Canonical

Ubuntu Server Hardware Certification Policies

Canonical

Contents

1. Introduction

This guide will provide a reference to the general policies of Ubuntu Server Hardware Certification and services provided by the Canonical Server Hardware Certification Team. This guide will be updated regularly as policies are updated, added or removed during the evolution of the Certification Programme. Audience This guide is intended to be read by anybody (internal or external to Canonical) involved in Ubuntu Server Certification efforts. It should be provided to anyone involved in this effort from engineering to management.

2. Services Provided

The Server Hardware Certification team provides the following services to our customers

2.1. Certification Review

We will review submissions from our Partners' Self-Testing efforts. We will work with the partner to ensure all coverage areas are tested and all required tests are passed. This is the most common means for a Partner's hardware to be tested and listed as Ubuntu Server Certified.

2.2. Certification Testing

While Self-Testing is by far the most common means of certifying servers under the programme, on occasion we will also provide one of the following services to the Partner. Each of the following, however, does come with different requirements and caveats and should be discussed thoroughly so that the you understand the limitations and potential costs involved.

2.2.1. In-House

We will, at the request of the client, perform certification testing in our lab in the Boston, MA, USA area on hardware sent from the partner to our Lab.

2.2.2. On-Site

We will, at the request of the client, travel to the partner facilities and perform certification at the partner facility. This service is not common and must be discussed as early as possible with the team.

2.2.3. Remote

We will, at the request of the client, perform testing remotely assuming that proper VPN-type access and admin control over the MAAS server, SUT, and any additional machines (such as iperf targets) is provided by the Partner. This service is not common and requires the OEM to perform a good bit of lab setup prior to our accessing the network and performing tests. This also requires fast, reliable internet access into the Partner Lab which not every lab can support.

2.3. Certificate Issuance and Publication

We will, upon completion of review, issue a certificate for the SUT and publish that certificate on our HCL (https://ubuntu.com/certified). We will not publish certificates that are created as part of a private engagement. We will not publish certificates for certification testing of hardware that has not yet been made Generally Available to the public. In those cases, we will reserve the certificate until such time as the Partner Server Model has been announced and the Partner has notified us that it's OK to publish the certificate.

In addition to publishing basic information about Server Models that are certified, we will publish the test and support status of all Vendor Approved Options that are applicable to that Server Model.

Note, a failure to adequately test the list of Vendor Approved Options that apply to a Server Model could mean that issuing of a certificate will be delayed or denied until an acceptable amount of Options testing is performed.

2.4. Test Tool Development

We will develop and maintain the Suite for Ubuntu Server Certification testing scenarios. We will make the Suite available in a publicly facing repository along with any necessary dependency packages that are not available in the Ubuntu Main or Universe repositories.

All test scripts and tools will be completely open source software where possible. Proprietary tools are generally not acceptable for official Ubuntu Server Certification Testing. Any exceptions to this rule will be decided on a case by case basis by the Certification Team.

2.4.1. Test Tool Maintenance and Bug Fixing

We will investigate and resolve reported bugs in the Suite. We will maintain the Suite code to ensure it runs reliably on the two most recent Ubuntu LTS versions. We will not actively maintain or update the Suite code for anything older than the two most recent Ubuntu LTS versions.

2.4.2. Website Maintenance and Bug Fixes

We will work with the web team to resolve any bugs or issues discovered with the public or private web sites.

3. Participation

To participate in the Ubuntu Server Certification Programme, the partner will need to meet one of the two following conditions:

- Has engaged with Canonical in our OEM partner program with an active SOA in place. (https://canonical.com/partners/ihv-and-oem).
- Has engaged with Canonical in our Small IHV program and has purchased at least one certification under that program.

3.1. Communications

The Server Certification Team maintains an announcement-only mailing list called `hwcert-announce` for communications that involve hardware certification. This list is low-traffic, opt-in and is used to pass along information regarding the programme, its tools, policies and procedures.

Some items distributed to the list include (but are not limited to):

- New releases of the test suite and related packages
- Critical bug announcements
- Policy changes
- Reminders of upcoming LTS releases

To join the list please send us an email[1].

Questions about the Ubuntu Server Certification Programme may be sent directly to the Certification Team (server-certification@canonical.com)

[1] hwcert-announce-join@lists.canonical.com?subject=Subscribe

4. General Policies

4.1. Comprehensive Server Certification

In order to ensure the best user experience possible when running Ubuntu on Partner Servers, Canonical requires that hardware partners sufficiently test the list of Vendor Approved Options that are applicable to a given Server Model.

As we understand this can be a very long list of devices, your Partner Engineer will work with you to determine a minimal amount of testing necessary to maximise coverage of options across all server models.

This means that not every single device will need to be tested, and none will need to be tested more than once or twice. For this, we require a spec sheet that includes a listing of any Vendor Approved Options for each Server Model to be certified so that we can help determine the matrix of tests needed.

Hardware Partners can send Spec Sheets directly to your Partner Engineer, or can provide a URL to online copies of Spec Sheets.

