# Canonical Certification Documentation

A. **Purpose:**

This document describes how to build a MAAS server in order to commission and deploy a system, install the certification test suite and then perform certification testing to the system. This document guide is modeled after Ubuntu Server Certified Hardware Self-Testing Guide (reference https://certification.canonical.com) with some modifications to tailor SMC System and requirements. Thus, this document is for SMC internal use and purposes only.

B. **Prepare the needed Hardware:**

MAAS server, IPERF server, KVM server (optional), Network Switch and Router, and at least one SUT. As shown below is the network logic diagram used for this document.
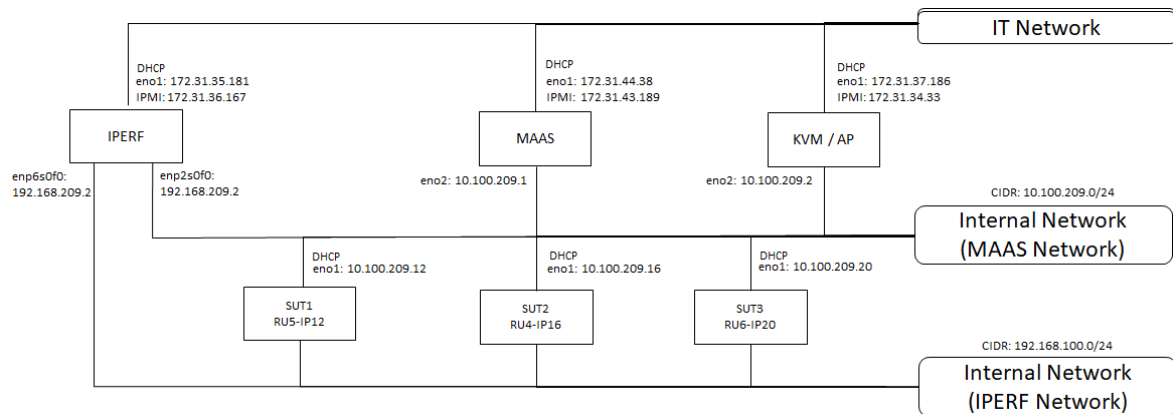
Hardware Required:

- MAAS Server – Ensure the computer has two network interfaces
- IPERF Server – Preferably a computer that has multiple NIC cards to be able to run iperf program to test all sort of System's network interfaces. Both iperf (version 2) and iperf3 MUST BE LOADED to the IPERF computer
- KVM/AP Server (optional) – This computer will serve as an access point to the System under test (SUT) for remote controlling and monitoring purposes. The computer must be loaded with a remote desktop sharing application (such as VNC or TeamViewer) to provide remote access to the node(s) in test
- SUT – at least one system to be used as a test unit that is capable to PXE boot through network and has IPMI capability
- Gigabit or faster Switch – to provide local area network to all devices defined in the network configuration above
- Router – to connect and communicate to outside networks (internet purposes)

C. **Installing and Configuring Ubuntu** (Ref: Certification/MAAS_Advanced_NUC_Installation_And_Configuration.pdf)

Once all basic hardware is assembled, prepare MAAS server for OS installation. This guide assumes the use of Ubuntu 16.04 and MAAS 2.3.0

- Install Ubuntu 16.04 (Xenial Xerus) to the MAAS server.
  https://www.ubuntu.com/download/server
- Boot the MAAS server and log in
- Configure your external network port (ex. eno1 as DHCP)
- Configure your MAAS server internal port (ex. eno2 as STATIC with an ip address
  10.100.209.1/24). Note: Avoid the use of 10.0.3.0/24 address range
- Do not specify a gateway for the private internal LAN. Below is an example of MAAS
  server network configuration:

```
cat /etc/network/interfaces

# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eno1
iface eno1 inet dhcp

auto eno2
iface eno2 inet static
    address 10.100.209.1
    netmask 255.255.255.0
    broadcast 10.100.209.255
```

- To build the MAAS server for canonical certification purposes, either you follow the
  step-by-step guideline stated in this document or execute the script at command line
  https://github.com/acduroy/bridge-network/blob/master/maas-cert-install.sh to
  partially automate your MAAS installation.

