Canonical

# Ubuntu Pro Description

## Valid since: 16 Dec 2025

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. For support and managed solutions customers, it also includes 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 *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 machine:** The subscription is attached to an Ubuntu virtual machine or automatically attached at launch under a public cloud (Google Cloud, AWS, Azure, etc.). This subscription covers Ubuntu images running on virtual machines or in containers.
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, Data Science Stack and Multipass.
4. **Device:** The subscription is attached to a physical device for *Device use cases* including customer's hardware that has been certified or enabled by Canonical.

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

1. **self-support**
2. **support (weekday)**
3. **support (24/7)**

and must cover all Ubuntu systems within an *Environment*.

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

Canonical

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.

Ubuntu Pro is for direct use by the organization you represent. If you wish to resell Ubuntu Pro, please contact Canonical sales. Without a reseller agreement, you may not transfer or provide your entitlement to any third party.

# 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 fixes for *CVEs (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 Ubuntu Pro Support (esm-infra)

1.3. Only Ubuntu Pro subscriptions cover packages in the *Ubuntu Universe* until the end of Ubuntu Pro Support (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*
- 1.4.4. Replacements for cryptography algorithms that are no longer secure

## 2. Legacy add-on

2.1. The Legacy add-on provides security maintenance (and optional break-fix support) between the end of Expanded Security Maintenance and the end of Legacy coverage.

2.2. The Legacy add-on carries the same limitations as those outlined for ESM in 1.4.

## 3. Other security fixes

3.1. Security fixes for OpenStack, Ceph, MAAS, Kubernetes

- 3.1.1. Supported versions of Canonical Kubernetes Platform's k8s snap include:
  - 3.1.1.1. for long-term supported (LTS) Kubernetes versions, released every two years, security patching for ten years in the "stable" release

channel and an additional five years in the “legacy” release channel from the release date of the Kubernetes version included in the release

3.1.1.2. to enable upgrades between Kubernetes LTS versions every two years, Canonical provides at least 12 months of security patching for non-LTS Kubernetes releases that are between the latest Kubernetes LTS and the previous one

3.1.2. Supported versions of Charmed Kubernetes and MicroK8s clusters include:

3.1.2.1. security patching for N-4 (the latest and previous four) releases in the “stable” release channel

3.2. 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’

## 4. Certified components for compliance, hardening and audit

4.1. FIPS 140-2 Level 1 certified modules for Ubuntu 20.04 LTS, 18.04 LTS and 16.04 LTS releases using the generic kernel

4.2. FIPS 140-3 Level 1 certified modules for Ubuntu 22.04 LTS releases using the generic kernel (24.04 LTS available for testing and preview)

4.3. Access to certified CIS Benchmark tooling Levels 1 and 2 for Ubuntu 18.04 LTS and 16.04 LTS

4.4. Ubuntu Security Guide (USG) for Ubuntu 20.04 LTS, 22.04 LTS, and 24.04 LTS which includes certified DISA-STIG profiles and CIS benchmark tooling Levels 1 and 2

4.5. Common Criteria EAL2 for Ubuntu 18.04 LTS and 16.04 LTS

## 5. Kernel Livepatch

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

5.2. Kernel Livepatch may provide non-security bug fixes as kernel livepatches

5.3. Only Livepatch Covered Kernels are available for livepatching

5.4. Access to Canonical’s Livepatch on-prem server

## 6. Access to other services

6.1. 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

6.2. Access to Canonical's Landscape systems management tool
6.3. 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.

## 7. Scope of Support

7.1. Included in all scopes
- 7.1.1. *Certified hardware*, including certified public cloud instances
  - 7.1.1.1. Support applies to the customer's hardware that has been certified or enabled.
- 7.1.2. Ubuntu releases
  - 7.1.2.1. *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
- 7.1.3. Supported Services
  - 7.1.3.1. Additional packages, kernels and services are within the scope of support:
    - 7.1.3.1.1. Packages in the Ubuntu Cloud Archive
    - 7.1.3.1.2. Supported or enabled Kernels
    - 7.1.3.1.3. Landscape client
    - 7.1.3.1.4. Kernel Livepatch
    - 7.1.3.1.5. Packages and profiles for FIPS, DISA-STIG and Common Criteria EAL2 provided by Ubuntu Pro
  - 7.1.3.2. Support is not provided for any packages that have been modified by the customer or third parties
- 7.1.4. Ubuntu Assurance Program
  - 7.1.4.1. Ubuntu Pro + support customers are entitled to the Ubuntu Assurance Programme. Canonical may update the Assurance Programme and its terms periodically

