The nist definition of cloud computing

Technology

Special Publication 800-145 (Draft) The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards andTechnologyPeter Mell Timothy Grance NIST Special Publication 800-145 (Draft) The NIST Definition of Cloud Computing (Draft) Recommendations of the National Institute of Standards and Technology Peter Mell Timothy Grance C O M P U T E R S E C U R I T Y Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 January 2011 U. S. Department of Commerce

Gary Locke, Secretary National Institute of Standards and Technology Dr. Patrick D. Gallagher, Director Reports on Computer Systems Technology The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U. S. economy and public welfare by providing technicalleadershipfor the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology.

ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, andacademicorganizations.

National Institute of Standards and Technology Special Publication 800-145 (Draft) 7 pages (January. 2011) Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose. ii Acknowledgements

The authors Peter Mell and Timothy Grance of the National Institute of Standards and Technology (NIST) would like to thank the many experts in industry and government who contributed their thoughts to the creation and review of this definition. We especially acknowledge Murugiah Souppaya and Lee Badger, also of NIST, whose advice and technical insight assisted this effort. Additional acknowledgements will be added upon the final publication of this guideline. iii 1. 1. 1 Introduction Authority The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal

Information Security Management Act (FISMA) of 2002, Public Law 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), " Securing Agency Information Systems," as analyzed in A-

130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. 1. 2 Purpose and Scope

The purpose of this publication is to provide the NIST definition of cloud computing. NIST intends this informal definition to enhance and inform the public debate on cloud computing. Cloud computing is still an evolving paradigm. Its definition, use cases, underlying technologies, issues, risks, and benefits will be refined and better understood with a spirited debate by the public and private sectors. This definition, its attributes, characteristics, and underlying rationale will evolve over time. 1. 3 Audience The intended audience is people adopting the cloud computing model or providing cloud services. 2. The NIST Definition of Cloud Computing Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g. , networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential

characteristics, three service models, and four deployment models. Essential Characteristics: On-demand self-service.

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider. Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e. g. , mobile phones, laptops, and PDAs). Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e. g. , country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in.

To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e. g. , storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported,

providing transparency for both the provider and consumer of the utilized service.

Service Models: Cloud 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 client 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.

Cloud 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 hostingenvironmentconfigurations. 1 Typically through a pay-per-use business model. Cloud 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).

Deployment Models: 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. 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 compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. 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). 3