Service Description

OpenText™ Network Observability Private Cloud

May 2025

opentext™

Contents

This Service Description describes the components and services included in OpenText™ Network Observability Private Cloud (which also may be referred to as "SaaS") and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service ("SaaS Terms") found at https://www.opentext.com/about/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

OpenText™ Network Observability Private Cloud is a native cloud solution focused on providing end to end observability of customer networks both off-cloud and in multi-cloud environments delivered as a Private Cloud offering. "Private Cloud" means a single tenant environment dedicated to one customer where the computing, storage, and network resources are owned and operated by OpenText.

SaaS Delivery Components

SaaS Delivery Components and Capabilities (Use Cases)	Included
OpenText™ Network Observability Private Cloud production instance	✓
OpenText™ Operations Platform	✓
Private (VPN) connection	✓
OpenText™ Network Observability Private Cloud non-production instance(s)	O
Enhanced High Availability / Disaster Recovery (eHA/DR) deployment option	O
Discovery & Monitoring	O
Digital Experience Monitoring	O
Network Traffic Analysis	O
Monitoring for Change	O
Configuration Change	O
NetOps++ Compliance	O
Network Reporting	O
✓ **= Included**	
O **= Optional via purchasing additional units to provision service(s) or enable use case(s)**	

SaaS Operational Services

Operational Services	Included
Onboarding:	
Kick-off meeting, handover of product and support materials, verification of online access, scope validation and service goals, discussion of training requirements	✓
Customer Success Management (CSM) Meetings	✓
Product Support	✓
Service Health portal	✓
✓ **= Included**	
O = Optional for a fee	

Architecture Components

OpenText™ Network Observability Private Cloud infrastructure consists of two (2) parts:

- **OpenText™ Network Observability Private Cloud** which is a cloud native platform that can deliver network discovery, network monitoring, configuration monitoring, event management, configuration change ability, network device policy compliance, NetDevOps (Ansible and Git integration), analytics, dashboarding, insights, and reporting.
- **Micro Focus provided on-premise components** used to optimize the device communication from inside Customer's firewall or other customer managed networks back to the OpenText Network Observability Private Cloud.

Micro Focus deploys **OpenText™ Network Observability Private Cloud** using a dedicated infrastructure platform, monitors the system for 24x7 availability, and provides related 24x7 infrastructure support, including application version upgrades. Customer accesses OpenText™ Network Observability Private Cloud application through the Internet (HTTPS).

Operations Platform
The Operations Platform is included as part of the OpenText Network Observability Private Cloud deployed infrastructure. Operations Platform offers the following capabilities used by the OpenText Network Observability Private Cloud applications:

- Identity Manager: manages user identity, including authentication, authorization, and password policies.
- AutoPass: manages product licenses, server users, and client users centrally.
- OPTIC Data Lake: to use common datastore, powered by Vertica, with the framework to ingest large volumes of data from independent data sources, in different formats.
- Operations Cloud: visualizes content as interactive reports and dashboards. Configure the reports and dashboards by using the widgets provided within the framework.

With Operations Platform the applications within OpenText Network Observability Private Cloud can use these shared capabilities. Thus, saving resources and enhancing the common infrastructure scalability.

Micro Focus provided on-premise edge components include:

- Network Edge Observer (NEO) is an optional edge component used to optimize the communication with network devices where network discovery, monitoring, trap reception etc. can happen locally from inside Customer's network and consolidated output is send to OpenText™ Network Observability Private Cloud securely.
- Network Edge Observer QA (NEO QA) is an optional edge component used to enable Digital Experience Monitoring
- Traffic Leaf Collectors – is an optional component used to collect the flow data from network devices to enable traffic analysis in OpenText™ Network Observability Private Cloud
- Satellite (NA Satellite) is an optional component used to enable communication between on-premise components for the purposes of configuration management from inside the customer's firewall or other locations and OpenText™ Network Observability Private Cloud

