Lakelse RA1 Review

NOTE: The review team concluded that RA1 had not changed significantly since the previous review (under OPNFV) in the fall of 2020, so given the limited time available, the review team focused its efforts on RA2.

2.2.1 Cloud Infrastructure Software Profile Requirements for Compute (source RM 5.2)

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
e.cap.001	Max number of vCPU that can be assigned to a single VM by the Cloud Infrastructure	At least 16	At least 16		
e.cap.002	Max memory that can be assigned to a single VM by the Cloud Infrastructure	at least 32 GB	at least 32 GB		
e.cap.003	Max storage that can be assigned to a single VM by the Cloud Infrastructure	at least 320 GB	at least 320 GB		
e.cap.004	Max number of connection points that can be assigned to a single VM by the Cloud Infrastructure	6	6		
e.cap.005	Max storage that can be attached / mounted to VM by the Cloud Infrastructure	Up to 16TB[1]	Up to 16TB[1]		
e.cap.006/ infra.com.cfg.003	CPU pinning support	Not required	Must support		
e.cap.007/ infra.com.cfg.002	NUMA support	Not required	Must support		
e.cap.018/ infra.com.cfg.005	Simultaneous Multithreading (SMT) enabled	Not required	Must support		
i.cap.018/ infra.com.cfg.004	Huge Pages configured	Not required	Must support		

Table 2-1: Reference Model Requirements: Cloud Infrastructure Software Profile Capabilities

> [1] *Defined in the `.bronze` configuration in RM section 4.2.6 Storage Extensions*

2.2.1.1 Cloud Infrastructure Software Profile Extensions Requirements for Compute

Reference	Description	Profile Extensions	Profile Extra-Specs	Specification Reference	Notes and GitHub Issue link
e.cap.008/ infra.com.acc.cfg.001	IPSec Acceleration using the virtio-ipsec interface	Compute Intensive GPU			
e.cap.010/ infra.com.acc.cfg.002	Transcoding Acceleration	Compute Intensive GPU	Video Transcoding		
e.cap.011/ infra.com.acc.cfg.003	Programmable Acceleration	Firmware-programmable adapter	Accelerator		
e.cap.012	Enhanced Cache Management: L=Lean; E=Equal; X=eXpanded	E	E		
e.cap.014/ infra.com.acc.cfg.004	Hardware coprocessor support (GPU/NPU)	Compute Intensive GPU			
e.cap.016/ infra.com.acc.cfg.005	FPGA/other Acceleration H/W	Firmware-programmable adapter			

2.2.2 Cloud Infrastructure Software Profile Requirements for Netwokring (source RM 5.2.3)

The features and configuration requirements related to virtual networking for the two (2) types of Cloud Infrastructure Profiles are specified below followed by networking bandwidth requirements.

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
infra.net.cfg.001	IO virtualisation using virtio1.1*	Must support	Must support		
infra.net.cfg.002	The overlay network encapsulation protocol needs to enable ECMP in the underlay to take advantage of the scale-out features of the network fabric	Must support VXLAN, MPLSoUDP, GENEVE, other	*No requirement specified*		
infra.net.cfg.003	Network Address Translation	Must support	Must support		
infra.net.cfg.004	Security Groups	Must support	Must support		
infra.net.cfg.005	SFC support	Not required	Must support		
infra.net.cfg.006	Traffic patterns symmetry	Must support	Must support		

Table 2-2a: Reference Model Requirements: Virtual Networking

> - *Workload Transition Guidelines might have other interfaces (such as SR-IOV VFs to be directly passed to a VM) or NIC-specific drivers on guest machines transiently allowed until more mature solutions are available with an acceptable level of efficiency to support telecom workloads (for example regarding CPU and energy consumption).*

The required number of connection points to a VM is described in `e.cap.004` above. The table below specifies the required bandwidth of those connection points.