As this testing is required to help guarantee the quality of Ubuntu on your hardware, and to ensure that end users have the best experience possible when deploying your hardware into an Ubuntu environment in their datacenters, failure to perform sufficient testing of options may result delayed or denied certification requests.

4.2. Devices Specific Information

4.2.1. Boot Device

The Server should be configured so that the only item in the boot order is a single network device configured for Network Booting. If it is impossible to remove HDD/SDD/NVMe devices from the boot menu, the Network Boot device should always be in the first position to ensure the machine ALWAYS boots from Network.

MAAS will instruct the server, during the network boot, to boot from onboard storage if necessary.

4.2.2. CPUs and RAM

Any CPU from a given CPU Family (e.g. Cascade Lake, Ice Lake, Rome, Milan) will count for the entire CPU family. You do not need to re-test for each CPU unless the CPU is from a different family. It is recommended that you do test different models of CPU across a given server line to help broaden the scope of testing.

Any DIMM size may be tested, though we strongly encourage you to use the largest DIMM size available.

Jumps in DIMM size do not require additional testing.

4.2.3. DCPMMs (NVDIMM devices)

Systems that support Intel's Optane DataCenter Persistent Memory Modules must include those DCPMM devices. For convenience, DPCMMs can be configured in mixed mode where supported in a mix of at least 30% RAM and 70% Storage. (That percentage will vary based on the amount of DCPMM storage installed).

Where Mixed Mode is not supported, then testers will need to test the DCPMM devices

in both Memory Mode and App Direct (Storage) Mode, which requires reconfiguring the DCPMM devices, then recommissioning in MAAS and re-running the appropriate test command (one of test-memory or test-storage).

When configuring the DCPMMs for storage a percentage should be dedicated to all block store modes: fsdax, sector, and raw. As with any other storage device, each DCPMM storage volume should be properly partitioned, formatted, and mounted prior to testing.

4.2.4. HDD, SSD, NVMe

For HDDs and SSDs, only one of each supported interface type needs to be tested. You should use the largest HDD or SSD of each type where possible.

Systems that support NVMe devices should include NVMes where possible as well.

4.2.5. RAID Controllers

ALL RAID controllers must be tested. Exceptions can be made to this for very minor variances in RAID Controller Models.

An example of this exception would be two SAS RAID Controllers where they are essentially identical except for the addition or deletion of a Cache Battery.

Your Partner Engineer or the Certification Team will work with you to determine if a RAID Controller is exempt from testing. This will be handled as we build the test matrix for all Vendor Approved Options that apply to each Server Model.

4.2.6. HBA

HBAs must be tested. We will work with you to determine which particular ones from the list of Vendor Approved Options will need to be tested and which can be risk assumed.

4.2.7. CNA and Network Devices

CNAs and NICs must be tested, CNAs should be tested in Network mode. Canonical reserves the right to require further CNA testing in other modes as necessary (for instance a CNA may need to be tested as an iSCSI initiator as well as a Network card).

For Network Devices, all ports must be configured and tested on appropriate network segments (e.g. a 100Gb port must be connected to a network segment that is at least 100Gb and the iperf target must also be at least 100Gb).

4.2.8. GPGPUs

GPGPU testing is supported for NVIDIA and AMD GPGPUs. This is a separate test. When used on NVIDIA GPGPUs, the test requires the installation of drivers, a system reboot, and running a separate test suite. All GPGPU models should be tested, at this time there is no allowance for “representative” samples on GPGPU devices. Please refer to Appendix G - Setting Up and Testing a GPGPU of the Self-Testing Guide for more information.

4.2.9. Anything Else

Any device not explicitly outlined above must be tested. If you have any questions about what should or should not be tested, please contact your Partner Engineer.

4.3. Application of Test Results for Vendor Approved Options

Once a Vendor Approved Option has been tested in ANY Model of a Partner’s Server Line, that Vendor Approved Option will be considered certified for the full Server Line.

Thus, if a Server Line has 10 Models, and the Vendor sells 1 (one) model of 100Gb Network Controller, once that controller has been validated in Model 1, it will also be automatically considered certified for Models 2 - 10.

This does not apply to Blade systems. A PCIe card tested in a rack or tower server chassis does not remove the need to test a Mezzanine card with the same chipset in a Blade or Compute Sled style system.

4.4. Display of Status of Vendor Approved Options

Once a Model is certified it will be publicly listed on the Ubuntu Certification Website[2] described later in this document. In addition to the Model, all Vendor Approved Options that apply to the Certified Model will be listed alongside that Model. Each Vendor Approved Option will show it's status (e.g. Certified, Untested, Unsupported, etc) and at least the Ubuntu Version or Kernel Version that the Option was tested against.

This will give customers a more complete view of what Models and Options are supported by Ubuntu Server.

This will also make creating BOMs for projects easier as there will no longer be any question if the components in a given BOM have been certified.

4.5. Inadequate Test Coverage of Vendor Approved Options

We do not expect the Partner to test all Vendor Approved Options, which is why your Partner Engineer will work with you to create a test matrix and highlight the minimum devices to be tested to provide the maximum coverage of all Options for the Partner Server Model.

