Cloud Center
of Excellence

Cloud Dictionary

DRAFT
9.5.2017

Dictionary of Cloud Computing Terms

Introduction

This document serves as a source for terms and definitions of cloud computing. It gathers material from the NIST Cloud Computing Reference Architecture (NIST SP 500-292), The USG Cloud Computing Technology Roadmap (NIST SP 500-293), and The NIST Definition of Cloud Computing (NIST SP 800-145). It also includes a section on typical cloud services.

Federal Cloud Computing and Related Terms and Definitions

Term	Definition	Source
Autoscaling	A method used in cloud computing, whereby the amount of computational resources in a server farm, typically measured in terms of the number of active servers, scales automatically based on the load on the farm.	
Cloud Access	To make contact with or gain access to Cloud Services.	NIST SP 500-292
Certification and Accreditation (C&A)	A four-phase process to certify a federal information system is compliant with mandated federal controls. Each phase must be completed before the next one begins. • Initiation and Planning • Certification • Accreditation • Continuous Monitoring	See NIST SP 800-37 - *Guide for the Security Certification and Accreditation of Federal Information Systems*
Capital Expenditure (CapEx)	Funds used by a company to acquire or upgrade physical assets such as property, industrial buildings or equipment. It is often used to undertake new projects or investments by the firm. This type of outlay is also made by companies to maintain or increase the scope of their operations. These expenditures can include everything from repairing a roof to building, to purchasing a piece of equipment, or building a brand-new factory.	http://www.investopedia.com/
Cloud Access Security Broker (CASB)	Cloud access security brokers (CASBs) are tools or services that enforce an organization's security policies in a public cloud environment.	whatis.com
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.	NIST SP 500-292
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.	NIST SP 500-292
Cloud Carrier	The intermediary that provides connectivity and transport of cloud services between Cloud Providers and Cloud Consumers.	NIST SP 500-292
Cloud Consumer	Person or organization that maintains a business relationship	NIST SP 500-

Term	Definition	Source
	with, and uses service from, Cloud Service Providers.	292
Cloud Distribution	The process of transporting cloud data between Cloud Providers and Cloud Consumers.	NIST SP 500-292
Cloud Provider (AKA Cloud Service Provider or CSP)	Person, organization or entity responsible for making a service available to service consumers.	NIST SP 500-292
Cloud Service Management	Cloud Service Management includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers.	NIST SP 500-292
Community Cloud	The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and NIST SP 500–292 NIST Cloud Computing Reference Architecture compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.	NIST SP 800-145
Content Delivery Network (CDN)	A system of distributed servers (network) that deliver webpages and other Web content to a user based on the geographic locations of the user, the origin of the webpage and a content delivery server.	
Data Portability	The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.	Federal Standard 1037C
DevOps	A software development and delivery process that emphasizes communication and collaboration between product management, software development, and operations professionals. It seeks to automate the process of software integration, testing, deployment, and infrastructure changes by establishing a culture and environment where building, testing, and releasing software can happen rapidly, frequently, and more reliably.	
Elasticity	A feature where physical or virtual resources can be adjusted, in some cases automatically, to quickly increase or decrease resources.	NIST SP 800-145
The Federal Risk and Authorization Management Program	A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.	www.fedramp.gov

Term	Definition	Source
Fixed Endpoints	A physical device, fixed in its location that provided a man/machine interface to cloud services and applications. A fixed endpoint typically uses one method and protocol to connect to cloud services and apps.	NIST SP 500-292
Fog Computing	A system-level horizontal architecture that distributes resources and services of computing, storage, control and networking anywhere along the continuum from Cloud to Things.	https://www.openfogconsortium.org/resources/#definition-of-fog-computing
Hybrid Cloud	The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).	NIST SP 800-145
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).	NIST SP 800-145
Infrastructure as Code	The process of managing and provisioning computer data centers through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.	
Internet of Things (IoT)	The Internet of Things (IoT) refers to the technologies and devices that sense information and communicate it to the Internet or other networks and, in some cases, act on that information.	https://www.gao.gov/assets/690/684590.pdf
Interoperability	The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions.	American National Standard Dictionary of Information Technology (ANSDIT)]
Metering	Provide a measuring capability at some level of abstraction appropriate to the type of service (e.g, storage, processing, bandwidth, and active user accounts).	NIST SP 500-292
Microservices	An approach to application development in which a large application is built as a suite of modular services. Each module supports a specific business goal and uses a simple, well-defined interface to communicate with other sets of services.	
Mobile Endpoints	A physical device, often carried by the user that provided a man/machine interface to cloud services and applications. A	?