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
n1, n2, n3, n4, n5, n6	1, 2, 3, 4, 5, 6 Gbps	Must support	Must support		
n10, n20, n30, n40, n50, n60	10, 20, 30, 40, 50, 60 Gbps	Must support	Must support		
n25, n50, n75, n100, n125, n150	25, 50, 75, 100, 125, 150 Gbps	Optional	Must support		
n50, n100, n150, n200, n250, n300	50, 100, 150, 200, 250, 300 Gbps	Optional	Must support		
n100, n200, n300, n400, n500, n600	100, 200, 300, 400, 500, 600 Gbps	Optional	Must support		

Table 2-2b: Reference Model Requirements: Network Interface Specifications

2.2.2.1 Cloud Infrastructure Software Profile Extensions Requirements for Networking

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
e.cap.013/ infra.hw.nac.cfg.004	SR-IOV over PCI-PT	N	Y		
e.cap.019/ infra.net.acc.cfg.001	vSwitch optimisation (DPDK)	N	Y		
e.cap.015/ infra.net.acc.cfg.002	SmartNIC (for HW Offload)	N	Optional		
e.cap.009/ infra.net.acc.cfg.003	Crypto acceleration	N	Optional		
infra.net.acc.cfg.004	Crypto Acceleration Interface	N	Optional		

2.2.3 Cloud Infrastructure Software Profile Requirements for Storage (source RM 5.2)

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
infra.stg.cfg.002	Storage Block	Must support	Must support		
infra.stg.cfg.003	Storage with replication	Not required	Must support		
infra.stg.cfg.004	Storage with encryption	Must support	Must support		
infra.stg.acc.cfg.001	Storage IOPS oriented	Not required	Must support		
infra.stg.acc.cfg.002	Storage capacity oriented	Not required	Not required		

Table 2-3: Reference Model Requirements: Cloud Infrastructure Software Profile Requirements

2.2.3.1 Cloud Infrastructure Software Profile Extensions Requirements for Storage

Reference	Description	Profile Extensions	Profile Extra-Specs	Specification Reference	Notes and GitHub Issue link
infra.stg.acc.cfg.001	Storage IOPS oriented	Storage Intensive High-performance storage			
infra.stg.acc.cfg.002	Storage capacity oriented	High Capacity			

2.2.4 Cloud Infrastructure Hardware Profile Requirements (source RM 5.4)

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
infra.hw.001	CPU Architecture (Values such as x64, ARM, etc.)				
infra.hw.cpu.cfg.001	Minimum number of CPU (Sockets)	2	2		
infra.hw.cpu.cfg.002	Minimum number of Cores per CPU	20	20		
infra.hw.cpu.cfg.003	NUMA	Not required	Must support		
infra.hw.cpu.cfg.004	Simultaneous Multithreading/Symmetric Multiprocessing (SMT/SMP)	Must support	Must support		
infra.hw.stg.hdd.cfg.001	Local Storage HDD	*No requirement specified*	*No requirement specified*		
infra.hw.stg.ssd.cfg.002	Local Storage SSD	Should support	Should support		
infra.hw.nic.cfg.001	Total Number of NIC Ports available in the host	4	4		
infra.hw.nic.cfg.002	Port speed specified in Gbps (minimum values)	10	25		
infra.hw.pci.cfg.001	Number of PCIe slots available in the host	8	8		
infra.hw.pci.cfg.002	PCIe speed	Gen 3	Gen 3		
infra.hw.pci.cfg.003	PCIe Lanes	8	8		
infra.hw.nac.cfg.003	Compression	*No requirement specified*	*No requirement specified*		

Table 2-4a: Reference Model Requirements: Cloud Infrastructure Hardware Profile Requirements

2.2.4.1 Cloud Infrastructure Hardware Profile-Extensions Requirements (source RM 5.4)

Reference	Description	Requirement for Basic Profile	Requirement for High Performance Profile	Specification Reference	Notes and GitHub Issue link
e.cap.014/ infra.hw.cac.cfg.001	GPU	N	Optional		
e.cap.016/ infra.hw.cac.cfg.002	FPGA/other Acceleration H/W	N	Optional		
e.cap.009/ infra.hw.nac.cfg.001	Crypto Acceleration	N	Optional		
e.cap.015/ infra.hw.nac.cfg.002	SmartNIC	N	Optional		
infra.hw.nac.cfg.003	Compression	Optional	Optional		
e.cap.013/ infra.hw.nac.cfg.004	SR-IOV over PCI-PT	N	Yes		