Micro Focus does not install, deploy, or manage on-premise edge components in Customer's environment. Customer is responsible for installing, configuring, deploying, and updating for any components in the monitored environment. The documentation for integrating on-premise components with the OpenText™ Network Observability Private Cloud instance is available at:
https://docs.microfocus.com/doc/2206/25.2/install

The complete documentation of OpenText™ Network Observability Private Cloud is available at:
https://docs.microfocus.com/doc/2206/25.2/home

OpenText™ Network Observability Private Cloud needs a VPN connection to connect to on-premise edge components or any other 3rd party applications deployed on-premise to integrate with SaaS service. It is Customer's responsibility to enable any required VPN connections and work with Micro Focus SaaS Operations team to establish end to end connectivity.

Offering Capabilities:

OpenText Network Observability Private Cloud service offers variety of Use Cases as follows:

- Discovery & Monitoring
- Digital Experience Monitoring
- Network Traffic Analysis
- Monitoring for change
- Configuration Management
- NetOps++ Compliance
- Network Reporting

Customer can choose to enable any of the available Use Cases. Once the Use Case is provisioned, the Units cannot be reallocated to a different capability or Use Case.

The OpenText™ Network Observability Private Cloud Use Cases are defined as:

Use Case	Capability	Off Cloud Equivalence
Discovery & Monitoring	Discovery and monitor network devices for fault, availability, and performance leveraging patented "Spiral Discovery" with event correlation and Root Cause Analysis (RCA)	NNM Express
Digital Experience Monitoring	Monitor quality of network services using synthetic tests and alert on any quality degradations.	NNM Premium (iSPI QA)
Network Traffic Analysis	Analysis based traffic flow patterns in an enterprise that is being collected via the industry-standard NetFlow, JFlow, SFlow, and IPFIX traffic data capture methodologies.	NNM Premium (iSPI Traffic)
Monitoring for change	Provides multi-vendor device configuration discovery, backup, and snapshots for change analysis as well as the ability to perform runtime diagnostics and limited NetDevOps capability. The NetDevOps feature can be enabled for the Monitoring for Change Use Case with additional Unit consumption.	NA Express
Configuration Management	Includes all of the Monitoring for Change capability as well as the ability to update device software, make configuration changes, create change plans, access the full functionality of NetDevOps, and export data to the OPTIC DL for reporting, dashboards, incident workflows, and performance troubleshooting. The NetDevOps feature can be enabled for the Configuration Management Use Case with additional Unit consumption.	NA Premium
NetOps++ Compliance	Includes all of the capability of Monitoring for Change and Configuration Management Use Cases plus it provides the full policy and compliance capability to author policies, import and execute security and compliance content (CVEs), perform compliance auditing with auto remediation, and run compliance reports. The NetDevOps feature can be enabled for the "NetOps++ Compliance" Use Case with additional Unit consumption.	NA Ultimate, NetDevOps
Network Reporting	Network Reporting delivers OPTIC Data Lake, Dashboarding, Performance Troubleshooting and Reporting for the OpenText Network Observability Private Cloud offering for the Network Monitoring and Configuration management Automation Insights Use Cases and also available for receiving data from an on-premise instances of customer hosted Network Node Manager or Network Automation	NOM Reporting, NA Automation Insights

Product Structure:

The OpenText™ Network Observability Private Cloud product consists of two (2) types of SKUs:

- **OpenText™ Network Observability Private Cloud Foundation 2000 Unit ("Foundation SKU")**
  - The Foundation SKU is mandatory and a minimum one quantity is required for each deployment.
  - The Foundation SKU is provided as a subscription SKU
  - Provides entitlement to a total of 2000 Units

- **OpenText™ Network Observability Private Cloud Additional Unit ("Additional Unit SKU")**
  - If the deployment needs more than 2000 Units for capabilities selected and their scale, then additional Units can be purchased using the Additional Unit SKU.

- The Additional Unit SKU can be purchased during the initial purchase along with the Foundation SKU (if more are needed) or purchased at anytime in the future as long as the Foundation SKU has previously been purchased
- A minimum of 50 Units of Additional Unit SKU needs to be purchased anytime additional Units are required for the deployment.

