# IBM Development and Test Environment Services

This Service Description describes the Cloud Service IBM provides to Client. Client means and includes the company, its authorized users or recipients of the Cloud Service.

## 1. Cloud Service

IBM Development and Test Environment Services (IDTES) Cloud Service provides virtual server environments that enable rapid deployment of development and testing environments to expedite the release of better quality software, optimize productivity and reduce costs. The Cloud Service provisions subscription virtual machines (SVMs), storage, networks, and available development collaboration tools from a shared infrastructure running in a SoftLayer datacenter. The Cloud Service allows users to create testing environments that closely mirror those in production, thereby enabling more frequent testing with reduced wait times. Available collaboration tools help users to detect errors early in the software development process to support delivery of high quality software.

The Cloud Service enables Client to create, manage, and network multiple SVMs and associated storage interactively using the IDTES self-service web application, or programmatically using the IDTES REST-based API. Although running on shared infrastructure, virtualization technologies keep environments isolated from each other. Clients can choose to have environments completely isolated or selectively exposed to the public internet. Users can manage their own virtual network services including DNS and/or DHCP, or IDTES can automatically provision independent DNS and DHCP service daemons for each environment. Client may connect IDTES networks to external networks through IPSec based VPN tunnels.

The Cloud Service has two types of subscriptions:

a. On Demand Subscription: Client selects and may use up to the specified total number of hours during a month.

b. Always On Subscription: Client has unlimited usage during a month.

Client may select any of the available Cloud Service subscription editions to specify the number of SVMs, amount of storage, number of networks and number of public IP addresses. Client may order additional options for a selected edition to increase hours (On-Demand subscription packages only), concurrent SVMs, storage capacity, number of networks or number of public IP addresses.

## 2. Security Description

The cloud infrastructure supporting the Cloud Service uses industry-standard 256bit SSL (Secure Sockets Layer) to provide secure communications over the Internet. Cloud Service operations, including accessing the IDTES web application; accessing SVM consoles using IDTES's software client or remote access; and transferring files between the Cloud Service and Client's systems, are encrypted using HTTPS. Both import and export of virtual machine images uses SFTP (Secure File Transfer Protocol) by default. The Client, however, may select FTP transfer if desired. Movement of data between the Cloud Service storage layer and the physical hardware occurs on an isolated management network that is not accessible by Client or through other customer environments.

Authentication and authorization to access the Cloud Service is controlled at all points of user contact using the following features:

a. Users login and password data is transmitted over an encrypted SSL channel via HTTPS;

b. Client can assign and manage role-based access to control individual user account privileges and may customize password management policies to meet Client's requirements;

c. IDTES supports a single sign-on (SSO) federated authentication using SAML 2.0 to enable access using Client's corporate directory credentials or supported Client applications;

d. IP-based access controls enable Client to set policies to restrict login to predefined source IP addresses requiring users to both authenticate successfully and originate from an authorized IP address; and

e. Single-use token authentication enables Client to provide a one-time validation code through a channel other than the browser. This secure browser token restricts user logins to specific machines that have been authorized to access IDTES.

For the base infrastructure that enables the Cloud Service IBM will:

a. manage the underlying infrastructure and account management;

b. monitor and log administrative activities to support and maintain the infrastructure;

c. perform vulnerability scanning on the base Cloud Service infrastructure. IBM does not scan Client's computing resources;

d. manage underlying network infrastructure and isolation; and

e. store content, including VM disk images, asset files, and shared drive contents, in virtualized network-attached data stores using independent network file-system mounts. This provides isolation between file data for different customers, and between all disk images. Only the disk images for a particular VM are exposed through the mounted file system, and only during the time the VM is running.

IBM has not determined compliance of this Cloud Service with the US-EU and US-Swiss Safe Harbor Frameworks.

**Client Security Responsibilities**

Client is responsible to:

a. maintain valid user email addresses in each user's profile for notification purposes;

b. manage the security setting for each VM and encompassing environment.

c. manage and allocate user access to the Cloud Services;

d. establish and enforce security practices for such access including protecting user IDs and passwords;

e. securely manage and control user access to Client VM and environments, including selection and implementation of all security, encryption, and patch management procedures;

f. adhere to the following guidelines when performing any technical security integrity review, penetration test, or vulnerability scan:

   (1) schedule any such review, test or scan with IDTES support at least three business days prior to such activity;

   (2) only test, scan or review the Client's IP addresses or VMs and not the shared portions of the data center or Cloud Service infrastructure;

   (3) maintain a record of the date and time of any review, penetration test, or vulnerability scan and provide to IBM upon request;

   (4) not perform such reviews more than once per calendar quarter; and

   (5) not perform or simulate denial-of-service attacks.

