Canonical

Ubuntu Pro Description

Valid since: 9 November 2023

Ubuntu Pro is a subscription that gives you an additional stream of security updates and packages that meet compliance requirements, such as FIPS or FedRAMP, on top of an Ubuntu LTS. It can also include expert support for *troubleshooting*, *break-fix* and *bug-fix* on the full open-source stack or on its subset (Infra-only).

As a customer, you are entitled to the following coverage, depending on the appropriate support level on a per-machine basis.

Each subscription can cover one or more:

1. **Physical server:** The subscription is attached to a physical host. If all physical hosts in the *production environment* are covered, then the Ubuntu Pro subscription also covers all *Ubuntu Guests* on those hosts and the subscription can be attached to those *Ubuntu Guests*.
2. **Virtual:** The subscription is attached to a Virtual Machine running on a hypervisor or *Ubuntu Certified Public Cloud*
3. **Desktop:** The subscription is limited to a machine with *Desktop use cases*. It can also cover Ubuntu on *Windows Subsystem for Linux* (WSL) and developer tools such as MicroK8s and Multipass

Each subscription can be purchased at one of three support levels:

1. **self-support** (previously known as Essential)
2. **support (weekday)** (previously known as Standard)
3. **support (24/7)** (previously known as Advanced)

and must cover all Ubuntu systems within a *production environment*.

Additionally, the subscription might cover the full stack (**Ubuntu Pro**), or a subset of the stack: just the infrastructure (**Ubuntu Pro (Infra-only), previously known as Ubuntu Advantage for Infrastructure)**. Unless otherwise stated, a subscription will be Ubuntu Pro.

Detailed pricing can be found at: https://ubuntu.com/pricing/pro

Ubuntu Pro subscriptions are governed by the terms at

https://ubuntu.com/legal/ubuntu-pro-service-terms unless otherwise agreed in writing with Canonical.

Table of Contents

Security and compliance

As an Ubuntu Pro or Ubuntu Pro (Infra-only) customer, with or without support, you are entitled

to the following:

1. Expanded Security Maintenance (*ESM*)

    1.1. Available *CVE fixes (high and critical)* and selected medium CVE fixes for a number of packages, as specified below
    1.2. Ubuntu Pro and Ubuntu Pro (Infra-only) subscriptions cover packages in the *Ubuntu Main* repository between End of Standard Support and End of Life (esm-infra)
    1.3. Only Ubuntu Pro subscriptions covers packages in the *Ubuntu Universe* until End of Life (esm-apps). This coverage is not included in Ubuntu Pro (Infra-only) subscriptions
    1.4. *ESM* does not guarantee:
        1.4.1. Fixes for architectures other than the *Covered Architectures*
        1.4.2. *Bug-fixes*, unless a bug was created by an ESM security fix
        1.4.3. A guarantee to fix all High or Critical *CVEs*

2. Other security fixes

    2.1. Security fixes for OpenStack, Ceph, MAAS, Kubernetes
    2.2. Available *High, Critical CVE* and selected medium fixes for a number of core ROS packages for ROS 1 Kinetic and Melodic, and ROS 2 Foxy. This includes packages in the REP-142 'ros_base'

3. Certified components for compliance, hardening and audit

3.1. FIPS 140-2 Level 1 certified modules for Ubuntu 20.04 LTS, 18.04 LTS and 16.04 LTS
3.2. FIPS 140-3 Level 1 certified modules for Ubuntu 22.04 LTS (coming soon)
3.3. Access to certified CIS Benchmark tooling Levels 1 and 2 for Ubuntu 18.04 LTS and 16.04 LTS
3.4. Ubuntu Security Guide (USG) for Ubuntu 20.04 LTS which includes certified DISA-STIG profiles and CIS benchmark tooling Levels 1 and 2
3.5. Ubuntu Security Guide (USG) for Ubuntu 22.04 LTS which includes CIS benchmark tooling Level 1 and 2 (DISA-STIG profile coming soon)
3.6. Common Criteria EAL2 for Ubuntu 18.04 LTS and 16.04 LTS

4. Kernel Livepatch

4.1. Access to Canonical's kernel livepatch client and security livepatches for selected High and Critical kernel CVEs

4.2. Kernel Livepatch may provide non-security bug fixes as kernel livepatches
4.3. Only Livepatch Covered Kernels are available for livepatching.
4.4. Access to Canonical's Livepatch on-prem server

5. Access to other services

5.1. Access to the real-time kernel maintained by Canonical for Ubuntu 22.04 LTS with the upstream 5.15-rt patches integrated is provided to meet the low latency requirements
5.2. Access to Canonical's Landscape systems management tool
5.3. Access to the support portal and Knowledge Base

Support

You can add different levels of technical support on top of your infra-only or full Ubuntu Pro subscription. All levels of support are available as a weekday or 24/7 service.

