High-Availability Practice of ZTE Cloud-Based Core Network

The Network Function Virtualization (NFV) technology provides telecommunications software functions on the universal COTS servers, for example, the vEPC and vIMS functions in cloud-based mobile core networks.

Based on an architecture of decoupling software from hardware, NFV breaks the limitations of dedicated hardware in traditional telecommunications networks, and implements the functions of telecommunications NEs through software rather than hardware. NFV implements rapid development and deployment of software functions as well as shared and unified management of hardware resources. In addition, virtualization technologies bring about automated installation and deployment of NEs and dynamic resource scheduling, providing flexible scalability and dramatically simplifying management and O&M, thereby winning wide recognition and attracting special attention from operators.

However, the numerous advantages and highlights of virtualization technologies are also accompanied by some new issues, of which reliability is a key matter. For example, decreased reliability of COTS hardware and the virtualization layer lead to increased fault points. In this case, can the NFV network meet the requirements of a carrier-class reliability (99.999%)?

Strictly put, the 99.999% reliability should be referred to as availability, which indicates that the availability percentage of a system reaches 99.999%. This indicator means that the average system breakdown time in a year should be less than 5 minutes and 15 seconds. It is calculated as follows:

\[ A = \frac{MTBF}{MTBF + MTTR} \]

- MTBF: Mean Time Between Failure.
- MTTR: Mean Time To Restoration.

It can be seen from the above formula that the availability can be enhanced in the following two ways:

1. Reduce the possibility of failures, and extend failure-free working hours of the system.
2. Shorten the MTTR, and restore the system to normal status as soon as possible.
Availability Analysis of NFV Networks

An NFV network can be divided into the following parts: NFVI layer, VNF application layer, and Management and Orchestration (MANO). The NFVI layer can be further divided into the hardware layer and virtualization layer (see the following figure).

![Figure 1 NFV System Architecture](image)

The availability of VNF depends on that of the entire NFV system, which is guaranteed by the collaboration among the hardware layer, virtualization layer, VNF, and the MANO node. To provide highly available network services, these layers must meet the following requirements:

- **Hardware layer:**

  The hardware layer involves compute resources, storage resources, and network resources.

  For compute resources, all server components, such as power supplies and fans, must be deployed with 1+1 or N+M redundancy.

  Storage resources are actually RAIDs or distributed storage that provide 1+1/1+M data backup, to ensure normal data access even if a single disk is faulty. The multipathing storage technology is used to increase the bandwidth and connection availability between the host and SAN devices.
Network resources are deployed with 1+1 redundancy for multi-link networking. Redundancy and load sharing are implemented on the interfaces, routes, and devices to prevent Single Points of Failure (SPOFs).

- **Virtualization layer:**

  The virtualization layer provides the functions of physical resource virtualization, and works with the MANO node for management and scheduling of virtual resource pools.

  The virtualization layer provides highly available deployment and recovery mechanisms for the application layer software:

  Anti-affinity deployment of Virtual Machines (VMs) is supported. Redundant VMs need to be deployed on more than two different servers so that the redundant virtual machines on the other servers can take over services in case of a failure on the active VM server. For example, neither the active/standby nor load sharing VMs can be deployed on the same server.

  Status detection and self-healing of VMs are supported. A VM failure or a physical hardware failure detected by the virtualization layer needs to be restored locally or migrated to another server.

- **Application layer:**

  The application layer implements Virtualized Network Functions (VNFs), such as the vMME, vPGW, vCSCF, and vSBC.

  The highly-available design of VNFs is vital to a cloud-based core network system. After the virtualization technology is used in telecommunications networks, the availability of hardware infrastructure becomes lower than that of the previous dedicated telecommunications hardware. Therefore, the software availability needs to be improved for compensation.

  ➢ **Hot standby of all components**

    VNF components support hot standby technology. The status information of online sessions is backed up to redundant components in real time. When a component fails, the other backup components seamlessly take over the services of the faulty component, guaranteeing service continuity and preventing bad effects of system faults on online and new services.
The hot standby capability of the application layer provides faster fault detection and recovery, more accurate application fault detection, a higher service recovery rate, and lower compute and network resource consumption than the backup and recovery mechanism in the virtualization layer, and is one of the essential functions for highly-available carrier-class virtual networks.

- **Rapid recovery of faulty components**
  Together with the MANO and virtualization layer, VNFs can implement rapid recovery of faulty components and rapid recovery by rebooting or recreating. After recovery, the VMs can take over the services of the faulty VMs, or be used as backup components without changing the redundancy in the system.
  
- **Remote disaster recovery**
  Disaster recovery is deployed to provide redundant VNF capabilities across Data Centers (DCs) in different geographical areas. In case of a regional/DC-level fault, services can be restored in other DCs. This is a very important mechanism for guaranteeing availability. For example, the traditional cross-regional pool disaster recovery provides load sharing and disaster recovery between NEs in the same pool.

### MANO

A MANO consists of three entities: VIM, VNFM, and Orchestrator, which are responsible for management and orchestration of the NFVI resources, as well as management of VNFs and Network Services (NSs).

Neither the faults nor upgrades of the MANO cause VNF service interruption. However, when a fault occurs on the MANO, some virtualization features become unavailable, such as automatic scaling and VM migration. Therefore, high availability of the MANO nodes is also indispensable.

The MANO nodes are generally deployed in 1+1 active/standby mode, with status and data synchronization between the active and standby nodes. When the active node fails, the standby node automatically becomes the active node and takes over the services to avoid service interruption.

In addition, the MANO also provides the mechanisms for status monitoring of the NFV, VNF, and NS, alarm collection, fault correlation, and automatic fault recovery to locate faults easily and reduce the complexity of O&M management.
High-Availability Practice of ZTE Cloud-Based Core Network

In order to provide carrier-class network applications with higher availability in a virtualized environment, the ZTE VNF system adopts a better design architecture, and takes full advantage of the features of NFV networks, thereby providing brand-new cloud-based core networks with higher availability, security, and resource saving.

ZTE's cloud-based core network had made the following improvements in availability:

- **Modular**
  
  In a modular design architecture, a VNF consists of various components, which are actually different VMs. By decoupling software modules from each other, this architecture improves fault tolerance between components, improves system maintainability, and lowers the impact on service availability.

- **Stateless**
  
  In a stateless design architecture, the service logic processing component is decoupled from service session data. The service logic processing component stores stateful data by using dedicated database components, and provides 1+M data redundancy. Therefore, without considering synchronous backup of online session information, this component simplifies the implementation of software logic and improves system availability.

- **N+M redundancy mechanism**
  
  The N+M redundancy mechanism provides higher availability with fewer redundant components. With the same number of components, the N+M redundancy mechanism provides much higher availability than the 1+1 redundancy backup mechanism. For example, five components work in parallel. In 1+1 backup mode, 5+5 components are needed. In N+M backup mode, only two redundant components are needed. Namely, 5+2 components can provide higher availability than the former.

- **Cross-DC disaster recovery**
  
  In a cross-DC disaster recovery solution, the active/standby or load-sharing components of a VNF are deployed in multiple DCs. When a DC fails, the redundant components of the other DCs can quickly take over its services. Compared with the traditional pool mode, the cross-DC deployment solution provides uninterrupted service continuity and hot disaster recovery.