## 3. Service Level Agreement

IBM provides the following availability service level agreement ("SLA") for the Cloud Service. The SLA is not a warranty and is available only to Client.

### 3.1 SLA Process

Client must log a Severity 1 support ticket with the IBM technical support help desk within 24 hours of first becoming aware of an event that has impacted the Cloud Service availability. Client must reasonably assist IBM with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within three business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the Cloud Service based on the duration of time during which the Cloud Service is unavailable ("Downtime"). The Cloud Service is unavailable when:

a. IDTES SVM has no external connectivity during a five-minute period and Client is unable to launch replacement configurations; or

b. IDTES virtual machines are unable to deploy or start.

Downtime is measured from the time Client reports the event until the time the Cloud Service is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond IBM's control; problems with Client or third party content or technology, designs or instructions; unsupported system configurations and platforms or other Client errors; or Client-caused security incident or Client security testing.

### 3.2 Service Level and Credit

Client is eligible for a service credit equal to 1% of their contracted monthly subscription fee for each cumulative whole hour of Downtime, up to a maximum of 20% service credit.

## 4. Technical Support

Support and planned maintenance window for periodic maintenance and updates to IDTES is published on the IDTES support pages. If Client encounters problems with connectivity, provisioning or use of Cloud Services Client may submit a service request using any of the available support methods.

| Technical Support Method | Support Hours |
|---|---|
| Telephone Support | 8:30AM PT to 5PM PT, M-F, excluding national holidays |
| Help desk support | 24 hours a day, 7 days a week, 365 days in a year |

Support response times may vary from event to event. IBM will use commercially reasonable business attempts to respond and resolve a technical support request and to communicate with Client regarding status of any requests. No service level agreements are provided for technical support and IBM does not provide any credits due to its failure to meet any specific objective.

| Severity Level | Severity Definition | Service Resolution Objective |
|---|---|---|
| Severity 1 | Critical business impact/service down: Client cannot use the Product or there is a critical impact on the customer's operations which requires an immediate solution. | Provide relief within 24 hours Provide final solution or fix within seven (7) days. |
| Severity 2 | Significant business impact/major impact: Client can use the Product, but an important function is not available or the customer's operations are severely impacted | Fourteen (14) calendar days |
| Severity 3 | Minor business impact: The Client can use the Product with some functional restrictions, but it does not have a severe or critical impact on Client operation | Thirty (30) calendar days |

Client will designate severity for each service request. IBM will validate such severity and reserves the right to re-prioritize based upon the above severity definitions.

## 5. Charges

The charges for a selected Cloud Service subscription edition and any optional components options ordered by Client are specified in the on-line order or in a paper form order Transaction Document.

The monthly charge for a Cloud Services will begin upon enablement of the selected Cloud Service subscription edition and will continue until the Cloud Service is cancelled or terminated. IBM will prorate the first months charge based on the date the Cloud Service is available for use through the end of the calendar month. IBM does not prorate the last month of the Cloud Service. Client will have access to a Cloud Service through the end of the month of cancellation notice.

### 5.1 Change to Charges

IBM may change subscription pricing by providing 30 days' notice to Client. Any changes made will be effective on the first of the month that follows the 30 day notice.

## 6. Term, Trial Option, and Termination

### 6.1 Term

The term of a Cloud Service ordered by Client begins on the date Client is notified the Cloud Service is enabled for use and continues on a month to month basis until Client cancels the Cloud Service by submitting a request of cancellation in the Cloud Marketplace or through IDTES technical support ticket at least 10 days before the end of the then current monthly term.

Upon such cancellation, Client will have access to the Cloud Service through the end of the month of cancellation, at which time the subscription to the Cloud Service will terminate and all content will be deleted.

### 6.2 Trial Option Term

If Client orders a free trial of IDTES through IBM Cloud marketplace, Client will have access to available editions of the Cloud Service for 30 days. No Service Level Agreements apply for trial use.

## 7. General

Where applicable, taxes are based upon the location(s) receiving the benefit of the Cloud Service; IBM will apply taxes based upon the business address listed in your order unless you provide additional information to IBM. Client is responsible for keeping such information current and providing any changes to IBM.