1. **OpsCare.** OpsCare includes access to Operational Onboarding and Operational Services under Cloud Operations Services.

2. **Cloud Operations Services**

2.1. **Operational Onboarding.** Operational Onboarding prepares Customer's cloud platform and personnel for Operational Services with the activities in Table 2.1, Operational Onboarding Activities.

Table 2.1, Operational Onboarding Activities

Activities	Description	MCP
Operational Readiness	• Setup and verification of Remote Access for the Operational Services team; • Mirantis Portal account creation for the Operational Services team; • OSS and Mirantis Portal coordination; • Review of the final configuration of OSS; and • Mirantis Portal account creation for Customer cloud administrators.	✓
Customer Orientation	• Create and review a Customer "Cloud Orientation Document" that includes the following information: o OpsCare roles and responsibilities, o Service management processes and flows, o How to contact the Operational Services team, o Customer contacts for Incident and non-Emergency change notification and approval, o Customer "on call" contacts for critical issues and emergency maintenance approval, o Approved maintenance window schedules, and o Escalation processes and contacts; and • Mirantis Portal training for Customer identified accounts (i.e. cloud administrators).	✓
Handover	The transition from a Mirantis Software deployment to Operational Services which includes: • Transfer of documentation of the cloud platform environment (e.g., deployment specifics, network diagrams, Bill of Materials, asset list) to the Operational Services team; and • Creation of internal technical wiki.	✓
Cloud Review	For a deployed MCP Software cloud: • Review the final configuration of OSS; and servers, storage, and network configurations; • Apply MCP Software maintenance updates, if applicable and available; and • Conduct: o Automated checks that execute basic cloud operations as well as verifying OpenStack API functionality, o Testing of the control plane for High-Availability ("**HA**"), and o Review of MCP Software functionality.	✓

Note: Operational Onboarding does not include (a) Integration with Customer's service desk tools except for sending automatic email notifications from Mirantis Portal when the services records are created or updated; or (b) Integration with Customer operations systems other than providing "view access" to Mirantis OSS and data.

2.2. Operational Services. Operational Services includes access to Operational Services Activities; Operational Services Desk for Incident Management, and Service Requests and Change Management; Customer Success Manager; and Cloud Services Availability Management with Monitoring.

2.2.1. Operational Services Activities. Operational Services Activities are described in Table 2.2.1, Operational Services Activities.

Table 2.2.1, Operational Services Activities

Activities	Operational Activities Description	MCP
MCP Software Monitoring	MCP Software logging, monitoring and alerting for MCP Software cloud services (e.g., Nova, Keystone, Cinder, Glance, Horizon, and Heat) API's; and, depending on components (devices Central Processing Unit ("CPU"), disk, memory, I/O and processes, etc.) using Mirantis OSS toolchain. Includes MCP Software anomaly and fault detection, MCP Software services events and logs correlation, and time series metrics collection and aggregation.	✓
Environment events, Incident & problem management	Manage Mirantis Software environment orchestration events, alerts, and tickets in Mirantis Portal using Incident management and problem management procedures for Mirantis Software services (i.e., Nova, Keystone, Cinder, Glance, Horizon, and Heat).	✓
Software Configuration & Deployment Management	Manage Mirantis Software maintenance updates planning, tests and execution, operating system patches, and Mirantis Software configuration changes described in Section 2.2.2.2	✓
MCP Software Upgrade	Upgrade planning and reviews to identify DriveTrain based updates including at least 1 upgrade to the OpenStack and/or Kubernetes software once per 12-month Subscription Services term. *Note: MCP Software Upgrade(s) are non-disruptive but may require multiple maintenance windows.*	✓
Monthly Reporting	Overview of the Operational Services Activities including information such as: • Cloud services availability metrics: o Control Plane API Availability, and o Compute & Storage Resources usage. • Service desk ticket records and trends: o Operational Service Desk records creation, closure, response, and resolution time, and o Change requests and maintenance windows.	✓

2.2.2. Operational Services Desk. The Operational Services Desk is made available using Mirantis Portal using Information Technology Infrastructure Library ("**ITIL**") based practices to provide access to the following:

2.2.2.1. Incident Management. Incident management assists Customer with recovery from, or prevention of, an interruption in service within the scope of OpsCare (an "**Incident**"). Incident management severity Level and Response for OpsCare is as shown in Exhibit A, Mirantis Subscription Services. Customer may report Incident(s) using the submission of a support ticket process for Mirantis Subscription Services through the Mirantis Portal. Within 5 business days of a Severity 1 Incident resolution affecting services in OpsCare, Mirantis will provide Customer with a root cause analysis ("**RCA**") report with status of triage including a probable or determined root cause. This report may include any remaining steps to confirm the root cause and, when appropriate, recommendations for future Incident prevention. Customer may request RCA information for Severity 2 Incidents and Mirantis will apply commercially reasonable efforts to provide it within 5 business days of Incident resolution. As required by Mirantis, and based on the Incident, Mirantis will escalate issues to the Customer's infrastructure service provider or Customer's data center operations contacts. Customer shall be responsible for obtaining, maintaining, and complying with the terms for all such maintenance agreements with such 3rd party support provider(s) and ensuring that such maintenance agreements allow Mirantis to escalate issues to relevant 3rd party support provider(s) on behalf of the Customer.

2.2.2.2. Service Requests and Change Management

a. Service Requests. A service request is a support request that may require changes to Customer's system(s) or Mirantis Software configuration. Request to modify or change Mirantis Software code relating to feature enhancement or new functionality are not included in the scope of the Operational Services.

b. Change Management. Mirantis provides the controlled identification and implementation of changes with the Customer's Mirantis Software environment within the scope of Operational Services as described directly below (each a "**Change**" or together, "**Changes**"). Changes are further defined as follows:

Changes	Description
Standard Change	Pre-authorized changes that are low risk, relatively common, and involve changes to OSS tooling monitoring, and alerting.
Normal Change	Planned changes to infrastructure supporting the service (disruptive or non-disruptive). For example, MCP Software maintenance updates, cloud platform patches, and host Operating System patches. A Normal Change follows the defined steps of this standard Change Management process.
Emergency Change	Changes that must be introduced as soon as possible outside of the approved maintenance schedule. This type of change may be necessary to reduce risk of potential service interruption or to address a Severity 1 Incident.

Unless a Change is identified by Mirantis as an Emergency Change, all changes will be available during the approved maintenance windows, which are defined during Operational Onboarding and documented in the Cloud Orientation Document.

For planned and Emergency Changes, Mirantis will provide Customer a maintenance plan that may include, for example, impact, execution steps, test procedures, a rollback plan (if applicable), and an estimate of the resources (e.g. time, effort) likely needed to apply the Change. Change Management status is available to Customer through the Mirantis Portal. For Changes that may be disruptive to Mirantis Software environment, Customer is responsible for providing written (i) approval for Changes prior to making the Change; and (ii) validation of the Change after implemented, using Mirantis Portal. Mirantis Software Upgrades and updates to the Customer's Mirantis Software environment are available using the Change Management process. Mirantis Software Upgrades and updates are limited to the Mirantis Software under OpsCare. Mirantis Software Upgrade(s) may require longer maintenance window execution and Customer resources for upgrade planning, assessment, testing, and validation. Mirantis Software Upgrade(s) do not include the maintenance of software of any custom pipelines, formulas, or any custom extension of Mirantis Software that were developed as part of separate services engagements.

2.2.3. Customer Success Manager. A Customer Success Manager will become familiar with the Customer's technical environment, business objectives, Mirantis Software roadmap, coordinate support services, and the following:

a. Assist with the development and maintenance of Customer plans that outline the critical factors, metrics, potential issues, and action plans;
b. Coordinate monthly operations reviews;
c. Establish meetings with Mirantis product team personnel to review status and action plans for open cases, on an if and when available basis;
d. Be the Customer's single point of contact for support services, to help drive critical issue management, escalation and resolution;
e. Coordinate access to community and Mirantis product team. Communicate Customer's position(s) for inclusion in future OpenStack software/product releases;
f. Provide guidance in Mirantis Software life cycle planning and coordinate impact analysis and approval of change requests; and
g. Inform Customer on key new features/fixes and assist with planning for new releases of Mirantis Software.

