

CUDB Virtual Infrastructure Requirements

USER GUIDE

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 to Virtual Infrastructure Requirements	1
1.1	Revision Information	1
2	Compute Requirements	3
3	Network Requirements	7
4	Storage Requirements	15
5	Security Requirements	17
6	Other Requirements	19
	Glossary	21
	Reference List	23





1 Introduction to Virtual Infrastructure Requirements

This document describes the requirements for the infrastructure as requested by virtualized CUDB.

1.1 Revision Information

Rev. A Initial release.





2 Compute Requirements

This section lists all compute requirements, see Table 1 for details.

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>[ETSI definition], Reference [4]: Device in the compute node, which provides the primary container interface. This is the generic processor, which executes the code of the Virtualized Network Function Component (VNFC).]</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: Validation and verification of virtualized CUDB was performed on single socket Generic Ericsson Processor version 5 (GEP5) boards which are equipped with Intel XEON E5-2658v2 (Ivy Bridge) processor.</p>
virtualized CPU	<p>Virtualized CPU-affinity can be used to isolate a physical CPU to a virtualized CPU, by pinning the virtualized CPU to a dedicated physical CPU.</p> <p>[ETSI definition], Reference [4]: The virtualized CPU created for a Virtual Machine (VM) by a hypervisor (see Section 6 on page 19). In practice, a virtualized CPU 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.]</p>	<p>Virtualized CPU affinity shall be used to ensure that virtualized CPUs of a VM never share (threads within) a physical CPU core with virtualized CPUs of other VMs.</p>

Table 1 Compute Requirements

Category	Category Definition	Requirement Text
Number of virtualized CPUs	[ETSI definition, Reference [4]: 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.]	Depending on the configuration choice, virtualized CUDB needs 2 virtualized CPUs per VM (vCUDB_2CPU_6GB) or 16 virtualized CPUs per VM (vCUDB_16CPU_47GB).
Memory Reference [5]	<p>Volatile RAM 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>[ETSI definition, Reference [5]: This represents the virtual memory needed for the Virtualization Deployment Unit (VDU) or the VM. The VDU is a construct used in an information model and the Virtualized Network Function (VNF) can be modeled using one or multiple such constructs, as applicable.]</p>	<p>Depending on the configuration choice, virtualized CUDB needs 6 GB memory per VM (vCUDB_2CPU_6GB) or 47 GB memory per VM (vCUDB_16CPU_47GB).</p> <p>If available, it is recommended to use Huge pages (typically, 1GB page size) for the memory allocation of virtualized CUDB VMs.</p>
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 Section 6 on page 19) may or may not be seen as part of the host.</p> <p>[No ETSI definition]</p>	<p>The recommended minimum number of compute hosts with hardware and software redundancy is at least four.</p> <p>Number of hosts should enable fulfilling CUDB High Availability requirements.</p> <p>For further details, refer to <i>CUDB Deployment Guide</i>, Reference [1].</p>



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>[ETSI definition, Reference [5]: 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.]</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>
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>[No ETSI definition]</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>





3 Network Requirements

This section lists all network requirements, see Table 2 for details.

Table 2 Network Requirements

Category	Category Definition	Requirement Text
Virtualized NICs per VM	<p>[ETSI definition], Reference [4]:</p> <ul style="list-style-type: none"> • Network Interface Card (NIC) is a device in a compute node that provides a physical interface with the infrastructure network. • Virtualized NIC is created for a VM by a hypervisor.] 	<p>Number of required virtualized NICs per VM depends on VM type:</p> <ul style="list-style-type: none"> • System Controller VM: 6 • Payload VM: 7
Virtual networks or VLANs per virtualized NIC	<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>[ETSI definition], Reference [6]: Virtual network is a topological component used to affect forwarding of specific characteristic information. The virtual network is bounded by its set of permissible network interfaces. 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.]</p>	<p>It is recommended to use VLANs for network isolation on the internal networks.</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 virtualized NIC assigned to the internal network.</p>	<p>The requirement about bandwidth is HW type dependent.</p> <p>Rx/Tx values:</p> <ul style="list-style-type: none"> • vCUDB_2CPU_6GB 105.50 Mb/s / 112.09 Mb/s • vCUDB_16CPU_47GB 788.84 Mb/s / 901.3 Mb/s

