

# Service Description

## **Micro Focus LoadRunner Cloud Software-as-a-Service**

June 2022

## Contents

|   |    |
|---|----|
| 1. Standard Service Features .....                | 3  |
| 2. Solution Data Backup and Retention.....        | 8  |
| 3. SaaS Security .....                            | 9  |
| 4. Audit .....                                    | 10 |
| 5. Micro Focus Security Policies .....            | 11 |
| 6. Security Incident Response .....               | 11 |
| 7. Micro Focus Employees and Subcontractors ..... | 11 |
| 8. Data Subject Requests.....                     | 11 |
| 9. Scheduled Maintenance .....                    | 11 |
| 10. Service Decommissioning.....                  | 12 |
| 11. Solution Availability SLA .....               | 12 |
| 12. Online Support Availability SLO.....          | 13 |
| 13. Standard Service Requirements .....           | 15 |

This Service Description describes the components and services included in Micro Focus LoadRunner Cloud Software-as-a-Service (which also may be referred to as “SaaS”). Unless otherwise agreed to in writing this Service Description is subject to the Micro Focus Customer Terms for SaaS and represents the only binding terms governing Micro Focus International plc and its affiliates (“Micro Focus”) respective obligations regarding its provision of this SaaS to the end-user customer. Any other descriptions of the features and functions of the SaaS, public statements, including advertisements, shall not be deemed as additional features or functionalities that Micro Focus is required to deliver.

## 1. Standard Service Features

### 1.1 High Level Summary

Micro Focus LoadRunner Cloud (“LoadRunner Cloud”) SaaS provides a cloud-based enterprise service that is intended for high volume performance testing of the Customer’s application.

### 1.2 SaaS Service Delivery Components

|  |
|--|
| <b>SaaS Delivery Components</b>                      |
| <b>One LoadRunner Cloud SaaS production instance</b> |

### 1.3 SaaS Operational Services

| <b>Operational Services</b>                |   |
|--|---|
| <b>SSO integration</b>                     | √ |
| <b>SaaS best practice document library</b> | √ |
| <b>Services support</b>                    | √ |
| <b>Dedicated IPs</b>                       | O |
| <b>Dedicated VPC</b>                       | O |
| <b>Multiple IPs</b>                        | √ |
| <b>External integrations support</b>       | O |
| √ = Included                               |   |
| O = Optional for a fee                     |   |

## 1.4 Architecture Components

LoadRunner Cloud consists of these two (2) parts: (a) a cloud-based management platform with an interactive dashboard for managing, storing, and analyzing performance tests; and (b) a Micro Focus-provided agent, installed by Micro Focus or by the Customer to execute the performance tests. Customer also subscribes to a protocol bundle that will be specified in the order document. Customer can purchase either Virtual User Hours (“Vuser hours”) or Virtual User (“Vuser”). A Customer that purchases Vusers, protocols included in the GUI bundle can use Micro Focus-provided agents up to 100 hours per month. The use of Micro Focus-provided agents for Vusers purchased from other protocols is unrestricted.

LoadRunner Cloud supports different Vuser types that are sold in protocol bundles as outlined below:

1. Dev bundle: Allows customers to run scripts developed using JMeter and Gatling.
2. Web bundle: Allows customers to run web (http/html), Mobile Application - HTTP/HTML, web services, DevWeb, and Java scripts created with Micro Focus virtual user generator as well as the TruAPI protocol, MQTT and Silk Performer scripts: Web low level, Web business transaction, HTTP Live Streaming, Kafka, and XML/SOAP. Subscribing to this bundle also includes a subscription to the Dev bundle. (\*)
3. GUI bundle: Allows customers to run TruClient – Web, TruClient - Mobile Web, TruClient - Native Mobile (requires a separate UFT Mobile license), Selenium and Silk Performer scripts: Web browser-driven (AJAX). Subscribing to this bundle also includes a subscription to the web and dev bundles
4. ERP bundle: Allows customers to run SAP – Web, SAP-GUI, Oracle NCA, Oracle Web, Siebel Web. (\*)
5. Legacy bundle: Allows customers to run Windows Sockets, RDP (Remote Desktop Protocol), RTE (Remote Terminal Emulator) Citrix ICA and .Net. (\*)
6. All Protocol bundle: Subscribing to this bundle allows customers to run scripts using any of the Vuser types that LoadRunner Cloud supports.