The Customer Success Manager is available during Business Hours (9:00 a.m. through 5:00 p.m. Monday-Friday) in the time zone in which the control plane is installed or the primary location of usage if installed in multiple time zones.

2.2.4. Cloud Services Availability Management

2.2.4.1. Monitoring. Operational Services include cloud services availability monitoring and alerting services 24 hours a day during the OpsCare Subscription Services term using the Mirantis OSS toolchain. Mirantis OSS operations framework is used as a flexible Service Level Objectives ("**SLO**") composition tool for Mirantis Software. SLOs are composed from Quality of Service ("**QoS**") measurements that are combined to produce a global (or macro) SLO achievement value. For example, the availability SLO for the control plane depends on the SLO of multiple components, resources, and services, each of which having their own QoS availability measurement. The Mirantis OSS toolchain combines and correlates QoS measurements of different components into one macro SLO achievement value. QoS availability measurements are reported according to five different states:

QoS States	Description
Down	One or several primary functions of a service have failed. Meaning, the OpenStack, or Kubernetes service is no longer accessible.
Critical	One or several primary functions of an OpenStack, or Kubernetes service are in critical state, meaning that the QoS can be severely degraded. It can also be indicative of a critical condition that must be immediately addressed.
Warning	One or several primary functions of an OpenStack, or Kubernetes service are slightly degraded meaning that the QoS can be slightly degraded. It can also be indicative of an anomaly that should be addressed.
Unknown	There is not enough data to infer an opinion about the availability state of an OpenStack, or Kubernetes service.
Okay	None of the above.

Using the global state evaluation aggregation and correlation mechanisms of the Mirantis OSS, QoS measurements are combined to produce macro availability SLO achievement value for the control plane. The control plane SLO achievement value is "Down" when OpenStack, or Kubernetes service is reported as "Down" or "Unknown"; or "Up" when OpenStack, or Kubernetes service is reported as "Critical", "Warning", or "Okay". Mirantis records and data are the basis for all availability calculations and determinations. Mirantis will generate an event ticket for each availability alert issued to Mirantis' Operational Services support engineers.

3. OpsCare Service Level Assurance

3.1. Control Plane API Monthly Availability

3.1.1. Control Plane APIs. Mirantis provides a service level assurance for the OpenStack Application Programming Interfaces ("**API**" or "**APIs**"), and Kubernetes APIs in the MCP Software control plane ("**Control Plane API**") under Operational Services. If the Control Plane API(s) are not available as shown in Table 3.1.2, Monthly Availability, Control Plane API service level credits ("**Credits**") are available to Customer as provided in Section 3.

3.1.2. Monthly Availability. Mirantis will measure the Monthly Availability of the Control Plane APIs using the Mirantis OSS installed and configured as part of OpsCare Subscription Services. Monthly Availability of the Control Plane API is calculated as Downtime during each month, as follows (represented as a percentage): 1- (Downtime (minutes) / month (minutes)). Monthly Availability of the Control Plane API is measured separately for all Control Plane APIs. Monthly Availability measured for Multi-Region requires all physically distinct fault domains with no single point of failure or shared resource between all cloud regions to have Downtime. "**Downtime**" means a period of five (5) consecutive minutes during which (i) Compute (Nova), Networking (Neutron), Image Service (Glance), Identity (Keystone), or Block Storage (Cinder) core OpenStack service APIs for the OpenStack API(s); or (ii) Kubernetes API (provided by kube-apiserver) for the Kubernetes API(s), is unreachable or requests are timing out. Downtime does not include periods during which the Control Plane API endpoint is unreachable or requests are timing out that are intermittent (e.g. less than 5 minutes); the result of Mirantis performing maintenance on the services during a maintenance window; or when services respond with any error code. Downtime does not include periods during which a Control Plane API is unreachable or requests are timing out when: caused by factors outside of Mirantis' reasonable and direct control, including any force majeure events, network access, delayed access or unavailability of logical access to Customer

