CANONICAL

Ubuntu Server Hardware Certification Policies (16.04 LTS)

Contents

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.

Definitions

Blacklist Test

Tests or areas that are not tested and not required 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.”

Greylist Test

Tests or areas that are tested but do not block Certification if they fail.

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.

Partner

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

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.

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.

Whitelist Test

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

Services Provided

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

Certification Services

In-House

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

On-Site

We will, at the request of the client, travel to the partner facilities and perform certification at the partner facility.

Remote

We will, at the request of the client, perform testing remotely via VNC or other means. 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.

Certification Review

We will review submissions from our partners from Self-Testing efforts. We will work with the partner to ensure all coverage areas are tested and all whitelist tests are passed.

Certificate Issuance and Publication

We will, upon completion of review, issue a certificate for the SUT and publish that certificate on our HCL (http://www.ubuntu.com/certification) 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 SUT has been made GA and the Partner has notified us that it's OK to publish the certificate.

Test Tool Development

We will develop and maintain the Suite for all testing situations. We will make available the Suite in a publicly facing repository along with any necessary dependency packages.

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 all current Ubuntu LTS versions.

Website Maintenance and Bug Fixes

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

Participation

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

- Has become a member of the Technical Partner Programme (http://partners.ubuntu.com/programmes/hardware).
- Has an existing or pending Ubuntu Advantage agreement for an existing or in-development deployment that needs Certification services to authenticate Technical Support access.

Ubuntu Server Certification is not sold ad-hoc and at this time is only open to Canonical's partners and customers.

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 visit https://lists.canonical.com/mailman/listinfo/hwcert-announce

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

General Policies

OS Versions

Certifications are available for the two most recent LTS versions of Ubuntu Server. At this time, this includes 14.04 LTS and 16.04 LTS

Certification is never granted for Interim releases of Ubuntu Server (non-LTS versions such as 15.04, 15.10 or 16.10).

Certification Testing is performed on the following LTS releases:

- LTS GA - ex. 14.04 LTS GA as released in April 2014
- Current LTS Point Release - ex 14.04.3 as released in August 2015

Package Versions

Installation should be performed using the custom MAAS images that the Server Certification Team provides. This provides a mechanism for quickly deploying the Suite and a known set of packages to the SUT.

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

Certification should always be performed using the most recent version of the Certification Suite. This is installed separately after the OS Vesrion has been installed on the SUT.

Certification Lifetime

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 14.04.2 LTS will be considered certified for 14.04.2, 14.04.3, 14.04.4 and any subsequent 14.04 point release but will *not* be considered certified for 16.04 or subsequent LTS releases.

Models

For the purpose of Ubuntu Server Certification, only specific configurations are considered certified. This is due to the vast array of optional components available on CTO server systems that may or may not have been tested with Ubuntu Server.

For each Certificate, we list the specific components that were tested and the sum of those parts is considered the Certified System. 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 plan to cover a model and its full breadth of component options.

Changes to the Test Suite

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. Test changes in a given LTS will *not* change the test requirements, and will likely only change the method used to test.

Newly introduced tests, however, are considered a Suite change and will not gate current LTS certifications

For example, the network testing may move from iperf2 to iperf3, which will not affect testing or certification. Conversely, the addition of an Apachebench based Network 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.

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 Greylist 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.

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 Greylist 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, Greylist tests are re-evaluated for promotion to Whitelist (Required) tests and likewise, Whitelist tests are evaluated for demotion to Greylist or removal altogether.

As a more concrete example, let's suppose a new Storage I/O stress test is introduced after 14.04 LTS is released but before 16.04 LTS. That new test would be introduced as a Greylist test, thus any failures would *not* gate 14.04 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 16.04, we would re-evaluate this new Storage Stress test. If it is seen as important and reliable enough, then it will be promoted to Whitelist for 16.04 and be required to pass for all 16.04 certifications.

Also keep in mind that even though this test would now be required for 16.04, it will still remain a Greylist item for 14.04 certifications.

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.

Virtualization

Ubuntu as Host

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

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 Account Manager if you need to certify Ubuntu as a guest on your hypervisor.

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 / `iperf` Target.

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

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.

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.

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 APM or Texas Instruments, OEM/ODMs who build servers based on that SoC cannot also claim certification for their server.

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.

Exceptions

As noted above, SoC 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.

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.

