

vMRF Infrastructure Requirements

Virtual Multimedia Resource Function

Requirements Specification

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.



Contents

1	Introduction	1
2	Compute Requirements	2
3	Network Requirements	5
4	Storage Requirements	12
5	Security Requirements	14
6	Other Requirements	16





1 Introduction

This document describes the requirements for the infrastructure resource as requested by IMS virtualized applications.



2 Compute Requirements

This section lists all compute requirements, see [Table 1](#).

Table 1 Compute Requirements

Category	Category Definition	Requirement Text
Physical CPU architecture	<p>A physical CPU in its simplest terms refers to a physical CPU core, that is, a physical hardware execution context (HEC), but can refer to a processor that manufactured to contain multiple physical cores.</p> <p>If the physical CPU supports hyperthreading, then that enables a single processor core to act like two processors, that is, logical processors.</p> <p><i>[ETSI definition: Device in the compute node, which provides the primary container interface. This is the generic processor, which executes the code of the VNFC⁽¹⁾.]</i></p>	<p>X86-64 architecture, Intel® Ivy Bridge or newer generation.</p> <p>AVX, AES, and SSE 4.2 support is required.</p>
vCPU ⁽²⁾	<p>vCPU-affinity can be used to isolate a physical CPU to a vCPU, by pinning the vCPU to a dedicated physical CPU.</p> <p><i>[ETSI definition: The vCPU created for a VM⁽³⁾ by a hypervisor (see Other Requirements on page 16). In practice, a vCPU may be a time sharing of a real CPU and/or in the case of multi-core CPUs, it may be an allocation of one or more cores to a VM.]</i></p>	<p>The following requirement ensures sufficient quality of service for media plane processing:</p> <ul style="list-style-type: none">• One vCPU must correspond to exactly one physical CPU core. <p>If hyperthreading is enabled on the compute host, vCPU affinity must be used, to ensure that only a single MRF VM runs within one physical CPU core. (That means only a single thread in the physical CPU core is allowed to run a MRF VM. No other MRF VM (or other VMs) is allowed to run on the other thread(s) within the same physical CPU core).</p>
Number of vCPUs	<p><i>[ETSI definition: VM is a virtualized computation environment that</i></p>	<p>At least four vCPUs are required per VM.</p>



Category	Category Definition	Requirement Text
	<i>behaves very much like a physical computer or server. A VM has all its ingredients (processor, memory/storage, interfaces/ports) of a physical computer or server and is generated by a hypervisor (see Other Requirements on page 16), which partitions the underlying physical resources and allocates them to VMs. VMs are capable of hosting a VNFC.]</i>	It is recommended to specify more vCPUs for optimum performance.
Memory	<p>Volatile RAM⁽⁴⁾ requires power to maintain the stored information. It retains its contents while powered on, but when the power is interrupted the stored data is lost very rapidly or immediately.</p> <p><i>[ETSI definition: This represents the virtual memory needed for the VDU⁽⁵⁾ or VM. VDU is a construct used in an information model and the VNF can be modelled using one or multiple such constructs, as applicable.]</i></p>	The required minimum amount of memory is 6 GB per VM.
Compute host	<p>A compute host (or simply host) is the whole server entity providing computing resources, composed of the underlying hardware platform: processor, memory, I/O devices, and disk. The hypervisor (see Other Requirements on page 16) may or may not be seen as part of the host.</p> <p><i>[No ETSI definition]</i></p>	<p>At least one compute host is required per vMRF VNF. It is recommended to specify at least two compute hosts for redundancy. It is not recommended to place all VMs of a vMRF VNF on the same compute host.</p> <p>A vMRF compute host must only run vMRF VMs, other VMs are not allowed on that host.</p> <p>For NIC, it is recommended to use Intel® 10 Gb Ethernet controllers for optimum performance.</p>
Overcommitting CPU	<p>CPU overcommitting is a hypervisor feature (see Other Requirements on page 16) that allows a VM to allocate more virtualized CPUs than physical CPUs the host has available.</p> <p>The term overallocation is also used for this feature.</p>	<p>Overcommitting CPU is not allowed.</p> <p>It compromises the predictability and dimensioning of capacity, latency, quality of service and other characteristics of the VM.</p>