\* Some of the protocols are supported on on-premises load generators only, full description can be found in this link at the LoadRunner Cloud online help center

[https://admhelp.microfocus.com/srl/en/latest/Content/Storm/lp\\_License.htm](https://admhelp.microfocus.com/srl/en/latest/Content/Storm/lp_License.htm)

LoadRunner Cloud is multi-tenant meaning that each customer of this SaaS offering receives its own segregated tenant on a multi-tenant farm.

Customer understands that the use of LoadRunner Cloud may involve (i) transmitting content over various networks, and (ii) changes to the content to conform and adapt to technical requirements of connecting networks or devices. Customer should always keep a copy of the original orders or make back-up copies of such content on Customer’s own system(s).

## Cloud Load Generator usage restrictions

Each of the supported protocol types is set with a default value for the maximum number of Vusers assigned to a Standard Cloud Load Generator Machine ('SCLGM'). The typical SCLGM provides 8 CPU cores, running either Windows or Linux operating system. Each protocol type has the following limit for the minimum number of Vusers that can run on a single SCLGM:

- Any protocol type included in DEV, WEB, or ERP protocol bundle: a minimum of 1,500 Vusers can run on a single SCLGM.
- Any protocol type included in GUI protocol bundle: a minimum of 15 Vusers can run on a single SCLGM.

Protocol type can be configured in a customer tenant to allow a lower number of Vusers per SCLGM. Using a protocol type with a lower number of Vusers per SCLGM will increase the license usage as described below.

The following Vusers multiplier ratios will apply for the purpose of calculating license usage when number of Vusers per SCLGM is set below 1,500 Vusers in a protocol type from the DEV, WEB, or ERP protocols bundles:

- Vusers per SCLGM is set between 500 and 1,499 – Vusers multiplier ratio is x2
- Vusers per SCLGM is set between 250 and 499 – Vusers multiplier ratio is x3
- Vusers per SCLGM is set between 100 and 249 – Vusers multiplier ratio is x4
- Vusers per SCLGM is set between 50 and 99 – Vusers multiplier ratio is x5
- Vusers per SCLGM is set between 15 and 49 – Vusers multiplier ratio is x10
- Vusers per SCLGM is set between 10 and 14 – Vusers multiplier ratio is x15
- Vusers per SCLGM is set between 5 and 9 – Vusers multiplier ratio is x20

The following Vusers multiplier ratios will apply for the purpose of calculating license usage when number of Vusers per SCLGM is set below 15 Vusers in a protocol type from the bundle GUI:

- Vusers per SCLGM is set between 10 and 14 – Vusers multiplier ratio is x1.25
- Vusers per SCLGM is set between 5 and 9 – Vusers multiplier ratio is x2

Examples for clarifications:

- Example A: a test with 2,000 concurrent Vusers using web http protocol type will consume 2,000 Vuser license when number of Vusers per cloud load generator in web http protocol type is set to 1,500. However, when setting the minimum number of Vusers per load generator for web http protocol type to 500, the same test will consume 4,000 Vuser license.
- Example B: a one-hour test with 2,000 concurrent Vusers using web http protocol type will consume 2,000 Vuser hours license when number of Vusers per cloud load generator in web http protocol type is set to 1,500. However, when setting the minimum number of Vusers per load generator for web http protocol type to 500, the same test will consume 4,000 Vuser hours.

The ability to modify the number of Vusers allocated to an SCLGM is not available by default. Customer can request this feature for their LoadRunner Cloud tenant under the above terms via a service request.

