This section about VIM High availability

5 VIM High availability

The VIM in the NFV reference architecture contains all the control nodes of OpenStack, SDN controllers and hardware controllers. It manages the NFVI according to the instructions/requests of the VNFM and NFVO and reports them back about the NFVI status. To guarantee the high availability of the VIM is a basic requirement of the OPNFV platform. Also the VIM should provide some mechanism for VNFs to achieve their own high availability.

5.1 Architecture requirement of VIM HA

The architecture of the control nodes should avoid any single point of failure and the management network plane which connects the control nodes should also be redundant. Services of the control nodes which are stateless like nova-API, glance-API etc. should be redundant but without data synchronization. Stateful services like MySQL, Rabbit MQ, SDN controller should provide complex redundancy policies. Cloud of different scale may also require different HA policies.

Requirement:

- In small scale scenario active-standby redundancy policy would be acceptable.
- In large scale scenario all stateful services like database, message queue, SDN controller should be deployed in cluster mode which support N-way, N+M active-standby redundancy.
- In large scale scenario all stateless services like nova-api, glance-api etc. should be deployed in all active mode.
- Load balance nodes which introduced for all active and N+M mode should also avoid the single point of failure.
- All control node servers shall have at least two network ports to connect to different networks plane. These ports shall work in bonding manner.
- Any failures of services in the redundant pairs should be detected and switch over should be carried out automatically in less than 5 seconds totally.
- Status of services must be monitored.

5.2 Fault detection and alarm requirement of VIM

Redundant architecture can provide function continuity for the VIM. For maintenance considerations all failures in the VIM should be detected and notifications should be triggered to NFVO, VNFM and other VIM consumers.

Requirement:

- All hardware failures of control nodes should be detected and relevant alarms should be triggered. OSS, NFVO, VNFM and other VIM consumers can subscribe these alarms.
- Software on control nodes like OpenStack or ODL should be monitored by the clustering software at process level and alarms should be triggered when exceptions are detected.
- Software on compute nodes like OpenStack/nova agents, ovs should be monitored by watchdog. When exceptions are detected the software should be restored automatically and alarms should be triggered.
- Software on storage nodes like Ceph, should be monitored by watchdog. When exceptions are detected the software should be restored automatically and alarms should be triggered.
- All alarm indicators should include: Failure time, Failure location, Failure type, Failure level.

- The VIM should provide an interface through which consumers can subscribe to alarms and notifications.
- All alarms and notifications should be kept for future inquiry in VIM, ageing policy of these records should be configurable.
- VIM should distinguish between the failure of the compute node and the failure of the host HW.
- VIM should be able to publish the health status of the compute node to NFV MANO.

5.3 HA mechanism of VIM provided for VNFs

When VNFs deploy their HA scheme, they usually require from underlying resource to provide some mechanism. This is similar to the hardware watchdog in the traditional network devices. Also virtualization introduces some other requirements like affinity and anti-affinity with respect to the allocation of the different virtual resources.

Requirement

- VIM should provide the ability to configure HA functions like watchdog timers, redundant network ports and etc. These HA functions should be properly tagged and exposed to VNF and VNFM with standard APIs.
- VIM should provide anti-affinity scheme for VNF to deploy redundant service on different level of aggregation of resource.
- VIM should be able to deploy classified virtual resources to VNFs following the SAL description in VNFD.
- VIM should provide data collection to calculate the HA related metrics for VNFs.
- VIM should support the VNF/VNFM to initiate the operation of resources of the NFVI, such as repair/reboot.
- VIM should correlate the failures detected on collocated virtual resources to identify latent faults in HW and virtualization facilities
- VIM should be able to disallow the live migration of VMs and when it is allowed it should be possible to specify the tolerated interruption time.
- VIM should be able to restrict the simultaneous migration of VMs hosting a given VNF.
- VIM should provide the APIs to trigger scale in/out to VNFM/VNF.
- When scheduler of the VIM use the Active/active HA scheme, multiple scheduler instances must not create a race condition
- VIM should be able to trigger the evacuation of the VMs before bringing the host down when *maintenance mode* is set for the compute host.
- VIM should configure Consoleauth in active/active HA mode, and should store the token in database.
- VIM should replace a failed VM with a new VM and this new VM should start in the same initial state as the failed VM.
- VIM should support policies to prioritize a certain VNF.

5.4 SDN controller

SDN controller: Distributed or Centralized

Requriements

- In centralized model SDN controller must be deployed as redundant pairs.

- In distributed model, mastership election must determine which node is in overall control.
- For distributed model, VNF should not be aware of HA of controller. That is it is a - logically centralized system for NBI(Northbound Interface).
- Event notification is required as section 5.2 mentioned.