6. Scope of Support

6.1. Included in all scopes
6.1.1. Certified hardware, including certified public cloud instances
6.1.1.1. Ubuntu Certified hardware has passed Canonical's extensive testing and review process. More information about the Ubuntu certification process and a list of certified hardware can be found on the Ubuntu Certification page
6.1.1.2. Full support applies only with respect to the customer's hardware that has been certified. In the event a customer requests the services with respect to hardware, which is not certified, Canonical will use reasonable efforts to provide support services, but may not adhere to the obligations described in this service description
6.1.2. Ubuntu releases
6.1.2.1. *Break-fix Support* for troubleshooting and usage, standard installation, configuration, and maintenance of all packages in the *Ubuntu Main* repository of an Ubuntu LTS release when installed using official sources and within the Ubuntu lifecycle

6.1.3. Supported Services

6.1.3.1. Additional packages, kernels and services are within the scope of support:

6.1.3.1.1. Packages in the Ubuntu Cloud Archive
6.1.3.1.2. Supported Kernels
6.1.3.1.3. Landscape client
6.1.3.1.4. Kernel Livepatch
6.1.3.1.5. Packages and profiles for FIPS, DISA-STIG and Common Criteria EAL2 provided by Ubuntu Pro

6.1.3.2. Support is not provided for any packages that have been modified by the customer or third parties

6.1.4. Ubuntu Assurance Program

6.1.4.1. Ubuntu Pro + support customers are entitled to the Ubuntu Assurance Programme. Canonical may update the Assurance Programme and its terms periodically

6.2. Infra-only support

6.2.1. Kubernetes, as defined in 7.1
6.2.2. OpenStack, as defined in 7.2
6.2.3. Ceph Storage, as defined in 7.3
6.2.4. MAAS, as defined in 7.4
6.2.5. LXD, as defined in 7.5
6.2.6. MicroCloud, as defined in 7.6
6.2.7. All packages in *Ubuntu Main*
6.2.8. LTS Ubuntu base images at https://hub.docker.com/_/ubuntu/, https://gallery.ecr.aws/lts/ubuntu

6.3. Ubuntu Pro + Support includes the following in addition to infra-only support:

6.3.1. All packages in *Ubuntu Universe*, starting with 18.04 LTS and onwards
6.3.2. Canonical-maintained applications published in the “stable” channel:

6.3.2.1. OCI-compliant application images listed in https://github.com/orgs/canonical/packages?ecosystem=container&tab=packages&ecosystem=container&q=charmed-, hub.docker.com/u/ubuntu/ and gallery.ecr.aws/ubuntu

6.3.2.1.1. Container images are made of multiple layers. The Ubuntu Pro maintenance and support scope is limited to layers with unmodified and up-to-date supported content

6.3.2.1.2. Where images are composed of additional layers, Canonical’s coverage will be limited to the Canonical-maintained Ubuntu container image layers and any packages installed from the *Ubuntu Main* and *Universe* repositories

6.3.2.1.3. Support exclusions

6.3.2.1.3.1. Outdated images: Canonical publishes “stable” channel content via OCI registry image tags, for each supported track. A track is typically associated with an Ubuntu LTS release; where the Canonical-maintained Ubuntu container image includes a specific application, the track may also be associated with an application version. Only the latest stable content is eligible for support under Ubuntu Pro. Any content that is not aligned with one of the available “stable” channel content tags for the given Canonical maintained Ubuntu container image is not considered the latest stable content

6.3.2.1.3.2. Third party software: Canonical may refuse to provide support for issues caused by software in the container image, a container orchestration platform or host operating system if the software, container orchestration platform or host operating system are provided by a third party and not maintained by Canonical

6.3.2.2. Canonical maintained snaps listed at https://snapcraft.io/publisher/canonical

6.3.2.3. Canonical maintained *charms* listed in Charmhub.io

6.3.2.4. Additional applications listed at https://ubuntu.com/support

7. Supported Products

7.1. Kubernetes

7.1.1. Kubernetes installations deployed via:

7.1.1.1. Charmed Kubernetes

7.1.1.2. MicroK8s

7.1.2. A kubeadm-deployed cluster of unmodified upstream Kubernetes binaries as published by the CNCF, deployed on Ubuntu as base OS, as long as Ubuntu is deployed using the official Canonical image repository