The primary unit of measure for OpenText™ Network Observability Private Cloud purchase is a "Unit"

- **Unit** is a credit that enables network management capabilities and related capacity
- Units can be used with any Use Cases. Once the Use Case is provisioned, Units cannot be de-provisioned and reallocated to a different capability or Use Case

Deployment options and Unit consumption

The OpenText™ Network Observability Private Cloud provides two deployment options based on Customer's requirements:

- Low Foot Print (LFP)
  - OpenText™ Network Observability Private Cloud with Low Footprint (LFP) option provides the standard backup and recovery services from the Micro Focus SaaS Operations team as described below in this document.
  - With this option, there is no built-in HA and it is deployed with minimal required hardware and hence saves on the total number of Units required to enable Customer's Use Cases
- Enhanced HA/DR (eHA/DR)
  - OpenText™ Network Observability Private Cloud with Enhanced HA/DR (eHA/DR) is deployed with a more robust configuration than the "Low Foot Print (LFP)" deployment option above to provide resiliency of the underlying infrastructure, OpenText applications, and related data generated. As the eHA/DR deployment requires additional hardware and services as compared to LFP, it consumes an increased number of Units to enable the required Customer deployment option.
  - The Enhanced HA/DR option provides deployment of the OpenText™ Network Observability Network Observability Private Cloud across multiple Availability Zones (AZs) and select application components deployed in a High Availability (HA) mode configuration.

	Low Footprint (LFP)	**Enhanced HA/DR (eHA/DR)**
System Availability	99.9% Service Level Objective (SLO)	99.9% Target Service Availability (TSA) SLA

Units consumption per Use Case is calculated as follows:

Use Case and Deployment Option Units Consumption

Use Case	Low Footprint (LFP)	Enhanced HA/DR (eHA/DR)
Discovery and Monitoring	• 800 Units + 250 Units per 1000 Nodes*	• 1350 Units + 375 Units per 1000 Nodes*
Digital Experience Monitoring	• 300 Units + 10 Units per 100 probes	• 550 Units + 15 Units per 100 probes
Network Traffic Analysis	• Traffic Analysis Aggregate: 500 Units + 110 Units per 100 flow exporting Interfaces • Raw Traffic: 900 Units + 200 Units per 50,000 flow records/ minutes flow rate	• Traffic Analysis Aggregate: 800 Units + 350 Units per 100 flow exporting Interfaces • Raw Traffic Detail: 1700 Units + 650 Units per 50,000 flow records/ minutes flow rate
Monitoring for Change	• 350 Units per 1000 Nodes** • 20 Units per 100 Nodes enabled for NetDevOps	• 525 Units per 1000 Nodes** • 20 Units per 100 Nodes enabled for NetDevOps
Configuration Management	• 1000 Units per 1000 Nodes** • 40 Units per 100 Nodes enabled for NetDevOps	• 1500 Units per 1000 Nodes** • 40 Units per 100 Nodes enabled for NetDevOps
NetOps++ Compliance	• 2000 Units per 1000 Nodes** • 50 Units per 100 Nodes enabled for NetDevOps	• 3000 Units per 1000 Nodes** • 50 Units per 100 Nodes enabled for NetDevOps
Network Reporting	• 1600 Units for Reporting Platform • 500 Units per 1000 Nodes* with performance monitoring • 500 Units per 1000 Nodes** enabled for Automation Insights	• 4000 Units for Reporting Platform • 875 Units per 1000 Nodes* with performance monitoring • 875 Units per 1000 Nodes** enabled for Automation Insights

Nodes = For “Discovery and Monitoring” a node is defined as an addressable entity, physical or virtual, including but not limited to router, switch, bridge, hub, server, PC, laptops, handheld device or printer that resides within the range defined for interrogation and asset tracking. For “Monitoring for Change”, “Configuration Management”, and “NetOps++ Compliance” a node is defined as a managed Device (module) that has its own configuration for the purpose of being managed Network Observability Private Cloud. Note: Network Devices and Nodes are not always the same thing e.g. a switch (one Network Device) may have three nodes: one switching card, one routing card and one backup routing card.

