

Virtualized MTAS Infrastructure Requirements

MTAS

REQUIREMENTS SPEC.

Copyright

© Ericsson AB 2016. 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.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

1	Introduction	1
2	Compute Requirements	3
3	Network Requirements	7
4	Storage Requirements	15
5	Security Requirements	17
6	Other Requirements	19





1 Introduction

This document describes the minimum infrastructure resource requirements to deploy virtualized MTAS application in a cloud deployment.





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>Physical CPUs with x86_64 architecture in the host that also supports: VT-x/AMD-V hardware acceleration and hyper-threading technology.</p> <p>Hyper-threading is recommended to be enabled.</p> <p>Note: The identification of the virtualized MTAS infrastructure requirement was performed on Generic Ericsson Processor 5 (GEP5) boards which are equipped with Intel XEON E5-2658v2 (Ivy Bridge) processor.</p>
vCPU ⁽²⁾	<p><i>[ETSI definition: The vCPU created for a VM⁽³⁾ by a hypervisor (see Section 6 on page 19). In practice, a vCPU can be a time sharing of a real CPU and/or in the case of multicore CPUs, it may be an allocation of one or more cores to a VM.]</i></p> <p>vCPU-affinity can be used to isolate a physical CPU to a vCPU, by pinning the vCPU to a dedicated physical CPU.</p>	vCPU-affinity can be used

Table 1 Compute Requirements

Category	Category Definition	Requirement Text
Number of vCPUs	<i>[ETSI definition: VM is a virtualized computation environment that 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 Section 6 on page 19), which partitions the underlying physical resources and allocates them to VMs. VMs are capable of hosting a VNFC.]</i>	The required minimum amount of vCPUs per VM is 3. The recommended minimum number of vCPUs per VM is 4.
vCPU clock	A minimum average vCPU frequency guaranteed by the hypervisor. <i>[No ETSI definition]</i>	No input available since qemu-KVM hypervisor was used during the verification activities and specifying the vCPU frequency for the VM is not supported by qemu-KVM.
Memory	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 rapidly or immediately. <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 modeled using one or multiple such constructs, as applicable.]</i>	The required minimum amount of memory per VM is 25 GB. This depends on the number of vCPUs specified per VM. The required minimum amount of memory per VM is heavily dependent on the following: <ul style="list-style-type: none"> • Number of vCPUs per VM • Collocated Application Server(s) • Traffic Mix offered For more details on VM memory requirements please refer to Virtualized MTAS dimensioning guides.
Compute host	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 Section 6 on page 19) may or may not be seen as part of the host. <i>[No ETSI definition]</i>	The required minimum number of compute hosts is 4 for the 4 VMs (that is, 2 SC and 2 PL VMs) one for each VM. VMs belonging to the same MTAS VNF are not to be collocated on the same compute host.



Table 1 Compute Requirements

Category	Category Definition	Requirement Text
Overcommitting CPU	<p>CPU overcommitting is a hypervisor feature (see Section 6 on page 19) 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><i>[ETSI definition: The VDU can coexist on a platform with multiple VDUs or VMs and is as such sharing CPU core resources available in the platform. It can 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></p>	Overcommitting CPU is not allowed.
Overcommitting memory	<p>Memory overcommitting is a hypervisor feature (see Section 6 on page 19) 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>	Memory overcommitting is not allowed.

(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>	<p>4 vNICs are required per MTAS VM using Virtio/vmxnet3 drivers:</p> <ul style="list-style-type: none"> • eth0 - <MTAS VNF>_internal network • eth1 - <MTAS VNF>_OM_int network • eth2 - <MTAS VNF>_om_sc_sp network • eth3 - <MTAS VNF>_sig_sc_sp network
Virtual networks or VLANs ⁽²⁾ per vNIC	<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>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>The following four VLAN separated virtual networks are required by MTAS each having its own vNIC:</p> <ul style="list-style-type: none"> • <MTAS VNF>_internal • <MTAS VNF>_OM_int • <MTAS VNF>_om_sc_sp • <MTAS VNF>_sig_sc_sp <p>It is recommended to use VLAN segmentation to separate virtual network.</p>