2.2.5 Cloud Infrastructure Management Requirements (source RM 4.1.5)

Reference	Description	Requirement (common to all Profiles)	Specification Reference	Notes and GitHub Issue link
e.man.001	Capability to allocate virtual compute resources to a workload	Must support		
e.man.002	Capability to allocate virtual storage resources to a workload	Must support		
e.man.003	Capability to allocate virtual networking resources to a workload	Must support		
e.man.004	Capability to isolate resources between tenants	Must support		
e.man.005	Capability to manage workload software images	Must support		
e.man.006	Capability to provide information related to allocated virtualised resources per tenant	Must support		
e.man.007	Capability to notify state changes of allocated resources	Must support		
e.man.008	Capability to collect and expose performance information on virtualised resources allocated	Must support		
e.man.009	Capability to collect and notify fault information on virtualised resources	Must support		

Table 2-5: Reference Model Requirements: Cloud Infrastructure Management Requirements

2.2.6 Cloud Infrastructure Security Requirements

2.2.6.1. System Hardening (source RM 7.9.1)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec.gen.001	Hardening	The Platform **must** maintain the specified configuration.	RA-1 6.3.6 "Security LCM", RA-1 7.2 "Cloud Infrastructure and VIM configuration management"	
sec.gen.002	Hardening	All systems part of Cloud Infrastructure **must** support password hardening as defined in CIS Password Policy Guide.	RA-1 6.3.1.3 "Password policy"	
sec.gen.003	Hardening	All servers part of Cloud Infrastructure **must** support a root of trust and secure boot.	RA-1 6.3.1.1 "Server boot hardening"	
sec.gen.004	Hardening	The Operating Systems of all the servers part of Cloud Infrastructure **must** be hardened by removing or disabling unnecessary services, applications and network protocols, configuring operating system user authentication, configuring resource controls, installing and configuring additional security controls where needed, and testing the security of the Operating System (NIST SP 800-123).	RA-1 6.3.1.4 "Function and Software"	

sec. gen. 005	Hardening	The Platform **must** support Operating System level access control.	RA-1 6.3.1.2 "System Access"	
sec. gen. 006	Hardening	The Platform **must** support Secure logging. Logging with root account must be prohibited when root privileges are not required.	RA-1 6.3.1.2 "System Access"	
sec. gen. 007	Hardening	All servers part of Cloud Infrastructure **must** be Time synchronized with authenticated Time service.	RA-1 6.3.7.6 "Security Logs Time Synchronisation"	
sec. gen. 008	Hardening	All servers part of Cloud Infrastructure **must** be regularly updated to address security vulnerabilities.	RA-1 6.3.1.5 "Patches", RA-1 6.3.6 "Security LCM"	
sec. gen. 009	Hardening	The Platform **must** support Software integrity protection and verification.	RA-1 6.3.3.2 "Integrity of OpenStack components configuration", RA-1 6.3.5 "Image Security"	
sec. gen. 010	Hardening	The Cloud Infrastructure **must** support encrypted storage, for example, block, object and file storage, with access to encryption keys restricted based on a need to know (Controlled Access Based on the Need to Know).	RA-1 6.3.3.3 "Confidentiality and Integrity of tenant data"	
sec. gen. 012	Hardening	The Operator **must** ensure that only authorized actors have physical access to the underlying infrastructure.	This requirement's verification goes beyond Anuket testing scope	
sec. gen. 013	Hardening	The Platform **must** ensure that only authorized actors have logical access to the underlying infrastructure.	RA-1 6.3.1.2 "System Access"	
sec. gen. 015	Hardening	Any change to the Platform **must** be logged as a security event, and the logged event must include the identity of the entity making the change, the change, the date and the time of the change.	RA-1 6.3.6 "Security LCM"	

