

IBM Cloud Service Description: IBM Performance Management (SaaS)

The following is the Service Description for your Order:

1. Cloud Service Description

Sections 1.1 through 1.3 below describe the base offerings that you may order to use the Cloud Service. The offerings that you have ordered are specified in your Order Document. For the purpose of this Cloud Service, the Order Document will consist of the Quotation that IBM presents to you and the Proof of Entitlement (PoE) that you will receive from IBM confirming the Cloud Services have been provisioned setting forth the beginning and end date for the term of the Cloud Service.

1.1 IBM Monitoring (SaaS)

The IBM Monitoring (SaaS) provides end-user experience and resource monitoring to alert users to problems with applications and help resolve them quickly and efficiently.

Entry users have the following capabilities:

- IBM Application Performance Management UI (APM UI) allows users to view the health of applications and drill down to see more details such as related events and KPIs for the components associated with that application.
- Automatically discovers and defines application structure, which can be modified or removed.
- Installs and configures agents automatically, with little to no manual intervention required.
- Allows users to identify real end user experience for the application with response time broken down across components.
- Allows users to see key health metrics for all monitored resources.
- Allows users to create and modify thresholds to visually identify issues and receive alerts.

1.2 IBM Application Diagnostics (SaaS)

The IBM Application Diagnostics (SaaS) provides deep diagnostic information to pinpoint the root cause of application performance issues, so they can be resolved quickly.

Diagnostics users have the following capabilities:

- IBM Application Performance Management UI (APM UI) allows users to view the health of applications and drill down to see more details such as related events and KPIs for the components associated with that application.
- Automatically discovers and defines application structure, which can be modified or removed.
- Installs and configures agents automatically, with little to no manual intervention required.
- Allows users to see key health metrics for their application servers.
- Breaks performance down to the code level and includes key diagnostic information such as context data and stack traces.

1.3 IBM Application Performance Management (SaaS)

The IBM Application Performance Management (SaaS) provides end-user experience, transactions tracking, and resource monitoring to alert users to problems with applications and help resolve them quickly and efficiently.

Users have the following capabilities:

- IBM Application Performance Management UI (APM UI) allows users to view the health of applications and drill down to see more details such as related events and KPIs for the components associated with that application.
- Automatically discovers and defines application structure, which can be modified or removed.
- Installs and configures agents automatically, with little to no manual intervention required.
- With Transactions Tracking, users can identify application performance bottlenecks across all monitored browsers, web servers, and application servers.

- Allows users to identify real end user experience for the application with response time as seen by supported mobile and desktop browser users, broken down across component.
- Allows users to see key health metrics for all monitored resources.
- Allows users to create and modify thresholds to visually identify issues and receive alerts.
- Supports the automatic generation of service requests to resolve an issue in IBM SmartCloud Control Desk, based on IBM Application Performance Management (SaaS) alerts.
- Supports integration of IBM Application Performance Management (SaaS) events into IBM Tivoli Netcool OMNIBus.

2. Security Description

IBM implements and maintains the practices and procedures described in this section.

2.1 Security Policies

IBM maintains privacy and security policies that are communicated to IBM employees. IBM requires privacy and security training to personnel who support IBM data centers. We have an information security team. IBM security policies and standards are reviewed and re-evaluated annually. IBM security incidents are handled in accordance with a comprehensive incident response procedure.

2.2 Access Control

Access to client data, if required, is allowed only by authorized IBM support representatives according to principles of segregation of duties. IBM staff use two-factor authentication to an intermediate "gateway" management host. All connections are encrypted channels when accessing client data. All access to client data and transfer of data into or out of the hosting environment is logged.

2.3 Service Integrity and Availability

Modifications to operating systems and application software are governed by IBM's change management process. Changes to firewall rules are also governed by the change management process and are reviewed by the IBM security staff before implementation. IBM monitors the data center resources 24x7. Internal and external vulnerability scanning is regularly conducted by authorized administrators and third party vendors to help detect and resolve potential system security exposures. Malware detection (antivirus, intrusion detection, vulnerability scanning, and intrusion prevention) systems are used in all IBM data centers. IBM's data center services support a variety of information delivery protocols for transmission of data over public networks. Examples include HTTPS/SFTP/FTPS/S/MIME and site-to-site VPN. Backup data intended for off-site storage is encrypted prior to transport.

2.4 Activity Logging

IBM maintains logs of its activity for systems, applications, data repositories, middleware and network infrastructure devices that are capable of and configured for logging activity. To minimize the possibility of tampering and to enable central analysis, alerting and reporting, activity logging is done in real-time to central log repositories. Data is signed to prevent tampering. Logs are analyzed in real-time and via periodic analysis reports to detect anomalous behavior. Operations staff is alerted to anomalies and contacts a 24x7 on-call security specialist when needed.