## **Dedicated IPs**

Customer can request Micro Focus SaaS to reserve and not change the IP addresses (“Dedicated IPs”) of the cloud-based load generators provisioned by Micro Focus through third party cloud providers. This will enable the Customer to modify firewall rules to allow traffic from external load generators to access their application. Customer can request Dedicated IPs to allow outbound connectivity between Micro Focus on premises load generators and LoadRunner Cloud runtime components in the cloud. This optional service is available for up to 10 Dedicated IPs with no additional cost, additional Dedicated IPs can be obtained with additional cost.

## **LoadRunner Cloud Dedicated VPC**

LoadRunner Cloud allows Customer to use LoadRunner Cloud agents in supported regions that have access to customer’s network by using a dedicated VPC provided by Micro Focus, the connection between the Micro Focus dedicated VPC and the customer network can be established by using Customer’s VPN, “AWS Direct Connect” (“DX”) or “AWS VPC Peering” services, this capability may have additional charges by Micro Focus. Contact Micro Focus representative to enable this capability. The following terms and conditions apply for customers that are subscribed to LoadRunner Cloud with the dedicated VPC capability enabled.

Customer is responsible for working with Micro Focus team for setting up the connectivity between their network and the Micro Focus dedicated VPC network.

Customer is responsible for any cost (including traffic cost) from customer’s environment and henceforth (to and not limited to customer’s AWS account, customer’s Azure account, and other customer’s third parties).

Load test with a dedicated VPC can be enabled in up to three supported regions that have been reviewed and approved by MF in advance, a dedicated VPC will be setup in each region.

To setup a dedicated VPC, the customer is responsible for certain activities, including but not limited to:

Providing IP CDIR blocks per region to support the expected network load to be generated by LoadRunner Cloud agents

Configuring DX to allow network connectivity with above-mentioned MF dedicated VPCs

Maintaining and monitoring the network connectivity with LoadRunner Cloud Dedicated VPCs

Have sufficient bandwidth when running LoadRunner Cloud tests to support the expected network load

Since the Dedicated VPC allows network connectivity from MF’s VPC to Customer’s network, it is Customer’s responsibility to apply required network access restrictions to their network through the MF Dedicated VPC. Customer agrees that Micro Focus will not be liable to Customer or to any third party for any damages or losses, including without limitation charges from AWS, Azure or any other third party to Customer.

To support accessing Customer’s applications and systems from LoadRunner Cloud scripts using DNS names, Customer will provide required internal DNS details and network access to the internal DNS service.

## **1.5 Application Administration**

Customer will access LoadRunner Cloud using a web browser and the URL provided to them. Once securely logged in, the Customer can perform administrative tasks such as adding

and deleting users, adding users to projects, allocating hardware, and running and scheduling performance tests.

## 1.6 Service Components

Micro Focus offers the following core SaaS support and operational services as part of LoadRunner Cloud.

### Service Support

The Customer may contact Micro Focus through a variety of methods such as online support tickets or telephone. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.

Online support is available at: <http://software.microfocus.com/myaccount/>

Micro Focus LoadRunner Cloud Community at: <https://community.microfocus.com/adtd/srload/>. Additional custom support, education or services can be purchased via FlexCare credits: <https://www.microfocus.com/en-us/services/flexible-credits>

Micro Focus staffs and maintains a 24x7x365 Service Operations Center, which will be the single point of contact for all issues related to the support for LoadRunner Cloud for the Customer. Customer will maintain a list of authorized users who may contact Micro Focus for support. The Customer's authorized users may contact Micro Focus for support via the Web portal or telephone 24 hours a day, 7 days a week.

### Service Features:

- System Availability SLO of 99.9%
- Customer Success Manager Services
- Solution Expert Services
- Welcome Package
- Technical Enablement and Pre-recorded enablement videos
- Email and Online Notifications
- Version updates. Notification period according to notification timelines via email, release notes and help resources available
- Regular Service Reviews to review service quality and to provide feedback on improvements required
- Regular Adoption Reviews to plan how best to adopt product features and best practices based on your business objectives

## 1.7 Service Monitoring

Micro Focus monitors LoadRunner Cloud components 24x7 availability. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages, and scheduled maintenance. Alerts and notifications are available to the Customer online at: <http://software.microfocus.com/myaccount/>

## 1.8 Capacity and Performance Management

The architecture allows for addition of capacity to applications, databases, and storage.