Category	Category Definition	Requirement Text
	<i>[ETSI definition: The VDU may coexist on a platform with multiple VDUs or VMs and is as such sharing CPU core resources available in the platform. It may be necessary to specify the CPU core oversubscription policy in terms of virtual cores to physical cores/ threads on the platform. This policy can be based on required VDU deployment characteristics such as high performance, low latency, and/or deterministic behavior.]</i>	
Overcommitting memory	<p>Memory overcommitting is a hypervisor feature (see Other Requirements on page 16) that allows the sum of all VM memory allocations to be bigger than the total memory of the host.</p> <p>The term overallocation is also used for this feature.</p> <p><i>[No ETSI definition]</i></p>	<p>Overcommitting memory is not allowed.</p> <p>It compromises the predictability and dimensioning of capacity, latency, quality of service and other characteristics of the VM.</p>

(1) Virtualized Network Function Component (VNFC)

(2) Virtual CPU (vCPU)

(3) Virtual Machine (VM)

(4) Random-Access Memory (RAM)

(5) Virtualization Deployment Unit (VDU)



3 Network Requirements

This section lists all network requirements, see [Table 2](#).

Table 2 Network Requirements

Category	Category Definition	Requirement Text
vNICs ⁽¹⁾ per VM	<p><i>[ETSI definition: NIC is a device in a compute node that provides a physical interface with the infrastructure network.]</i></p> <p><i>[ETSI definition: vNIC is a virtualized NIC created for a VM by a hypervisor.]</i></p>	Each vMRF VM requires four vNICs.
Virtual networks or VLANs ⁽²⁾ per vNIC	<p>A VLAN is the logical grouping of network nodes, which allows geographically dispersed network nodes to communicate as if they were physically on the same network.</p> <p><i>[ETSI definition: Virtual network is a topological component used to affect forwarding of specific characteristic information.</i></p> <p><i>The virtual network is bounded by its set of permissible network interfaces.</i></p> <p><i>Virtual network forwards information among the network interfaces of VM instances and physical network interfaces, providing the necessary connectivity and ensures secure isolation of traffic from different virtual networks.]</i></p>	<p>The following 4 (four) VLAN separated virtual networks are required by vMRF each having its own vNIC:</p> <ul style="list-style-type: none"> • VNF Internal • O&M • Signaling • Media (IMS Core) <p>The virtual networks VLANs above are not visible to the vMRF (that means traffic is "untagged").</p>
Bandwidth of internal network	<p>Internal network is a virtual network used for TIPC, Internal INET, and boot traffic.</p> <p>The bandwidth is measured on the vNIC assigned to the internal network.</p>	No specific requirements apply.
Bandwidth of the external networks	External networks are the virtual networks used for communication	It is strongly recommended to have dpdk optimized OVS (2.4 or later)

Category	Category Definition	Requirement Text
	<p>external to the VNF. For example network function (other VNFs or PNFs), network management systems, charging system.</p> <p>The sum of the measured bandwidth of all vNICs (except the vNIC for VNF internal network) connected to the VM.</p>	to be installed. Without dpdk optimized OVS the throughput on the host is too low for traffic, the packet loss gets to high, and the latency has an impact on speech quality.
Pinning vNICs	<p>Pinning vNICs to physical ports enables to manage the distribution of traffic. When pinning is set, all traffic from the vNIC travels through the I/O module to the specified Ethernet port.</p> <p><i>[No ETSI definition]</i></p>	Pinning vNICs to physical ports is not required.
L2 redundancy	<p>To achieve telecom grade failure recovery, the vNIC interface is protected in the L2 infrastructure, for example, by using two physical NICs to achieve resiliency in the external switches, in case one switch plane is broken (assuming duplicated L2 switch).</p> <p><i>[No ETSI definition]</i></p>	Telecom grade availability of the virtual network is required for vMRF, therefore L2 redundancy must be secured by the virtualization infrastructure.
L2/L3 QoS ⁽³⁾	<p>QoS settings at L2/L3 for the traffic are not changed within the virtual network boundaries.</p> <p><i>[ETSI definition: Describes the QoS options to be supported on the VL⁽⁴⁾, for example, latency and jitter.]</i></p>	No specific requirements apply.
L3 network separation	<p>Overlap between the IP addresses used for a given network, and the IP addresses used for part of another network, where these networks are adjacent in the communication path.</p> <p><i>[No ETSI definition]</i></p>	No specific requirements apply.
L2 path diversity	<p>Having multiple routes at L2 to reach a destination.</p> <p><i>[No ETSI definition]</i></p>	No specific requirements apply.
vNIC type	vNIC can be of access or trunk type. Each vNIC can have multiple	Access port vNICs are required.