- Starts here are your step-by-step guidelines to install MAAS for canonical certification
  testing:
- Update the software on your MAAS server to the latest versions available

```
$ sudo apt-get update

$ sudo apt-get dist-upgrade -y
```

- Reboot the computer

D. Installing and Configuring MAAS:
- Installing MAAS for certification testing. Almost all files will be installed in subdirectories
  of /usr/share/maas-cert-server

```
$ sudo apt-add-repository ppa:hardware-certification/public

$ sudo apt-get update
```

```
$ sudo apt-get install maas-cert-server
```

- Verify that you've installed MAAS 2.1.2 or later

```
$ dpkg -s maas | grep Version

Output:
Version: 2.3.0-6434-gd354690-0ubuntu1~16.04.1
```

- Check or edit /etc/maas-cert-server/config file for correct parameters of INTERNAL_NET and EXTERNAL_NET
- Note: NO spaces surrounding the equal signs (=) in the assignments!

```
$ sudo vi /etc/maas-cert-server/config

INTERNAL_NET=eno2
EXTERNAL_NET=eno1
MIRROR_HOME=/srv/mirrors
```

- You might use this feature if your iperf server is not the SUTs' network gateway or if you have multiple iperf servers.
- This setting can be overridden on SUTs by editing the /etc/xdg/canonical-certification.conf file on the SUT
- Optionally create an /etc/maas-cert-server/iperf.conf file to identify your iperf server(s)

```
$ cd /etc/maas-cert-server
$ ll
-rw-r--r--   1 root root    61 Apr 10 18:47 config
-rw-r--r--   1 root root    28 Apr 27 14:21 iperf.conf

$ sudo vi iperf.conf
10.100.209.50,192.168.209.2
```