2.5 Physical Security

IBM maintains physical security standards designed to restrict unauthorized physical access to IBM data centers. Only limited access points exist into the IBM data centers, which are controlled by two-factor authentication and monitored by surveillance cameras. Access is allowed only to authorized staff that have approved access. Operations staff verifies the approval and issues an access badge granting the necessary access. Employees issued such badges must surrender other access badges and can only possess the data center access badge for the duration of their activity. Usage of badges is logged. Non-IBM visitors are registered upon entering on premises and are escorted when they are on the premises. Delivery areas and loading docks and other points where unauthorized persons may enter the premises are controlled and isolated.

2.6 Compliance

IBM reviews security and privacy-related activities for compliance with IBM's business requirements. Assessments and audits are conducted regularly by IBM to confirm compliance with its information security policies. IBM employees and vendor employees complete workforce security education and awareness training annually. Personnel are reminded of their job objectives and their responsibility to meet ethical business conduct, confidentiality, and IBM's security obligations annually.

3. Service Level Commitment

IBM provides the following service level agreement (“SLA”) for the Cloud Service. You understand that the SLA does not constitute a warranty to you.

3.1 Definitions

- a. “Authorized Contact” means the individual you have specified to IBM who is authorized to submit Claims under this SLA.
- b. “Availability Credit” means the remedy IBM will provide for a validated Claim. The Availability Credit will be applied in the form of a credit or discount against a future invoice of subscription charges for the Service.
- c. “Claim” means a claim submitted by your Authorized Contact to IBM pursuant to this SLA that a Service Level has not been met during a Contracted Month.
- d. “Contracted Month” means each full month during the term of the Service measured from 12:00 a.m. Eastern US time on the first day of the month through 11:59 p.m. Eastern US time on the last day of the month.
- e. “Customer” means an entity subscribing for the Service directly from IBM, which has entitlement for use of the Service at the time of submitting a Claim, and which is not in default of any material obligations, including payment obligations, under its contract with IBM for the Service.
- f. “Downtime” means a period of time during which production system processing for the Service has stopped and all of your users are unable to use all aspects of the Service for which they have appropriate permissions. By way of clarification, there is no “Downtime” if any user can use any aspect of the Service for which they have appropriate permissions. Downtime does not include the period of time when the Service is not available as a result of:
 - Planned System Downtime
 - Force Majeure.
 - Problems with Customer or third party applications, integrations, equipment or data.
 - Customer or third party acts or omissions (including anyone gaining access to the Service by means of your passwords or equipment).
 - Failure to adhere to required system configurations and supported platforms for accessing the Service.
 - IBM’s compliance with any designs, specifications, or instructions provided by Customer or a third party on Customer’s behalf.
- g. “Event” means a circumstance or set of circumstances taken together, resulting in a failure to meet a Service Level.
- h. “Force Majeure” means acts of God, terrorism, labor action, fire, flood, earthquake, riot, war, governmental acts, orders or restrictions, viruses, denial of service attacks and other malicious conduct, utility and network connectivity failures, or any other cause of Service unavailability that was outside IBM’s reasonable control.
- i. “Planned System Downtime” means a scheduled outage of the Service for the purpose of service maintenance or system updates, such as but not limited to, when a release, patch or hot fix is applied.
- j. “Service” means the IBM Performance Management (SaaS) production instance to which this SLA applies, as shown on the first page of this Service Description. This SLA applies to each Service individually and not in combination.
- k. “Service Level” means the standard set forth below by which IBM measures the level of service it provides in this SLA.

3.2 Availability Credits

- a. In order to be eligible to submit a Claim you must have logged a support ticket for each Event with the IBM customer support help desk for the applicable Service, in accordance with IBM procedure for reporting Severity 1 support issues. You must provide all necessary detailed information about the Event, including the time you were first impacted by the Event, and reasonably assist IBM with the diagnosis and resolution of the Event to the extent required for Severity 1 support tickets. Such ticket must be logged within twenty-four (24) hours of your first becoming aware that the Event has impacted your use of the Service.