*7.2. Infra-only support*
- 7.2.1. Kubernetes, as defined in 8.1
- 7.2.2. OpenStack, as defined in 8.2

7.2.3. Ceph Storage, as defined in 8.3
7.2.4. MAAS, as defined in 8.4
7.2.5. LXD, as defined in 8.5
7.2.6. MicroCloud, as defined in 8.5
7.2.7. Enterprise Store, as defined in 8.7
7.2.8. All packages in *Ubuntu Main*
7.2.9. LTS Ubuntu base images at https://hub.docker.com/_/ubuntu/, https://gallery.ecr.aws/lts/ubuntu

7.3. Ubuntu Pro + Support includes the following in addition to infra-only support:
7.3.1. All packages in *Ubuntu Universe*, starting with 18.04 LTS and onwards
7.3.2. Canonical-maintained applications published in the "stable" channel:
7.3.2.1. 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
7.3.2.1.1. 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

7.3.2.1.2. 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

7.3.2.1.3. Support exclusions

7.3.2.1.3.1. 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

7.3.2.1.3.2. 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

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

7.3.2.3. Canonical maintained *charms* listed in https://charmhub.io/.

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

7.4. The Legacy add-on, if purchased, extends the support term. The scope of the Legacy add-on is limited regarding:

7.4.1. Severity 1 issues: the maximum level of support provided is Severity 2. All Severity 1 issues will be prioritised as Severity 2.

7.4.2. Bug-fix: Bug-fix support is provided only in cases where a bug is preventing migration to a newer version.

## 8. Supported Products

8.1. Kubernetes

8.1.1. Installations of Kubernetes which are within their support lifecycle and which are deployed via:

8.1.1.1. Canonical Kubernetes Platform

8.1.1.2. Charmed Kubernetes

8.1.1.3. MicroK8s

8.1.1.4. 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

8.1.2. For any deployment of *Charmed Kubernetes* and *Canonical Kubernetes Platform* 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.

8.1.2.1. All software, including charms, snaps, images and debs, required to deploy Kubernetes is covered by *bug-fix* and *break-fix support*

8.2. OpenStack

8.2.1. Support for OpenStack deployments is limited to Canonical OpenStack (based on OpenStack Charms), aka Charmed OpenStack and Canonical OpenStack (based on Sunbeam).
  8.2.1.1. Support can only be provided for *Environments* with at least 3 deployed nodes for eligible Canonical OpenStack (based on Sunbeam) releases and 12 deployed nodes for any eligible Canonical OpenStack (based on OpenStack Charms) release.

8.2.2. The duration of support depends on the OpenStack product being used and the installed software version. Please refer to the Canonical OpenStack documentation for detailed information on supported products and versions.
8.2.3. Charmed OpenStack requirements:
  8.2.3.1. Hardware must meet the minimum criteria as specified by Canonical as part of the Private Cloud Build or other Canonical consulting engagements.
  8.2.3.2. Deployment was done by Canonical via Private Cloud Build or it was validated by Canonical.
8.2.4. Canonical OpenStack based on Sunbeam requirements:
  8.2.4.1. Hardware must meet the minimum criteria as specified in the Canonical OpenStack documentation
  8.2.4.2. The OpenStack cloud was deployed with Sunbeam
8.2.5. OpenStack support includes access to Canonical-provided Microsoft-certified drivers in Windows virtual machine instances
8.2.6. OpenStack support requires all *nodes* that participate in the OpenStack deployment to be covered under an active support agreement
8.2.7. Ironic service: In order to be eligible for support, all machines managed by Ironic must be covered under a standalone MAAS support agreement or an Ubuntu Pro subscription. Machines not running Ubuntu can still be covered by MAAS support, even in the absence of Ubuntu Pro eligibility.
8.2.8. Scope of OpenStack support:
  8.2.8.1. *Charms* used for deployment
  8.2.8.2. All Canonical-provided packages, Canonical-maintained snaps and OCI images required to deploy and run OpenStack
  8.2.8.3. 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 following a documented process as specified by Canonical as part of the Private Cloud Build, Cloud Validation or in Canonical OpenStack (based on Sunbeam) documentation
8.2.9. Limited OpenStack Support