* Usage should not exceed 6 performance polled interfaces, 15 sensors, and 1 custom collection for each Node. If usage exceeds the above, the number of Nodes will need to be adjusted to ensure that the average is within these limits and Units will be consumed accordingly.

** Usage should not exceed 5 tasks/ day on an average for each Node. If usage exceeds, the number of Nodes will need to be adjusted so the average is within these limits and Units will be consumed accordingly.

Usage of the following advanced features is not included and require additional Units:

- Firewall Deep Monitoring
- SD-WAN Tunnels
- SDN Overlays
- Traffic Subtypes
- Non-Default Polling Frequency
- Non-Default Extended Data Retention Period

Application Administration

Customer accesses OpenText™ Network Observability Private Cloud using a supported web browser and the URL provided to them. Micro Focus SaaS Operations team will create the necessary roles, groups and users for the customer to access OpenText Network Observability Private Cloud.

Users with administrative rights will be able to access select administration pages to configure OpenText™ Network Observability Private Cloud capabilities and to integrate data sources into OpenText Network Observability Private Cloud. Micro Focus reserves the right to determine which administrative features will be made available in the OpenText™ Network Observability Private Cloud instance.

Customer will open a ticket with Micro Focus SaaS Operations team to execute tasks such as, but not limited to, unlocking user accounts, CLIP integrations, customer provided business intelligence tools integration, on-premise software integration and attribute customizations.

Service Support

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

Online support for OpenText™ Network Observability Private Cloud is available at: https://pcs.saas.microfocus.com

OpenText™ Network Observability Private Cloud includes an extensive online contextual help to aid with tailoring and configuration of OpenText™ Network Observability Private Cloud to align with your business requirements. Full documentation of the capabilities of OpenText™ Network Observability Private Cloud and the optional capabilities outlined in this service description is available at: https://docs.microfocus.com/doc/2206/25.2/getstarted

As the OpenText™ Network Observability Private Cloud offering is part of the OpenText™ Network Operations Management community, you can get additional assistance and aid from your peers as well as get access to live and recorded webinars (practitioner forum series). OpenText™ Network Observability Private Cloud community is available at: https://community.microfocus.com/it_ops_mgt/nom/

Your suggestions for enhancements to OpenText™ Network Observability Private Cloud are important to us. We encourage you to share your ideas, vote for your favorite ones, and enhance existing ideas with your feedback and comments. The popularity of an idea is measured through votes and comments at: https://community-telligent.microfocus.com/it_ops_mgt/nom/i/nomideaexchange

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 OpenText Network Observability Private Cloud. Customer will maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal 24 hours a day, 7 days a week.

Assistance for the on-premise components will be provided through the standard support channels.

Activity	Included
Customer Success Management	✓
Email and Online Notifications	✓
On-boarding: **Kick-off meeting, handover of product and support materials, VPN connectivity, verification of online access, scope validation and service goals, discussion of training requirements**	✓
Version Updates: **Major version updates, minor version updates, patches, and security fixes. Notification period according to notification timelines via release notes and help resources available**	✓[1]
Service Reviews **Meeting reviewing service quality, and to provide feedback on improvements required**	Yearly
Assisting with the implementation/ configuration and tailoring	Available at additional cost
Availability SLO for Low Footprint deployment (LFP)	99.9% SLO
Availability SLA for Enhanced deployment (eHA/DR)	99.9% SLA
✓ **= Included**	

[1]*Notifications regarding release updates to the OpenText™ Network Observability Private Cloud will be provided via email.*

Service Monitoring

Micro Focus monitors the availability of OpenText™ Network Observability Private Cloud components deployed in SaaS 24x7. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages, and scheduled maintenance.