## 1.9 Operational Change Management

Micro Focus follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables beneficial changes to be made with minimal disruption to the service.

## 2. Solution Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to Customer of LoadRunner Cloud and access to LoadRunner Cloud Customer data, following an outage or similar loss of service.

The following types of Customer-specific data are included in the LoadRunner Cloud database that resides in the Micro Focus SaaS environment: Customer inserted data (for example attachments, scripts, documents, and files).

The Data Backup Frequency is one (1) day and Micro Focus performs that daily backup of the LoadRunner Cloud database (including configuration data). The Backup Retention Time is seven (7) days, meaning Micro Focus retains each daily backup for the most recent seven (7) days ("Data Retention Time").

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data. Customer may request via a service request for Micro Focus to attempt to restore such data from Micro Focus's most current backup. Micro Focus will be unable to restore any data not included in the database (not properly entered by the user or lost or corrupted etc.) at the time of backup or if Customer's request comes after the Data Retention Time of such backup.

LoadRunner Cloud's standard retention policy for test results archives results data from test runs that are over 18 months old and deletes results data from test runs that are over 3 years old. Customer may request via a service request for Micro Focus to restore test results from an archived test run or to extend the standard period to delete results data of old test runs.

### 2.1 Disaster Recovery

#### 1. Business Continuity Plan

Micro Focus SaaS continuously evaluates different risks that might affect the integrity and availability of Micro Focus SaaS. As part of this continuous evaluation, Micro Focus SaaS develops policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. Micro Focus documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). Micro Focus utilizes the BCP to provide core Micro Focus SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus SaaS implements and tests Micro Focus SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

#### 2. Backups

Micro Focus SaaS performs both on-site and off-site backups with a 24 hours recovery point objective (RPO). Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances. The backup includes a snapshot of production data along with an export file of the production database. The production data is then backed up at a remote site. Micro Focus uses storage and database replication for its remote site backup process. The integrity of backups are validated by (1) real time monitoring of the storage snapshot process for system errors, (2) validating CHECKSUM at the end of a backup



process to assure the same number of bits exists on both source and destination storage systems, and (3) and annual restoration of production data from an alternate site to validate both data and restore flows integrity.

LoadRunner Cloud is implemented using AWS technology service stack in a redundant mode over two availability zones (“AZs”). Each AZ is designed to be insulated from failures in other AZs. The DRP’s target is to provide restoration of the Micro Focus SaaS within twelve (12) hours following Micro Focus’s declaration of a disaster, excluding, however, a disaster or multiple disasters causing the compromise of data centers in the separate AZs simultaneously, and excluding non-production environments.

### **3. SaaS Security**

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability and integrity of Customer Personal Data and confidential information (the “Micro Focus Security Program”).

#### **3.1 Technical and Organizational Measures**

This section describes Micro Focus’s standard technical and organizational measures, controls, and procedures, which are intended to help protect the Customer-provided SaaS Data.

Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures are or can be completely effective against all security threats, present and future, known and unknown. The measures set forth in this section may be modified by Micro Focus but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

#### **3.2 Physical Access Controls**

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include Micro Focus data centers and data centers operated by third parties. This is accomplished through the following practices:

- presence of on-site security personnel on a 24x7 basis
- use of intrusion detection systems
- use of video cameras on access points and along perimeter
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises
- monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities
- maintaining an audit trail of access

#### **3.3 Access Controls**

Micro Focus maintains the following standards for access controls and administration designed to make Customer-provided SaaS Data accessible only by authorized Micro Focus personnel who have a legitimate business need for such access:

- secure user identification and authentication protocols
- authentication of Micro Focus personnel in compliance with Micro Focus standards and in accordance with ISO27001 requirements for segregation of duties
- Customer provided SaaS data is accessible only by authorized Micro Focus personnel who have a legitimate business need for such access, with user authentication, sign-on and access controls