systems, or related problems beyond the demarcation point of OpsCare; resulting from any actions or inactions of Customer or any third party; planned maintenance; acts of the Customer, its contractors, subcontractors, and/or agents; network underlay services unavailability; or resulting from Customer equipment, software, or other technology and/or third party equipment, software, or other technology (other than third party equipment within Mirantis' direct control). Credits may be available to Customer based upon the Monthly Availability and Credit Percentage in Table 3.1.2, Monthly Availability. "**Single-Region**" means a full set of OpenStack and/or Kubernetes services running in one (1) physically distinct fault domain. "**Multi-Region**" means a full set of OpenStack services or Kubernetes services in two (2) or more physically distinct fault domains with no single point of failure or shared resource between any cloud region. Each Multi-Region consists of only one of either OpenStack services or Kubernetes services.

Table 3.1.2, Monthly Availability

Monthly Availability	MCP Multi-Region Credit Percentage	MCP Single-Region Credit Percentage
100% - 99.99%	None	None
< 99.99% - 99.9%	10%	None
< 99.9% - 99%	20%	15%
< 99%	30%	30%

Note: In addition to OpsCare Assumptions and Customer Responsibilities, requirements for Credit(s) eligibility are as follows: (a) Customer is responsible for datacenter facilities, hardware, network underlay management and network monitoring, and related 3rd party software management and operations such as 3rd party Software Defined Network not defined in the Standard Configuration, or 3rd party Storage solutions not defined in the Standard Configuration; (b) Customer is responsible for underlying software failures; and (c) Customer shall purchase 24 x 7 / 365 support, facilitate data center remote-hands, and parts replacement for all hardware and 3rd party software components on which the MCP Software cloud depend and that are not provided with OpsCare.

3.1.3. **Conditions.** OpsCare Service Level Assurance will not apply (a) in the event that Customer opts-out of using the Mirantis monitoring tool set for Operational Services or disables, blocks, removes, or otherwise interferes with Mirantis OSS monitoring and components of the control plane; or (b) if Customer chooses to use configurations and 3rd party software that are not the Standard Configuration.

3.2. **Credits.** Mirantis will monitor the Monthly Availability of the Control Plane API and Credits will be calculated by taking the Credit Percentage for the applicable Monthly Availability percentage in Table 3.1.2, Monthly Availability, multiplied by 1/12th Customer's annual OpsCare Subscription Services Fee for each month during the Subscription Services term. If entitled, Credits may be applied to an OpsCare Subscription Services renewal under the following conditions:

- **a.** Customer shall request application of Credit(s) within thirty (30) days of the Monthly Reporting ("**Credit Period**");
- **b.** Credit(s) requested after the Credit Period will be forfeited;
- **c.** Notwithstanding anything to the contrary, the maximum total Credit for each month shall not exceed 30% of 1/12th Customer's annual OpsCare Subscription Services Fees paid for the affected MCP Software cloud t; and
- **d.** Credits are Customer's sole and exclusive remedy for Control Plane API unavailability and any Mirantis Software OpsCare Subscription Services issues.

4. **OpsCare Assumptions and Customer Responsibilities.** The following are assumptions and Customer responsibilities for OpsCare. Should Customer not be able to carry out any Customer responsibility or obligation or should any assumption set out or referenced in this Attachment 1 prove to be invalid, Mirantis will not be able to provide OpsCare Subscription Services as described herein and will be entitled to appropriate relief including, but not limited to, adjusting response times of applicable services, adjusting the timing of providing any services, charging Customer of a time & materials basis.

4.1. **Remote Access.** Customer shall enable, grant, and secure physical Remote Access to Customer's cloud facility for OpsCare. Remote Access requires that Customer provides "datacenter remote hands"; and a highly available remote access gateway to allow the Mirantis Operational Services team to connect to the Customer environment. Remote

Access shall be available over the public internet either via VPN or directly as a "point-of-entry" for Mirantis OSS tooling and support. Specifically, the Customer will provide Remote Access via VPN or direct SSH to the hosts being provisioned. For Remote Access, Customer will provide Mirantis with necessary access to all key hardware and software resources that are a part of OpsCare prior to Mirantis Software deployment. Please note that initial deployments cannot be performed using remote desktop tools such as WebEx, GotoMeeting, TeamViewer, etc. For Remote Access, Customer shall grant administrative (root and cloud administrator) level access to the managed MCP Software cloud to the Operational Services team. Customer Remote Access shall be provided to Mirantis within 15 minutes of emergencies identified by Mirantis. The Service Level Assurance does not apply when Remote Access is, for any reason, not available, denied, or is inaccessible due to events that are not managed by or within direct control of Mirantis. Customer will ensure Mirantis has access to, or receives information or data, that only requires standard commercial confidentiality coverage.