As part of OpenText™ Network Observability Private Cloud, we also include a Service Health portal for the SaaS-deployed components which allows the Customer to see:

- Current availability of the OpenText™ Network Observability Private Cloud environment
- Details of any upcoming planned maintenance
- Outage reports for any incidents that have been identified by our support teams
- Historical SLO data

The Link to Service Health portal for your tenant will be provided as part of your onboarding to Micro Focus SaaS. Details are also available via the support portal: https://pcs.saas.microfocus.com

Any required on-premise component, not within the sole control of Micro Focus, is Customer's sole responsibility. Micro Focus does not commit to any SLO for the on-premise components.

Capacity and Performance Management

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

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.

Data Backup and Retention

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

SaaS Data

Customer is solely responsible for the data, text, audio, video, images, software, and other content input into a Micro Focus system or environment during Customer's (and its Affiliates' and/or Third Parties') access or use of Micro Focus SaaS ("SaaS Data"). The following types of SaaS Data reside in the SaaS environment:

- Customer authorized user details (for instance, customer administrator users, operator users)
- Configuration information that may include credentials necessary for integrations with service management tools, customer provided business intelligence tools, certificates necessary to trust connectivity with on-premise OpenText™ Network Observability Private Cloud points of presence.
- Resulting information collected during product feature use such as events, topology, metrics, health indicators, KPI status.
- Reports, dashboards and reporting data
- Audit logs

Micro Focus performs a backup of SaaS Data every 6 hours. Micro Focus retains each backup for the most recent seven (7) days. The backup data is replicated to a protected vault within the same AWS Region as the Customer running service. The backup includes a snapshot of production database, including transactional database and analytics database, a copy of files stored on persistent volume and an export of all the Kubernetes objects.

Micro Focus' standard storage and backup measures are Micro Focus' only responsibility regarding the retention of the SaaS Data, despite any assistance or efforts provided by Micro Focus to recover or restore the SaaS Data. Customer may request via a service request for Micro Focus to attempt to restore SaaS Data from Micro Focus' most current backup. Micro Focus will be unable to restore any data not properly entered by Customer or lost or corrupted at the time of backup or if Customer´s request comes after the 7 days data retention time of such backup.

The OpenText™ Network Observability Private Cloud with Enhanced HA/DR (eHA/DR) deployment option is implemented over AWS technology service stack in a redundant mode over multiple Availability zones (AZs) with elastic load balancing allowing us to quickly recover service in case of a disaster. Availability zones (AZs) are distinct geographical locations that are engineered to be insulated from failures in other AZs.

Disaster Recovery for SaaS

Business Continuity Plan
Micro Focus continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, Micro Focus 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 SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that implements and tests SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

The OpenText™ Network Observability Private Cloud with Enhanced HA/DR (eHA/DR) deployment option is implemented using a cloud-based technology service stack in a redundant mode over multiple availability zones. The failure of one zone will not impact the service availability as the system will automatically failover from the other zones. In the event of a disaster impacting more than one zone at the same time, such as a complete cloud region, the DRP's target is to provide restoration of the OpenText™ Network Observability Private Cloud within 24 hours (Recovery Time Objective, RTO) following Micro Focus' declaration of a disaster.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability, and integrity of SaaS Data.

Technical and Organizational Measures

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.

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

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make 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
- 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 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"
- Prohibition of shared accounts

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' 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

Data Segregation

SaaS environments are segregated logically by 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.

Data Encryption

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

Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's execution of Micro Focus' 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 SaaS no more than once per year. Such information security questionnaire will be considered Micro Focus confidential information.

Micro Focus Security Policies

Micro Focus conducts annual reviews of its policies around the delivery of SAAS against ISO 27001, which includes controls derived from ISO 27034 – "Information Technology – Security Techniques – Application Security".

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.

Customer initiated security testing is not permitted, which includes application penetration testing, vulnerability scanning, application code testing or any other attempt to breach the security or authentication measures of the SaaS.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to reasonably 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 SED@opentext.com.

Micro Focus Employees and Subcontractors

Micro Focus requires that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of SaaS Data. Micro Focus requires that any affiliate or third party subcontractor involved in processing 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.