7.1.3. Support must be purchased for all *Nodes* in the supported Kubernetes cluster

7.1.4. Supported versions of Kubernetes include:

7.1.4.1. Weekday or 24/7 Support for N-2 (the latest and previous two) releases in the “stable” release channel

7.1.4.2. *ESM* security patching for N-4 (the latest and previous four) releases in the "stable" release channel

7.1.5. For any deployment of *Charmed Kubernetes* carried out by Canonical while under contract for a deployment, which results in the customisation of any *Charms*, those custom charms will be supported for 90 days after the release of new versions of the charms containing the customization. All software, including charms, snaps, images and debs required to deploy Kubernetes is covered by *bug-fix* and *break-fix support*

7.2. OpenStack

7.2.1. Full Support for OpenStack deployments is limited to Charmed OpenStack and MicroStack

7.2.2. The duration of Full Support depends on the OpenStack product being used and the installed software version. Please refer to the OpenStack release cycle page for detailed information on supported products and versions

7.2.3. Charmed OpenStack requirements:

7.2.3.1. Hardware must meet the minimum criteria as specified by Canonical as part of the Private Cloud Build or Cloud Validation consulting engagements

7.2.3.2. Deployment was done by Canonical via Private Cloud Build or it was validated by Canonical through Cloud Validation

7.2.4. MicroStack requirements:

7.2.4.1. Hardware must meet the minimum criteria as specified in MicroStack documentation

7.2.4.2. The OpenStack Cloud was deployed with MicroStack

7.2.5. OpenStack support includes access to Canonical-provided Microsoft-certified drivers in Windows virtual machine instances

7.2.6. OpenStack support requires all *nodes* that participate in the OpenStack deployment to be covered under an active support agreement

7.2.7. Scope of OpenStack support:

7.2.7.1. *Charms* used for deployment

7.2.7.2. All Canonical-provided packages, Canonical-maintained snaps and OCI images required to deploy and run OpenStack

7.2.7.3. Incidents found during the upgrades between major versions of OpenStack or LTS versions of Ubuntu, Juju, and MAAS are supported as long as the upgrade is performed. Incidents found during the upgrades between major versions of OpenStack or LTS versions of Ubuntu, Juju, and MAAS are supported as long as the upgrade is performed following a documented process as

specified by Canonical as part of the Private Cloud Build, or Cloud Validation Package or MicroStack documentation

7.2.8. Limited OpenStack Support

7.2.8.1. OpenStack clouds not deployed through Private Cloud Build or MicroStack, or validated through Cloud Validation Package are limited to *Bug-fix Support*

7.2.8.2. OpenStack support does not include support beyond *Bug-fix Support* during the deployment or configuration of an OpenStack cloud

7.2.9. Exclusions

7.2.9.1. Full Stack Support excludes customisations which are not considered Valid Customisations or are not covered in MicroStack documentation

7.2.9.2. Support for workloads other than those required to run an OpenStack deployment

7.2.9.3. Full stack support for virtual machine instances other than *Ubuntu Guests*

7.2.9.4. Support for incidents and performance degradations resulting from decisions made when self-deployed by the customer and not validated by Canonical or including customizations that are not *valid customization*

7.3. Ceph Storage

7.3.1. Ceph storage support depends on the Ubuntu release deployed on the underlying storage *nodes*:

7.3.1.1. The version of Ceph initially included in the release of an LTS version of Ubuntu is supported for the entire lifecycle of that Ubuntu version

7.3.1.2. Updated releases of Ceph are made available in the Ubuntu Cloud Archive after an LTS version is released. Each Ceph release in the Ubuntu Cloud Archive is supported on an Ubuntu LTS version for a minimum of 18 months from the *release date* of the Ubuntu version that included the applicable Ceph version

7.3.2. Canonical will provide support for 192TB of raw storage per Ceph storage *node*. Please note that only Ceph storage *nodes* count towards the 192TB free tier of raw storage per *node*

7.3.3. If the *Node* allowance is exceeded, additional Ceph storage support needs to be acquired

7.3.4. Customers who have purchased Ceph storage support for an unlimited amount of storage are limited to support of a single *Ceph cluster*

7.3.5. Ceph storage support requires all *nodes* that participate in the Ceph storage cluster to be covered under an active support agreement

7.3.6. Full Ceph storage support

7.3.6.1. Requirements:

7.3.6.1.1. The Ceph storage cluster was deployed via a Private Cloud Build, *Ceph Cluster* Build or was validated through a Cloud Validation engagement

7.3.6.2. Scope:

7.3.6.2.1. Support for the *Charms* or Snaps deployed

7.3.6.2.2. Support is included for all packages required to run Ceph as deployed

7.3.6.2.3. Any incidents found during the upgrades of Ceph components as part of the regular Ubuntu LTS maintenance cycle