- employment termination or role change is conducted in a controlled and secured manner
- administrator accounts should only be used for the purpose of performing administrative activities
- each account with administrative privileges must be traceable to a uniquely identifiable individual
- all access to computers and servers must be authenticated and within the scope of an employee's job function
- collection of information that can link users to actions in the Micro Focus SaaS environment
- collection and maintenance of log audits for the application, OS, DB, network, and security devices according to the baseline requirements identified
- restriction of access to log information based on user roles and the "need-to-know;" and prohibition of shared accounts

### 3.4 Availability Controls

Micro Focus's business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus's continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Controls regarding disruption prevention include:

- uninterruptible power supplies (UPS) and backup power generators
- at least two independent power supplies in the building
- robust external network connectivity infrastructure

### 3.5 Data Segregation

Micro Focus SaaS environments are segregated logically by Micro Focus SaaS access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies, and content-based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

### 3.6 Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt Customer-provided SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted.

### 3.7 Customer code

Code written to emulate load testing scenarios in LoadRunner Cloud will be reviewed by Customer prior to execution to ensure that the code, when executed, does not have any other effect than load test scenario emulation.

## 4. Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide LoadRunner Cloud. A summary report or similar documentation will be provided to Customer upon request. Subject to the execution of Micro Focus's standard confidentiality agreement, Micro

Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to Micro Focus SaaS provided pursuant to the applicable Supporting Material no more than once per year. Such information security questionnaire will be considered Micro Focus Confidential Information.

## **5. Micro Focus Security Policies**

Micro Focus conducts annual reviews of its policies around the delivery of SaaS against ISO 27001. Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge, or new threats are identified.

## **6. Security Incident Response**

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure, or alteration of Customer-provided SaaS Data (“Security Incident”), Micro Focus will notify Customer of the Security Incident and work to mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer’s account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via [softwaresoc@microfocus.com](mailto:softwaresoc@microfocus.com).

## **7. Micro Focus Employees and Subcontractors**

Micro Focus requests that all employees involved in the processing of Customer-provided SaaS Data are authorized personnel with a need to access the Customer-provided SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requests that any affiliate or third-party subcontractor involved in processing Customer-provided SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

## **8. Data Subject Requests**

Micro Focus will, within three (3) business days of receipt, refer to Customer any queries from data subjects in connection with Customer-provided SaaS Data.

## **9. Scheduled Maintenance**

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis. Micro Focus reserves a weekly two (2) hours window (Sunday 00:00 to 02:00 Pacific Standard Time) and one (1) monthly four (4) hour window (Sunday in the 00:00 to 08:00 Pacific Standard Time block). These windows will be used on an as-needed basis.

Planned windows will be scheduled at least two (2) weeks in advance when Customer action is required, or at least four (4) days in advance otherwise.

### **9.1 Scheduled Version Updates**

“SaaS Upgrades” are defined as both major version updates, minor version updates and binary patches applied by Micro Focus to Customer’s LoadRunner Cloud in production. These may or may not include new features or enhancements. Micro Focus determines whether and when to develop, release and apply any SaaS Upgrade. Customer is entitled to SaaS Upgrades as part of LoadRunner Cloud service unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus will use the Scheduled Maintenance windows defined above to apply the most recent service packs and hot fixes and to perform upgrade to minor versions of LoadRunner Cloud. To enable Customers to plan for scheduled major version updates by Micro Focus, Micro Focus will be scheduling major version updates at least two (2) weeks in advance.

## 10. Service Decommissioning

Customer may cancel Micro Focus SaaS by providing Micro Focus with sixty (60) days written notice prior to the expiration of the SaaS Order Term ("Cancellation"). Such Cancellation shall be effective upon the last day of the then current SaaS Order Term. Upon Cancellation, expiration, or termination of the SaaS Order Term, Micro Focus may disable all Customer access to LoadRunner Cloud, and Customer shall promptly return to Micro Focus (or at Micro Focus's request destroy) any Micro Focus Materials.

Micro Focus will make available to Customer such data in the format generally provided by Micro Focus. The target timeframe is set forth below in the Termination Data Retrieval Period SLO section. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course.

