NTT DATA Service Description

NTT DATA Cloud on Demand with Six Degrees Group

Introduction

NTT DATA Cloud On Demand (the “Service”) is an infrastructure as a service (“IaaS”) offering designed to extend an existing internal VMware implementation into a secure private cloud environment or as a stand-alone secure hosted public cloud solution. This Service Description and the attached appendices (collectively, the “Service Description”) describe the Service being provided by Six Degrees Group (“6DG”).

Offer Description

Service Tiers

6DG will offer 3 tiers of Service based on VMware vCloud Director: Pay-as-You-Go (“PAYGO”), Reserved Capacity (“Reserved”) and Dedicated Capacity (“Dedicated”). Customers will designate the desired amount of virtual CPUs (“vCPU”) and virtual RAM (“vRAM”) for their desired implementation. A maximum ratio of 4GB of vRAM per vCPU will be enforced across the entire pool of capacity (e.g., a Reserved capacity of 100 vCPUs can have a maximum of 400GB of vRAM). See Table 1 for a summary of the offering and billing metrics.

- **PAYGO** is a multi-tenant service that enables a customer to place VMware vSphere workloads on NTT DATA’s cloud on a month-by-month basis. Customers are committed for only one month at a time with most fees charged on an hourly basis (when virtual machines (“VMs”) are “powered-on”). Capacity is on a first-come-first-served basis and is not guaranteed.
- **Reserved** is a multi-tenant service whereby a customer can ask NTT DATA to set aside a fixed amount of cloud capacity for their use. The minimum commitment for this level of service is one year. Additional networking, storage, and security options are available.
- **Dedicated** is a single-tenant service whereby a customer occupies entire servers for their Service environment. Server capacity is purchased in increments of 1 server, with a minimum order of 2 servers. Storage and networking are shared with the other servers in NTT DATA’s cloud. The minimum commitment for this level of service is one year. Additional networking, storage, and security options are available.

Billing for each tier is done on a monthly basis in advance or in arrears, as specified in the Order Form, and will include both fixed and variable costs.

No hardware or software is being transferred, sold, leased or licensed to Customer under this Service Description. To the extent 6DG uses hardware or software as part of its delivery of the Service, such hardware or software will be licensed, owned or otherwise held by 6DG.

Table 1: Product Offering with Billing Metrics

Description		PAYGO	Reserved	Dedicated
vCPU	vCPU (~1 Core @ 1 GHz)	Hourly	Monthly	N/A
RAM	vRAM (GB)	Hourly	Monthly	N/A
Dedicated Server	Per Server	N/A	N/A	Monthly
Storage	Basic Storage (GB) (where available)	Monthly	Monthly	Monthly
	High Performance Storage (GB)	Monthly	Monthly	Monthly
	Backup and Recovery (GB of source VM)	Per GB		
	Trend Micro SecureCloud™ Storage Encryption (key for each encrypted volume)	Per Key		
Software	Customer-supplied OS image	No Charge	No Charge	No Charge
	SUSE Linux	No Charge	No Charge	No Charge
	Windows Server 2003/2008 license (included in VM template)	No Charge	No Charge	No Charge
Network	Multi-Protocol Label Switching (MPLS) bandwidth	Per MB per second	Per MB per second	Per MB per second
	Static IP addresses (minimum quantity = 2)	No Charge	No Charge	No Charge
	VMware vShield™ Edge (per VM)	No Charge	No Charge	No Charge
	F5 Load Balancer - LTM Virtual Edition	200MB/1Gb	200MB/1Gb	200MB/1Gb

Guest Operating Systems

Customers may use one of 6DG's operating system ("OS") templates or import their own OS image. The current list of VMware vSphere supported guest operating systems can be found here: http://www.vmware.com/pdf/GuestOS_guide.pdf. Customer is responsible for obtaining software license rights for any software used in connection with the Service.