Likewise, testing of Vendor Approved Options can be spread out over time and across Certification tests for several servers. Thus if you have a list of 20 Vendor Approved Options and 10 Server Models, you could spread that test effort out so that each Server Model only features 2 Options.

However, as alluded to above, if adequate coverage is not seen within a reasonable amount of time, we reserve the right to delay or reject certificates, and possibly revoke existing certifications as a last resort.

4.6. OS and Kernel Versions

Certifications are available for the two most recent LTS versions of Ubuntu Server. At this time, this includes **22.04 LTS** and **24.04 LTS**.

Certification is never granted for Interim releases of Ubuntu Server (non-LTS versions such as 22.10, 23.04, or 23.10).

Certification Testing should be performed using the LTS release and GA kernel initially (e.g. 24.04 LTS and the ga-24.04 kernel option in MAAS).

When hardware cannot pass certification because of hardware support issues with the GA kernel, testers may use the most recent HWE kernel option (e.g. 24.04 LTS and the hwe-24.04 kernel option in MAAS) to perform testing.

Certification is valid from the certified kernel onward including all subsequent kernel updates and HWE kernel releases for that LTS.

In other words, if a system is certified using 22.04 LTS and the 5.15 GA kernel, that system is certified for the 5.15 (22.04 GA, 22.04.1 GA), 5.19 (22.04.2 HWE), 6.2 (22.04.3 HWE), 6.5

[2] https://ubuntu.com/certified/server

(22.04.4 HWE) and eventually 6.8 (22.04.4 HWE) kernels that comprise the 22.04 LTS and LTS Point Release family.

If a system is certified using 22.04 LTS and the HWE kernel, then the certification is valid from that HWE kernel version onward. Thus if the system was certified using 22.04.3 LTS and the 6.2 HWE kernel, the system is considered certified for the 22.04.3 LTS HWE Kernel version 6.2, the 22.04.4 LTS HWE Kernel version 6.5, and the 22.04.4 LTS HWE Kernel version 6.8.

Any exceptions to this policy will be decided on a case by case basis before the certification can be issued.

4.7. Package Versions

Installation should be performed using the Ubuntu images and kernels provided by the default MAAS image stream hosted at https://maas.io

Deployed OSs for Certification should *not* be updated with current package versions unless explicitly instructed to by the Server Certification Team.

Testing should always start with the GA version of Ubuntu unless the HWE kernel is necessary to provide support for newer hardware. Doing certification primarily on the GA release will ensure the longest support lifetime for customers, while the HWE release will ensure customers are able to use the newest hardware.

Certification should always be performed using the most recent version of the Certification Suite. This is installed separately after the OS Version has been installed on the SUT. Installation is usually performed automatically as part of the deployment process.

4.8. Certification Lifetime

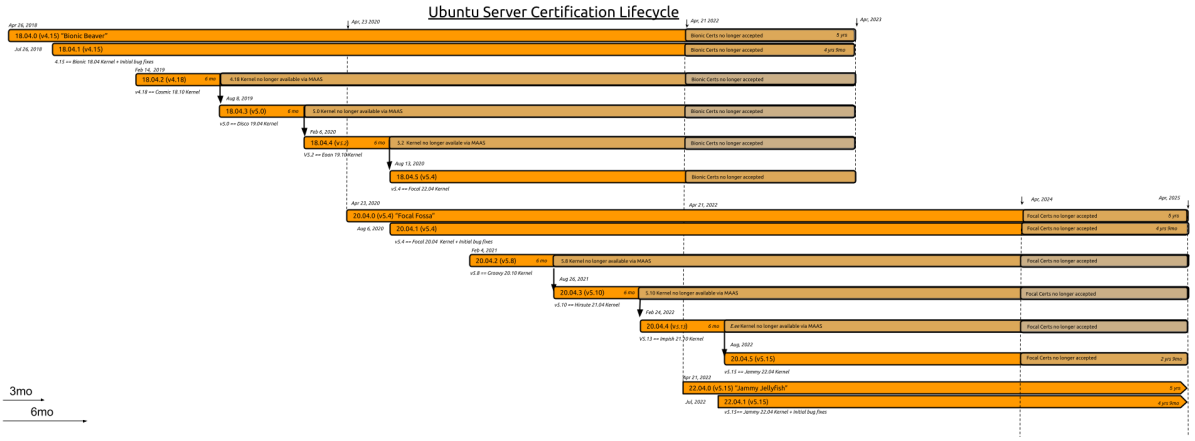

Figure 1: The typical Ubuntu Server Certification LTS Support Schedule. This is also available for download and closer examination from the Certification Portal: https://certification.canonical.com/server/lifecycle/

Certifications are valid from the point release they are issued against until the end of the lifetime for that LTS. For example, a system certified on Ubuntu 22.04.2 LTS will be considered certified for 22.04.2, 22.04.3 and 22.04.4 but will *not* be considered certified for 24.04 LTS or subsequent LTS releases.

Those subsequent LTS releases will constitute a new LTS release family and will require separate certification of each Model and Vendor Approved Option.