Table 2 *Network Requirements*

Category	Category Definition	Requirement Text
Bandwidth of the external networks	<p>External networks are the virtual networks used for communication external to the VNF. For example, network function (other VNFs or PNFs), network management systems, and charging system.</p> <p>The sum of the measured bandwidth of all virtualized NICs (except the virtualized NIC for VNF internal network) connected to the VM.</p>	<p>The requirement about bandwidth is HW type dependent.</p> <p>Rx/Tx values:</p> <ul style="list-style-type: none"> • vCUDB_2CPU_6GB 35.35 Mb/s / 27.49 Mb/s • vCUDB_16CPU_47GB 625 Mb/s / 694 Mb/s <p>These values shall be understood as maximum values for single VNF node setups; specific bandwidth varies depending on target traffic model and virtualized CUDB system solution, and may be further analysed on solution dimensioning.</p>
Pinning virtualized NICs	<p>Pinning virtualized NICs to physical ports enables to manage the distribution of traffic. When pinning is set, all traffic from the virtualized NIC travels through the I/O module to the specified Ethernet port.</p> <p>[No ETSI definition]</p>	<p>Pinning virtualized NICs to physical ports is not required.</p>
L2 redundancy	<p>To achieve telecom grade failure recovery, the virtualized NIC 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>[No ETSI definition]</p>	<p>Telecom grade availability of the virtual network is required, therefore L2 redundancy must be secured by the cloud infrastructure.</p>



Table 2 Network Requirements

Category	Category Definition	Requirement Text
L2/L3 QoS	<p>Quality Of Service (QoS) settings at L2/L3 for the traffic are not changed within the virtual network boundaries.</p> <p>[ETSI definition, Reference [6]: Describes the QoS options to be supported on the Virtual Link (VL), for example, latency and jitter.]</p>	Differentiated Services Code Point (DSCP) passthrough is required.
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>[No ETSI definition]</p>	Virtual Routers (VRs) should be used per Traffic Type, typically to separate OAM from User signalling traffic. If physical separation is possible, those VRs should be assigned physically separated uplinks. Traffic separation serves also the purpose of a more secure network design.
Virtualized NIC type	<p>Virtualized NIC can be of access or trunk type. Each virtualized NIC 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. 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>[No ETSI definition]</p>	Access type virtualized NICs are required.

Table 2 *Network Requirements*

Category	Category Definition	Requirement Text
IP address allocation	<p>The process of assigning IP addresses to the virtualized NICs that are associated to the VNF, including the permission for the assigning.</p> <p>[No ETSI definition]</p>	It should be possible to self-assign addresses to the virtualized NIC instances.
Path supervision	<p>Any path supervision protocols can be used, such as Gratuitous Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), or Bidirectional Forwarding Detection (BFD).</p> <p>[No ETSI definition]</p>	BFD support is required.
L3 redundancy	<p>L3 redundancy can be provided by the Virtual Router Redundancy Protocol (VRRP).</p> <p>[No ETSI definition]</p>	VRRP support is required.
Booting network	<p>The Preboot eXecution Environment (PXE) 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 Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP). The 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>[No ETSI definition]</p>	The virtualization infrastructure must allow PXE booting.
IPv4 or IPv6	<p>Internet Protocol version 4 (IPv4) and 6 (IPv6).</p> <p>[No ETSI definition]</p>	IPv4 need to be supported.