8.2.9.1. OpenStack clouds, other than Sunbeam-based, not deployed through Private Cloud Build or otherwise validated through Cloud Validation, are limited to *Bug-fix Support*

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

8.2.10. Exclusions

8.2.10.1. Support excludes customisations which are not considered *Valid Customisations* or are not covered in Canonical OpenStack (based on Sunbeam) documentation

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

8.2.10.3. Support for virtual machine instances other than *Ubuntu Guests*

8.2.10.4. Support for incidents and performance degradations resulting from decisions made when self-deployed by the customer and not validated by Canonical or including customisations that are not *Valid Customisation*

8.3. Ceph Storage

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

8.3.1.1. Support can only be provided for *environments* with at least three infra nodes and nine storage nodes for eligible Charmed Ceph releases or 3 Ceph nodes for eligible MicroCeph releases

8.3.1.2. 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

8.3.1.3. 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

8.3.2. Canonical will provide support for 384TB of raw storage per Ceph storage *node*. Note that only Ceph storage *nodes* count towards the 384TB free tier of raw storage per *node*

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

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

8.3.5. Ceph storage support requires all *nodes* that participate in the Ceph

storage cluster to be covered under an active support agreement

8.3.6. Full Ceph storage support

8.3.6.1. Requirements:

8.3.6.1.1. The Ceph storage cluster was deployed via a Private Cloud Build, *Ceph Cluster* Build or was validated through a Cloud Validation engagement. These requirements don't apply to MicroCeph.

8.3.6.2. Scope:

8.3.6.2.1. Support for the *Charms*, Rocks, or Snaps deployed

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

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

8.3.6.2.4. 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

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

8.3.6.3. Covered Software

8.3.6.3.1. All software, including *charms*, snaps, images and debs required to deploy Ceph as defined under 8.3.1 and 8.3.2. is covered by *bug-fix* and *break-fix support*

8.3.7. Limited Ceph storage support

8.3.7.1. 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

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

8.4. MAAS

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

8.4.2. Support scope:

8.4.2.1. Support for the ability to boot machines using operating system images provided by Canonical

8.4.2.2. Support for the tooling required to convert certified operating system images not provided by Canonical into MAAS images

8.4.3. To be supported, all managed machines must be covered by an Ubuntu Pro subscription if they are running Ubuntu or a standalone MAAS support agreement if they are not. The MAAS controllers require a dedicated Ubuntu Pro (Infra-only) or Ubuntu Pro subscription.

8.4.4. Out of scope. MAAS support does not provide:

8.4.4.1. Support for workloads, packages and service components other than those required to run a MAAS deployment

8.4.4.2. Support for the *nodes* deployed using MAAS but not covered under Ubuntu Pro

8.4.4.3. Support for design and implementation details of a MAAS deployment

8.4.4.4. Access to Landscape and Canonical Livepatch Service for machines deployed with MAAS

8.5. LXD and MicroCloud

8.5.1. Versions of LXD and MicroCloud within their support lifecycle and all supported versions of Canonical-provided packages and Canonical-maintained snaps required to deploy and run MicroCloud (MicroCloud, MicroCeph. MicroOVN, LXD)

8.5.2. Support needs to be purchased for all MicroCloud cluster members

8.6. Dedicated Snap Store: When purchased on top of Ubuntu Pro (Infra-only) + Infra Support or Ubuntu Pro + Support, Canonical will provide support for associated Store Services.

8.7. Enterprise Store

8.7.1. Customer is entitled to a license to use the Enterprise Store per subscription, and may use as many Enterprise Store instances as the number of Ubuntu Pro (Infra-only) or Ubuntu Pro subscriptions purchased.

8.7.2. Canonical will provide Customer support for the Enterprise Store.

## 9. Exclusions

9.1. 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:

9.1.1. Issues relating to dual-booting (cohabitating with other operating systems)

9.1.2. Peripherals which are not certified to work with Ubuntu

9.1.3. Community flavours of Ubuntu

9.1.4. Experimental or beta features.

9.2. 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

## 10. Service initiation

10.1. Upon commencement of the services, Canonical will provide access for a single technical representative to Landscape, the support portal, and the online Knowledge Base

10.2. 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* or 50,000 devices under support, but not more than a total of 15 credentials

10.3. The customer may change their specified technical representatives at any time by submitting a support request via the support portal

## 11. Submitting support requests

11.1. The customer may open a support request once the customer account has been provisioned within the support portal

11.2. The customer may submit support cases through the support portal or by contacting the support team by telephone, unless otherwise noted