4.9. Models

For the purpose of Ubuntu Server Certification, we encourage the testing and certification of a Partner's entire server line, including user selectable Vendor Approved Options.

For each Server Model, we will list all Vendor Approved Components that were tested. We will also list the supported/certified status of each of those components and that information will be plainly visible on the public certification website for each model the Vendor Approved Components are applicable. In order to ensure coverage of as many component options as possible, the Certification team will work with the Partner to decide on a test matrix to cover a model and its full breadth of component options.

4.10. Changes to the Test Suite

4.10.1. Suite Changes

The Certification Suite is constantly evolving as new testing methods are employed, as technology changes, and as bugs are discovered and resolved within the Suite.

Changes to existing test cases in a given LTS will *not* change the test requirements, and will likely only change the method used to test.

Newly introduced tests are considered a Suite change and will not block current LTS certifications.

For example, the KVM test has moved from using qemu directly to using LXD to manage the virtual machine. As this only changes how the test is conducted, the VM test is still considered a blocking test Conversely, the addition of a TPM 2.0 test would constitute a suite change and would *not* gate current LTS certifications, but MAY become a blocker for future LTS releases.

Likewise, tests specifically for new technologies will not be blockers on the current LTS, but could become blockers on the next LTS.

4.10.2. Test Requirements Changes

The requirements for Certification are considered fluid up to the day the LTS is released. At that point, certification requirements are locked in and will not change for the life of that LTS. Any new test cases will be introduced as Non-Blocking items and will not gate certifications.

Note that this only applies to additions to the requirements. Requirements can be eased (tests removed) at any time and *will* be applicable to all certifications going forward. An example of this would be the removal of the requirement for floppy disk testing as such devices are not in use any longer.

4.10.3. Progression of New Tests

As the Suite *is* constantly evolving, there is a natural progression for tests that is applied throughout the development cycle.

Any new test is introduced as a Non-Blocking item. This implies that the test must be run, but will *not* gate the certification effort for the current LTS. As we approach the next LTS, Non-Blocking tests are re-evaluated for promotion to Blocking (Required) tests and likewise, Blocking tests are evaluated for demotion to Non-Blocking or removal altogether.

As a more concrete example, let's suppose a new Storage I/O stress test is introduced after 24.04 LTS is released but before 26.04 LTS. That new test would be introduced as a Non-Blocking test, thus any failures would *not* gate 24.04 certifications. This "Break-In" period is a chance to review and improve the test as well as gather data from various testing scenarios to determine its viability later on.

As we approach 26.04, we would re-evaluate this new Storage Stress test. If it is seen as

important and reliable enough, then it will be promoted to Blocking for 26.04 and be required to pass for all 26.04 certifications.

Also keep in mind that even though this test would now be required for 26.04, it will still remain a Non-Blocking item for 24.04 certifications.

4.10.4. Changes to Certification Policies

The policies for Certification are subject to change at any time for any reason. That said, we make every effort to minimize policy changes and make modifications only where necessary for changing business needs.

4.11. Virtualization

4.11.1. Ubuntu as Host

For all Servers that support virtualization, the KVM and LXD tests must be run with Ubuntu as the host OS. This will launch an Ubuntu guest and validate that virtualization functions. Certification does not apply to using any other operating systems as a virtualization guest OS.

4.11.2. Ubuntu as Guest

In special situations, we will provide Certification of Ubuntu as a guest OS on a different host OS. These certifications are provided on a case-by-case basis and must be agreed upon by both Canonical and the Partner. Please discuss this with your Partner Engineer if you need to certify Ubuntu as a guest on your hypervisor.

4.11.3. Virtual Machine Requirements

Guests or VMs created for the purpose of certifying Ubuntu as Guest on a non-Ubuntu host OS should have a minimum of 4 GiB RAM and at least 100 GiB of disk space to ensure the tests run successfully.

Guests should also have at least one virtual NIC that can successfully ping the MAAS server and iperf target.

Certifications of this type will use the “virtual-machine-full” test plan, which is a subset of the full server suite defined by the “server-full” test plan.

KVM testing is generally not required for certification of Ubuntu as Guest scenarios as nested virtualization (e.g. running KVM inside a VM is considered an advanced/non-standard configuration.) This exception may not apply to certain special situations that are business goal dependent. That determination will be made by the Certification Team.

4.12. System on Chip Certification

The Server Hardware Certification Team also provides System on Chip Certification Services for companies that produce SoCs meant to be used in server systems built by OEM/ODMs down the road.

4.12.1. Application

SoC Certification applies *only* to Systems on Chip and reference boards that showcase those SoCs. It does not apply to production server systems based on SoCs.

Additionally there is no inheritance upstream. So though an SoC may be certified by an SoC vendor like Ampere or HiSilicon, OEM/ODMs who build servers based on that SoC cannot also claim certification for their server.

4.12.2. Server Certification Application

ARM64 SoC based servers can ONLY be certified if the SoC in use is also SoC certified. This is due to the need for enablement and ongoing maintenance of code specific to numerous SoCs.

Also, SoC certification does not imply Server certification and Server certification does not imply SoC certification.