E. **Running the Setup Script:**
- Running the Setup Script:
- Below is the sample output of the setup script

```
$ sudo maniacs-setup

        Output (from maniacs-setup script):
        ################################################################
        ****************************************************************
        * Identified networks:
        *   INTERNAL: 10.100.207.1 on eno2
        *   EXTERNAL: 172.31.40.40 on eno1
        *
        * Is this correct (Y/n)? Y
        ****************************************************************
```

```
* Reconfiguring maas-region-controller
apache2.service is not a native service, redirecting to systemd-sysv-install
Executing /lib/systemd/systemd-sysv-install is-enabled apache2
* Reconfiguring maas-rack-controller
***************************************************************

* Verifying that MAAS is running....
MAAS is running
***************************************************************
* A MAAS administrative account with a name of alecd is being
* created.
*
* Please enter a password for this account:
* Please re-enter the password for verification:
* Setting up the alecd MAAS account using the supplied password

You are now logged in to the MAAS server at
http://10.100.207.1/MAAS/api/2.0/ with the profile name 'admin'.

For help with the available commands, try:
 maas admin --help


***************************************************************

* Setting up SSH keys for alecd

***************************************************************
* NAT enables this computer to connect the nodes it controls to the Internet
* for direct downloads of package updates and to submit certification results
* to C3.
*
* You can configure this computer to automatically start NAT. If you do so, you
* can disable it temporarily by using the 'flushnat.sh' script or permanently
* by removing the reference to /usr/sbin/startnat.sh from /etc/rc.local.
*
* Do you want to set up this computer to automatically enable NAT (Y/n)? Y


***************************************************************

* Mirroring an archive site is necessary if you'll be doing testing while
* disconnected from the Internet, and is desirable if your test site has
* poor Internet connectivity. Performing the mirroring operation takes
* time and disk space, though -- about 150 GiB per release mirrored.
* To defer this task, respond 'N' to the following question.
*
```

```
* Do you want to mirror an archive site for local use (y/N)? N

* You can set up a local mirror later by running this script with the
* --mirror-archives (or -m) option.
*
*********************************************************************
* An Ubuntu cloud image is required for virtualization tests. Having such
* an image on your MAAS server can be convenient, but downloading it can
* take a while (each image is about 250MiB). This process will import cloud
* images for whatever releases and architectures you specify.
*
* To defer this task, respond 'N' to the following question.
*
* Do you want to set up a local cloud image mirror for the virtualization
* tests (Y/n)? Y
* Cloud Mirror does not exist.  Creating.
* Do you want to get images for trusty release (y/N)? N
* Do you want to get images for xenial release (Y/n)? Y
* Do you want to get images for artful release (y/N)? N
* Do you want to get images for bionic release (y/N)? N
*
* Do you want to get images for amd64 architecture (Y/n)? Y
* Do you want to get images for i386 architecture (y/N)? N
* Do you want to get images for arm64 architecture (y/N)? N
* Do you want to get images for armhf architecture (y/N)? N
* Do you want to get images for ppc64el architecture (y/N)? N
* Do you want to get images for s390x architecture (y/N)? N
* Downloading cloud images.  This may take some time.
*
* Downloading images for xenial on amd64....
* Succeeded downloading xenial-server-cloudimg-amd64-disk1.img
* Succeeded downloading xenial-server-cloudimg-amd64-lxd.tar.xz
* Succeeded downloading xenial-server-cloudimg-amd64-root.tar.xz
*
* Virtualization image mirror is stored as /srv/cloud
* and is available at http://10.100.209.1/cloud/

*********************************************************************
* Setting up MAAS IP address ranges:
*    Low IP address = 10.100.209.10
*    High IP address = 10.100.209.250
* Initializing rack controller
Success.
*
```

```
*********************************************************************
* Configuring MAAS to use 10.2.1.205 as upstream DNS server
Success.
Machine-readable output follows:
OK
squid.service is not active, cannot reload.
invoke-rc.d: initscript squid, action "reload" failed.

*********************************************************************
* Now configuring MAAS to use the 'flat' storage model by default....
*
Success.
Machine-readable output follows:
OK

*********************************************************************
* MAAS tells nodes to look to an Ubuntu repository on the Internet. You

* can customize that site by entering it here, or leave this field blank
* to use the default value of http://us.archive.ubuntu.com/ubuntu/.
*
* Type your repository's URL, or press the Enter key:
* Setting the repository URL to http://us.archive.ubuntu.com/ubuntu/

Success.
Machine-readable output follows:
OK

*********************************************************************
* Setting up certification preseed files....
*
*********************************************************************
* MAAS requires boot resource images to be useful; however, importing them
* can take a LONG time. You can perform this task now or defer it until
* later (or do it manually with the MAAS web UI).
*
* Do you want to import boot resources now (Y/n)? Y
* Importing boot resources. This can take a LONG time....

*********************************************************************
* Ubuntu hardware certification is done using point-release images. These
* can take a LONG time to download. You can do so now or defer this task.
*
* Do you want to import point-release images now (Y/n)? Y
```

```
*
* Do you want to import 17.04 (1 image) (y/N)? N
*
* Do you want to import the 16.04 series (3 images) (Y/n)? Y
* Loading Ubuntu 16.04.2 GA (amd64)
100%[===============================>] 422.56M  3.83MB/s   in 2m 9s
* Loading Ubuntu 16.04.1 GA (amd64)

ubuntu-16.04.1-server-amd64-curtin.tar.
100%[=============================>] 379.26M  3.88MB/s   in 2m 35s

* Loading Ubuntu 16.04 GA (amd64)
ubuntu-16.04-server-amd64-curtin.tar.gz
100%[================================>] 373.98M  6.92MB/s   in 93s

*
* Do you want to import the 14.04 series (6 images) (Y/n)? n
* Waiting for default image to become available (this can take
* a few minutes)....
* Setting deployment OS to 'custom'

Success.
Machine-readable output follows:
OK
* Setting OS release to u16.04.2_amd64
Success.
Machine-readable output follows:
OK
*************************************************************
* The /usr/sbin/maniacs-setup script has finished! <-------- You should see
this message to have a successful setup

NOTE: total runtime; start-time=10:50 end-time=11:06
##########################################################################
```
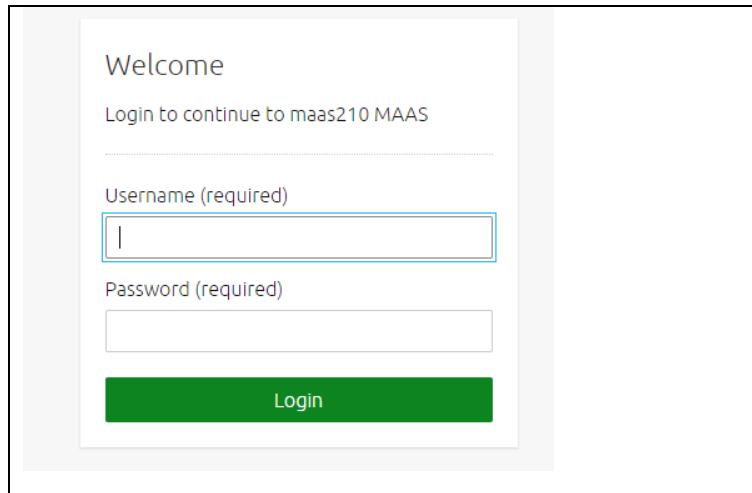
F. **Checking the MAAS Configuration:**
   - Verify you can access the MAAS web UI:
     Two ways to access MAAS web UI. 1) If you're Launching a browser from the internal MAAS network, point it to your internal port (in this case; http://10.100.209.1:5240/MAAS/) 2) If you're launching a browser from the IT network, point it to your external port (in this case; http://172.31.44.38:5240/MAAS/)
   - You should see a login prompt

- Enter your regular username and password that you gave to the setup script. Once login, you will be directed to the Ubuntu Images and architecture for update selection. Choose image versions and architectures that you need to import. Click continue once you're done.
- The next page shows SSH keys. If you did not input any SSH key during the setup, the script will automatically enter an SSH keys for you. You can add as many keys as you want. Once you're done adding SSH keys, proceed to Dashboard at the bottom page.
- Click the Subnets link to review the DHCP options. Verify the subnet range for your internal network
- Make sure MAAS web UI settings are, refer below images

172.31.36.58:5240/MAAS/settings/

MAAS   Nodes   Pods   Images   DNS   Zones   Subnets   **Settings**

Settings

General   DHCP snippets   Package repositories

Users and Keys

ID	Number of nodes in use	Last seen	MAAS Admin	
acd	2	Tue, 24 Jul. 2018 15:32:02	Yes	✎

Add user

Commissioning scripts

No commissioning scripts.

