SoftLayer Technologies, Inc.
Infrastructure as a Service (IaaS)

Report on SoftLayer Technologies, Inc.'s Description of its Infrastructure as a Service (IaaS) System
and on the Suitability of the Design and Operating Effectiveness of
Controls Relevant to the Security and Availability Principles

For the period November 1, 2015 to April 30, 2016

Prepared in Accordance with:
AT 101 pursuant to *TSP Section 100A: Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*)

SoftLayer Technolgies, Inc.
Infrastructure as a Service (IaaS) System
AT 101 Report Relevant to the Security and Availability Principles (SOC 3)
For the period November 1, 2015 to April 30, 2016

Table of Contents

pwc

Report of Independent Service Auditors

To the Management of SoftLayer Technologies, Inc.:

We have examined management's assertion that SoftLayer Technologies, Inc. (the "Company"), during the period November 1, 2015 to April 30, 2016, maintained effective controls over the Infrastructure as a Service (IaaS) system that were suitably designed and operating effectively to provide reasonable assurance that:

- the system was protected against unauthorized access, use, or modification; and
- the system was available for operation and use as committed or agreed,

based on the criteria to meet the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) ("applicable trust services criteria"). The Company's management is responsible for the assertion. Our responsibility is to express an opinion on the assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and, accordingly, included (1) obtaining an understanding of the controls over the security and availability of the Infrastructure as a Service (IaaS) system, (2) testing and evaluating the operating effectiveness of the controls, and (3) examining, on a test basis, evidence supporting management's assertion and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, SoftLayer Technologies Inc.'s management assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

PricewaterhouseCoopers LLP

August 11, 2016

SOFTLAYER

SoftLayer Technologies, Inc.
14001 North Dallas Parkway,
Suite M100
Dallas, Texas 75240

Management of SoftLayer Technologies, Inc.'s Assertion Regarding its Infrastructure as a Service (IaaS) System throughout the Period November 1, 2015 to April 30, 2016

We confirm, to the best of our knowledge and belief, that during the period November 1, 2015 to April 30, 2016, SoftLayer Technologies, Inc. maintained effective controls over its Infrastructure as a Service (IaaS) system that were suitably designed and operating effectively to provide reasonable assurance that:

- the system was protected against unauthorized access, use, or modification; and
- the system was available for operation and use as committed or agreed,

based on the criteria to meet the security and availability principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Principles and Criteria*) ("applicable trust services criteria").

Our attached description of our Infrastructure as a Service (IaaS) system throughout the period November 1, 2015 to April 30, 2016, identifies the aspects of the Infrastructure as a Service (IaaS) system covered by our assertion.

III. SoftLayer Technologies, Inc.'s Description of its Infrastructure as a Service (IaaS) System throughout the period November 1, 2015 to April 30, 2016