11.3. A support case should consist of a single discrete problem, issue, or request

11.4. 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

11.5. 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

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

11.7. 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

Canonical

## 12. Support severity levels

12.1. 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

12.2. Canonical will work 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

12.3. 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

| | **Self-support**[1] | **Weekday support** | | **24/7 support** | | **Firefighting support (24/7 support add-on)** | |
|---|---|---|---|---|---|---|---|
| **Hours of coverage** | N/A | 8/5[2] | | 24/7/365 | | 24/7/365 | |
| **Available channels** | Knowledge Base | Support portal, including Knowledge Base, phone, and ticket | | Support portal, including Knowledge Base, phone, and ticket | | Video call during Sev 1 case (one at a time per environment), Support portal, including Knowledge Base, phone, and ticket | |
| **Number of cases allowed** | N/A | Unlimited | | Unlimited | | One firefighting Sev 1 case at a time per environment, unlimited cases otherwise | |
| **Response times** | **First response** | **First response** | **Ongoing response**[3] | **First response** | **Ongoing response**[3] | **First response** | **Ongoing response**[3] |
| **Severity 1** Production service down. Critical impact on core | N/A | 4 business hours | 2 business hours | 1 hour | 2 hours | 1 hour | Continuous video call until issue is de-escalated to Severity 2 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| functionality in a production environment | | | | | | | if issue affects all users or 4 hours of enhanced support since initial response if issue affects some users |
| **Severity 2** Core functionality is severely degraded in a production environment | N/A | 8 business hours | 8 business hours | 2 hours | 8 business hours | 2 hours | 8 business hours |
| **Severity 3** Issues with a medium to low impact on a production environment | N/A | 12 business hours | Weekly | 6 hours | Weekly | 6 hours | Weekly |
| **Severity 4** Non-urgent requests with low to no impact on production environments | N/A | 24 business hours | N/A | 12 hours | NA | 12 hours | N/A |

[1]Included with all Ubuntu Pro subscriptions

[2]8:00 AM to 5:00 PM at the Customer's location as set in the Canonical Support portal. Weekends are not included.

[3]Canonical Support will provide follow-up updates within defined time frames after responding to a customer inquiry. These ongoing response time frames are defined based on the severity level of the issue, and counted from the time of the latest severity update.

## 13. Customer assistance

13.1. 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

## 14. Hotfixes

14.1. 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*, or Canonical hosted store.

14.2. A patch may be rejected by the applicable upstream project, in which case 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

## 15. Support language

15.1. Canonical will provide the support in English unless specified otherwise

## 16. Remote sessions

16.1. 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

## 17. Ask for a Peer Review

17.1. 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

## 18. Management escalation

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

18.1.1. 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

18.1.2. 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 Support Director at operations-director@canonical.com

## 19. Levels of Support

19.1. Canonical provides Support at the following levels:

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

19.1.2. 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

19.1.3. 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 with respect to solely Ubuntu and OpenStack as deployed using Canonical's tooling (Juju and MAAS)

# Add-Ons

## 20. Managed Services

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

Environments benefiting from Managed Services can be deployed on-premises, in the public cloud, or on a combination of the two. To be eligible for Managed Services, the Environment must be deployed (manually or automatically) or validated by Canonical.

20.2. The Managed Services team will remotely operate, monitor, and manage the *Environment* by:

20.2.1. Service continuity

20.2.1.1. 24/7 Monitoring, excluding security-related monitoring

20.2.1.2. 24/7 Alerts

20.2.1.3. Telemetry Dashboards (accessible also to customers)

20.2.2. (Non-security) Incident management

20.2.2.1. Prevention and recovery of platforms (ie network, power, compute, storage) and services (ie cloud APIs, observability, connectivity) outages