Term	Definition	Source
	Mobile Endpoint may use multiple methods and protocols to connect to cloud services and applications.	
Monitoring and Reporting	Discover and monitor the virtual resources, monitor cloud operations and events, and generate performance reports.	?
Multi-tenancy	A feature where physical or virtual resources are allocated in such a way that serves multiple customers and their computations and data are isolated from and inaccessible to one another.	NIST SP 800-145
Operating Expense (OpEx)	An operating expense is an expense a business incurs through its normal business operations. Often abbreviated as OPEX, operating expenses include rent, equipment, inventory costs, marketing, payroll, insurance and funds allocated toward research and development. One of the typical responsibilities that management must contend with is determining how low operating expenses can be reduced without significantly affecting a firm's ability to compete with its competitors.	http://www.investopedia.com
Performance Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria.	NIST SP 500-292
Physical Resource Layer	Includes all the physical resources used to provide cloud services, most notably, the hardware and the facility.	NIST SP 500-292
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.	NIST SP 800-145
Portability	1. The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. 2. The ability of software or of a system to run on more than one type or size of computer under more than one operating system. See POSIX. 3. Of equipment, the quality of being able to function normally while being conveyed.	Federal Standard 1037C
Privacy	Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) throughout its life cycle.	Adapted from OASIS
Privacy-Impact Assessment (PIA)	Structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system.	NIST SP 800-122
Private Cloud	The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. (Source: NIST CC Definition)	NIST SP 800-145
Provisioning/Configuration	process of preparing and equipping a cloud to allow it to provide (new) services to its users	NIST SP 800-145
Public Cloud	The cloud infrastructure is made available to the general public or	NIST SP 800-

Term	Definition	Source
	a large industry group and is owned by an organization selling cloud services. (Source: NIST CC Definition)	145
Rapid provisioning	Automatically deploying cloud system based on the requested service/resources/capabilities	NIST SP 800-145
Resource Abstraction and Control Layer	Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established.	NIST SP 500–292
Resource change	Adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud.	?
Security	Refers to information security. „information security‟ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (C) availability, which means ensuring timely and reliable access to and use of information.	Title III of the E-Government Act, entitled the Federal Information Security Management Act of 2002 (FISMA)
Security Audit	Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria.	
Service Aggregation	A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.	NIST SP 500-292
Service Arbitrage	Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated aren't fixed. Indeed the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator, e.g., providing multiple email services through one service provider or providing a credit–scoring service that checks multiple scoring agencies and selects the best score.	NIST SP 500-292
Service Consumption	A Cloud Consumer in the act of using a Cloud Service.	?
Service Deployment	The activities and organization needed to make a cloud service available.	?
Service Intermediation	An intermediation broker provides a service that directly enhances a given service delivered to one or more service consumers, essentially adding value on top of a given service to enhance some specific capability.	NIST SP 500-292
Service Interoperability	The capability to communicate, execute programs, or transfer data among various cloud services under specified conditions.	Modified from American National