Upload script

Test scripts

No test scripts.

Upload script

Commissioning

Default Ubuntu release used for commissioning

Ubuntu 16.04 LTS "Xenial Xerus"   ⌄

Default Minimum Kernel Version

--- No minimum kernel ---   ⌄

The default minimum kernel version used on all new and commissioned nodes.

Save

Deploy

Settings

Deploy

Default operating system used for deployment

```
Ubuntu                                                    ▾
```

Default OS release used for deployment

```
Ubuntu 18.04 LTS "Bionic Beaver"                          ▾
```

Save

Windows

Windows KMS activation host

```

```

FQDN or IP address of the host that provides the KMS Windows activation service. (Only needed for Windows deployments using KMS activation.)

Save

Global Kernel Parameters

Boot parameters to pass to the kernel by default

```

```

Save

MAAS Configuration

MAAS name (required)

```
maas202
```

☑ Enable Google Analytics in MAAS UI to shape improvements in user experience

Save

Proxy

HTTP proxy used by MAAS to download images, and by provisioned machines for APT packages.

Nodes | maas209 MAAS ✕ | Settings | maas202 MAAS ✕

← → C ⓘ 172.31.36.58:5240/MAAS/settings/

▦ Free Hotmail 📙 Supermicro ⬇ Downloads 📄 Welcome to Chrome ⬛ HireRight Applicant ○ Sign in to GitHub · G M my-gmail 📄 Linux Device Drivers 📙 MAAS Servers 📙 RHEL

Settings

Proxy

HTTP proxy used by MAAS to download images, and by provisioned machines for APT packages.

○ Don't use a proxy
● MAAS Built-in
○ External
○ Peer

Save

DNS

Upstream DNS used to resolve domains not managed by this MAAS (space-separated IP addresses)

10.2.1.205

Only used when MAAS is running its own DNS server. This value is used as the value of 'forwarders' in the DNS server config.

Enable DNSSEC validation of upstream zones

Automatic (use default root key)   ⌄

Only used when MAAS is running its own DNS server. This value is used as the value of 'dnssec_validation' in the DNS server config.

Save

NTP

Addresses of NTP servers

ntp.ubuntu.com

NTP servers, specified as IP addresses or hostnames delimited by commas and/or spaces, to be used as time references for MAAS itself, the machines MAAS deploys, and devices that make use of MAAS's DHCP services.

☐ Use external NTP servers only

Configure all region controller hosts, rack controller hosts, and subsequently deployed machines to refer directly to the configured external NTP servers. Otherwise only region controller hosts will be configured to use those external NTP servers, rack contoller hosts will in turn refer to the regions' NTP servers, and deployed machines will refer to the racks' NTP servers.

Save

Network Discovery

Enabled   ⌄

Nodes | maas209 MAAS ✕   Settings | maas202 MAAS ✕

← → C   ⓘ 172.31.36.58:5240/MAAS/settings/

⊞ Free Hotmail   Supermicro   ± Downloads   Welcome to Chrome   HireRight Applicant   Sign in to GitHub · G   M my-gmail   Linux Device Drivers   MAAS Servers   RHEL

Settings

Network Discovery

Enabled   ˅

When enabled, MAAS will use passive techniques (such as listening to ARP requests and mDNS advertisements) to observe networks attached to rack controllers.
Active subnet mapping will also be available to be enabled on the configured subnets.

Active subnet mapping interval

Every 3 hours   ˅

When enabled, each rack will scan subnets enabled for active mapping. This helps ensure discovery information is accurate and complete.

Save

Third Party Drivers Configuration

☑ Enable the installation of proprietary drivers (i.e. HPVSA)

Save

Storage

Default storage layout (required)

Flat layout   ˅

Storage layout that is applied to a node when it is commissioned.

☐ Erase nodes' disks prior to releasing

Forces users to always erase disks when releasing.

☑ Use secure erase by default when erasing disks

Will only be used on devices that support secure erase. Other devices will fall back to full wipe or quick erase depending on the selected options.

☐ Use quick erase by default when erasing disks.

This is not a secure erase; it wipes only the beginning and end of each disk.