20.2.2.2. Diagnosis of external service issues (ie firewall, DNSs, proxies)

20.2.2.3. Root Cause Analysis for S1 incidents

20.2.2.4. Node crash recovery

20.2.3. Operations

20.2.3.1. Backup/Restore of control plane services

20.2.3.2. Patching/Rebooting (cadence)

20.2.3.3. Packages refreshed (cadence)

20.2.3.4. Upgrades (with tailored cadence depending on the offer)

20.2.3.5. Storage and capacity management/warnings

20.2.3.6. *CVEs (High and Critical)* patching/mitigation

20.2.3.7. Compute expansion/contraction/replacement

20.2.3.8. Storage expansion/contraction/replacement

20.2.3.9. SSL certificate rotation and updates

20.2.3.10. Support for OpenStack roles: Admin, Reader, and Member

20.2.3.11. Permission and authorization

20.2.3.12. Admin creation and revocation

20.2.3.13. Performance tuning and diagnostics

20.2.4. Coordination

20.2.4.1. Weekly meeting (more than a total of 20 nodes)

20.2.4.2. Monthly as requested by the customer

20.2.5. Ticket-based tracking of cases

20.2.6. Administrative access. Managed Services will provide the customer with access to the following applications and/or services:

20.2.6.1.1. The OpenStack or Kubernetes dashboard, API and CLI
20.2.6.1.2. Landscape (restricted to read-only access)
20.2.6.1.3. Monitoring and logging system (restricted to read-only access)
20.2.6.1.4. Only Canonical will have login access to *Environment* *nodes*

20.2.7. *Environment* size. Managed Services 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*. As all *Environment* *nodes* must be covered under the service, additional fees may apply.

20.2.8. OpsConsultancy packages. Managed Services will provide hours of OpsConsultancy required by the customer through a support ticket, provided that the activity the consultancy is required is pertinent with the Environment. The OpsConsulting additional fees apply and will be charged the month after the completion of the consultancy .

20.2.9. For Environments deployed directly from public cloud marketplaces, Customer is responsible for configuring the Environment's upper and lower node limits at the time of deployment, within the options presented by the marketplace listing. Customer can request to change these limits via Support ticket or, where possible, directly on the marketplace dashboard.

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

20.2.10.1. Upgrades will be performed on a per-AZ basis within maintenance windows decided in agreement with Customer.

20.2.10.2. Downtime should be expected for non-cloud-native workloads

that cannot be migrated away from the availability zone undergoing upgrade.

20.2.10.3. If cloud utilization 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.

20.2.10.4. For applications deployed directly from public cloud marketplaces, Managed Services will perform upgrades in pre-defined standing maintenance windows. These upgrades will be announced with reasonable notice, and Customer may opt to skip to the next standing maintenance window if required.

20.2.10.5. Customer may pin its project to a specific version by asking Managed Services to disable the upgrades. Subsequent requests for upgrades will be evaluated.

20.2.10.6. Managed Services will provide planned upgrades and maintenance Monday to Friday during Canonical working days. Standing maintenance periods may be pre-appointed following mutual agreements with Customer.

20.2.10.7. Customer may skip upgrades up to three times, after which automated upgrades will be disabled.

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

20.3. No other operations will be provided by Managed Services unless contractually agreed between Canonical and Customer prior to the Environment's deployment. The Managed Service does not provide:

20.3.1. For managed Infrastructure:

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

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

20.3.2. For self-deployed applications on public clouds, Canonical will not provide

Managed Services for external or third-party components integrated within the Canonical-operated Environment.

20.3.3. Evaluation and resolution of any incompatibility or malfunction of external components caused by updates to the *Environment* remains the responsibility of the Customer.

20.3.4. Alternative scheduling of updates or upgrades

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

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

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

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

20.4.1. 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

20.4.2. Coordination of any applicable training (if purchased)

20.4.3. For self-deployed applications, Managed Services will transfer the access to the environment's resources exclusively to Customer. This cannot be undone, and future deployments will use the most current component version which may cause incompatibilities with decommissioned *Environments*.

20.5. Customer dependencies. Managed Services requires:

20.5.1. 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)

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

20.5.3. For self-deployed Environments, continuous access to the Environment's resources

20.5.4. 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

20.5.5. 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*

20.5.6. The *entire* Environment to be covered by Managed Services

20.6. Minimum size requirement. Managed Services can only be provided for Environments with:

20.6.1.1. At least 12 deployed nodes for any eligible OpenStack release

20.6.1.2. At least 9 deployed nodes for any other compatible product

20.6.1.3. For Environments deployed directly from public cloud marketplaces, there is no minimum size requirement.

20.7. Uptime service level

20.7.1. 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% |

20.7.2. Data plane includes:

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

20.7.2.2. Storage (block & object)

20.7.2.3. Network for instances

20.7.3. 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

## 21. Firefighting Support

21.1. Firefighting Support is an add-on to Ubuntu Pro + *Infra Support* (24/7) or Ubuntu Pro + Support (24/7). When added, Canonical will support the *Environment* as described below.