Table 2: Guest Operating System Templates

Guest Operating System Template	32-bit x86	64-bit x64
SUSE Linux Enterprise Server 11 (SP1)	●	●
Windows Server 2003, Datacenter Edition (SP2)	●	●
Windows Server 2008 R2, Datacenter Edition (SP1)		●

Networking

The networking portion of this Service consists of physical and virtual components. Customer may be charged for data leaving 6DG's datacenter going to the Internet. Data bandwidth in and data between VMs in the same datacenter will not be charged. 6DG is responsible for operating, maintaining, and troubleshooting all physical network components residing in 6DG datacenters. Customer is responsible for operating, maintaining, and troubleshooting all virtual networking components created in its virtual environments. 6DG will provide Customers with a minimum of 2 static IP addresses.

Optional Network Features:

VMware vShield Edge provides perimeter security and network services such as DHCP, NAT, and VPN service. vShield Edge is a virtual firewall appliance that can be provisioned on-demand and its services enabled on-demand to meet the flexibility requirement of cloud deployments. Implementing this service is optional; there is no additional charge for use of this software. Please consult the vShield Edge Design Guide for more information.

F5 Local Traffic Manager (LTM) Virtual Edition – Load Balancer is optionally available for customers requiring application connections persistence. The virtual edition provides functionality similar to that provided by the hardware version of the BIG-IP LTM appliance, including comprehensive load-balancing, in-band server health monitoring, device service clustering, security, as well as iRules and iControl for customization. This service is available at additional cost for two rates: 200 Megabits per second (Mbps) and/or 1 Gigabit per second (Gbps). 6DG support will assist Customers in loading the virtual appliance and load-balancing two virtual machines. Capabilities beyond this can be installed with help from www.askf5.com or a 6DG consulting engagement and may be subject to additional cost.

6DG supports optional dedicated network connections from multiple telecommunications carriers based on Multi-Protocol Label Switching (MPLS). The minimum requirement for dedicated bandwidth is at least 2 megabits per second (Mbps). A 3-way agreement between Customer, 6DG, and the selected carrier must be executed prior to or concurrently with the execution of this Service Description. Customer is responsible for establishing network connectivity on its side.

Backup and Recovery

6DG will perform daily snapshots of all storage arrays and maintain copies for a rolling 7 day period; this is included in the standard offering at no additional charge. For an additional charge, an optional backup service is also available where 6DG will perform daily backups on a rolling 7 day schedule and retain weekly backups for a rolling 6 month period. Backup is done at a VM level (selection of individual files is not supported). Please consult Getting Started – NTT DATA Cloud On Demand for implementation details.

Optional Storage Encryption:

Customers may choose to protect storage data “at rest” with Trend Micro SecureCloud™ encryption (the “Encryption Service”). Each encryption key purchased from 6DG protects one logical disk (volume) of storage. If Customer elects to purchase the Encryption Service, 6DG will transfer certain Customer information (name and e-mail address of the applicable Customer contact authorized to receive the encryption key(s) and company name, city, state/province, and country) to Trend Micro, Incorporated or one of its affiliates (in Germany) (“Trend Micro”) that manages the encryption keys using a Key Management Portal in their datacenter. Once the Customer information is provided to Trend Micro, Trend Micro will e-mail Customer with instructions on how to obtain and use the encryption keys. Use of the encryption keys will require the download and installation of an operating system specific agent from Trend Micro. Customer must agree to Trend Micro's terms and conditions in order to receive Encryption Services. 6DG has no access to the encryption keys.