4.12.3. Requirements

SoC certification is best thought of as a subset of Server Certification. The tools and test cases are the same, but SoCs have less stringent requirements for certification. For example, SoCs can have non-functional blocks at the time of Certification.

The implication is that while an SoC may have non-functional blocks (such as USB3), those blocks will and should be enabled by the time an OEM/ODM is creating a server based on that SoC. Note that once a server product based on a certified SoC is presented for Server Certification, it must adhere to the more stringent Server Certification rules. In other words, once the SoC becomes a server, all hardware must work, with the only exception being non-accessible/non-included blocks. A compute card with no externally accessible USB ports, for example, will not need to pass the USB tests.

Additionally, SoC certification does not imply any level of support beyond basic functionality where Server Certification does imply a level of support including Ubuntu Advantage and other avenues.

4.12.4. Exceptions

As noted above, SoC Certification is a subset of Server Certification with less stringent rules. Thus exceptions can be made for items that are non-functional at the time of SoC Certification. When these are encountered, the certification will have a note attached indicating what items are not considered certified and are non-functional or untested.

4.13. Performance / Benchmark Testing

Canonical does not perform performance or benchmark testing as part of certification. Any benchmark or stress tools utilized are used strictly with the goal of introducing significant load to the system. It is the responsibility of the Partner to properly benchmark their own hardware with Ubuntu installed.

4.14. Third Party Testing

Third Party Testing means testing hardware on behalf of another company. This happens when an OEM produces a system that is sold to a reseller who re-brands the hardware and sells at retail under the reseller's name and marketing model.

Third Party Testing for Certification is ONLY allowed on a case-by-case basis and must be agreed upon by Canonical, the OEM who will be doing the testing and the Reseller (who may also be an OEM) who will be selling the hardware at retail.

Any system tested in this manner MUST be readily identifiable as being the Reseller's system. See *System Identification* for more information

4.15. Public Web Site

All published Certificates are accessible via our public certification website found at

- http://ubuntu.com/certified/server
- http://ubuntu.com/certified/soc

Public certificates will include Make/Model, release and pertinent hardware information including certification/supported status of any Vendor Approved Options applicable to the certified Make/Model.

Public certificates will *not* include any Pass/Fail test information, private system data or other details that are not meant to be publicly accessible.

4.16. Private Web Site

The private certification portal can be found at:

- https://certification.canonical.com

This site is often referred to as C3.

Access to C3 is available only to Canonical employees and designated employees of partners participating in the Programme.

The private site will provide the Partner with a history of all certified and registered models and a history of all submitted test results and all certificates.

People with access must have an account on Launchpad (https://launchpad.net) and their account must be added to the appropriate access group by the Partner's PE or a member of the Certification team.

4.17. Documentation

All documentation for the Certification Programme is available on C3 in both PDF and HTML versions.

5. Certification Process

Most of the Certification process is defined in the Self-Test Guide. This document is meant to provide additional information and guidance on the Certification process.

5.1. Timeframe

Depending on the activity, the following should apply as far as time estimates:

- Self-Testing reviews should be completed within 2 business weeks from initial submission to completion or publishing.
- Onsite testing should be completed within 2 business weeks from initial testing to completion or publishing.
- Remote testing should be completed within 2 business weeks from initial testing to completion or publishing.
- Publishing of certificates is instantaneous as soon as the certificate is marked as passing.
- Replies to inquiries should happen within 3 business days (this only applies to replies, it does not imply that a resolution to any inquiry will occur within that time).
- Hardware enablement or bug fixing has no set timeframe due to the nature of those issues. Bugs will be resolved as quickly as we can; however, due to the variations in severity, complexity, and impact on other releases and systems, the actual time to fix and SRU a bug fix can vary from a few days to several weeks. Additionally, hardware enablement may require hardware to be present in our lab and may take several weeks to develop and then push into the kernel, MAAS, or wherever is appropriate.

5.2. Test Lab

The test lab should be as clean as possible and should have as simple a network as possible. Network segments need to match the fastest supported speed of any NIC on the SUT. (e.g. a 100 Gb NIC must be connected to a 100 Gb LAN and the `iperf` target must also have a 100 Gb connection).

The lab will work best when there is unfettered Internet access for downloading test tools and dependency packages as well as MAAS images, cloud images, and so forth.

If Internet access is spotty or not permitted, local repository mirrors can be employed, but those require additional setup and maintenance.

If the Certification Team requires access, access should be provided via VPN or some similar means of ingress.

SUT BMCs should be connected and configured as described in the Self-Testing Guide. (See the *Documentation* section above)

Certification requires MAAS to be used to deploy all test systems.

5.3. Hardware

Hardware to be Certified should be GA level hardware, *not* development level hardware, SDV, BBVT, FVT or any other non-ready-for-production level. The hardware should be the same hardware that customers are able to purchase.

5.4. Firmware

Firmware should be GA or similar level. In all cases, firmware should be GA level, with the only exception being the need to use unsigned versions in order to maintain the ability to flash revisions up or down as needed.