- b. Your Authorized Contact must submit your Claim for an Availability Credit no later than three (3) business days after the end of the Contracted Month which is the subject of the Claim.
- c. Your Authorized Contact must provide to IBM all reasonable details regarding the Claim, including but not limited to, detailed descriptions of all relevant Events and the Service Level claimed not to have been met.
- d. IBM will measure internally total combined Downtime during each Contracted Month. Availability Credits will be based on the duration of the Downtime measured from the time you report that you were first impacted by the Downtime. For each valid Claim, IBM will apply the highest applicable Availability Credit corresponding to the total combined availability during each Contracted Month, based on the table below. IBM will not be liable for multiple Availability Credits for the same Event in the same Contracted Month.
- e. For Bundled Services (individual Services packaged and sold together for a single combined price), the Availability Credit will be calculated based on the single combined monthly price for the Bundled Services, and not the monthly subscription fee for each individual Services. You may only submit Claims related to one individual Service in a bundle in any Contracted Month, and IBM will not be liable for Availability Credits with respect to more than one Service in a bundle in any Contracted Month.
- f. The total Availability Credits awarded with respect to any Contracted Month shall not, under any circumstance, exceed 10 percent (10%) of one twelfth (1/12th) of the annual charge paid by you to IBM for the Service.
- g. IBM will use its reasonable judgment to validate Claims based on information available in IBM's records, which will prevail in the event of a conflict with data in your records.
- h. THE AVAILABILITY CREDITS PROVIDED TO YOU IN ACCORDANCE WITH THIS SLA ARE YOUR SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM.

3.3 Service Levels

Availability of Service during a Contracted Month

Availability during a Contracted Month	Availability Credit (% of Monthly Subscription Fee for Contracted Month which is the subject of a Claim)
Less than 99.8%	2%
Less than 98.8%	5%
Less than 95.0%	10%

“Availability” percentage is calculated as: (a) the total number of minutes in a Contracted Month, minus (b) the total number of minutes of Downtime in a Contracted Month, divided by (c) the total number of minutes in a Contracted Month, with the resulting fraction expressed as a percentage.

Example: 432 minutes total Downtime during Contracted Month

43,200 total minutes in a 30 day Contracted Month - 432 minutes Downtime = 42,768 minutes <hr style="width: 50%; margin: 0 auto;"/> 43,200 total minutes in a 30 day Contracted Month	= 2% Availability Credit for 99.0% availability during the Contracted Month
---	--

3.4 Exclusions

This SLA is made available only to IBM Customers. This SLA does not apply to the following:

- Beta and trial Services.
- Non-production instances, including but not limited to test, disaster recovery, training, Q&A, or development.

- Claims made by an IBM Customer's users, guests, and participants of the Service.
- Services, programs, enabling software or agents running on client systems or third party-provided systems
- If you have breached any material obligations under the Terms of Use, Acceptable Use Policy or your contract for the Service, including without limitation, breach of any payment obligations.

4. Entitlement and Billing Information

4.1 Charge Metrics

The Cloud Service offerings are sold in accordance with the following metric(s):

- Average Managed Virtual Server is a unit of measure by which the Cloud Service can be obtained. A server is a physical computer that is comprised of processing units, memory, and input/output capabilities and that executes requested procedures, commands, or applications for one or more users or client devices. Where racks, blade enclosures, or other similar equipment is being employed, each separable physical device (for example, a blade or a rack-mounted device) that has the required components is considered itself a separate server. A Virtual Server is either a virtual computer created by partitioning the resources available to a physical server or an unpartitioned physical server. Sufficient Average Managed Virtual Server entitlements must be obtained to cover the average number of Virtual Servers managed by the Cloud Service during the measurement period specified in Customer's Order Document.

4.2 Charges and Billing

The amount payable for the Cloud Service is specified in the Order.

4.3 Partial Month Charges

The partial month charge is a pro-rated daily rate. The partial month charges are calculated based on the remaining days of the partial month starting on the date you are notified by IBM that your access to the Cloud Service offering is available.

4.4 Overage Charges

If your actual usage of the Cloud Service during the measurement period exceeds the entitlement stated on the PoE portion of the Order Document, then you will be invoiced for the overage, as set forth in the Order Document.

5. Term and Renewal Options

5.1 Term

The term of the Cloud Service begins on the date that IBM notifies you that you have access to the Cloud Service, as described in the Order Document. The PoE portion of the Order Document will confirm the exact date of the start and end of the term,. You are permitted to increase your level of use of the Cloud Service during the term by contacting IBM or you IBM Business Partner. We will confirm the increased level of usage in the Order Document.

5.2 Cloud Services Term Renewal Options

Your Order Document will set forth whether the Cloud Service will renew at the end of the term, by designating the term as one of the following:

5.2.1 Automatic Renewal

If your Order Document states that your renewal is automatic, you may terminate the expiring Cloud Service term by written request, at least ninety (90) days prior to the expiration date of the term that is set forth in the Order Document. If IBM or your IBM Business Partner does not receive such termination notice by the expiration date, the expiring term will be automatically renewed for either a one year term or the same duration as the original term as set forth in the PoE.

5.2.2 Continuous Billing

When the Order Document states that your billing is continuous, you will continue to have access to the Cloud Service following the end of your term and will be billed for the usage of the Cloud Service on a continuous basis. To discontinue use of the Cloud Service and stop the continuous billing process, you must provide IBM or your IBM Business Partner with ninety (90) days written notice requesting that your Cloud Service be cancelled. Upon cancellation of your access, you will be billed for any outstanding access charges through the month in which the cancellation took effect.