4.2. Operational Onboarding. Customer will provide the following:

a. 3rd party support agreement points of contact, including contact information, with whom Mirantis will coordinate to provide OpsCare Subscription Services, and other associated operational and support details for such 3rd party support;
b. Customer points of contact, including contact information, for critical issues and emergency maintenance approval; and
c. Approval for Changes as follows:

Change	Recommended	Required
Standard	Daily	Weekly
Planned, non-disruptive	Daily	Weekly
Planned, disruptive	Weekly	Monthly

4.3. MCP Software Staging Environment. The MCP Software Staging Environment shall be (i) sufficiently representative of the associated production cloud environment and used by Customer; and (ii) used only by Mirantis under OpsCare Subscription Services; Customer use is secondary to Mirantis Subscription Services use.

4.4. Operational Services. The following are the responsibility of Customer and/or Customer's third-party provider:

a. Datacenter and Facilities Management. Manage physical access, redundancy (e.g., UPS, generators), climate control, fire suppression, and all other environmental controls. Manage "data center remote-hands".
b. Hardware Support and Parts Replacement. Manage and support infrastructure hardware, parts replacements, and/or hardware manufacturer/reseller communications. *These Customer activities are required and should be carefully coordinated with the Operational Service team.*
c. Network Underlay Management. Administer and monitor all underlay networking devices, access to the internet and associated services (e.g. core, distribution and access networks, firewalls, load balancers, access policies, access control lists, and VPN access gateways).
d. Tenants Support & Tenants Administration. Management of tenants, tenant user accounts, tenant images, volumes, instances etc. These administrative tasks are performed through Kubernetes or OpenStack Graphical User Interface or the appropriate API services for MCP Software. These are the responsibility of Customer's administration team or Customer tenant administrators.
e. Workloads Management. Manage workloads, deployments, setups, administration, monitoring, performance, availability, backup, and/or recovery.
f. Information Security and Risk Management. Perform internal and external security scans, analysis and penetration testing on cloud platform, cloud applications, and cloud infrastructure. Manage information security risks and audits.
g. Customer Premises, Equipment, & Devices
  1. Equipment and installation must meet the following criteria prior to any deployment of MCP Software:
     - Hardware devices must be supported on the Canonical Ubuntu HCL;
     - Hardware "bill of materials" or BoMs must meet minimum criteria on the Mirantis Standard Configuration for Subscription Services and OpsCare at https://docs.mirantis.com; and
     - Deployment of the Hardware infrastructure must meet criteria specified in infrastructure readiness checklist
  2. The management and support of the physical devices and underlay network remains the responsibility of the Customer or the Customer infrastructure service provider. These infrastructure support operations are tightly coordinated with Operational Services through disciplined Change Management. Device operations are subject

to the operating characteristics of the device and the infrastructure service provider support agreement (e.g., SLA and parts replacement policy). Mirantis deploys control plane services in a redundant configuration to help maintain high availability. Mirantis will work with the Customer's IT Operations or the Customer infrastructure service provider to identify failed hardware components and help remediate impact on cloud services.

3. Mirantis will use commercially reasonable efforts to maintain services availability of the cloud infrastructure components. If a hardware device is not operating properly Mirantis will engage with the Customer infrastructure service provider contact to assist with Cloud Operations Services related to the device replacement within a commercially reasonable time period. Customer is responsible for managing and maintaining all support and service agreements for such devices. Since control plane is setup in HA, Customer will, under normal circumstances, be able to operate during a control plane partial failure without affecting overall infrastructure services. In the event of multiple device failures, Mirantis will endeavor to maintain cloud services but cannot guarantee that the cloud services will be available, depending on the failure scenario.