Save

MAAS name: maas202 MAAS

- Also check the Package repositories

G. Testing the MAAS Server:

- Prepare a server that you plan to certify. In this guide, this computer is referred as SUT.
- Connect the SUT (all NIC interfaces and IPMI) to the internal MAAS network as shown in the network configuration diagram above. Power it on
- Modify and configure the BIOS' SUT according to the steps/procedures below.
  1. First, set the bios to default factory settings
  2. Go to PCI Bus Configuration. Set all AOCs, RSCs, Onboard LAN OPROM type to "UEFI", and "Enabled" the Network Stack and Ipv4 PXE Support
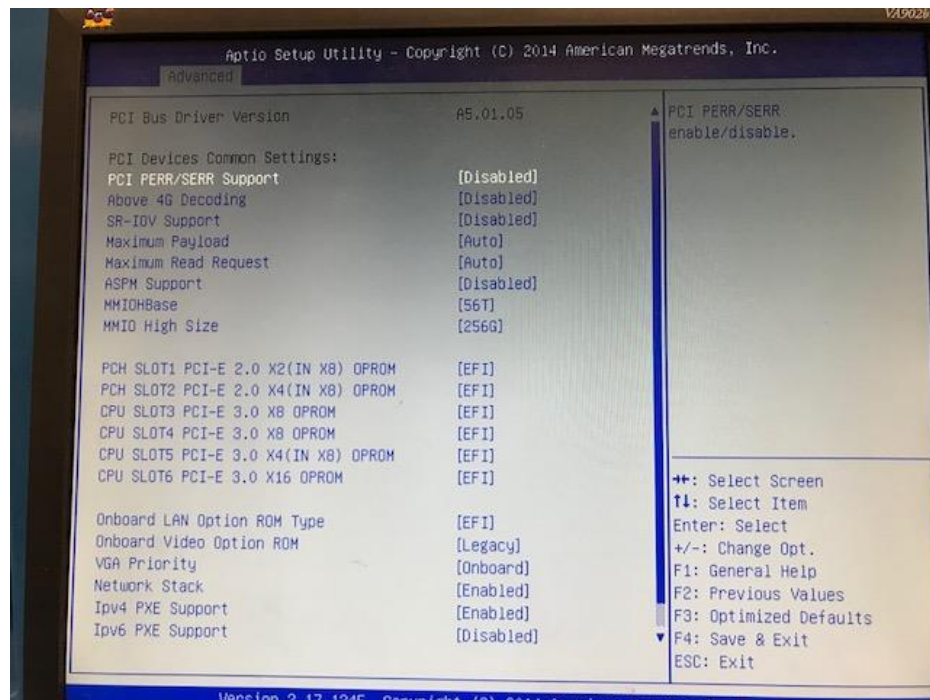
3. Go to Boot Configuration. Boot Mode Select set to "DUAL". At system boot order, set 1st boot order to "UEFI Network: IP4 <NIC>" and 2nd boot order to "UEFI:Hard Disk", while the rest boot order devices are disabled.
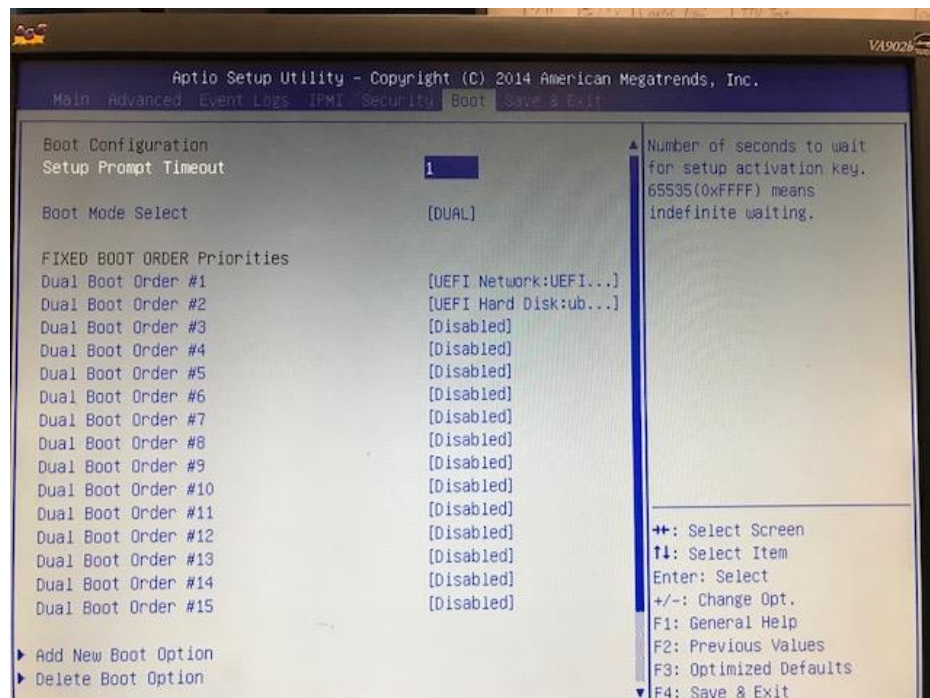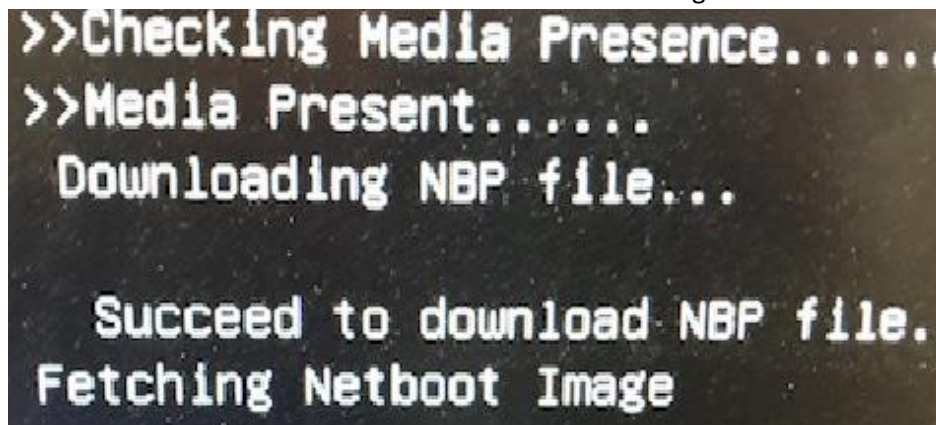