A. System Overview

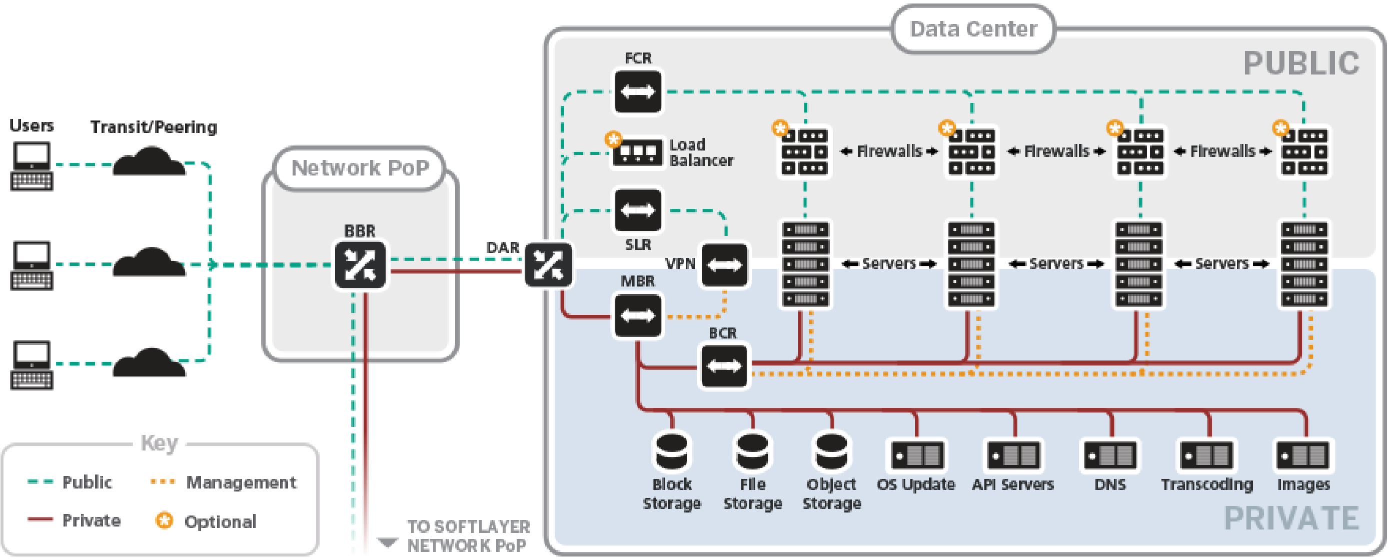
Background

SoftLayer Technologies, Inc., also referred to as "IBM SoftLayer" or "SoftLayer," an IBM Company, provides on-demand cloud infrastructure as a service (IaaS) to its customers, allowing them to create scalable bare metal server, virtual server, or hybrid computing environments, via SoftLayer's Customer Portal, leveraging global data centers and points of presence (PoP).

SoftLayer's IaaS is built using a Network-Within-A-Network topology that provides remote access to allow customers the ability to build and manage computing environments remotely. SoftLayer's "Network-Within-A-Network" configuration includes three (3) network interfaces. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management functions.

- Public Network - Network traffic from anywhere in the world will connect to the closest network PoP, and it will travel directly across the network to its data center, minimizing the number of network hops and handoffs between providers.
- Private Network - Provides a connection to the customer's servers (bare metal or virtual) in SoftLayer data centers around the world. Data can be moved between servers through the private network; and customers can utilize various services, update and patch servers, software repositories, and backend services, without interfering with public network traffic.
- Management Network - Each server within the SoftLayer IaaS is connected to the management network. This out-of-band management network, accessible via VPN, allows access to each server for maintenance and administration, independent of its CPU and regardless of its firmware or operating system.

Public, Private and Management Network Diagram:



SoftLayer delivers its IaaS through the Internal Management System (IMS) customer relationship management (CRM) system, which is an internally developed customer relationship management system used to track customers' hardware and services. IMS allows customers to manage their cloud environments. Customer capabilities include management of system and network devices provisioned by the customer, account management, ordering and deployment, and customer support.

IMS has two components: IMS, as viewed by internal employees, and the Customer Portal, as available to users of SoftLayer's IaaS. The Customer Portal allows customers to:

- Create and manage tickets for incident response and resolution
- Review account information
- View information and certain configuration data regarding their purchased solutions
- Perform functions such as OS reloads, and access RescueLayer
- Maintain customer provisioned firewall and DNS configurations that affect their bare metal servers
- Purchase or upgrade services to initiate the automated provisioning process for new systems

Customers build their environments using virtual servers and/or bare metal servers.

- Virtual servers are computing "instances" that are complete computing environments that include a full hardware and software stack accessed and controlled over the Internet. The computing resources can be scaled on demand, adding or resizing instances as needed, but without having to purchase physical systems. Public and private virtual nodes are available.
- Bare metal servers are dedicated physical servers. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.

SoftLayer personnel also have access to IMS to set up and configure purchased solutions, assist in troubleshooting technical issues, and respond to customer requests.