Public Web Site

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

http://www.ubuntu.com/certification/server
http://www.ubuntu.com/certification/soc

Public certificates will include Make/Model, release and pertinent hardware information including the exact configuration that was used for Certification.

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

Private Web Site

The private web 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 TPM or a member of the Certification team.

Documentation

All documentation can be accessed by several methods:

- C3 has links to all document files
- The *certification-docs* package available from the Hardware Certification Public PPA contains copies of all documents in both PDF and HTML versions.
- The *certification-docs* package is also installed on every SUT as a suggested package for *canonical-certification-server*
- MAAS servers installed following our MANIAC guide provide the docs via html locally (http://maas.server.ip/doc)

Certification Process

Most of the Certification process is defined in the Self-Testing Guide. (See the *Documentation* section above)

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 2 business days (this only applies to replies, it does not imply that a resolution to any inquiry will occur within that time).

- Web updates should be completed within 3 - 4 business weeks depending on the necessary changes to the website and when those changes are requested as they must undergo a completely different development and acceptance procedure that has a minimum 3 week development cycle.
- 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 requires hardware access in our labs and may take several weeks to develop, push into MAAS and then find its way into a MAAS update.

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 10 Gb NIC must be connected to a 10 Gb LAN and the `iperf` target must also have a 10 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 appropriately.

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

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.

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.

Installation

Installation must be performed by Canonical's MAAS (Metal-As-A-Service). MAAS must use the custom images provided by the Certification team 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.

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.

Third Party / Proprietary Drivers

Hardware that requires a third party driver must meet the following requirements:

- Driver must be packaged in the proper format
- Driver must be accessible to a MAAS server
- Instructions must be clearly provided to users that explain how to add that driver to MAAS
- The driver must be tested.

For more information, please contact your account representative.

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` whitelist for this purpose.

USB Testing

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

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 10 Gb NIC must be connected to a 10 Gb LAN and the `iperf3` target must also have a 10 Gb NIC connected to the same LAN. A 1 Gb NIC may be connected to either a 1 Gb or 10 Gb LAN.

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, certification agreements do not imply any prioritizing of bugs found over any other bug. If bugs are discovered that block certification, the Partner and their Account Manager should work to have those bugs addressed appropriately.

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.

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.

OS Bugs

Bugs found in the OS will be filed by either the TPM or the Certification team. It is up to the TPM 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.

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 16.04 when a SUT is certified and package X is version 1.10 in 16.04.2 and causes a failure during regression testing, your original 16.04 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.

Submission of Results

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

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 14.04.2, you do *not* need a new certificate for 14.04.3 and 14.04.4.

Certificates *are* necessary for each LTS family. If a system is certified for 14.04.3, it *does* need a new certificate for 16.04 LTS.

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 need a private certification, please contact your account manager for more information.

Zero-Day Certification

We will allow for "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).

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.

Regression Testing

The Certification Team performs regression testing on a pool of certified hardware at each Point Release and Interim Release. 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 and in the OIL programme.

The pool of hardware tested by the Certification Team for each release rotates so not every model is tested on every release.

Regressions do not affect existing certifications.

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 system that should be certified for the new LTS will need to be re-certified.

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. Haswell -> Broadwell -> Skylake)
- Memory technology updates (e.g DDR3 to DDR4)
- Changing an on-board device

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

- CPU Speed bumps (e.g. Haswell 1.6GHz -> Haswell 2.4GHz)
- 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.

- Adding or removing a PCI optional device such as a RAID or external network controller

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.

Physical Certificates

Typically, the entry on the Ubuntu HCL (http://www.ubuntu.com/certification) 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.

Sending Canonical Hardware

As a condition of Certification, a sample of each certified system must be made available to Canonical engineers whenever needed for bug fixes, support escalations and for other similar reasons.

This does not mandate that hardware is required to be sent to Canonical; *however*, partners are not prohibited from sending sample hardware to Canonical on a loan or permanent basis to be placed into our labs for ongoing testing or support or other related work.

OpenStack Interoperability Labs

Canonical offers Partners the option of participating in our OpenStack Interoperability Lab (http://partners.ubuntu.com/programmes/openstack).

Participation in OIL does not automatically grant certified status; however, any server that is placed into OIL must be certified before it can be placed in OIL.

The typical workflow looks like this:

1. Hardware sent to Canonical Lab
2. Certification Team tests and certifies
3. Hardware transferred to OIL
4. Interoperability testing begins.