Firmware should be available somewhere online and not a secret build that is only available internally to the Partner or Canonical. The only exception here is for initial release firmware that comes on a newly released system.

You do not need to recertify on updated versions of firmware. We will list the firmware in use at the time of certification and will support users from that firmware level onwards.

That is not to say we won't recommend a firmware update where appropriate, but rather sets a baseline firmware level with the expectation that the Partner will continue to ensure that updates to firmware do not cause issues with running Ubuntu on already certified hardware.

5.5. System Identification

Data in firmware must contain valid and correct identifiers for the make/model being tested. Typically this information is contained in DMI Types 1, 2 and 3.

If the system is sold by a Partner ODM, then the DMI data must include the correct Make and Model for the SUT.

If the system is sold by a Partner OEM and intended for resale by a different brand or under a different mark, then DMI must include SOME sort of verifiable identifier that shows the SUT is, in fact, the model being tested. This distinction is allowed as in many cases, OEM systems may not have the Make/Model fields filled out.

In cases where one OEM/ODM is performing testing on behalf of another OEM/ODM who re-sells hardware from the primary OEM/ODM, that hardware MUST be identifiable in firmware as belonging to the reseller OEM/ODM.

Example: If Vendor A is testing hardware on behalf of Vendor B, the firmware must clearly show that the hardware is a model produced by Vendor B. Typically, this requires that DMI Type 1 (System) shows Vendor B as the Manufacturer and uses the Vendor B Marketing Model for the Product field. In these cases, DMI Types 2 and 3 can indicate Vendor A as the manufacturer.

5.6. Installation

Installation must be performed by Canonical's MAAS (Metal-As-A-Service). MAAS must use the default Ubuntu images and kernels provided via https://maas.io for all Certification deployments.

If a System cannot be deployed via MAAS and it is determined that this is a lack of support or bug in MAAS, then we will work with the partner and the MAAS development team and Server Hardware Enablement to resolve issues that prevent successful deployments of the SUT.

5.7. Custom Kernels and Drivers

Custom kernels are not allowed for Certification. Certified hardware must work with the standard Ubuntu kernel for the SUT's architecture. No unaccepted kernel patches will be allowed.

The standard Ubuntu Kernel includes the GA kernel or any released HWE kernel.

The exception to this involves kernel modules as outlined below.

Modules injected via DKMS generally are not allowed for certification.

5.7.1. Third Party / Proprietary Drivers

Hardware should be tested and certified using in-band drivers provided by the Ubuntu kernel. In cases where hardware is not supported by the current Ubuntu kernel, testing should then focus on the current HWE kernel.

Partners should work with their IHV upstreams to ensure necessary driver support is present in the Linux Kernel and will thus land naturally in the Ubuntu kernel.

Out-of-Band (Proprietary) drivers may be considered for use in Certification but that must be approved by the Canonical Hardware Certification Team.

For more information, please contact your Partner Engineer.

5.8. Storage Options

Certification testing should be performed for each storage mode supported. Thus if a system supports JBOD and onboard RAID plus an optional PCIe add-in RAID card (that controls onboard disks), the storage tests should be run against all three configurations.

The Server Test Suite provides a `storage-only` test plan for this purpose.

5.8.1. Storage Management Software

Any storage management software meant to manage, modify, monitor storage devices including internal and/or external arrays, JBODs, or other storage subsystems should be provided to Ubuntu users in a manner equal to the way it is presented to users of other operating systems. The preferred method is via a Debian package provided via download from the Partner's website, or as a Snap package available via the Snap Store. The package should be presented equally with the same software packaged for other Operating Systems.

5.9. USB Testing

USB Testing requires at least one USB stick matching the fastest type of port (USB2, USB3). Thus if a SUT has both USB2 and USB3 ports, you will need at least one USB3 thumb drive plugged into the appropriate port prior to testing.

5.10. Network Testing

Network testing requires a second system to serve as a network target running `iperf3` in Server modes.

Network devices must be connected to clean networks of at least the maximum supported speed for the device. Thus, a 100 Gb NIC must be connected to a 100 Gb LAN and the `iperf3` target must also have a 100 Gb NIC connected to the same LAN. A 1 Gb NIC may be connected to either any LAN segment that is 1Gb or faster.

All onboard network devices and ports MUST be tested.

As described in the Self-Testing Guide a separate server is NOT required as the MAAS server

can also function as the `iperf3` target provided the MAAS server has appropriate network ports to match the speed of the fastest NIC to be tested.

5.11. Bugs

It is not normal to encounter significant bugs during certification, or at least it should not be expected; however, bugs are found from time to time and must be addressed. In general, your Partner Engineer will work with your teams to shepherd bugs through our bug process with some level of priority given to bugs that block certification.

5.11.1. Bugs from Tier 1 Partners

Bugs from vendors that recognize Ubuntu as a Tier 1 OS will receive priority over other bugs. This does not imply any specific SLA or time frame, but we will work with engineering teams within Canonical to escalate bugs from Tier 1 vendors with the understanding that those engineering teams will have the right to decline or delay fixing a bug depending on business needs at the time.