Boundaries of the System

This report covers the services managed by SoftLayer, including global data center physical locations, the IMS portal and the supporting infrastructure devices. Additionally, this report includes network devices that are managed by SoftLayer supporting the IMS portal and infrastructure, and network devices that support customer environments but are not provisioned/managed by customers within the SoftLayer IaaS. The report includes supporting services to the virtual and bare metal services, such as storage. These devices can either be locally attached or accessible via a storage area network. The Storage Area Network (SAN) is architecture to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached. Within each customer environment, servers, VMs and other systems/devices are managed by SoftLayer's customers and are not included within the boundaries of the system. This report does not extend to the workloads (data, files, information) sent by SoftLayer IaaS customers to the SoftLayer IaaS system. The integrity and conformity with regulatory requirements of such data are solely the responsibility of the applicable SoftLayer IaaS customer. Additionally, this report does not extend to business process controls, automated application controls, or key reports.

The accompanying description includes only those controls directly impacting SoftLayer's IaaS and customers' hosting environments utilizing SoftLayer's IaaS, and does not include controls over other services. SoftLayer also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by SoftLayer include, but are not limited to, load balancing, intrusion detection and prevention, standard and dedicated hardware firewalls, anti-virus, anti-spyware, anti-malware, VeriSign® and GeoTrust® SSL Certificates. This report does not extend to controls over SoftLayer's other services and tools.

Components, infrastructure, network devices, software, and data center location system boundaries:

Service Offering	Data Center / Hardware Locations	Network	Operating System Infrastructure	System Software	Applications	Customer Data
IBM SoftLayer	29 data centers (See Infrastructure section below)	Customer provisioned and managed network devices, firewalls and VPNs are solely the responsibility of the customer and are not within the boundaries of the system.	Customer environments (including the development and maintenance) provisioned and managed using the Customer Portal, including OS, system software, and applications are solely the responsibility of the customer and are not within the boundaries of the system.			Customer data is solely the responsibility of the customer and is not within the boundaries of the system.
		Network devices supporting customer managed environments and managed by SoftLayer are within boundaries of the system including: Routers, Switches, Firewalls, VPNs				
		Network devices directly in support of the IMS portal are within the boundaries of the system including: Routers, Switches, Firewalls, VPNs	Operating systems directly in support of the IMS portal are within boundaries of the system including: Linux, UNIX, Windows, CentOS	System software directly in support of the IMS portal are within boundaries of the system including: Radius, Citrix, Active Directory	Internal Management System (IMS)/ Customer Portal	

B. System Components

Infrastructure

SoftLayer provides the Infrastructure as a Service (IaaS) system using 29 locations, as of November 1, 2015, and uses multiple telecom service providers for backbone connectivity and multiple co-location management providers for data center facility management. Refer to the table below for a list of data center vendors that provide facility management services in the SoftLayer facilities included within the boundaries of the system.

Facility	Physical Location	Facility Manager
AMS01	Amsterdam, Netherlands	Digital Realty
AMS03	Almere, Netherlands	KPN
DAL01	Dallas, TX	ViaWest
DAL02	Dallas, TX	SoftLayer
DAL05	Dallas, TX	Digital Realty
DAL06	Dallas, TX	SoftLayer
DAL07	Plano, TX	SoftLayer
DAL08	Richardson, TX	Digital Realty
DAL09	Richardson, TX	Digital Realty
FRA02	Frankfurt, Germany	Zenium Technology
HKG02	Hong Kong, China	Digital Realty
HOU02	Houston, TX	SoftLayer
LON02	Chessington, London	Digital Realty
MEL01	Melbourne, Australia	Digital Realty
MEX01	Queretaro, Mexico	Alestra
MIL01	Milan, Italy	DATA4
MON01	Montreal, Canada	COLO-D