Table 2 Network Requirements

Category	Category Definition	Requirement Text
Routing protocol	<p>Open Shortest Path First (OSPF) 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. 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>[No ETSI definition]</p>	OSPF and Equal-Cost Multipath (ECMP) capable virtual router is necessary.
LBaaS	<p>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.</p> <p>[No ETSI definition]</p>	No specific requirements apply.
NTP	<p>NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.</p> <p>[No ETSI definition]</p>	All the VM instances must be able to access an appropriate NTP server.

Table 2 Network Requirements

Category	Category Definition	Requirement Text
DNS	<p>The Domain Name System (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>[No ETSI definition]</p>	No specific requirements apply.
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, Reference [8] and ITU-T G.1020, Reference [9]. For the recommended values, refer to ITU-T Y.1541, Reference [10] and ITU-T G.114, Reference [11].</p> <p>[ETSI definition, Reference [7]: Packet delay is the elapsed time between a packet being presented to the Network Function Virtualization (NFV) 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.]</p>	NFV Infrastructure latency shall be less than 500 microseconds.



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, Reference [8], ITU-T G.1020, Reference [9], and RFC 3393, Reference [12]. For the recommended values, refer to ITU-T Y.1541, Reference [10].</p> <p>[ETSI definition, Reference [7]: Packet delay variance (that is, jitter) is the variance in packet delay.]</p>	Jitter is required to meet general Telecom grade requirements.
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. For the recommended values, refer to ITU-T Y.1541.</p> <p>[ETSI definition, Reference [7]: 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.]</p>	Packet loss for the NFV infrastructure must be less than 0.001%.

Table 2 Network Requirements

Category	Category Definition	Requirement Text
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>[No ETSI definition]</p>	The externally routed networks should use VLAN tagging.
MTU Size	<p>The Maximum Transmission Unit (MTU) 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>	MTU shall be set to 1500 bytes.
Virtualized NIC sub-interfacing		ARP unicast that contains MAC address, which is not assigned to the interfaces by the infrastructure should be allowed.
IP Multicast		Multicast traffic should be possible in the infrastructure.



4 Storage Requirements

This section lists all storage requirements, see Table 3 for details.

Table 3 Storage Requirements

Category	Category Definition	Requirement Text
Storage	<p>Persistent storage space used for storing and retrieving digital information.</p> <p>ETSI definition, Reference [5]: Required storage characteristics (for example, size), including Key Quality Indicators (KQIs) for performance and reliability/availability.]</p>	<p>The requirement about VM storage size is HW type dependent:</p> <ul style="list-style-type: none"> • vCUDB_2CPU_6GB <ul style="list-style-type: none"> - System Controller VM: 80GB - Payload VM: 20GB • vCUDB_16CPU_47GB <ul style="list-style-type: none"> - System Controller VM: 670GB - Payload VM: 400GB
Storage performance	<p>Performance capability of a storage device is determined by the following three factors:</p> <p>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)</p> <p>Latency: how long it takes for a storage device to start an I/O task (measured in fractions of a second).</p> <p>Speed values vary depending on the access operation (sequential or random).</p> <p>ETSI definition, Reference [6] for latency: The latency in accessing a specific state held in storage to execute an instruction cycle.]</p>	<p>The requirement about read and write speed is HW type dependent:</p> <p>Read/write speed:</p> <ul style="list-style-type: none"> • vCUDB_2CPU_6GB 2.112 MB/s / 110.433 MB/s • vCUDB_16CPU_47GB 47.911 MB/s / 83.906 MB/s





5 Security Requirements

This section lists all security requirements, see Table 4 for details.

Table 4 Security Requirements

Category	Category Definition	Requirement Text
Virtualized NIC traffic separation	Different types of traffic are separated to provide security.	Network separation should be maintained
Trunk virtualized NIC support	To support a high number of VLANs.	Trunk virtualized NIC support is not required.
Virtual Switch traffic separation	Different types of traffic are separated to provide security.	Please refer to “L3 network separation” in Network related requirements
Physical interfaces traffic separation	Different types of traffic are separated to provide security.	No specific requirements apply.
VNF isolation by the hypervisor	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 from other VNFs.
Hypervisor security against VM escape attempts	VMs are protected and isolated from other VMs 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).
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.



