OPNFV Requirement

[1 Hardware HA—reference to doctor 1](#_Toc409427674)

[2 Software resource 2](#_Toc409427675)

[2.1 Host OS 2](#_Toc409427676)

[2.2 Hypervisor 2](#_Toc409427677)

[3 Virtual infrastructure HA—Ian 2](#_Toc409427678)

[3.1 Compute 2](#_Toc409427679)

[3.2 Storage 2](#_Toc409427680)

[3.3 Network 2](#_Toc409427681)

[3.3.1 Virtual network (“network” in OpenStack term) 2](#_Toc409427682)

[3.3.2 SDN controller 2](#_Toc409427683)

[3.3.3 vSwitch 2](#_Toc409427684)

[4 VIM---Yuan Yue 2](#_Toc409427685)

[4.1.1 Control Node 2](#_Toc409427686)

[5 VNF HA--Maria 3](#_Toc409427689)

[5.1 Service Availability 3](#_Toc409427690)

[5.1.1 Service Availability Classification Levels 3](#_Toc409427691)

[5.1.2 Metrics for Service Availability 3](#_Toc409427692)

[5.2 Service Continuity 3](#_Toc409427693)

[5.3 Redundancy Mechanism 3](#_Toc409427694)

# Hardware HA—reference to doctor

The hardware HA can be solved by several legacy HA schemes. However, when considering the NFV scenarios, hardware failure will cause collateral damage to not only virtual infrastructures but also services running on it. Therefore, fault detection and report of HW failure from the hardware to VIM, VNFM and Orchestrator is necessary for the HA approaches in OPNFV.

* Hardware failure detection and prediction is necessary for NFV
* Possible fault table can be found in the Doctor project. <https://wiki.opnfv.org/doctor/faults>
* Hardware Failure should be informed to the NFVI instead of directly reporting to the NF in the traditional way, so that the NFVI may solve the failure without further need of VNF notice.
* Hardware failure detection message should be informed to the VIM for further operation if the NFVI can’t solve.
* Direct notice from the hardware to some specific VNFs is possible.
* Periodical update of hardware running conditions to the NFVI and VIM is required for further operation, which may include fault prediction, failure analyses, and etc..

Open questions:

Shall all hardware faults at the compute nodes go to VIM? Or hardware shall first report to Host OS or hypervisor, if the fault can not be solved, then an alarm shall send to the control node.

# Software resource

* The NFVI will try to solve HW failure when receiving alarms from the HW. If failed, the NFVI will inform VIM to take over solving the failure.
* The NFVI should support VM migration
* The NFVI should provide isolation for VMs, so that multiple VMs on the same hardware use separate CPU and storage resources. Failure in a certain VM will not influence the service on other VMs.
* The NFVI should support VM restoration. Possible restoration scenarios may include:
  + - HW failure, when VMs on the failed HW should be restored on other HWs.
    - VNF failure, when service itself can not recover and may request VNFM and VIM to restore the VNF.
    - VNF migration scenarios, where VNFs are directed by the user to migrate to another spot.
* Fault update capability. The NFVI is responsible for update the HW and OS fault to VIM.
* The hypervisor should record VM information regularly and provide the “last words” of VMs for future diagnoses and analyze.

# Virtual infrastructure HA—Ian

## Compute

VM including CPU, memory and ephemeral disk (“server” in OpenStack term)

## Storage

Virtual block disk (“volume” in OpenStack term)

## Network

### Virtual network (“network” in OpenStack term)

### SDN controller

* Distributed
* Centralized

### vSwitch

# VIM---Yuan Yue

### Control Node

* MySQL
* RabbitMQ
* OpenStack APIs (Nova-api)
* Nova-scheduler
* Neutron/Nova-network
* Glance
* Swift

# VNF HA--Maria

## Service Availability

### Service Availability Classification Levels

### Metrics for Service Availability

## Service Continuity

## Redundancy Mechanism