4. Also, under UEFI Network Drive BBs Priorities, select only one IP4 NIC network connection and the rest are disabled.
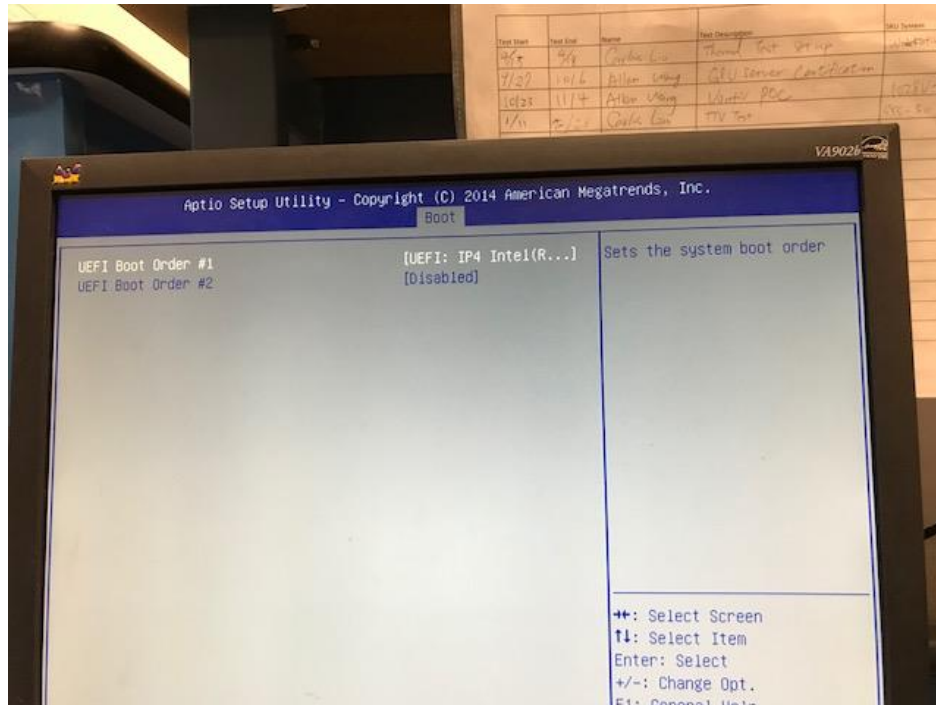
5. Save the changes and reboot the system

- At the node's screen, a "Boot Ready" prompt will appear in screen. During PXE boot, NBP file will start to download and fetch the Netboot image.