7.3.6.2.4. Any incidents found during the upgrades between versions of Ceph or LTS versions of Ubuntu, Juju, and MAAS are supported as long as the upgrade is performed following a documented process as specified by Canonical as part of the Private Cloud Build or Cloud Validation Package

7.3.6.2.5. The addition of new Ceph storage *nodes* and the replacement of existing *nodes* with new *nodes* of equivalent capacity are both supported

7.3.6.3. Covered Software

7.3.6.3.1. All software, including *charms*, snaps, images and debs required to deploy Ceph as defined under 7.3.1 and 7.3.2. is covered by *bug-fix* and *break-fix support*

7.3.7. Limited Ceph storage support

7.3.7.1. Stand-alone storage clusters not deployed through a Ceph Cluster Build Package or cloud-attached Ceph storage clusters not validated using a Cloud Validation Package are limited to *Bug-fix* Support only

7.3.7.2. Ceph storage support does not include support beyond *Bug-fix* Support during the deployment or configuration of a standalone or cloud-attached storage cluster

7.4. MAAS

7.4.1. In order to be eligible for MAAS support, all machines managed by MAAS need to be covered under a standalone MAAS support agreement or Ubuntu Pro. Ubuntu Pro subscription can be purchased for all machines running Ubuntu, whereas other machines can be covered by standalone MAAS support

7.4.2. When running on top of Ubuntu, versions of MAAS are supported on a corresponding LTS version of Ubuntu for N-3 MAAS versions

7.4.3. Support scope:

7.4.3.1. Support for the ability to boot machines using operating system images provided by Canonical
7.4.3.2. Support for the tooling required to convert certified operating system images not provided by Canonical into MAAS images
7.4.4. Out of scope. MAAS support does not provide:
7.4.4.1. Support for workloads, packages and service components other than those required to run a MAAS deployment
7.4.4.2. Support for the *Nodes* deployed using MAAS but not covered under Ubuntu Pro
7.4.4.3. Support for design and implementation details of a MAAS deployment
7.4.4.4. Access to Landscape and Canonical Livepatch Service for machines deployed with MAAS

7.5. LXD
7.5.1. In order to be eligible for LXD support, all machines connected to a LXD cluster need to be covered under Ubuntu Pro support agreement.
7.5.2. Versions of LXD are supported on a corresponding LTS version of Ubuntu for a period of five years from the date that the LXD version is released
7.5.3. Every release with minor version '0' (ex. 3.0, 4.0, 5.0) is an LTS release supported for 5 years since the day of the release. These versions can be found in snap channels “X.0/stable”, where X is 3, 4, 5, etc.
7.5.4. Out of scope
7.5.4.1. LXD monthly releases, with a minor version other than 0 (ex. 4.2, 5.4 etc), including the version found in the “latest/stable” snap channel, are temporary feature releases and not covered by Ubuntu Pro

7.6. MicroCloud
7.6.1. In order to be eligible for support, MicroCloud needs to be deployed across at least three machines, and all machines need to be covered under Ubuntu Pro support agreement.
7.6.2. Versions of MicroCloud are supported on a corresponding LTS version of Ubuntu for a period of five years from the date that the MicroCloud LTS version is released
7.6.3. Scope of the support
7.6.3.1. All Canonical-provided packages and Canonical-maintained snaps required to deploy and run MicroCloud

8. Exclusions

8.1. Ubuntu Pro Desktop support only covers packages installed from the base Ubuntu desktop image as well as packages necessary for basic network authentication. It does not cover:
  8.1.1. Issues relating to dual-booting (cohabitating with other operating systems)
  8.1.2. Peripherals which are not certified to work with Ubuntu
  8.1.3. Community flavours of Ubuntu
8.2. Container images may be generated from Ubuntu Pro bits only if the resulting container images are deployed to Ubuntu Pro-covered machines

Support Services Process

9. Service initiation

9.1. Upon commencement of the services, Canonical will provide access for a single technical representative to Landscape, the support portal, and the online Knowledge Base
9.2. The customer, through their initial technical representative, may select their chosen technical representatives who act as primary points of contact for support requests. The customer will receive up to 5 dedicated, personalised credentials for technical representatives per every 500 *Nodes* under support, but not more than a total of 15 credentials
9.3. The customer may change their specified technical representatives at any time by submitting a support request via the support portal

10. Submitting support requests

10.1. The customer may open a support request once the customer account has been provisioned within the support portal
10.2. The customer may submit support cases through the support portal or by contacting the support team by telephone, unless otherwise noted
10.3. A support case should consist of a single discrete problem, issue, or request
10.4. Cases are assigned a ticket number and responded to automatically. All correspondence not entered directly into the case, including emails and telephone calls, will be logged into the case with a timestamp for quality assurance