21.2. Environments benefiting from Firefighting Support can be deployed on-premises, in the public cloud, or on a combination of the two. To be eligible for Firefighting Support, the Environment must be deployed (manually or automatically) or validated by Canonical.

21.3. The Managed Services team, which provides Firefighting Support, will remotely support the *Environment* by doing incident management, either:

21.3.1. On-call, for a live resolution of Severity 1 incidents.

21.3.2. On-call, for a live de-escalation of Severity 1 incidents to lower severities, which then will be taken over by the other Support teams

21.3.3. Available via OpsConsultancy:

21.3.3.1. Operational tasks included in the Managed service and in the OpsConsultancy Section

21.3.3.2. Planning or executing cloud upgrades/reboots/package or charms refresh

## 22. OpsConsultancy

22.1. OpsConsultancy is an add-on to Managed Services or Firefighting Support offering. When added, Canonical will provide consultancy hours, from remote, for the topics described below.

22.2. Architectural changes

22.2.1. Planning or executing changes in network topology

22.2.2. Planning or executing changes to disk layouts

22.2.3. Integrate/Install new applications/agents/software after deployment

22.2.4. Enabling HW offloading or CPU pinning adjustments after deployment

22.2.5. Implement new data replication scenarios after deployment

22.2.6. Addition of any non-standard packages or applications

22.2.7. Migration of the Cloud to alternative Data Centers

22.2.8. Creation of custom dashboards

22.2.9. Permission adjustments (policy changes)

22.2.10. Security Audits other than CVE and CIS scan reports

22.2.11. User permissions changes

22.2.12. Training on Canonical products

22.2.13. Support for custom OpenStack roles

22.2.13.1. Creation and revocation

22.2.13.2. Custom permission and authorization

22.3. Customer-specific training

22.3.1. Training/coaching on Canonical products

22.3.2. Customer's specific organizational training

22.3.3. Customer's specific security training

22.4. Only for Firefighting Support customers (all the above plus)

22.4.1. Operational tasks included in the Managed service

22.4.2. Planning or executing of cloud upgrades/reboots/package or charms refresh

## 23. Professional Support Services

23.1. The Technical Account Manager service (TAM) is an add-on service offering to enhance support

23.1.1. Under these services offerings, Canonical will provide a TAM, who will perform the following services:

23.1.1.1. Act as the primary point of contact for all support requests

originating from the customer department for which the TAM is responsible

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

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

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

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

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

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

23.1.3. If a TAM 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 leave

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

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

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

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

23.2.1. Canonical will provide a DSE, who will perform the following services during local *Business Hours* during the term of service:

23.2.1.1. 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

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

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

23.2.1.4. If applicable, act as a point of communication and coordination for changes that need to be applied by Managed Services

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

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

23.2.1.7. 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

23.2.1.8. Attend applicable Canonical internal training and development activities

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

23.2.3. 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

23.2.4. 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

Canonical

## 24. Embedded Services

24.1. 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.

24.2. Scope

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

24.3. Engineering Support-only, processes:

24.3.1. 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

24.3.2. 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

24.3.3. 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

24.3.4. 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 - 17:00 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

**Certified Hardware:** any Ubuntu-certified hardware identified at https://ubuntu.com/certified running a Canonical-provided Ubuntu image certified for that hardware.

**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 interacting through a display and input devices – such as a keyboard, mouse, trackpad, or assistive technology – to run multiple general-purpose applications in a typical workplace environment. Desktop use cases may also involve developer tools such as MicroK8s and Multipass

**Device use case:** unlike desktop use cases, device use cases involve hardware with specialized, application-specific purposes that may support multiple users or operate unattended, running a limited set of applications for dedicated functions. May or may not include a monitor. Examples:

Canonical

Gateways, Industrial PCs, Robots, Kiosks, Point of Sale devices, Medical devices.

**Enabled kernel**: Kernel version provided as part of Canonical Enablement service, unmodified and supported

**Environment**: all machines (or devices) in a private cloud, cluster, fleet, or similar grouping of instances

**End of Life:** a date on which an Ubuntu LTS reaches end of Legacy coverage or end of Expanded Security Maintenance if the Legacy add-on is not available

**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

**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

Canonical

Ubuntu operating system

**Ubuntu Core:** Ubuntu Core is a version of the Ubuntu operating system designed and engineered for IoT and embedded systems.

**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