Onboarding Process

6DG's Provisioning and Onboarding Team will collaborate with designated Customer contacts to provide standardized onboarding of the Service. The standard onboarding Service will include:

- Following the date on which the related Order Form is executed by the Customer and accepted by NTT DATA ("Activation Date") an assigned 6DG representative will contact Customer to enable onboarding
- A phased project management process with defined project deliverables (kick off, provisioning, validation testing, training)
- An assigned 6DG Project Manager and Technical Consultant for the duration of the onboarding project
- Provisioning is considered complete when Customer is capable of accessing and operating the vCloud Director console
- Creation of and troubleshooting of one or more of the Customer's vCloud Organization virtual datacenters ("vDC")
- Enabling one vCloud Organization vDC administrator
- Working with Customer to set up any dedicated VPN links over the Internet or dedicated WAN links
- Providing Customer virtual access to its vCloud Organization vDC
- Providing Customer access to its 6DG Portal
- A 1 hour Customer walk-through training session on its vDC and Portal
- Transition to 6DG Support

Billing will begin at the conclusion of provisioning (the "Billing Start Date").

Support

Customer can identify up to 10 administrators to contact 6DG support via email, phone, or online chat. Administrators can be updated by the Customer at any time. Support may be provided outside of the country or region in which Customer or Customer's end users reside.

Customer Responsibilities

- Customer will support onboarding/provisioning activities set forth herein for the Service.
- Customer represents and warrants that it has or it will have prior to using the Service all licenses necessary in connection with all software and applications used for or with the Service.
- Customer will provide timely access to Customer resources, including but not limited to, virtualization administrators, and engineering and project management. 6DG and the Customer to agree on standard access protocols.

- The Customer is responsible for modifying and tracking changes to its environment
- Configuration/software/data backups. It is the Customer's responsibility to perform complete backups of all existing data, software, and programs. NOTWITHSTANDING ANYTHING CONTAINED HEREIN TO THE CONTRARY OR 6DG'S PERFORMANCE OF BASIC SNAPSHOT SERVICES OR BACKUP AND RECOVERY SERVICES, 6DG WILL HAVE NO LIABILITY FOR LOSS OR RECOVERY OF DATA OR PROGRAMS or loss of use of system(s) arising out of the Service or support or any act or omission, including negligence, by 6DG or a third-party service provider.
- Customer is responsible for all design and implementation of network security settings and requirements definition.
- If Customer purchases the optional MPLS Service a 3-way agreement between Customer,6DG, and the selected carrier must be executed prior to or concurrently with the execution of this Service Description. Customer is responsible for establishing network connectivity on its side.
- Customer is responsible for all application and performance monitoring.

6DG Support Responsibilities

- Assist Customer in identifying causes of issues experienced in Customer's virtual environment
- Assist in troubleshooting the Customer's vCloud Organization vDC
- Assist in troubleshooting the Customer's VMware vCloud vDC
- Support backup/recovery requests, which may include additional costs and be subject to a separate agreement
- Work with Customer to troubleshoot any dedicated VPN links over the Internet or dedicated WAN links
- Answer questions related to billing and invoices

Miscellaneous

6DG will provide security in connection with the Service in accordance with the Security Statement attached as Appendix B.

For the avoidance of doubt, the following activities are not included in the scope of this Service Description:

- Any services, tasks or activities other than those specifically noted in this Service Description
- The development of any intellectual property created solely and specifically for the Customer
- Virtualization design
- Evaluation of Customer's IT operations and organization
- Migration of any existing physical servers into a virtualized server environment
- Virtualization platform software licenses, and
- Application profiling, which includes identification of applications compatible with virtualization and analysis of server/application interdependencies

This Service Description does not confer on Customer any warranties which are in addition to the warranties provided under the terms of their master services agreement or Agreement, as applicable.

To the extent applicable, Customer agrees that 6DG's privacy and security requirements satisfy any and all obligations under the Family Educational Rights and Privacy Act, 20 USC 1232g, and its implementing regulations, 34 CFR pt. 99 (collectively, "FERPA") that 6DG may have as a recipient of education records and personally identifiable information contained in such records.

NTT DATA Services Terms & Conditions

Availability varies by country. To learn more, customers and 6DG Channel Partners should contact your sales representative for more information.

Appendix A

Service Level Agreement for NTT DATA Cloud On Demand

Once the Service has been provisioned, 6DG will use commercially reasonable efforts to achieve a Monthly Uptime Percentage of at least 99.95% (the “Cloud SLA”). If 6DG do not meet this Cloud SLA, and the Customer account with 6DG is current and not suspended, 6DG may be obligated to pay the Customer a credit.