10.5. When reporting a case, the customer should provide an impact statement to help Canonical determine the appropriate severity level. Customers with multiple concurrent support cases may be asked to prioritise cases according to severity of business impact

10.6. The customer is expected to provide all information requested by Canonical as we work to resolve the case

10.7. Canonical will keep a record of each case within the support portal enabling the customer to track and respond to all current cases and allowing for review of historical cases

11. Support severity levels

11.1. Once a support request is opened, a Canonical support engineer will validate the case information and determine the severity level, working with the customer to assess the urgency of the case

11.2. Canonical will work as described in the table below to provide the customer with restoration of the issue, i.e. a temporary work-around or a permanent solution, following the severity levels as described below. As soon as the impacted core functionality is available, the severity level will be lowered to the new appropriate severity level

11.3. Canonical will use reasonable efforts to respond to support requests made by the customer within the initial response times set forth below, based on the applicable service and severity level, but cannot guarantee a work-around, resolution or resolution time

SEVERITY LEVEL	DESCRIPTION	WEEKDAY INITIAL RESPONSE TIME	24/7 INITIAL RESPONSE TIME
1	Core functionality critical impact/Service down	4 hours, excluding weekends and holidays	1 hour
2	Core functionality severely degraded	8 Business hours	2 hours
3	Standard support request	12 Business hours	6 Business hours
4	Non-urgent requests, including cosmetic, informational and feature requests.	24 Business hours	12 Business hours

12. Customer assistance

12.1. Continuous effort support is dependent on the customer being available at all times to assist Canonical, otherwise Canonical may need to reduce the severity level and its ability to respond accordingly

13. Hotfixes

13.1. To temporarily resolve critical support cases, Canonical may provide a version of the affected software (e.g. package) that applies a patch. Such versions are referred to as “hotfixes”. Hotfixes provided by Canonical are supported for 90 days after the corresponding patch has been incorporated into a release of the software in the Ubuntu Archives. However, if a patch is rejected by the applicable upstream project, the hotfix will no longer be supported, and the case will remain open. The final fix will be provided when the upstream accepts it and incorporates it into a release of the software. The customer should update the software to the new release including the stable fix

14. Support language

14.1. Canonical will provide the support in English, unless specified otherwise

15. Remote sessions

15.1. At the discretion of a Canonical engineer, a remote access service might be offered to access a supported system. In such a case, Canonical will determine which remote access service to use. Canonical engineers expect to have read-only access and do not perform any remote actions on a supported system

16. Ask for a Peer Review

16.1. As a normal business practice, Canonical performs peer reviews on a percentage of all cases. Customers can specifically request a peer review on a case within the case comments or by calling the phone number listed in the support portal. An impartial engineer will be assigned to review the case and provide feedback

17. Management escalation

17.1. The customer may escalate support issues following the escalation process:

17.1.1. Non-urgent needs: Request a management escalation within the case itself. A manager will be contacted to review the case and post a response within 1 business day

17.1.2. Urgent needs can be escalated to Canonical's Support Engineering Management by emailing support-manager@canonical.com. If you require further escalation, email Canonical's SupportDirector at operations-director@canonical.com

18. Levels of Support

18.1. Canonical provides Support at the following levels:

18.1.1. Level 1 Support: Assistance in *troubleshooting* and restoring your broken application

18.1.2. Level 2 Support: *Troubleshooting* and *break-fix* of defects that are rare or need advanced knowledge to resolve. Typically advanced functionality, advanced configuration, or unexpected behaviour

18.1.3. Level 3 Support: Complex defects involving *bug-fixes* on Ubuntu and upstream software. Complex defects involving either core functionalities unavailable, severely degraded, or a complex configuration failure WRT solely Ubuntu and OpenStack as deployed using Canonical's tooling (Juju and MAAS)

Canonical

Add Ons

19. Managed Services

19.1. Managed Services are an add-on to Ubuntu Pro + *Infra Support* (24/7) or Ubuntu Pro + Support (24/7). When added on, Canonical will manage the *Environment* as described below

19.2. Following Canonical's building and initialising of the *Environment* (subject to separate service engagement), the Managed Service will re-deploy the *Environment* to reset credentials and validate the deployment process. The Managed Service will also provide documentation providing further detail on the working relationship with Canonical. Additional services can be offered subject to purchasing Professional Support Services (as listed in the section below)