Table 2 Network Requirements

Category	Category Definition	Requirement Text
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>	<p>The cloud infrastructure must provide at least about 40 Mb/s per VM of bandwidth for 2+2 cluster with 4 vCPU on eth0 interface (200 Mb/s is needed for a 2+10 cluster with 10 vCPU).</p> <p>Note:</p> <ul style="list-style-type: none"> During PL/cluster reboot, the throughput can increase to 200 Mb/s
Bandwidth of the total virtual networks	The sum of the measured bandwidth of all vNICs connected to the VM.	<p>The cloud infrastructure must provide at least the following bandwidth per VM for:</p> <ul style="list-style-type: none"> vNIC eth1 <<1 Mb/s vNIC eth2 typically < 8 Mb/s (but it depends on: 1. How fast the charging data buffer is supposed to be emptied in the case of Rf link reestablishment, 2. How fast the charging data is supposed to be fetched from the ACR storage) vNIC eth3 8 Mb/s for a 2+2 cluster with 4 vCPUs (around 64 Mb/s for a 2+10 cluster with 9 vCPUs) <p>Total throughput of 57 Mb/s non-blocking switching is required from the underlying virtual switching infrastructure per VM for a 2+2 cluster with 4vCPU.</p>
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>[No ETSI definition]</p>	Hardware accelerated virtual I/O is not required but it can increase the performance of MTAS.



Table 2 Network Requirements

Category	Category Definition	Requirement Text
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>	Tele-grade availability of the virtual networks is required for MTAS therefore L2 redundancy is supposed to be secured by the cloud 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, for example, latency and jitter.]</i></p>	MTAS supports DSCP marking of outgoing packets therefore it is recommended that the Differentiated Services Code Points are considered at the L3 boundaries of the virtual networks.
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>	L3 network separation is not required for MTAS on the <MTAS VNF>_internal and <MTAS VNF>_OM_int networks. On the other hand globally routable subnets have to be reserved for the OM (sysgmt) and VIP FEE networks.
vNIC type	<p>vNIC can be of access or trunk type. Each vNIC can have multiple 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>	<p>Support of multiple IP interfaces on access vNICs is provided. This includes the following:</p> <ul style="list-style-type: none"> Multiple IP interfaces of the same IP version (alias interfaces) are required on the <MTAS VNF>_internal network (NFS, CP-M MIP addresses). Dual stack configuration, that is, both IPv4 and IPv6 interfaces.

Table 2 Network Requirements

Category	Category Definition	Requirement Text
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>The MTAS application must be able to create its own IP interfaces. The cloud manager can assign subnets to the MTAS as long as the IP addresses in these subnets can be used freely by the MTAS application.</p> <p>Moreover the cloud infrastructure must allow packets to pass through virtual ports regardless of the subnet associated with the network.</p>
Path supervision	<p>Any path supervision protocols can be used, such as Gratuitous ARP⁽⁴⁾, ICMP⁽⁵⁾, or BFD⁽⁶⁾.</p> <p><i>[No ETSI definition]</i></p>	<p>BFD (along with OSPF or static routing) must be permitted on the <MTAS VNF>_om_sc_sp and <MTAS VNF>_sig_sc_sp virtual networks</p> <p>For further details refer to <i>MTAS Internal and External Connectivity</i></p>
L3 redundancy	<p>L3 redundancy can be provided by the VRRP⁽⁷⁾.</p> <p><i>[No ETSI definition]</i></p>	<p>Redundant L3 routers (gateway routers) are required to provide the redundant static default routes on the VIP FEE networks.</p> <p>Redundant gateways must provide a VRRP protected default route on the OM_ext infrastructure.</p>



Table 2 Network Requirements

Category	Category Definition	Requirement Text
Booting network	<p>The PXE⁽⁸⁾ 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⁽⁹⁾ and TFTP⁽¹⁰⁾.</p> <p>The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.</p> <p><i>[No ETSI definition]</i></p>	The virtualization infrastructure must not block PXE booting traffic generated by the MTAS. The cloud infrastructure provided DHCP service must be disabled.
IPv4 or IPv6	<p>Internet Protocol version 4 (IPv4) and 6 (IPv6).</p> <p><i>[No ETSI definition]</i></p>	Virtualization infrastructure must support IPv4/IPv6 at the transport layer.
Routing protocol	<p>OSPF⁽¹¹⁾ is an Interior Gateway Routing Protocol for IP networks based on the shortest path first or link-state algorithm.</p> <p>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.</p> <p>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.</p> <p><i>[No ETSI definition]</i></p>	<p>The L2/L3 ecosystem must support both OSPFv2/3 with BFD and VRRP</p> <p>Static routing might be used over the <MTAS_VNF>_om_sc_sp, <MTAS_VNF>_sig_sc_sp infrastructure.</p> <p>For further details refer to <i>MTAS Internal and External Connectivity</i></p>

