

Resilient Security

As cyberattacks evolve and become better at avoiding detection, it is not a question of "if" but "when" your network will be attacked. The concept of resilient security refers to how quickly your architecture and team can identify and contain an attack or breach. While security prevention still needs to be maintained, there has to be equal, if not greater, effort placed on recovering the network and limiting the damage. Learn more in the white paper: Best Practices for Security Resilience.

Rightsize

The concept of modifying your cloud infrastructure to match actual demand. The on-demand nature of cloud computing allows companies to save money by eliminating over-provisioning to handle surges in demand.

Sensors

Containerized, Docker-based software that sits within the source instances that are to be monitored. Sensors and connectors, which sit within instances, are how CloudLens accesses metadata.

Service-Oriented Architecture (SOA)

Software design in which modular Web services are leveraged across a network to provide various application components. SOA enables businesses to improve agility and time-to-market (TTM) and is, thus, well-suited for cloud computing applications.

Shadow IT

Infrastructure services within an organization that are not supported by the central IT department. Cloud computing has dramatically increased shadow IT, which can introduce security risks when governance policies and rules are not applied.

Software Agent

A persistent, goal-oriented computer program that reacts to its environment and runs without continuous direct supervision to perform some function for an end user or another program. CloudLens sensors and connectors are technically agents that are containerized.

Software as a Service (SaaS)

A software licensing and delivery model in which access to software is provided on a subscription basis and is delivered over the internet. Maintenance and upgrades are commonly managed by the provider. Examples include e-mail, customer relationship management (CRM), virtual desktops, and gaming.

Security Operations Center (SOC) or Information Security Operations Center(ISOC)

A centralized unit that deals with the people, processes, and technologies to handle the detection, containment, and remediation of IT threats. An SOC monitors applications to identify possible cyberattacks or intrusions and will manage any potential impact to the business.

Software-Defined Everything (SDx)

Extension of virtualization that abstracts an application or function from its underlying hardware, separating the control and data planes and adding programmability. Beginning with software-defined networking (SDN), SDx now encompasses software-defined storage (SDS), software-defined computing, software-defined security, and software-defined data centers (SDDC), among others.

Subscription-Based Pricing Model

Pricing model that lets customers pay a fee to use the service for a particular time period, often used for SaaS services—also called a consumption-based pricing model.

Vendor Lock-In

Dependency on a specific cloud vendor and difficulty moving from one cloud vendor to another due to lack of standardized protocols, application program interfaces (APIs), data structures, and service models.

Vertical Scale

Ability to increase the capacity of existing hardware or software by adding resources. Vertical scaling is limited by the fact that you can only get as big as the size of the server. Traditionally, this is all that is available with hardware or on-premise solutions.

Virtual Local Area Network (VLAN)

Network of computers that behave as if they are connected to the same wire even though they may be physically located on different segments of a local area network (LAN). VLANs areconfigured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Virtual Machine (VM)

Software-based server that, like a physical server, runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by the physical resources of a host.

Virtual Network Traffic

East-west and north-south traffic in a virtual network. A virtual network is made up of a virtualized network interface controller (NIC) and virtualized local area network (LAN). It consists of one or more virtual machines that can send data to and receive data from one another.

Virtual Switch (vSwitch)

Software application that allows communication between virtual machines. A vSwitch does more than just forward data packets; it intelligently directs the communication on a network by checking data packets before moving them to a destination.

Visibility-as-a-Service (VaaS)

Enables IT organizations to access network traffic across their entire infrastructure on demand, whether it resides in a public or private cloud, branch office, campus, or data center.

vMotion

Developed by VMware, it enables the live migration of running virtual machines from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity.

Learn more at: www.ixiacom.com

For more information on Ixia products, applications or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info