19.3. The Managed Service will remotely operate, monitor, and manage the *Environment*. Concrete examples include:

19.3.1. backing up and restoring of the management infrastructure suite
19.3.2. hardware and software failure monitoring and alerting
19.3.3. capacity and performance reporting
19.3.4. security patching and bug fixing
19.3.5. scaling to deal with changes in demand
19.3.6. version upgrades and data migration
19.3.7. administrator credential management
19.3.8. operational monitoring and addressing issues of performance, capacity and alerting
19.3.9. patching and updates. Canonical will install relevant (e.g., security) patches and updates from the Ubuntu Cloud Archive to all the components of any environment covered by the managed service agreement (e.g. the Ubuntu operating system, software packages and dependencies, charms, supported applications)

19.3.10. Administrative access. The Managed Service will provide the customer with access to the following applications and/or services:

19.3.10.1.1. The OpenStack or Kubernetes dashboard, API and CLI
19.3.10.1.2. Landscape (restricted to read only access)
19.3.10.1.3. Monitoring and logging system (restricted to read only access)
19.3.10.1.4. Only Canonical will have login access to *Environment* *Nodes*

19.3.11. *Environment* size. The Managed Service will add or remove *Nodes* from the *Environment* as requested by the customer through a support ticket, provided that the *Environment* does not go under the *Minimum Size Requirement*. All *Environment* *Nodes* must be covered under the service, so additional fees may apply

19.3.12. Ubuntu, OpenStack and Kubernetes upgrades. The Managed Service will ensure the customer's *Environment* remains on a supported LTS version of Ubuntu and OpenStack and/or Kubernetes

19.3.12.1. Upgrades will be performed on a per-AZ basis within maintenance windows decided in concert with the client

19.3.12.2. Downtime should be expected for non-cloud-native workloads that cannot be migrated away from the availability zone undergoing upgrade

19.3.12.3. If cloud utilisation is very high and spare capacity is below 20%, upgrade risks will need to be carefully evaluated with the customer, potentially causing delays or preventing the project from being undertaken

Project work. The Managed Service will provide planned upgrades and maintenance Monday to Friday during Canonical working days

19.3.13. Managed Apps. Canonical will manage Applications from its managed applications portfolio. Canonical will expose only API and other user-level interfaces of the Applications

19.4. Out of scope. The Managed Service does not provide:

19.4.1. For managed OpenStack and managed Kubernetes:

19.4.1.1. Managing, monitoring, backup or recovery of the operating system, customer generated data and any applications running within virtual machine instances or Container Instances

19.4.1.2. Support for the ability to run virtual machine instances using images other than those provided by Canonical

19.4.2. Architectural changes to the *Environment*

19.4.3. Alternative scheduling of updates or upgrades

19.4.4. Unsupported versions of Ubuntu, OpenStack, Kubernetes, or applications

19.4.5. Installation of additional components (e.g. LBaaS, VPNaaS, SDN or SDS) beyond the software installed as part of the building of the *Environment*

19.4.6. Adherence to the Customer's Change Management requirements/regulations without a DSE

19.4.7. Integration with Customer's ticketing system without a TAM

19.5. Service conclusion. At the end of the service term, the Managed Service will initiate an operational transfer. Operational transfer includes:

19.5.1. Hand over of all credentials of the hosts, management software, Landscape and Applications to the customer. The continued operation of Landscape is subject to purchase and agreement of appropriate licence terms

19.5.2. Coordination of any applicable training (if purchased)

19.6. Customer dependencies. The Managed Service requires:

19.6.1. Credentials to the Infrastructure being used for the Applications in the case in which such infrastructure is not managed by Canonical, i.e., Managed OpenStack

19.6.2. Continuous VPN access for Canonical support personnel to the *Environment*

19.6.3. Utilisation parameters per *Node* to be kept below the maximum specified in the design document provided by Canonical when the *Environment* is delivered to the customer

19.6.4. The facility where the *Environment* is hosted to comply with the minimum required measures to function, including but not limited to, connectivity, sufficient power supply, sufficient cooling system, and physical access control to the *Environment*

19.6.5. The *Minimum Size Requirement* for the Cloud or Kubernetes cluster maintained at all times

19.7. Uptime Service Level

19.7.1. The Managed Service includes the following uptime service levels:

	DATA PLANE FOR CUSTOMER WORKLOADS THAT ARE DISTRIBUTED ACROSS TWO REGIONS	DATA PLANE FOR CUSTOMER WORKLOADS THAT ARE IN A SINGLE REGION	CONTROL PLANE (OPENSTACK/ KUBERNETES API, WEB UI AND CLI)
Uptime	99.9%	99.5%	99%