## 11. Solution Availability SLA

Solution Availability is defined as the LoadRunner Cloud production application being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus will provide Customer access to LoadRunner Cloud production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("SaaS Service Uptime Metric").

### 11.1 Measurement Method

SaaS Service Uptime Metric shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing.

On a quarterly basis, the SaaS Service Uptime Metric will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

### 11.2 Boundaries and Exclusions

The SaaS Service Uptime Metric shall not apply in any of the following exceptions, and neither LoadRunner Cloud will be considered unavailable, nor any Service Level Failure be deemed to occur in connection with any failure to meet the requirement or impaired ability of Customer or its Authorized Users to access or use LoadRunner Cloud:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of the SaaS agreement
- Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus

- Scheduled Maintenance
- Scheduled Version Updates

### 11.3 Reporting

Micro Focus will provide self-service access to Customer to the availability data online at <https://home.software.microfocus.com/myaccount/>

In addition, Micro Focus will provide a SaaS Service Uptime Metric Report (“Uptime Metric Report”) in accordance with this attachment to the Customer upon request. If the Customer does not agree with the Uptime Metric Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the Uptime Metric Report.

### 11.4 Remedies

Micro Focus’s exceeding, meeting, or failing to meet the SaaS Service Uptime Metric as measured over any quarter may be reflected in adjustments to the duration of the initial contract term for Micro Focus SaaS pursuant to the following schedule (“Availability SLA Service Credits”):

| Quarterly Micro Focus SaaS Rating | Rating       | Micro Focus SaaS Service Credit   |
|-----------------------------------|--------------|---|
| Between 99.9 % - 100%             | Meets Goals  | Not Applicable  |
| Between 98.0% - 99.8%             | Tolerable    | Five (5) day extension of LoadRunner Cloud SaaS Order term at no cost to Customer |
| Below 98.0%                       | Unacceptable | Ten (10) day extension of LoadRunner Cloud SaaS Order term at no cost to Customer |

Micro Focus SaaS Ratings below 98% for a quarter shall be escalated by both parties to the Vice President (or equivalent), as outlined in this schedule.

Customer must request all service credits or extensions in writing to Micro Focus within thirty (30) days of the end of the month in which the SaaS Service Uptime Metric was not met and identify the support requests relating to the period where LoadRunner Cloud production application was not available for access and use by Customer and its authorized users over the internet.

Micro Focus SaaS Service Credits shall be cumulative over the SaaS Order term. If Customer renews service, Micro Focus SaaS Service Credits will be applied to a service extension at the end of the renewed subscription term at no additional charge. If Customer does not renew service Micro Focus SaaS Service Credits will be applied towards a service extension at no additional charge. Micro Focus SaaS Service Credits are capped at thirty (30) days per annum.

## 12. Online Support Availability SLO

Online Support Availability is defined as the Micro Focus SaaS support portal

<https://login.software.microfocus.com/msg/actions/showLogin>

being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus targets to provide Customer access to the Micro Focus SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% ("Online Support Uptime").

### **1. Measurement Method**

Online Support Uptime shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing.

On a quarterly basis, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

### **2. Boundaries and Exclusions**

Online Support Uptime shall not apply to any of the following exceptions:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of agreement
- Actions or inactions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled Maintenance

## **12.1 Initial SaaS Response Time SLO**

The Initial SaaS Response Time refers to the Service Support. It is defined as the acknowledgment of the receipt of a customer request and the assignment of a case number for tracking purposes. Initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of a customer request.

## **12.2 SaaS Support SLOs**

There are two types of SaaS Support SLOs: Service Request and Support Request SLOs.

- The Service Request SLO applies to the majority of routine system requests. This includes functional system requests (product add/move/change), informational, and administrative requests.
- The Support Request SLO applies to issues that are not part of the standard operation of the service and which causes, or may cause, an interruption to or a reduction in the quality of that service.

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Micro Focus SaaS support teams. They in no way create a legal requirement or obligation for Micro Focus to always respond in the stated time.

## **12.3 Termination Data Retrieval Period SLO**

The Termination Data Retrieval Period is defined as the length of time in which Customer can retrieve a copy of

their Customer LoadRunner Cloud data from Micro Focus. Micro Focus targets to make available such data for download in the format generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term.