5.11.2. Test Suite Bugs

Bugs found in the Suite *will* be treated with priority over feature additions or other work. We will work with the partner to resolve any bugs in the Suite in a timely manner, and will provide modified versions of the various files affected if necessary to speed a certification along. It is very important for the Partner and Tester to work directly with the Certification Team to resolve any bugs found in the Suite, including being available to re-run tests, commands, participate in debugging, replacing or patching the Suite, etc.

When such bugs are discovered, please reach out to your Partner Engineer for guidance.

5.11.3. Hardware Bugs

Bugs found in hardware or firmware are solely the responsibility of the partner to fix. The timeframe for doing so is entirely at the Partner's discretion, and thus could cause a certification to be significantly delayed.

5.11.4. OS Bugs

Certification blocking bugs found in the OS may be filed by either the Partner or the PE or Certification team.

It is up to the PE and Partner to work together to get any bugs filed against the OS resolved in a timely manner. Note that OS bugs could result in certification being delayed until the OS SRU process is completed and any fix has been introduced to the OS via the Updates repository.

Additionally, membership in the Canonical OEM Partner Programme does not imply any sort of special handling of OS bugs. We will make a best effort to escalate bugs from our Partners, but Canonical's engineering teams are under no obligation to accept that escalation outside of a special engineering engagement.

5.11.5. Regression Bugs

Bugs found in the OS during re-certification, or during regression testing, will be handled with higher priority than normal bugs. A bug found in a later package version will *not* jeopardize an existing certification. In other words, if package X is version 1.01 in 20.04 when a SUT is certified and package X is version 1.10 in 22.04 and causes a failure during regression testing, your original 20.04 certification will not be affected, and the regression introduced in version between version 1.01 and 1.10 of package X will be treated with higher priority as a regression in the OS.

5.11.6. Enablement Bugs

Bugs determined to require hardware enablement for a Model to pass Certification will need to be examined and discussed with the Partner Engineer and Canonical to determine the best course of action. This may require a paid Non-Recurring Engineering engagement with Canonical to perform the enablement work necessary.

Examples of Enablement NRE would include, but are not limited to, a new server management engine that requires use of a special API for hardware management or the inclusion of a new driver that is not supported by the current HWE kernel.

We will, at our discretion, attempt to do cherry picks of enablement patches from the Mainline kernel into the LTS GA kernel but do not guarantee that service. It is performed as a courtesy and is entirely dependent on the Partner Engineer's workload and acceptance by the relevant engineering team within Canonical.

5.12. Submission of Results

Results should be submitted using the process outlined in the Self-Testing Guide.

5.13. Requesting Certificates

Certificates should only need to be requested *one* time per System per Release.

If re-tests are needed to satisfy testing requirements, do *not* create separate certificates.

Certificates are not necessary for subsequent point releases. If a system is certified already on 20.04.2, you do *not* need a new certificate for 20.04.3 and 20.04.4.

Certificates *are* necessary for each LTS family. If a system is certified for 20.04.3, it *does* need a new certificate for 22.04 LTS.

5.14. Verifying Results

The Model certified should be maintained in the Partner's Lab for a period of up to 30 days (unless discussed with your Partner Engineer) and said lab should be made accessible via VPN or similar access to the Hardware Certification team, including root/admin level access to the MAAS and iperf servers and BMCs so that the Hardware Certification engineers can periodically validate the test results with spot checks.

This policy does not imply that validation will happen with every submission, but upon request. If the hardware cannot be held for a reasonable period of time, the Partner should make arrangements to re-acquire the hardware for a brief period as soon as possible, OR communicate the need for urgency to the Hardware Certification Team or Partner Engineer for advice.

5.15. Private Certificates

Private certifications are available but are only allowed on a case-by-case basis. Private certifications are generally used for pending tenders that the Partner wishes to participate in, or for certification on a pre-GA system with the expectation that such certification will be made public after the system GAs. If you believe you need a private certification, please contact your Partner Engineer for more information.

5.16. Zero-Day Certification

We encourage "Zero-Day Certification" for a new LTS release. This allows our Partners to advertise certified status on the latest LTS release of Ubuntu Server on the day it is released. In order to participate in Zero-Day Certification, the following applies:

- SUTs must be tested within the testing window prior to LTS release, usually a 2- to 3-week period before release. Testing is conducted on the RC or last Beta of the LTS release.
- SUTs must subsequently be *re-tested* for official certification using the GA/Release version of the new LTS within 60 days of Release. Thus, if Server A is certified Zero-Day, it must also be re-tested for official certification within 60 days following the LTS Release Day (GA +60).
- SUTs that are *not* re-tested within the Cert Window will lose their certified status until such time as they are tested on the GA version of the LTS in question.
- All other requirements must be met for Zero-Day Certification (e.g. MAAS for deployments, GA firmware, etc).

5.17. Re-Testing

Occasionally, re-testing is necessary to satisfy testing requirements, resolve bugs or other needs. The Certification Team will assist with guidance on what to re-run and how/when to do so.

Results from re-runs should be submitted to the same hardware entry as the original certification results. A private "Note" should be added to any existing certificate request that provides a link to the new retest results.