Table 4 Security Requirements

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
IP packet filtering	IP packet filtering functionality	<p>Cloud Infrastructure routers and switches must provide tools to:</p> <ul style="list-style-type: none">• Perform IP filtering and VLAN encapsulation• Disable Processing of Packets Utilizing IP Options or alternative means• Support filtering based on the value(s) of any portion of the protocol headers for IP, TCP, UDP, and ICMP• Filter both incoming and outgoing traffic on any IP interface. The router to be used in cloud deployments must provide a similar feature to ACLs• Provide a iptables-like feature for equivalent filtering of traffic from/to the VMs• It shall be possible to log all routing/traffic filter actions



6 Other Requirements

This section lists all other requirements, see Table 5 for details.

Table 5 Other Requirements

Category	Category Definition	Requirement Text
Hypervisor	<p>A hypervisor, or Virtual Machine Monitor (VMM), 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>[ETSI definition, see Reference [6]: Hypervisor is a piece of software that partitions the underlying physical resources and creates VMs, and isolates the VMs from each other. 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.]</p>	<p>Virtualized CUDB is a software-only product verified with QEMU-KVM on x86 64-bit processors with VT-x extension. In theory any kind of hypervisor can be suitable that meets the computing, virtual networking and storage-related infrastructure requirements. The hypervisor shall support the SUSE Linux Enterprise Server 12 (SLESv12) guest operating system.</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 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>[No ETSI definition]</p>	Data Plane Development Kit (DPDK) support is required.
Installation	Any tools and environment-related software that is needed for installation.	<p>Heat Orchestration Template (HOT) - version 2014-10-16 -based installation method should be supported.</p> <p>The HOT based installation for CEE/Openstack includes qcow2 images.</p>
Cloud administration related security		Cloud administrative operations shall not simultaneously impact compute nodes hosting redundant virtualized CUDB components (refer to <i>CUDB High Availability</i> , Reference [2]) in order not to impact VNF functionality.
Geographical distribution across datacenters		All elements of a CUDB VNF shall be instantiated in the same datacenter.



Glossary

For the terms, definitions, acronyms and abbreviations used in this document, refer to *CUDB Glossary of Terms and Acronyms*, Reference [3].





Reference List

CUDB Documents

- [1] *CUDB Deployment Guide*
- [2] *CUDB High Availability*
- [3] *CUDB Glossary of Terms and Acronyms*

Other Documents and Online References

- [4] *Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV* http://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.02.01_60/gs_NFV003v010201p.pdf
- [5] *Network Functions Virtualisation (NFV); Management and Orchestration* http://www.etsi.org/deliver/etsi_gs/NFV-MAN/001_099/001/01.01.01_60/gs_NFV-MAN001v010101p.pdf
- [6] *Network Functions Virtualisation (NFV); Infrastructure Overview* http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf
- [7] *Network Functions Virtualisation (NFV); Service Quality Metrics* http://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/010/01.01.01_60/gs_NFV-INF010v010101p.pdf
- [8] *Y.1540 : Internet protocol data communication service - IP packet transfer and availability performance parameters* <https://www.itu.int/rec/T-REC-Y.1540>
- [9] *G.1020 : Performance parameter definitions for quality of speech and other voiceband applications utilizing IP networks* <https://www.itu.int/rec/T-REC-G.1020/en>
- [10] *Y.1541 : Network performance objectives for IP-based services* <https://www.itu.int/rec/T-REC-Y.1541/en>
- [11] *G.114 : One-way transmission time* <https://www.itu.int/rec/T-REC-G.114/en>
- [12] *IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). IETF RFC 3393* <https://www.ietf.org/rfc/rfc3393.txt>