19.7.2. Data plane includes:

19.7.2.1. Virtualisation (for workloads that are architected to not depend on a single compute *node*)

19.7.2.2. Storage (block & object)

19.7.2.3. Network for instances

19.7.3. Downtime must be directly attributable to Canonical in order for it to count against the service level and is measured across a 12-month period. Planned maintenance windows and any requests by the customer are not taken into account when calculating uptime. Planned maintenance is carried out as required by Canonical, Monday to Friday during Canonical working days

20. Professional Support Services

20.1. The Technical Account Manager service (TAM) and Dedicated Technical Account Manager service (DTAM) are add-on service offerings to enhance support

20.1.1. Under these services offerings, Canonical will provide a TAM, who will perform the following services for up to 10 hours per week, or a DTAM, who will perform the same services for up to 40 hours per week during local *Business Hours* under the term of service:

20.1.1.1. Act as the primary point of contact for all support requests originating from the customer department for which the TAM/DTAM is responsible

20.1.1.2. Provide support and best-practice advice on platform and configurations covered by the applicable Ubuntu Pro services

20.1.1.3. Participate in review calls every other week at mutually agreed times addressing the customer's operational issues

20.1.1.4. Organise multi-vendor issue coordination through TSANet or

Canonical's direct partnerships where applicable. When the root cause is identified, the TAM/DTAM will work with the vendor for that sub-system, working to resolve the case through their normal support process

20.1.1.5. Manage support escalations and prioritisation in accordance with Canonical's standard support response definitions and customer needs

20.1.1.6. Attend applicable Canonical internal training and development activities (in-person and remote)

20.1.2. The TAM/DTAM is available to respond to support cases during the TAM/DTAM's working hours. Outside of *Business Hours*, support will be provided per the Ubuntu Pro Support Process

20.1.3. If a TAM/DTAM is on leave for longer than five consecutive days, Canonical will assign a temporary remote resource to cover the leave period. Canonical will coordinate with the customer with respect to foreseeable TAM/DTAM leave

20.1.4. Canonical will hold a quarterly service review meeting with the customer to assess service performance and determine areas of improvement

20.1.5. If required, the TAM/DTAM may facilitate the integration of the Customer's ticketing system with Canonical's one

20.1.6. The TAM/DTAM will visit the customer's site annually for on-site technical review

20.2. Dedicated Support Engineer (DSE) is an add-on service to enhance support

20.2.1. Canonical will provide a DSE, who will perform the following services during local *Business Hours* for up to 40 hours per week (subject to Canonical leave policies) during the term of service:

20.2.1.1. Be available on site as required to meet the customer's requirements

20.2.1.2. Understand the products utilised in the customer's *Environment* that need to be integrated with Canonical's offerings and assist with those products, to the extent reasonable based on the DSE's expertise, to ensure the successful usage of offerings from

Canonical

20.2.1.3. Provide support and best-practice advice on platforms and configurations covered by the applicable Ubuntu Pro services

20.2.1.4. Act as the primary point of contact for all support requests originating from the customer department for which the DSE is responsible

20.2.1.5. Act as a Canonical representative for Change Management protocols, in turn defending, coordinating and executing required Changes by Managed Services

20.2.1.6. Manage support escalations and prioritisation in accordance with Canonical's standard support response definitions and customer needs

20.2.1.7. Participate in regular review calls addressing the customer's operational issues

20.2.1.8. Organise multi-vendor issue coordination through TSANet or Canonical's direct partnerships where applicable. When the root cause is identified, the DSE will work with the vendor for that sub-system, working to resolve the case through their normal support process

20.2.1.9. Attend applicable Canonical internal training and development activities

20.2.2. Canonical will hold a quarterly service review meeting with the customer to assess service performance and determine areas of improvement

20.2.3. The DSE is available to respond to support cases during the DSE's working hours. Outside of *Business Hours*, support will be provided per the Support Services Process

20.2.4. If a DSE is on leave for longer than five consecutive business days, Canonical will assign a temporary remote resource to cover the leave period. Canonical will coordinate with the customer with respect to foreseeable DSE leave

21. Embedded Services

21.1. With Embedded Services you will receive the engineering support and access to Expanded Security Maintenance. Canonical will provide such technical support to

unmodified Ubuntu LTS release images when installed using official sources and within its product life cycle.

