

CNTT Hardware Delivery Validation (01-2020 DDF)

Objective

To develop and agree the requirements of the hardware delivery validation, per the CNTT request, which may be included as part of the OVP Infrastructure testing requirements.

Notes

There are a number of open questions that should reach community agreement BEFORE trying to reach agreement on specific tooling (basically, lets agree the WHAT before the HOW). The following questions have inputs have been pulled from email discussions intended to drive input input this working session for Prague.

Overall Objective:

1. Process, requirements (developed within CNTT RC), and tooling to enable automated checking of hardware and settings installed a lab that will be used for NFVI or VNF testing.
2. First "release" is focused on "read-only" vie of the hardware / settings. Future releases might add "read/write" configuration.

What specifically needs to be "checked" in the validation, in terms of parameters and configuration? (RAM, Disks and Disk Sizes, CPU info, Network Interfaces, Network Connectivity, etc.)

Test Type	Purpose	Examples	Check ed When (via)
BIOS Settings	Verifies all applicable BIOS settings per hardware model.	• Boot mode • Boot Sequence Retry • AC Power Recovery • Power Setting (balanced / performance) • Virt. Technology • Hyper Threading • Trusted platform module	
Firmware Settings	Verifies all applicable Firmware settings	• BIOS • Storage Array Controller • NIC (Intel X710) • PXE Enabled Ports	
Boot Order	Verifies applicable boot order settings	First boot, Second boot	
Hardware Health	Queries Intelligent Platform Management Interface (IPMI) is for all hardware components and their health status	• Raid • System Board • CPU temp • Power Supply	
PCI Slot Status & MAC	Which cards are in which slot, which slot is assigned to which CPU, slot type	• card(s) in slot/port/PCI partition • Slot speed / type • CPU / Slot assignment	
NIC	Validates that all NICs are in the correct slots, with a healthy status (per IPMI), have correct MAC addresses, and are detecting a cable connection (or not).	• Correct LLDP neighbor • MAC Addresses(es)	
IPMI Logs	Check for existence of logs	Physical event logged. E.g. chassis open on power up	

Attendees

- Lincoln Lavoie
- Vaibhav Chopra
- Satyawar Jangra
- Daniel Balsiger
- Mark Beierl
- Trevor Cooper
- Kanagaraj Manickam
- David Paterson
- Michael Fix (AT&T) (michael.fix@att.com)
- Qiao Fu

Volunteers (for HDV development)

- @name

Reference Materials

[cnnt-ri chapter 05-V2.pptx](#)

File	Modified
Microsoft Powerpoint Presentation cnn t-ri chapter 05-V2.pptx	Dec 23, 2019 by Liang Chen
Microsoft Powerpoint Presentation H W Validation with Configuration using Redfish APIs- v0.1.pptx	Jan 14, 2020 by Satyawar Jangra

[Download All](#)

discription file for CNTT RI:

<https://wiki.opnfv.org/display/CIRV/CNTT+RI+installer+description+file>

IPMI Users	Check for existence of user accounts	• Check if IPMI is available on the network • Check existing accounts • Check for use of default credentials	
Hardware Inventory	Inventory of h/w on platform..	CPU and count, NUMA topology, CPU Freq., RAM, speed, size, model, etc	
Physical Disk Configuration	Verifies storage / disk config (type, size)	• Physical disk type • card/port location • capacity	
SRIOV Port Validation	Verifies global and NIC level enabled	Confirm setting is enabled (or none)	
Hardware Check	Verifies basic OS config attributes (i.e. Linux running on the host and reporting these values)	• RAM size • # of cores (/proc/cpu)	

Out of scope for HDV (possibly for Functest):

- MTU path verification

Note as per email discussion:-

"What needs to be validated",

We can share the details which p/m are validating as per table above or any addition"

the first goal is validation of the hardware against a bill of material or similar. This would also check against minimums agreed / set by the CNTT, so the environment or lab can be vetted to meet the requirements for VNF certification, etc.

"How it is validated"

We can present a small demo with our automated architecture approach"

What is the entry to the HDV (hardware delivery validation)? Is this information contained / pulled from the PDF type "file," if yes, does that "file" contain all required info? If not, then what?

- Mike: Entry will be remote access into the host. IPMI interface / logs used for verification. Tool /discussion will be needed for access and automation.
- FQ: I would think the entry would be from PDF.
- Vaibhav: For Validation, Remote access to host will definitely be needed, but results need to be compared with the expected outcome (PDF, or a yaml contains all p/ms.
- dbalsige: The PDF/IDF information should be there before running validation. Validation would compare reality in Lab environment with PDF/IDF information. Therefore the PDF/IDF should contain all detailed information required for HDV.

When does the HDV occur, pre stack deployment, post stack deployment? How does this handle the cloud native environment (i.e. no open stack)?

- Mike: Pre-software stack deployment. i.e. RI Design complete (PDF) > Rack, Stack/Cabling > Network Config > "HVD" > then, passed on to software deployment team.
- FQ: Agree. HDV is before any software is deployed in the infrastructure.
- Vaibhav : Agree, it would be Pre-stack deployment to verify HDV.
- dbalsige: Agree. as early as possible. Some HDV tests (see above) will probably require booting an OS (e.g. introspection kernel + ramdisk) in my opinion. What about doing "in-between" stack validation, by either an CNTT-HDV-ramdisk before the final Operating System installation or even on the final Operating System? The PDF/IDF would also contain physical lab setup (different physical networks, underlay addressing, VLANs, NIC mappings, storage layout, etc...) but no stack specific (OpenStack or K8s) configuration. From that point on, the stack software (K8s or OpenStack) could be installed in an automated way. We would leave every option open and decouple the physical Lab properties from the stack software installation & configuration.

If the requirement is pre stack deployment, how is the validation done, i.e using the BMC interfaces? (this will require significant hardware vendor input).

- Mike: Yes, this Baseboard Management Controller (BMC), or Integrated Lights Out (iLO) management / NIC port, dedicated to accessing the host for remote management.
- [fq]we are using IPMI at first, and now also utilize redfish. It really requires significant hardware vendor input, and lots of adaptation effort
- Vaibhav : Our automated validation is also designed based on redfish and in my view each H/w vendors support that as well.
- dbalsige: In a perfect world the BMC approach could work. Completely depends on the H/W vendor, as mentioned above. Some HDV (e.g. basic network connectivity on all (bonded and DPDK) NICs is very hard to check from the BMC). In my opinion, booting an Operating system in some form is still the simplest approach to verify such H/W settings.

What are the required output / formats, etc.?

- Mike: Varies by test type: Either Boolean, Text, Size, Version/Value, OK (health), Serial #s, etc

Notes:

- Part of CNTT certification is checking the hardware
- What things are important to check?
- When do these things get checked (pre/post stack)?
- Potential futures:
 - Switches (check ports, vlan trunks, etc)
 - PDUs
 - Intelligent racks
 - ...?