Definitions:

- Downtime: The time during which Customer’s powered-on virtual machines not capable of being accessed or used by Customer, as determined by 6DG.
- Monthly Uptime Percentage: The total number of minutes in a month (43,800 minutes) minus the number of minutes of Downtime, the balance is then divided by the total number of minutes in the month.

Credits:

If 6DG does not meet the Cloud SLA for a particular month during the term, 6DG will, at Customer’s request, provide the applicable credit (“Credit”) set out below:

Monthly Uptime Percentage	Credit as a Percentage of Monthly Service Fees Billed
100% - 99.95%	0%
<99.95% - 99.50%	10%
<99.50% - 99.00%	25%
<99.00% - 98.00%	50%
<98.00% - 96.50%	75%
<96.50%	100%

The maximum Credit available is up to 100% of the Monthly Service Fees for the month of the occurrence. Credits will be applied to fees due for the Service, and will not be paid as a refund. All claims for Credit are subject to review and verification by 6DG, and all Credits will be based on 6DG’s measurement of its performance of the Service and will be final. Customer’s sole and exclusive remedy, and 6DG’s sole liability, with respect to 6DG’s inability to meet any Cloud SLA are the Credits described above. In order to be eligible to receive Credits, customers using the PAYGO Service must have their virtual machines powered on for the entire month.

Claims Process:

To receive a Credit, Customer must make a claim alleging 6DG’s failure to achieve the Cloud SLA within 30 days of the last date of the reported Downtime. The claim must be sent by e-mail to noc@6dg.co.uk and include: Customer name and account number, the name of the service to which the claim relates, a contact name, e-mail address and telephone number, the dates and time(s) Customer was affected, and demonstration that Customer was adversely affected.

Exclusions from Downtime:

Downtime is not triggered by Service unavailability that results from maintenance or from events outside the reasonable control of 6DG or its subcontractor(s), including hacks or the failure/unavailability of Customer's systems, the Internet, or any other service or third-party used by Customer to use, connect to, or access the Service.

Appendix B Security Statement

Commitment to Security

The Service is an Infrastructure as a Service (IaaS) offering designed to extend an existing internal VMware implementation into a secure cloud environment or as a stand-alone hosted cloud solution.

The Service is designed and built to address key security aspects, including:

- Integrity: Through Internet Protocol Security (IPsec) and Secure Socket Layer (SSL) connections, the Service provides industry standard encryption and message authentication to help ensure that customer data cannot be modified during transmission.
- Confidentiality: The Service is designed to allow only authorized users to access information within their virtual environment.
- Availability: The Service uses mission-critical, highly robust, top-tier datacenters, designed to enable service availability at all times.

Overview

The Service uses the following controls to help ensure that the integrity, confidentiality and availability of Customer information meet strong standards:

- Physical controls, including environmental controls, are countermeasures that affect the physical environment; for example, access controls, fire prevention systems, cooling systems, exit routes, security personnel and datacenter surveillance monitoring.[1]
- Technical controls (also called logical controls) are countermeasures that rely upon use of technology to mitigate risk; for example, firewalls, intrusion detection and prevention systems, and encryption mechanisms.
- Administrative controls are countermeasures that involve policy and procedures; for example, security and escalation policies, log audits, vulnerability scanning and penetration testing.

Physical Controls

6DG datacenters are designed to support and protect mission-critical operations. These datacenters provide multi-level physical security features and a rigidly-controlled operating environment to help protect customer assets and operations. The datacenters are audited annually to the SAS-70 Type 2 / SSAE 16 Type 2 standard and maintain ISO/IEC 27001 certification.