- At MAAS web UI, you should see the node uploads data and enlist to the MAAS. Once enlisting is successful, the Node powers off and the MAAS shows node as "New".
- Select Commissioning from MAAS UI. As per canonical advice (refer to the comment under bugs.launchpad.net report bug #1770404), if MAAS version is 2.3.X, it is desirable to use Ubuntu 16.04 LTS as the commissioning OS release. Also on some systems, it is necessary to remove the smartctl-validate option under hardware tests before clicking Commission Machine.
- Click "Take Action" followed by "Commission Node" from drop-down menu, the Node will remotely powers on and PXE boots from MAAS, Node loads ephemeral and introspects hardware and firmware, then tests will perform and uploads the data to

MAAS. Once all tests are passed, the Node powers-off and MAAS shows node as "Ready"

- Select Deploy from MAAS UI choosing the Ubuntu version you wish to deploy. Click Deploy Machine to begin deployment, the Node will remotely powers on and PXE boots from MAAS, the Node loads ephemeral and begins installation process, Node reboots and PXE boots from MAAS, MAAS tells node to "Boot from HDD", Node boots installed OS, Node performs post-install stuff via cloud-init. Once successful, the MAAS shows node as "Deployed" and the node is accessible either via SSH or directly to the node's console. The default given user name is "ubuntu" with password "ubuntu" as well.

H. Prepare the IPERF Server:

- Network test software – The certification suite for Ubuntu 14.04 relies on iperf (version 2), but this has changed to iperf3 for Ubuntu 16.04 and above releases. Thus, you may need to be prepared to run both programs. Download the latest iperf (version 2) and iperf3 program to the Iperf Server.

```
iperf@iperf-Super-Server:~$ sudo apt-get install iperf

iperf is already the newest version 2.0.5 (08 Jul 2010)

iperf@iperf-Super-Server:~$ sudo apt-get install iperf3

iperf3 is already the newest version (3.0.11-1).
```

- Multiple NIC interface cards – Most systems have multiple type of NIC interfaces installed. The IPERF server must be able to test 1Gb/s Ethernet, 10Gb/s Ethernet, or 10Gb/s SFP type of network interfaces. In this guide, the IPERF server is configured with 10Gb/s Ethernet and 10Gb/s SFP type of NIC. Network configuration as shown below.

```
iperf@iperf-Super-Server:~$ cat /etc/network/interfaces

auto lo
iface lo inet loopback

auto eno1
iface eno1 inet dhcp

#10Gb RJ45 NIC - connected at internal MAAS Ethernet network
auto enp2s0f0
iface enp2s0f0 inet static
    address 10.100.209.50/24
    netmask 255.255.255.0
    broadcast 10.100.209.255

#10Gb SFP NIC – connected at internal SFP network
auto enp6s0f0
iface enp6s0f0 inet static
    address 192.168.209.2/24
    netmask 255.255.255.0
```

broadcast 192.168.209.255

I. Running the Certification Tests:

- The node is accessible either via SSH or directly to the node's console. To log into the node from the MAAS server using SSH, use user-name "ubuntu". Below is an example of SSH session from MAAS to the node.

> supermicro@maas209:~$ ssh ubuntu@10.100.209.128
>
> Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)
> Last login: Fri May 11 15:54:41 2018 from 10.100.209.1
>
>
> ubuntu@GPU-IP128:~$

To login directly to the node, use user-name "ubuntu" and password "ubuntu" as well.

- Configure all the network interfaces appropriately by editing the file /etc/netplan/50-cloud-init.yaml. After proper configuration is employed, run "sudo netplan apply" command to take effect the new modified network settings.
- Plug in the type of media card that suits to the SUT's provided ports (usb2, usb3, SD card, CD)
- Make sure that program iperf3 is running from the iperf server - if certifying 16.04 and above releases or iperf version 2 - if certifying 14.04 and below releases.
- If having issues and failing LXD and KVM check test, download the relevant virtualization Images on the SUT. For certifying xenial release, obtain the following files; xenial-server-cloudimg-amd64.img, xenial-server-cloudimg-amd64.squashfs, xenial-server-cloudimg-amd64-lxd.tar.xz. For certifying bionic; the following files are needed; bionic-server-cloudimg-amd64.img, bionic-server-cloudimg-amd64.squashfs, bionic-server-cloudimg-amd64-lxd.tar.xz
- Copy these image files to any desired directory on the SUT and supply the full paths in the /etc/xdg/canonical-certification.conf file
- Use the ff. commands to download the needed 18.04LTS bionic images. Replace the word "bionic" with "xenial" to download 16.04LTS images
  $ wget https://cloud-images.ubuntu.com/bionic/current/bionic-server-cloudimg-amd64.squashfs
  $ wget https://cloud-images.ubuntu.com/bionic/current/bionic-server-cloudimg-amd64-lxd.tar.xz
  $ wget https://cloud-images.ubuntu.com/bionic/current/bionic-server- cloudimg-amd64.img