Table 2 Network Requirements

Category	Category Definition	Requirement Text
NTP ⁽¹²⁾	<p>NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.</p> <p><i>[No ETSI definition]</i></p>	All the VM instances must be able to access an appropriate NTP server.
DNS	<p>The DNS is a hierarchical distributed naming system for 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>	All the VM instances must be able to access an appropriate DNS server.
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⁽¹³⁾ 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.]⁽¹⁴⁾</i></p>	Latency is required to meet general Tele-grade requirement.



Table 2 Network Requirements

Category	Category Definition	Requirement Text
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><i>[ETSI definition: Packet delay variance (that is, jitter) is the variance in packet delay.]</i></p>	Jitter is required to meet general Tele-grade requirement.
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>	Packet loss is required to meet general Tele-grade requirement.



Table 2 *Network Requirements*

- (1) Virtualized Network Interface Controller (vNIC)*
- (2) Virtual Local Area Network (VLAN)*
- (3) Quality of Service (QoS)*
- (4) Address Resolution Protocol (ARP)*
- (5) Internet Control Message Protocol (ICMP)*
- (6) Bidirectional Forwarding Detection (BFD)*
- (7) Virtual Router Redundancy Protocol (VRRP)*
- (8) Preboot eXecution Environment (PXE)*
- (9) Dynamic Host Configuration Protocol (DHCP)*
- (10) Trivial File Transfer Protocol (TFTP)*
- (11) Open Shortest Path First (OSPF)*
- (12) Network Time Protocol (NTP)*
- (13) Network Function Virtualization*
- (14) There are other types of latencies defined in the ETSI specification.*



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 System Controller VM must be configured with a disk.</p> <p>The block device sizes supported by virtualized MTAS are:</p> <ul style="list-style-type: none"> • 200 GB • 600 GB • 950 GB <p>Note: The size of the attached block device heavily depends upon the amount of charging data that needs to be stored by charging backup handler (ACR storage) in case of Rf communications failure.</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>	<p>Typical read and write speed of block storage is 40 Mb/s which can increase to 120 Mb/s during upgrade</p>

(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.	Traffic separation is secured in-line with Ericsson IMS security principles for further details refer to <i>MTAS Internal and External Connectivity</i>
Trunk vNIC support	To support a high number of VLANs.	Trunk vNICs are not used by the virtualized MTAS for further details refer to <i>MTAS Internal and External Connectivity</i>
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 to be accessible to other VNFs.
Hypervisor security against VNF escape attempts	VNFs are protected and isolated from other VNFs in the environment.	The hypervisor must prevent VNFs 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 VNF to escape to the hypervisor).

*Table 4 Security Requirements*

Category	Category Definition	Requirement Text
OAM authentication and authorization	OAM protection of the hypervisor.	The hypervisor must implement proper authentication and authorization mechanisms to prevent users from accessing the hypervisor and perform malicious activities. Different accounts with different roles must be implemented. Audit trails logs must be implemented.
OAM access control to VNFs	Restrict access to VNFs.	OAM access control is required



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>MTAS is a software only product verified with qemu-KVM 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 minimum cloud requirements as detailed above.</p>

Table 5 Other Requirements

Category	Category Definition	Requirement Text
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 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 allows 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>	<p>MTAS requires support for para-virtualized drivers. This is required to achieve high performance and capacity characteristics in the system.</p>
Installation	<p>Any tools and environment-related software that is needed for installation.</p>	<p>To support OVF installation method, the following tools must be supported:</p> <ul style="list-style-type: none"> • An OVF installer such as the Ericsson ATLAS tool. <p>Note: Heat Orchestration Template (HOT) based installation is a viable alternative of the OVF installation method.</p>

(1) Virtual Machine Monitor (VMM)