5.2.3 Renewal Required

When the Order Document states that your renewal type is “terminate”, the Cloud Service will terminate at the end of the term and your access to the Cloud Service will be removed. To continue to use the Cloud Service beyond the end date, you must place an order with your IBM sales representative or IBM Business Partner to purchase a new subscription term.

6. Technical Support

Technical support for the Cloud Service is available during the subscription period.

Email Support & SaaS Support Portal Hours of Operation are as follows:

8:00 a.m. – 8:00 p.m. Eastern Standard Time zone, U.S., Monday – Friday (excluding holidays)

Support Hotline: 1-855-221-1166 in the U.S.

Email: support@ibmserviceengage.com

After Hours & System Down Support:

After Hours & System Down Support is available only for Severity 1 issues on business days, weekends, and holidays.

Severity	Severity Definition	Response Time Objectives	Response Time Coverage
1	Critical business impact/service down: Business critical functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations. This condition requires an immediate solution.	Within 1 hour	24x7
2	Significant business impact: A service business feature or function of the service is severely restricted in its use or you are in jeopardy of missing business deadlines.	Within 2 business hours	M-F business hours
3	Minor business impact: Indicates the service or functionality is usable and it is not a critical impact on operations.	Within 4 business hours	M-F business hours
4	Minimal business impact: An inquiry or non-technical request	Within 1 business day	M-F business hours

7. Enabling Software

This Cloud Service offering may include enabling software. You may use the enabling software only in association with your use of the Cloud Service for the length of the term of the Cloud Service. To the extent that the enabling software contains sample code, you have the additional right to make derivative works of the sample code and use them consistent with this grant. The enabling software is provided subject to the SLA, if any, as a component of the Cloud Service, and is subject to the applicable license agreement(s).

This Cloud Service offering includes the following enabling software provided by IBM: Monitoring Agent for Linux OS, Monitoring Agent for Windows OS, Monitoring Agent for Unix OS, Monitoring Agent for Linux KVM, Monitoring Agent for Ruby, Monitoring Agent for MongoDB, Monitoring Agent for MySQL, Monitoring Agent for WebSphere Applications, Monitoring Agent for PHP, Monitoring Agent for Python, Monitoring Agent for PostgreSQL, Monitoring Agent for .NET, Monitoring Agent for Tomcat, Monitoring Agent for Node.js, Integration Agent for Netcool/OMNibus, and Response Time Monitoring Agent. Additional agents may be added over time and will be covered by this Agreement.

For IBM SaaS offerings designated as “Step-up for existing Customers” (“Step-up SaaS”), the following enabling software is provided by IBM: IBM Performance Management (SaaS) Agent Converter for Linux Servers, IBM Performance Management (SaaS) Agent Converter for Windows Servers, IBM Performance Management (SaaS) Agent Converter for AIX Servers.

8. Additional Information

8.1 Step up Limitation

- For IBM SaaS offerings designated as “Step-up for existing Customers” (“Step-up SaaS”), customer must have previously acquired appropriate license entitlements to the associated IBM program as identified in the name of the Step-up SaaS offering. For example, Customer who purchases IBM

Monitoring (SaaS) Step up for existing IBM Tivoli Monitoring Customers must have licensed entitlements to the associated IBM program of IBM Tivoli Monitoring. Customer's entitlements to the Step-up SaaS cannot exceed Customer's entitlements to the associated IBM program.

When acquiring Step-up SaaS, Customer may not use the same associated IBM program license entitlements within their on-premise installed environment as well as with the Step-up SaaS entitlements. For example, if Customer has 23 Managed Virtual Server entitlements to the associated IBM program and chooses to purchase 10 Step-up SaaS Average Managed Virtual Server entitlements, Customer can monitor 10 Step-up SaaS Average Managed Virtual Servers from the IBM SaaS environment and 13 Managed Virtual Servers from the software installed on-premise.

The Step-up SaaS does not include Subscription and Support for the associated IBM program. Customer represents they have acquired the applicable (1) license entitlements and (2) Subscription and Support for the associated IBM program(s). During the Subscription Period of the Step-up SaaS, Customer must maintain current Subscription and Support for the IBM program entitlements used in conjunction with the Step-up SaaS entitlements. In the event either Customer's license to use the associated IBM program(s) or Customer's Subscription and Support for the associated IBM program(s) is terminated, Customer's right to use the Step-Up SaaS will terminate.

8.2 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) you identify as receiving benefit of the Cloud Services. IBM will apply taxes based upon the business address listed when ordering a Cloud Service as the primary benefit location unless you provide additional information to IBM. You are responsible for keeping such information current and providing any changes to IBM.