21.2. Scope

21.2.1. The scope of the service is limited to the appropriate level as listed above.

21.3. Engineering Support-only, processes:

21.3.1. You are responsible for resolving all end user issues. Canonical will not be supporting end-users directly. You should utilise the Knowledge Base, Launchpad, and other resources in addition to your own resolution systems to find workarounds or resolutions for any issue prior to opening a support case with Canonical

21.3.2. You will search Launchpad, to ensure that the issue is not already known and being resolved and, if it is, provide suspected bug number to Canonical support as reference. Canonical reserves the right to redirect low-level and untriaged issues to you

21.3.3. You are responsible for specifying how an issue arises and in what sub-system it is taking place. You must provide a repeatable test case that Canonical can recreate on the hardware systems to which Canonical has access

21.3.4. You will work with Canonical to provide any debugging or further testing required. You will provide any technical information as requested to resolve the problem. Failure to provide required information or assistance in gathering such information may result in closure of the case. When the final solution has been provided by Canonical, you are responsible for verifying that it solves the issue

Definitions

Applications: Applications supported or managed by Canonical (Managed Applications as described in the Add-ons section, under Managed Services, and at https://ubuntu.com/managed)

Break-fix Support: request assistance in the event of an incident and answer questions about Supported Packages and products

Bug-fix Support: support for reported software bugs in Supported Packages only. This does not include *troubleshooting* of issues to determine if a bug is present

Business Hours: 08:00 - 18:00 Monday - Friday local to the customer's headquarters unless

another location is agreed. All times exclude public holidays at the customer's location.

Ceph Cluster: a single Ceph installation in a single physical data center and specified by a unique identifier

Charm: a set of scripts compatible with Juju application modelling for the purpose of deploying and configuring relationships between software packages

Charmed Kubernetes: Kubernetes deployed using Juju and the official Canonical-Kubernetes bundle on bare metal, Ubuntu Guests, or virtual machines

Covered Architectures:

architecture/ release	14.04 LTS	16.04 LTS	18.04 LTS	20.04 LTS and newer
x86	Yes	Yes	Yes	Yes
arm64	No	No	Yes	Yes
s390x	No	No	Yes	Yes
power	No	No	Yes	Yes
risc-v	No	No	No	Yes

CVEs (High and Critical): High and Critical Common Vulnerabilities and Exposures as assessed by the Ubuntu Security Team. More details can be found at https://ubuntu.com/security/cves

Desktop use case: unlike Ubuntu machines operated in the datacenter or public clouds, desktop use cases require a human in front of the screen. The support for Desktop is limited to the base Ubuntu Desktop image, with the addition of packages necessary for basic authentication and networking. Desktop use cases may also involve developer tools such as MicroK8S and Multipass

Environment: a cloud or cluster, as applicable to the particular service offering

End of Life: a date (10 years after the *Release Date*) on which the *Expanded Security Maintenance* service for an Ubuntu LTS expires

End of Standard Support: a date (5 years after the *Release Date*) on which free standard security maintenance service for the *Ubuntu Main* repository of an Ubuntu LTS expires

Expanded Security Maintenance (ESM): an additional scope of security patching service

delivered by the Ubuntu Security Team as found at https://ubuntu.com/security/esm. It covers fixes to *High and Critical CVE* for 10 years and could be offered for *Ubuntu Main* repository, or both *Ubuntu Main* and *Universe* repositories, depending on the Ubuntu Pro subscription (infra-only, Apps-only, or the full Ubuntu Pro)

Infra support: support for the base Ubuntu OS image and a set of open source infrastructure components, such as MAAS, Ceph storage and OpenStack. It also covers Kubernetes, MicroCloud and LXD

Knowledge Base: the knowledge base is a database of articles for Customer technical operators

Kubernetes: the container orchestration software known as "Kubernetes" as distributed by Canonical

Node: a physical node or virtual machine provided to Canonical (or paid for) by the Customer for the purposes of running the environment. Any further machines (whether virtual (VM) or container) created on top of a Node are not themselves considered to be Nodes

OpenStack: the cloud computing software known as "OpenStack" as distributed by Canonical with Ubuntu

Production environment: a production environment is where end users can access the latest version of a software, product, or update, for its intended use

Release date: the general availability release date of an Ubuntu version as found at https://ubuntu.com/about/release-cycle

Troubleshooting: the process of identifying, diagnosing, and resolving problems or issues that arise when using a software application or infrastructure, in order to ensure its proper functionality

Ubuntu Archive: official online repositories that store software packages and updates for the Ubuntu operating system

Ubuntu Guest: a virtual machine instance or Container Instance of Ubuntu

Ubuntu Main: the deb package repository of an Ubuntu identified by Canonical as Ubuntu Main

Ubuntu Universe: the deb package repository of an Ubuntu identified by Canonical as Ubuntu Universe

Valid Customisations: configurations made through Horizon or the OpenStack API of the OpenStack Packages. For the avoidance of doubt, valid customisations do not include architectural changes that are not expressly executed or authorised by Canonical. Configuration

options set during a Private Cloud Build should be considered critical to the health of the Cloud. Any changes to these may render the cloud unsupported. Requests for changes should be validated by Canonical to ensure continued support