Data Subject Requests

Micro Focus will refer to Customer any queries from data subjects in connection with SaaS Data.

Scheduled Maintenance

To enable Customer 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) hour window (Scheduled to occur on Sunday in the 00:00 to 23:00 Greenwich Mean Time, the exact 2-hour time block is dependent on the location of the OpenText™ Network Observability Private Cloud instance) and one (1) monthly eight (8) hour window (Scheduled to occur on Sunday in the 00:00 to 23:00 Greenwich Mean Time, the exact 8-hour block is dependent on the location of the OpenText™ Network Observability Private Cloud instance). 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.

Scheduled Version Updates

"SaaS Upgrades" are defined as major version updates, minor version updates, and binary patches applied by Micro Focus to Customer's SaaS 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 during the applicable SaaS Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's SaaS. Unless Micro Focus anticipates a service interruption due to a SaaS Upgrade, Micro Focus may implement a SaaS Upgrade at any time without notice to Customer. Micro Focus aims to use the Scheduled Maintenance windows defined herein to apply SaaS Upgrades. Customer may be required to cooperate in achieving a SaaS Upgrade that Micro Focus determines in its discretion is critical for the availability, performance or security of SaaS.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, and Customer shall promptly return to Micro Focus (or at Micro Focus' request destroy) any Micro Focus materials.
Micro Focus will make available to Customer any SaaS Data in Micro Focus' possession in the format generally provided by Micro Focus. The target timeframe is set forth below in Termination Data Retrieval Period SLO. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted.

Service Level Objectives

Micro Focus provides clear, detailed, and specific Service Level Objectives (SLOs) for SaaS. These SLOs are targets used by Micro Focus to deliver the service and are provided as guidelines. They in no way create a legal requirement or obligation for Micro Focus to meet these objectives. OpenText Network Observability Private Cloud deployed in the Low Footprint (LFP) configuration option, provides SLO targets only.

Micro Focus will provide self-service access to Customer to the Service Level Objectives data online at https://pcs.saas.microfocus.com

1. **SaaS Provisioning Time SLO**
   SaaS Provisioning Time is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within five (5) business days of Customer's Order for SaaS being booked within the Micro Focus order management system.

   Customer is responsible for installing, configuring, deploying, updating and paying any additional fees (if required) for any additional on-premise components for its applications. Any on-premise components are not in scope of the SaaS Provisioning Time SLO.
   Additionally, the import of SaaS Data into the application is not in scope of the SaaS Provisioning Time SLO.

2. **SaaS Availability SLO**
   SaaS Availability is defined as the SaaS production application being available for access and use by Customer over the Internet. Micro Focus will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("SaaS Uptime". OpenText Network Observability Private Cloud deployed in the Low Footprint (LFP) configuration option provides SLO targets only.

3. **Measurement Method**
   SaaS 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, SaaS 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.

Boundaries and Exclusions
SaaS Uptime shall not apply to or include any time during which SaaS is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events
- 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 SaaS upgrades

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://pcs.saas.microfocus.com being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the 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 or include any time during which the SaaS support portal is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):
   - Overall Internet congestion, slowdown, or unavailability
   - Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks

- Force majeure events
- 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
- Scheduled SaaS Upgrades

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the support described herein. It is defined as the acknowledgment of the receipt of Customer's 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 Customer's request.

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 respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described at https://pcs.saas.microfocus.com.

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 SaaS 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.

Service Level Commitments

Micro Focus provides the following Service Level Commitments for the purpose of further measuring the quality of service that Micro Focus is delivering to the Customer.

1. **SaaS Availability SLA**
   SaaS availability is the SaaS production application being available for access and use by Customer over the Internet. Micro Focus will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("Target Service Availability" or "TSA") for the Enhanced HA/DR (eHA/DR) deployment option of OpenText Network Observability Private Cloud.

This SLA only applies to the Enhanced HA/DR (eHA/DR) deployment option for OpenText Network Observability Private Cloud and is not applicable to the Low Footprint (LFP) deployment option of OpenText Network Observability Private Cloud.