## 13. Standard Service Requirements

### 13.1 Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to LoadRunner Cloud. Micro Focus’s ability to fulfill its responsibilities relative to SaaS is dependent upon Customer fulfilling the responsibilities described below and elsewhere herein:

### 13.2 Customer Roles and Responsibilities

| Customer Role          | Responsibilities   |
|------------------------|--|
| <b>Business Owner</b>  | <ul style="list-style-type: none"> <li>• Owns the business relationship between the customer and Micro Focus</li> <li>• Owns the business relationship with the range of departments and organizations using LoadRunner Cloud</li> <li>• Manages contract issues</li> </ul>  |
| <b>Project Manager</b> | <ul style="list-style-type: none"> <li>• Coordinates customer resources as necessary</li> <li>• Serves as the point of contact between the customer and Micro Focus</li> <li>• Drives communication from the customer side</li> <li>• Serves as the point of escalation for issue resolution and service-related issues</li> </ul>           |
| <b>Administrator</b>   | <ul style="list-style-type: none"> <li>• Serves as the first point of contact for LoadRunner Cloud end user for problem isolation</li> <li>• Performs LoadRunner Cloud administration</li> <li>• Provides tier-1 support and works with Micro Focus to provide tier-2 support</li> <li>• Coordinates end-user testing as required</li> </ul> |

|                              |  |
|------------------------------|--|
|                              | <ul style="list-style-type: none"> <li>Leads ongoing solution validation</li> <li>Trains the end-user community</li> <li>Coordinates infrastructure-related activities at the customer site</li> <li>Owns any customization</li> </ul> |
| <b>Subject Matter Expert</b> | <ul style="list-style-type: none"> <li>Leverages the product functionality designed by Customer's LoadRunner Cloud administrators.</li> <li>Provides periodic feedback to the LoadRunner Cloud Administrator</li> </ul>                |

### 13.3 Micro Focus Roles and Responsibilities

| Micro Focus Role                             | Responsibilities   |
|--|--|
| <b>Service Operations Center Staff (SOC)</b> | <ul style="list-style-type: none"> <li>Primary point of contact for service requests. The customer can contact the Service Operations Center for all services such as support and maintenance, or issues regarding availability of LoadRunner Cloud</li> <li>Provides 24x7 application support</li> <li>Provides 24x7 SaaS infrastructure support</li> </ul> |
| <b>Operations Staff (Ops)</b>                | <ul style="list-style-type: none"> <li>Monitors the Micro Focus systems and LoadRunner Cloud for availability</li> <li>Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices</li> </ul>  |

### 13.4 Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- Customer must have internet connectivity to access LoadRunner Cloud
- LoadRunner Cloud will be performed remotely and delivered in English only
- A SaaS Order term is valid for a single application deployment, which cannot be changed during the SaaS Order term
- The service commencement date is the date on which Customer's purchase order (PO) is booked within the Micro Focus order management system
- The import of Customer data into the LoadRunner Cloud during the implementation requires that the information is made available to Micro Focus at the appropriate step of the solution implementation and in the Micro Focus designated format
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus



SaaS

- Customer has determined, selected, and will use options in the Customer environment that are appropriate to meet its requirements, including information security controls, connectivity options, and business continuity, backup, and archival options
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability

Furthermore, LoadRunner Cloud is provided based on the assumption that Customer will implement and maintain the following controls in its use of LoadRunner Cloud:

- Configuring Customer's browser and other clients to interact with LoadRunner Cloud
- Configuring Customer's network devices to access LoadRunner Cloud
- Appointing authorized users
- Configuring its LoadRunner Cloud account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications, and terminations

### **13.5 Good Faith Cooperation**

Customer acknowledges that Micro Focus's ability to perform the Services depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Micro Focus. Where this Service Description requires agreement, approval, acceptance, consent, or similar action by either party, such action will not be unreasonably delayed or withheld. Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Micro Focus in performing its obligations under this Service Description, Micro Focus will not be liable for such.