Facility	Physical Location	Facility Manager
PAR01	Paris, France	Global Switch
SAO01	Sao Paulo, Brazil	Ascenty
SEA01	Tukwila, WA	Internap
SJC01	Santa Clara, CA	Digital Realty
SJC03	Santa Clara, CA	Digital Realty
SNG01	Singapore	Digital Realty
SYD01	Sydney, Australia	Global Switch
TOK02	Tokyo, Japan	@Tokyo
TOR01	Ontario (Markham), Canada	Digital Realty
WDC01	Chantilly, VA	Digital Realty
WDC03	Ashburn, VA	Digital Realty
WDC04	Ashburn, VA	Digital Realty

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities (i.e., DAL02, DAL07 and HOU02) house both co-location servers and Infrastructure as a Service (IaaS) related servers. Co-location customers do not have logical or physical access to the SoftLayer Infrastructure as a Service (IaaS) system. As such, co-location cages housing customer's servers are not included within the boundaries of the system.

Software

SoftLayer IaaS customers are solely responsible for customer owned and managed software and applications as these components are not within the boundaries of the system. SoftLayer IaaS does not maintain responsibility for customer software and applications that SoftLayer IaaS customers run on their bare metal, virtual, or hybrid environment; the software and applications are the responsibility of SoftLayer IaaS customers.

For components of the environment managed by SoftLayer IaaS, software systems are managed centrally by SoftLayer using consistent controls and processes. SoftLayer manages the Customer Portal (IMS), IMS infrastructure and operating systems, network devices supporting IMS and certain network devices supporting customer environments within the SoftLayer environment.

People

Key SoftLayer positions of authority and responsibility are documented in a formal organizational chart via IBM's BluePages, which evidences key organizational structures and reporting lines. The organizational chart is reviewed by HR and updated periodically for accuracy by managers.

Within the organization, roles and responsibilities are defined and communicated. SoftLayer leverages participation from multiple organizational levels, sites, locations, geographies and organizations are involved, as required, to perform the day-to-day oversight of service delivery related functions, matters, responsibilities and issues. Functional roles may be combined within management positions to deliver services in a cost effective manner.

The SoftLayer IaaS teams are diverse teams of development and operations professionals, which maintain and follow IBM's industry leading processes, standards and procedures in the execution of their work. Security and availability requirements are generated from senior management. These requirements are distributed to the operational management leaders. These leaders are responsible for the implementation and monitoring of security controls. The IBM General Manager, Cloud Services (GM) leads SoftLayer. The GM of Cloud Services for SoftLayer reports to the Senior Vice President of IBM Cloud.

The SoftLayer Chief Operating Officer oversees daily operations. Supporting the Chief Operating Officer are Senior Executives and Vice Presidents that manage and perform the daily operations of SoftLayer. These core competencies have been established to provide full capabilities to serve customers worldwide. Functional and administrative responsibilities are broadly defined and communicated through organizational charts, which are reviewed and updated regularly. The Vice Presidents guide the management of the business units.

Procedures

Customers are provided and required to agree to a Master Service Agreement (MSA) during the ordering process. The MSA acts as the formal contract and usage policy for customer users of the SoftLayer IaaS system. The MSA documents the contractual obligations of SoftLayer and the customers using SoftLayer IaaS. Any updates to the MSA are communicated to the existing customers through the Customer Portal.

The policies and procedures are a series of documents, which are used to describe the controls implemented within the SoftLayer IaaS system. The purpose of the policies and procedures is to describe the environment and define the practices performed on behalf of the customer. The policies and procedures include diagrams and descriptions of the network, infrastructure, environment and SoftLayer's commitments. These policies and procedures are available to all SoftLayer employees that support the SoftLayer IaaS system. Additionally, each of the policies and procedures are reviewed by SoftLayer management on a periodic basis, per the defined policy.

Data

The integrity and conformity with regulatory requirements of workloads sent to the SoftLayer IaaS system are solely the responsibility of SoftLayer IaaS customers. SoftLayer IaaS does not maintain responsibility for the data SoftLayer IaaS customers store on their bare metal, virtual, or hybrid environment. The data is the responsibility of SoftLayer IaaS customers.