Category	Category Definition	Requirement Text
	<p>IP interfaces either of the same or different type.</p> <p>IP aliasing is the concept of creating or configuring multiple IP addresses on a single network interface.</p> <p>In dual-stack configuration, the device is configured for both IPv4 and IPv6 network stacks. The dual-stack configuration can be implemented on a single interface or with multiple interfaces. In this configuration, the device decides how to send the traffic based on the destination address of the other device.</p> <p><i>[No ETSI definition]</i></p>	
IP address allocation	<p>The process of assigning IP addresses to the vNICs that are associated to the VNF, including the permission for the assigning.</p> <p><i>[No ETSI definition]</i></p>	<p>vMRF uses the virtualization infrastructure to allocate IP addresses via DHCP.</p> <p>NAT or NAPT cannot be used in the virtualization infrastructure.</p>
Path supervision	<p>Any path supervision protocols can be used, such as Gratuitous ARP⁽⁵⁾, ICMP⁽⁶⁾, or BFD⁽⁷⁾.</p> <p><i>[No ETSI definition]</i></p>	ICMP support is required.
L3 redundancy	<p>L3 redundancy can be provided by the VRRP⁽⁸⁾.</p> <p><i>[No ETSI definition]</i></p>	VRRP support is required for the O&M
Bootimg network	<p>The PXE⁽⁹⁾ specification describes a standardized client-server environment that boots a software assembly, retrieved from a network, on PXE-enabled clients. On the client side, it requires only a PXE-capable NIC, and uses a small set of industry-standard network protocols, such as DHCP⁽¹⁰⁾ and TFTP⁽¹¹⁾.</p> <p>The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on IP networks for dynamically distributing network configuration</p>	No specific requirements apply.

Category	Category Definition	Requirement Text
	parameters, such as IP addresses for interfaces and services. [No ETSI definition]	
IPv4 or IPv6	Internet Protocol version 4 (IPv4) and 6 (IPv6). [No ETSI definition]	The virtualization infrastructure must support IPv4 and IPv6 at the transport layer.
Routing protocol	OSPF ⁽¹²⁾ is an Interior Gateway routing protocol for IP networks based on the shortest path first or link-state algorithm. BFD is a network protocol used to detect faults between two forwarding engines connected by a link, even on physical media that do not support failure detection of any kind. Static routing is a form of routing that occurs when a router uses a manually configured routing entry, rather than information from a dynamic routing traffic. Static routes are fixed and do not change if the network is changed or reconfigured. [No ETSI definition]	No specific requirements apply.
LBaaS ⁽¹³⁾	LBaaS is a feature available through OpenStack Neutron. It allows for proprietary and open-source load balancing technologies to drive the actual load balancing of requests, allowing OpenStack operators to use a common interface and move seamlessly between different load balancing technologies. [No ETSI definition]	No specific requirements apply.
NTP ⁽¹⁴⁾	NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. [No ETSI definition]	All the VM instances must be able to access an appropriate NTP server.
DNS	The DNS is a hierarchical distributed naming system for	All VM instances must be able to access an appropriate DNS server.



Category	Category Definition	Requirement Text
	<p>computers, services, or any resource connected to Internet or to a private network. It translates domain names, which can be easily memorized by humans, to the numerical IP addresses.</p> <p><i>[No ETSI definition]</i></p>	
Latency	<p>Network latency in a packet switched network is measured either one way (the time from the source sending a packet to the destination receiving it), or round-trip delay time (the one-way latency from source to destination plus the one-way latency from the destination back to the source).</p> <p>For a definition, refer to ITU-T Y.1540 and ITU-T G.1020.</p> <p>For the recommended values, refer to ITU-T Y.1541 and ITU-T G.114.</p> <p><i>[ETSI definition: Packet delay is the elapsed time between a packet being presented to the NFV⁽¹⁵⁾ virtual network from one VNFC guest OS instance to that same packet being presented to the destination VNFC guest OS instance. Packets that are delivered with more than the maximum acceptable packet delay for the VNF are counted as packet loss events and excluded from packet delay measurements.]⁽¹⁶⁾</i></p>	<p>Infrastructure latency is recommended to be less than 1 ms.</p> <p>Latency must be minimized to achieve good quality of service.</p>
Jitter	<p>In packet switched networks, jitter is the variation in latency as measured in the variability over time of the packet latency across a network. Packet jitter is expressed as an average of the deviation from the network mean latency.</p> <p>For a definition, refer to ITU-T Y.1540, ITU-T G.1020, and RFC 3393.</p> <p>For the recommended values, refer to ITU-T Y.1541.</p>	<p>The expected internal jitter is recommended to be less than 5 ms.</p> <p>Jitter must be minimized to achieve good quality of service.</p>