- Sample file of /etc/xdg/canonical-configuration.conf from SUT

  ----
  ubuntu@RU13-buck:/etc/xdg$ vi canonical-certification.conf
  #   - This will tell the script to download the file server-cloudimg-amd64.squashfs

```
#    from the remote server.
# - file:///local/path/to/server-cloudimg-amd64-lxd.tar.xz
#   - This will tell the script to look at the path specified on the local
#    filesystem for server-cloudimg-amd64-lxd.tar.xz to use.
#
# Note that a MAAS server set up via the MANIACS guide may optionally house
# copies of the LXD images under http://{ip-address}/cloud/.
#
# UNCOMMENT BOTH OF THE FOLLOWING 2 LINES nad set the proper URLs as
necessary
# OR leave them commented out and the LXD test will obtain the needed images
# from cloud-images.ubuntu.com.
LXD_ROOTFS = file:///home/ubuntu/xenial-server-cloudimg-amd64.squashfs
LXD_TEMPLATE = file:///home/ubuntu/xenial-server-cloudimg-amd64-lxd.tar.xz

# For network testing:
#
# TEST_TARGET_IPERF is the IP/Hostname of the iperf server for network testing.
#
# UNCOMMENT THE FOLLOWING LINE and set the IP/Hostname of your iperf target
# system as necessary:
TEST_TARGET_IPERF = 10.100.202.5,10.200.202.4
--------------------------------------------------------------------------------------------------------------------
-------------
```

- If prefer to run the certification test via SSH, it is necessary to run first the "**screen"**
  command before running test suite to avoid issues of disconnection by the network
  tests or for other reasons that may affect the result of the testing.
- You could run canonical-certification-precheck to double check if the server's
  configuration is correct. If the script identifies any problems, be sure to correct them.
- In the node, type the appropriate command to run the certification test.

```
$ certify-18.04 (if performing full test of Ubuntu 18.04 installation)
$ certify-16.04 (if performing full test of Ubuntu 16.04 installation)
$ certify-advanced (if you want to see all the test suit)
$ test-firmware (to runs firmware tests only)
$ test-functional-18.04 or test-functional-16.04 (to runs functional tests only for 16.04
or 18.04)
$ test-network-18.04 or test-network-16.04 (to runs network tests only for 16.04 or
18.04)
$ test-storage (to runs tests of storage devices)
$ test-usb (to runs tests of USB ports)
$ test-virtualization ( to runs virtualization of KVM and LXD tests)
```

J. Uploading the Test Results to the Certification site:
- When the test run is complete, you should see a summary of test run. The files are
  located at .local/share/checkbox-ng/. Below is an example of submission test results

```
ubuntu@GPU-IP128:~/.local/share/checkbox-ng$ ll

-rw-rw-r-- 1 ubuntu ubuntu 3662734 May 14 22:08 submission_2018-05-
14T22.08.20.535794.html

-rw-rw-r-- 1 ubuntu ubuntu    1567 May 14 22:08 submission_2018-05-
14T22.08.20.535794.junit.xml

-rw-rw-r-- 1 ubuntu ubuntu  953924 May 14 22:08 submission_2018-05-
14T22.08.20.535794.tar.xz

-rw-rw-r-- 1 ubuntu ubuntu  774002 May 14 22:08 submission_2018-05-
14T22.08.20.535794.xlsx
```

- If you're connected to the internet, typing y at this query should cause the results to be submitted. You'll need either a Secure ID value or to have already entered this value in the /etc/xdg/canonical-certification.conf file if this Secure ID was provided during precheck test.

- You could also manually upload the Test Results to the Certification Site from another computer that runs Ubuntu by performing the following steps/procedures
  1. First, transfer the test results from SUT to the computer where you're going to use to submit the test results. In this case, the KVM server was used to upload the data. The sample below is using a scp command to transfer all data files (submission*.*) from SUT directory "/home/Ubuntu/.local/share/checkbox-ng/" to the "sample" directory in KVM server.

```
supermicro@kvm210:~$ scp -r
ubuntu@10.100.210.147:/home/ubuntu/.local/share/checkbox-ng/submission_2018-
05-08T18.40.13.639765.* sample/
```

  2. After transferring the results, add Hardware Certification PPA to the server to be used to upload the data

```
supermicro@kvm210:~$ sudo apt-add-repository ppa:hardware-certification/public

supermicro@kvm210:~$ sudo apt-get update
```

  3. Install the package

```
supermicro@kvm210:~$ sudo apt-get install checkbox-ng
```

  4. Run the following command:

```
supermicro@kvm210:~$ checkbox-cli submit <SUT_SECURE_ID>
<PATH_TO>/submission_<DATECODE>.tar.xz
```

- Once results submission is complete, use the provided link in the output to review the results and confirm that they are correct.

K. Requesting a Certificate:

- Once it passed, the system's certification will be published at canonical websites link https://certification.canonical.com/certificates/.