Term	Definition	Source
		Standard Dictionary of Information Technology (ANSDIT)
Service Layer	The middle layer between the user and the data store. In cloud computing, there are 3 service layers – SaaS, PaaS & IaaS	NIST SP 500-292
Service Orchestration	Refers to the arrangement, coordination and management of cloud infrastructure to provide different cloud services to meet IT and business requirements.	NIST SP 500-292
Service Provision	A Cloud Provider or Cloud Broker in the act of providing a Cloud Service.	NIST SP 500-292
Service Level Agreement (SLA)	Documented agreement between the service provider and customer that identifies services and service targets.	NIST SP 500-293
SLA management	Encompasses the SLA contract definition (basic schema with the quality of service parameters), SLA monitoring, and SLA enforcement, according to the defined policies.	NIST SP 500-292
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various clients and devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.	NIST SP 800-145
Software Defined Network (SDN)	The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices.	https://www.opennetworking.org/sdn-resources/sdn-definition
System Portability	The ability of a service to run on more than one type or size of cloud.	Modified from Federal Standard 1037C
Third Party Assessment Organization (3PAO)	An organization that has been certified to help cloud service providers and government agencies meet FedRAMP compliance regulations. Under FedRAMP, CSP authorization packages must include an assessment by an accredited 3PAO to ensure a consistent assessment process. Accredited 3PAOs perform initial and periodic assessment of CSP systems per FedRAMP requirements, provide evidence of compliance, and play an on-going role in ensuring that CSPs meet requirements.	www.fedramp.gov
Trusted Internet Connection (TIC)	Outlined in OMB Memorandum M-08-05, is to optimize and standardize the security of individual external network connections currently in use by federal agencies, including	https://www.dhs.gov/trusted-internet-

Term	Definition	Source
	connections to the Internet. The initiative will improve the federal government's security posture and incident response capability through the reduction and consolidation of external connections and provide enhanced monitoring and situational awareness of external network connections. The goals are: • Reduce and consolidate external access points across the federal enterprise, • Manage the security requirements for Network and Security Operations Centers (NOC/SOC), Establish a compliance program to monitor department and agency adherence to TIC policy	connections
Web Application Firewall (WAF)	Filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while regular firewalls serve as a safety gate between servers. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS) and security misconfigurations.	

Examples of Cloud Services

These tables are meant to provide a small representation of available cloud services. They are not exhaustive.

SaaS Services

Email and Office Productivity	Applications for email, word processing, spreadsheets, presentations, etc.
Billing	Application services to manage customer billing based on usage and subscriptions of products and services.
Customer Relationship Management (CRM)	CRM applications that range from call center applications to sales force automation.
Collaboration	Tools that allow users to collaborate in workgroups, within enterprises, and across enterprises.
Content Management	Services for managing the production of and access to content for web-based applications.
Document Management	Applications for managing documents, enforcing document production workflows, and providing workspaces for groups or enterprises to find and access documents.
Financials	Applications for managing financial processes ranging from expense processing and invoicing to tax management.
Human Resources	Software for managing human resources functions within companies.
Sales	Applications that are specifically designed for sales functions such as pricing, commission tracking, etc.
Social Networks	Social software that establishes and maintains a connection among users that are tied in one or more specific types of interdependency.
Enterprise Resource Planning (ERP)	Integrated computer-based system used to manage internal and external resources, including tangible assets, financial resources, materials, and human resources.

PaaS Services

Business Intelligence	Platforms for the creation of applications such as dashboards, reporting systems, and data analysis.
Database	Services offering scalable relational database solutions or scalable non-SQL datastores.
Development and Testing	Platforms for the development and testing cycles of application development, which expand and contract as needed.
Integration	Development platforms for building integration applications in the cloud and within the enterprise.
Application Deployment	Platforms suited for general purpose application development. These services provide databases, web application runtime

	environments, etc.

IaaS Services

Backup and Recovery	Services for backup and recovery of file systems and raw data stores on servers and desktop systems.
Compute	Server resources for running cloud-based systems that can be dynamically provisioned and configured as needed.
Content Delivery Networks (CDNs)	CDNs store content and files to improve the performance and cost of delivering content for web-based systems.
Services Management	Services that manage cloud infrastructure platforms. These tools often provide features that cloud providers do not provide or specialize in managing certain application technologies.
Storage	Massively scalable storage capacity that can be used for applications, backups, archival, and file storage.

Appendix C: Acronyms	
CDN	Content Delivery Networks
CIO	Chief Information Officer
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
HVAC	Heating, Ventilation and Air Conditioning
IaaS	Cloud Infrastructure as A Service
IT	Information Technology
MID	Mobile Internet Devices
NIST	National Institute of Standards and Technology
OS	Operating System
QoS	Quality of Service
SaaS	Cloud Software As A Service
SAJACC	Standards Acceleration to Jumpstart the Adoption of Cloud Computing
SDO	Standards Development Organization
SLA	Service Level Agreement
PaaS	Cloud Platform As A Service
PI	Personal Information
PII	Personally Identifiable Information
USG	US Government