[1] The controls outlined in this Appendix are designed to provide strong data security safeguards that meet the needs of a typical user. They are not intended or designed to address all industry specific requirements that are driven by regulatory requirements such as HIPAA or PCI. Users with specific data security requirements that exceed the controls listed in this Appendix should discuss alternative cloud solutions with their 6DG representative. To the extent 6DG receives or otherwise has access to Customer's "education records" and "personally identifiable information" contained in such records, as such terms are defined in FERPA, 6DG acknowledges that it is subject to the requirements of 34 CFR § 99.33(a) governing the use and redisclosure of personally identifiable information in education records.

Access and Security Controls

Access to 6DG datacenters is highly controlled. All entrances are monitored and have alarms for protection. These datacenters are staffed with 24-hour security officers to augment physical security features, providing protection of Customer operations.

CCTV Digital Recorders

CCTV security cameras monitor designated sensitive areas.

Fire Suppression

Industry standard fire suppression systems for multi-tenant datacenters are in use.

Environmental Controls

6DG datacenters are constructed to meet the highest standards of redundancy. 6DG datacenters also include critical power and cooling systems that are provisioned with appropriate redundant failover infrastructure. The critical power and cooling infrastructure is backed up by an emergency power generation system.

Technical Controls

Network and System Security

Multiple levels of disparate defenses are used to protect customer information and strictly control network access to the datacenter. Customers connect with the Service via IPsec and SSL connections to provide industry-standard link encryption and message authentication to help ensure that customer data cannot be modified during transmission. All access to servers is strictly monitored. In addition, Service servers are configured to prevent intrusions and protect against day-to-day threats. The servers are selected and configured to maximize their reliability, security, scalability and efficiency. Trend Micro’s SecureCloud™ encryption service provides optional data volume encryption with third-party key escrow for customers requiring additional data safeguards for their data volumes. This optional encryption service help ensures that neither 6DG nor Trend Micro administrators can access the encrypted data volumes in clear text.

Customer isolation is implemented by leveraging VMware vShield products, as well as Layer 2 VLANs. In addition, Trend Micro's SecureCloud encryption service is an optional service for providing an added layer of security against unauthorized access.

VM processing is performed within region only. Data hosted on virtual machines that are provisioned in Studley is not replicated or otherwise transferred to other 6DG datacenters located in other regions. Customer account information, however, is processed in other regions for billing and support.

Firewalls

Customer data transfers are made from the customer’s environment to the Service system via standard Internet Protocol Security (IPsec) or Secure Socket Layer (SSL) connections through the customer’s firewall. All non-required firewall ports are blocked on the Service firewalls.

Intrusion Prevention Systems

6DG uses enterprise-grade intrusion detection / intrusion prevention systems (IDS/IPS) within the Service infrastructure to provide another mechanism for the early detection and prevention of data breaches.

Security Operations Center Monitoring
6DG monitors all firewalls, web application firewalls and other network probes within the Service infrastructure to facilitate early detection of any attempted data breaches.

Access Controls
Access to corporate systems is restricted, based on procedures to help ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties and least privileges. Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place. Specific event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations by recognized experts in this area.

Vulnerability Scanning and Penetration Testing
Internal and external vulnerability scans are performed on 6DG's cloud infrastructure periodically and after any significant change in the network. External and internal penetration tests, including network- and application-layer penetration tests are performed annually and after any significant infrastructure or application upgrades or modifications.

Administrative Controls

Data Center Access History
Physical access history to the datacenters is recorded.

Personnel Security
All users with access to the Service environment are responsible for compliance with 6DG's information security policies and standards. As part of the employment process, employees undergo a screening process.

Communications and Operations Management
Changes to the Service infrastructure, systems and applications are managed through a centralized change management program, which includes testing, back out procedures, business impact analysis and management approval, where appropriate.

Incident response procedures exist for security and data protection incidents. The procedures include incident analysis, containment, response, remediation, reporting and procedures for returning to normal operations.

To protect against malicious use of assets and malicious software, the following additional controls are implemented: designated development and test environments; malware detection on servers, desktops and notebooks; email attachment malware scanning; and information handling procedures based on data type, application and network security.