Do *not* request further certificates each time retest results are submitted to C3.

When performing retests, you MUST run the full requested test plan. We provide targeted test plans and launchers to assist with this. For example, if you are asked to re-run a storage test, you should run the `test-storage` command which runs a small storage only subset of tests.

You should never modify a test plan. Modifying a test plan will result in the submission being rejected by the certification team. The only exception to this rule is for test launchers such as `test-network` which do allow you to deselect undesired network devices to save time on the retest.

5.18. Regression Testing

The Certification Team performs regression testing on a pool of certified hardware on a regular cadence to ensure and improve the quality of Ubuntu SRU kernels and point releases. Partners should likewise include a regression testing component in their own testing programs.

The Certification Team runs regression testing on hardware contained in the Certification Lab.

Any regressions discovered do not affect existing certifications.

5.19. Re-Certification

Re-Certification is necessary in certain circumstances. Primarily, when a new LTS is released, certification from the previous LTS does not carry forward, thus any currently certified system that should be certified for the new LTS will need to be re-certified on the new LTS version.

Additionally, there are occasional changes that mandate re-certification. Anything that fundamentally alters a SUT's electronic profile requires re-certification. This includes, but is not limited to:

- CPU Family updates (e.g. system refreshes that change from Cascade Lake to Ice Lake to Sapphire Rapids)
- Memory technology updates (e.g DDR4 to DDR5)
- Changing an on-board device, on-board meaning soldered to the main or daughter board. Changing out a PCIe or Mezzanine device may require testing of the new device, but will not trigger a full recertification.

The following are examples of things that do not require re-certification (again, this list is not limited to the following):

- CPU Speed bumps or core count increases (e.g. AMD Milan -> AMD Milan X)
- Memory amount changes (e.g. 4 GiB to 16 GiB) *unless* that includes an increase in the number of memory slots physically on the board.

Whenever a question of re-certification comes up, the Certification Team will investigate the situation and make a decision on a case-by-case basis.

5.20. Physical Certificates

Typically, the entry on the Ubuntu Certification Website (https://ubuntu.com/certified) is considered the "Certificate"; however, on occasion where a PDF certificate is needed, such as for a tender or business case, we will create and provide an official PDF Certificate for your system.

To request a physical certificate, please contact your Partner Engineer.

5.21. Hardware for Regression Testing and Other Needs

For members of the full SOA programme, Canonical reserves the right to purchase at a negotiated discount, up to two (2) of each certified model of server, and a selection of Vendor Approved Options for purposes including, and not limited to, regression testing, bug investigation, test development and other needs.

If your company is a member of the Small IHV program and purchasing Certifications ad hoc, you are required to provide Loaner servers to our lab.

Please refer to your Certification Supplement and contact your Partner Engineer for any questions about hardware purchases or loaners.

6. Glossary

This glossary is intended to provide a common understanding of terms used in the Server Certification Programme.

Blocking Test
: Tests or coverage areas that are required to be tested and required to pass for Certification.

Certificate
: An indicator that a system has been tested and is considered fully supported by Ubuntu Server.

Certification
: The process by which a system is tested and deemed “Ubuntu Server Certified.”

Non-Blocking Test
: Tests or areas that are tested but do not block Certification if they fail. These could be newly introduced test cases, informational jobs, or other items that we want to have run but will not block a certification.

IHV
: Independent Hardware Vendor, or the entity that builds components and accessories meant to be used as part of a broader whole system (e.g. network or storage device manufacturers.)

Make
: The OEM/ODM/IHV that makes the device or system (e.g. HP, Dell, Broadcom, Intel)

Model
: The Model of the hardware being tested, the Family. For example, DL385. This is the superset of a “Model” that includes all the variants of that model.

ODM
: Original Design Manufacturer, or the entity that designs and produces and retails the hardware.

OEM
: Original Equipment Manufacturer, or the entity that designs and produces the hardware with the intention that the hardware will be re-branded and sold by a third party

Partner
: The OEM, ODM, IHV or System Builder who has joined the Programme and is engaged in Certification efforts.

Partner Engineer
: The Partner’s technical contact within Canonical. Formerly known as a TPM or Technical Partner Manager.

SOA
: Standard OEM Agreement. This is the agreement that defines the Hardware Partner and Canonical relationship with regard to our Partner Engineering team and Server Hardware Certification.

Self-Testing
: The Partner is allowed to perform certification testing on their own, using their own lab and engineering resources with Canonical providing review, guidance and acceptance.

Small IHV Programme
: A program aimed at smaller manufacturers who seek Certification but do not have catalogs large enough to benefit from the full SOA.

SUT
: System Under Test, the system that is being proposed for Certification

Suite
: The Server Certification Test Suite.

Ubuntu Server Certified
: Indicates, via a published and/or approved Certificate, that a System has been tested and is shown to be fully supported by Ubuntu Server.

Variant
: A subclass of a Model, for example, a Model may have two variants that feature different network devices.

Vendor Approved Option
: Any device that can be ordered by the customer for a given Server Model. This includes Network devices, HBAs, RAID controllers, and so forth.