2. **Measurement Method**

TSA 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 TSA will be measured using the measurable hours in the quarter (total time minus Downtime Exclusions) 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.

3. **Downtime Exclusions**

The TSA shall not apply to or include any time during which SaaS is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Outages caused by disruptions attributable to force majeure events (i.e., unforeseeable events outside of Micro Focus' reasonable control and unavoidable even by the exercise of reasonable care
- Customer-caused outages or disruptions
- Outages not caused by Micro Focus or not within the control of Micro Focus (i.e. unavailability due to problems with the Internet), unless caused by Micro Focus' service providers
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance activities
- Scheduled SaaS Upgrades
- Customer exceeding the service restrictions, limitations or parameters listed in this Service Description and/or the Order
- Unavailability due to customizations made to the Micro Focus SaaS which are not validated, reviewed and approved in writing by both parties
- System downtime requested by Customer
- Suspensions of the Micro Focus SaaS by Micro Focus as a result of Customer's breach of the SaaS Terms

4. **Reporting**

Micro Focus will provide self-service access to Customer to the availability data online at https://pcs.saas.microfocus.com
In addition, Micro Focus will provide an Actual Service Availability Report ("ASA Report") in accordance with this Service Level Commitments section to Customer upon request. If Customer does not agree

with the ASA Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the ASA Report.

5. **Remedies for Breach of Service Levels**
   - **i. Sole remedy.** Customer's rights described in this section state Customer's sole and exclusive remedy for any failure by Micro Focus to meet the agreed service levels.
   - **ii. Escalation.** Quarterly ASA below 98% shall be escalated by both parties to the Vice President (or equivalent).
   - **iii. Credit.** Subject to the terms herein, Micro Focus will issue a credit reflecting the difference between the measured ASA for a quarter is less than the TSA. ("**Remedy Percent**"). For clarity, several example calculations using this formula are illustrated in the table below:

Target Service Availability (TSA)	Actual Service Availability	Result	Remedy Percent
99.9 %	99.9%		Not Applicable
99.9%	94.9%	5% missed	5%
99.9%	90.9%	9% missed	9%

Customer must request credits in writing to Micro Focus within ninety (90) days of receipt of the ASA Report resulting in such credit and identify the support requests relating to the period where the SaaS production application was not available for access and use by the Customer over the internet. Micro Focus shall apply the requested credits on a quarterly basis. Records and data shall be the basis for all service level remedy calculations. The credit paid will be calculated by multiplying the Remedy Percent by the Quarterly. These remedies or credits are not applicable to the Low Footprint (LFP) deployment option of OpenText Network Observability Private Cloud.

Standard Service Requirements

Roles and Responsibilities

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

Customer Roles and Responsibilities

Customer Role	Responsibilities
Business Owner	• Owns the business relationship between the customer and Micro Focus • Owns the business relationship with the range of departments and organizations using SaaS • Manages contract issues

Project Manager	• Coordinates customer resources as necessary • Serves as the point of contact between the customer and Micro Focus • Drives communication from the customer side • Serves as the point of escalation for issue resolution and service-related issues
Administrator	• Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Provides tier-1 support and works with Micro Focus to provide tier-2 support • Coordinates end-user testing as required • Leads ongoing SaaS validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site • Owns any customization
Subject Matter Expert	• Leverages the product functionality designed by Customer's SaaS administrators. • Provides periodic feedback to the SaaS Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Service Centre (CSC)	• 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 SaaS • Provides 24x7 application support
Operations Staff (Ops)	• Monitors the Micro Focus systems and SaaS for availability • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus' standard practices • Provides 24x7 SaaS infrastructure support

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 SaaS
- SaaS will be delivered remotely 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 Order is booked within the Micro Focus order management system
- The import of SaaS Data into SaaS 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
- 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, SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of SaaS:

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

Good Faith Cooperation

Customer acknowledges that Micro Focus' ability to provide SaaS and related 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 failure or delay.