Category	Category Definition	Requirement Text
	<i>[ETSI definition: Packet delay variance (that is, jitter) is the variance in packet delay.]</i>	
Packet loss	<p>Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss is measured as a percentage of packets lost divided by packets sent.</p> <p>For a definition, refer to ITU-T Y.1540 and ITU-T G.1020.</p> <p>For the recommended values, refer to ITU-T Y.1541.</p> <p><i>[ETSI definition: Packet loss is the rate of packets that are either never delivered to the destination or delivered to the destination after the maximum acceptable packet delay of the VNF.]</i></p>	<p>Packet loss for the infrastructure is recommended to be less than 1×10^{-4}.</p> <p>Packet loss must be minimized to achieve good quality of service.</p>
VLAN tagging	<p>VLAN Tagging is used to separate the traffic of different VLANs when VLANs span multiple switches. VLAN Tagging is done by inserting a VLAN ID into a packet header to identify to which VLAN the packet belongs.</p> <p><i>[No ETSI definition]</i></p>	<p>No specific requirements apply.</p> <p>When using VLAN network separation, VLAN tagging is performed by the vSwitch and other physical network infrastructure, but is not visible to the VNF. (The VNF sees all packets as "untagged" by the different access vNICs).</p>
MTU size	<p>The MTU⁽¹⁾ is the largest packet size, measured in bytes that can be transmitted over a network. Any messages larger than the MTU are divided into smaller packets before being sent. Breaking them up slows down transmission speeds. Ideally, the MTU size should be the same as the smallest MTU size of all the networks between the local computer and a message's final destination.</p> <p>Fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.</p>	<p>The recommended default IP MTU setting for IMSv VNF applications is 1452 on the core network interfaces.</p>

(1) Virtualized Network Interface Controller (vNIC)



- (2) Virtual Local Area Network (VLAN)*
- (3) Quality of Service (QoS)*
- (4) Virtual Link (VL)*
- (5) Address Resolution Protocol (ARP)*
- (6) Internet Control Message Protocol (ICMP)*
- (7) Bidirectional Forwarding Detection (BFD)*
- (8) Virtual Router Redundancy Protocol (VRRP)*
- (9) Preboot eXecution Environment (PXE)*
- (10) Dynamic Host Configuration Protocol (DHCP)*
- (11) Trivial File Transfer Protocol (TFTP)*
- (12) Open Shortest Path First (OSPF)*
- (13) Load-Balancing-as-a-Service (LBaaS)*
- (14) Network Time Protocol (NTP)*
- (15) Network Function Virtualization*
- (16) There are other types of latencies defined in the ETSI specification.*
- (17) Maximum Transmission Unit (MTU)*

4 Storage Requirements

This section lists all storage requirements, see [Table 3](#).

Table 3 Storage Requirements

Category	Category Definition	Requirement Text
Storage	<p>Persistent storage space used for storing and retrieving digital information.</p> <p><i>[ETSI definition: Required storage characteristics (for example, size), including KQIs ⁽¹⁾ for performance and reliability/availability.]</i></p>	<p>Each vMRF VM must be configured with a disk of at least 6 GB.</p> <p>A VM can use local or network storage.</p>
Storage performance	<p>Performance capability of a storage device is determined by the following three factors:</p> <ul style="list-style-type: none"> • Speed or throughput or bandwidth: the speed at which data is transferred out of or into the storage device (normally measured in megabytes per second) • IOPS: Input/Output Operations per Second (read and write) • Latency: how long it takes for a storage device to start an I/O task (measured in fractions of a second). <p>Speed and IOPS values vary depending on the access operation (sequential or random).</p> <p><i>[ETSI definition for latency: The latency in accessing a specific state held in storage to execute an instruction cycle.]</i></p>	No specific requirements apply.
Shared storage	<p>Required if the announcement service from vMRF is used. vMRF supports SSHFS storage as a service. The storage solution can be a physical server or a virtualized solution. (For example,</p>	<p>SSHFS remote mount is required for persistent storage of data and announcement service.</p>



Category	Category Definition	Requirement Text
	any VM, acting as SSHFS server, where the announcements are stored).	

(1) Key Quality Indicator (KQI)



5 Security Requirements

This section lists all security requirements, see [Table 4](#).

Table 4 Security Requirements

Category	Category Definition	Requirement Text
vNIC traffic separation	Different types of traffic are separated to provide security.	Support for vNIC traffic separation is required.
Trunk vNIC support	To support a high number of VLANs.	Trunk vNIC support is not required.
Virtual Switch traffic separation	Different types of traffic are separated to provide security.	Virtual Switches in the hypervisor must be capable of switching packets based on the VLAN tags and provide separation for traffic with different VLAN tags.
Physical interfaces traffic separation	Different types of traffic are separated to provide security.	No hard requirement on physical separation. Traffic separation to be sorted out with VLAN segmentation on L2 level.
VNF isolation	VNFs are to be protected and isolated from other VNFs in the environment.	The hypervisor must ensure the security of VNFs by preventing interferences from other VNFs in the deployment, that is, memory, storage, and other resources assigned to a VNF are not accessible to other VNFs.
Hypervisor security against VM escape attempts	VMs are protected and isolated from other VMs in the environment.	The hypervisor must prevent VMs from "escaping" to the hypervisor. The hypervisor software is to be upgraded to remove security issues (several vulnerabilities on different hypervisors have been reported, which allows a VM to escape to the hypervisor).
OAM authentication and authorization	OAM protection of the hypervisor.	The hypervisor must implement proper authentication and authorization mechanisms to prevent unauthorized users from accessing the hypervisor and perform malicious activities. Different accounts with different roles must be implemented. Audit trails logs must be implemented.



Category	Category Definition	Requirement Text
OAM access control to VNFs	Restrict access to VNFs.	The hypervisor must implement control about which hypervisor accounts are capable of managing specific VNFs in the cloud environment.
Deployment-related security	Applications can have more deployment requirements in the security area.	No specific requirements apply.



6 Other Requirements

This section lists all other requirements, see [Table 5](#).

Table 5 Other Requirements

Category	Category Definition	Requirement Text
Hypervisor	<p>A hypervisor, or VMM⁽¹⁾, is a piece of computer software, firmware, or hardware that creates and runs VMs. A computer on which a hypervisor is running one or more VMs is defined as a host machine. Each VM is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of various operating systems can share the virtualized hardware resources.</p> <p><i>[ETSI: Hypervisor is a piece of software that partitions the underlying physical resources and creates VMs, and isolates the VMs from each other.</i></p> <p><i>The hypervisor is a piece of software running either directly on top of the hardware (bare metal hypervisor) or running on top of a hosting operating system (hosted hypervisor). The abstraction of resources comprises all those entities inside a computer or server that are accessible, like processor, memory/storage, or NICs. The hypervisor enables the portability of VMs to different hardware.]</i></p>	<p>vMRF is a software only product verified with qemu-KVM and VMWare/ESXi on X86_64 processors with VT-x extension.</p> <p>In theory any kind of hypervisor can be suitable that meets the computing, virtual networking, and storage-related cloud requirements.</p> <p>The hypervisor shall support the MontaVista Linux guest operating system.</p>
Para-virtualized drivers	<p>Para-virtualization is a virtualization technique that presents a software interface to VMs that is similar, but not identical to, the underlying hardware. The intent of the modified interface is to reduce the</p>	<p>vMRF requires support for one of the following para-virtualized drivers: Virtio for KVM or vmxnet3 for VMware.</p>



Category	Category Definition	Requirement Text
	<p>portion of the execution time spent for the guest performing operations that are substantially more difficult to run in a virtual environment compared to a non-virtualized environment.</p> <p>Para-virtualized drivers are I/O device drivers that interact directly with the virtualization platform (with no emulation) to deliver disk and network access. This allow the disk and network subsystems to operate at near native speeds even in a virtualized environment, without requiring changes to existing guest operating systems.</p> <p><i>[No ETSI definition]</i></p>	
Installation	Any tools and environment-related software that is needed for installation.	<p>vMRF provides OVF 1.1 based installation for VMWare and HOT based installation for CEE/ OpenStack (OpenStack Kilo⁽²⁾).</p> <p>Both the OVF 1.1 based installation and the HOT based installation include vmdk images "monolithicSpars" format.</p>
VM evacuation	Virtualization environments may provide capabilities to move a VM from one compute host.	<p>vMRF VMs can be evacuated to another compute host.</p> <p>The move of running VMs from one compute host to another is not supported. Moving a running VM is possible only after it has been locked to avoid traffic disturbance.</p>

(1) Virtual Machine Monitor (VMM)

(2) The HOT based installation for a vanilla OpenStack Kilo deployment may require changes to the supplied HOT templates.