Table 2-6: Reference Model Requirements: System Hardening Requirements

2.2.6.2. Platform and Access (source RM 7.9.2)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. sys. 001	Access	The Platform **must** support authenticated and secure access to API, GUI and command line interfaces	RA-1 6.3.2.4 "RBAC"	
sec. sys. 002	Access	The Platform **must** support Traffic Filtering for workloads (for example, Fire Wall).	RA-1 6.3.4 "Workload Security"	
sec. sys. 003	Access	The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic.	RA-1 6.3.3.1 "Confidentiality and Integrity of communications"	
sec. sys. 004	Access	The Cloud Infrastructure **must** support authentication, integrity and confidentiality on all network channels.	RA-1 6.3.3.1 "Confidentiality and Integrity of communications"	
sec. sys. 005	Access	The Cloud Infrastructure **must** segregate the underlay and overlay networks.	RA-1 6.3.3.1 "Confidentiality and Integrity of communications"	
sec. sys. 006	Access	The Cloud Infrastructure **must** be able to utilize the Cloud Infrastructure Manager identity lifecycle management capabilities.	RA-1 6.3.2.1 "Identity Security"	
sec. sys. 007	Access	The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control).	RA-1 6.3.2.4 "RBAC"	
sec. sys. 008	Access	The Platform **must** be able to assign the Entities that comprise the tenant networks to different trust domains. (Communication between different trust domains is not allowed, by default.)	RA-1 6.3.4 "Workload Security"	

sec. sys. 009	Access	The Platform **must** support creation of Trust Relationships between trust domains. These maybe uni-directional relationships where the trusting domain trusts another domain (the “trusted domain”) to authenticate users for them or to allow access to its resources from the trusted domain. In a bidirectional relationship both domain are “trusting” and “trusted”.		
sec. sys. 010	Access	For two or more domains without existing trust relationships, the Platform **must not**allow the effect of an attack on one domain to impact the other domains either directly or indirectly.		
sec. sys. 011	Access	The Platform **must not** reuse the same authentication credentials (e.g., key pairs) on different Platform components (e.g., different hosts, or different services).	RA-1 6.3.1.2 "System Access"	
sec. sys. 012	Access	The Platform **must** protect all secrets by using strong encryption techniques and storing the protected secrets externally from the component (e.g., in OpenStack Barbican)		
sec. sys. 013	Access	The Platform **must** generate secrets dynamically as and when needed.		
sec. sys. 015	Access	The Platform **must not** contain back door entries (unpublished access points, APIs, etc.).		
sec. sys. 016	Access	Login access to the Platform's components **must** be through encrypted protocols such as SSH v2 or TLS v1.2 or higher. Note: Hardened jump servers isolated from external networks are recommended	RA-1 6.3.6 "Security LCM"	
sec. sys. 017	Access	The Platform **must** provide the capability of using digital certificates that comply with X.509 standards issued by a trusted Certification Authority.	RA-1 6.3.3.1 "Confidentiality and Integrity of communications"	
sec. sys. 018	Access	The Platform **must** provide the capability of allowing certificate renewal and revocation.		
sec. sys. 019	Access	The Platform **must** provide the capability of testing the validity of a digital certificate (CA signature, validity period, non revocation, identity).		

Table 2-7: Reference Model Requirements: Platform and Access Requirements

2.2.6.3. Confidentiality and Integrity (source RM7.9.3)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec.ci. 001	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of data at rest and in transit.	RA-1 6.3.3 "Confidentiality and Integrity"	
sec.ci. 003	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of data related metadata.		
sec.ci. 004	Confidentiality	The Platform **must** support Confidentiality of processes and restrict information sharing with only the process owner (e.g., tenant).		
sec.ci. 005	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of process-related metadata and restrict information sharing with only the process owner (e.g., tenant).		
sec.ci. 006	Confidentiality/Integrity	The Platform **must** support Confidentiality and Integrity of workload resource utilization (RAM, CPU, Storage, Network I/O, cache, hardware offload) and restrict information sharing with only the workload owner (e.g., tenant).		
sec.ci. 007	Confidentiality/Integrity	The Platform **must not** allow Memory Inspection by any actor other than the authorized actors for the Entity to which Memory is assigned (e.g., tenants owning the workload), for Lawful Inspection, and for secure monitoring services. Administrative access must be managed using Platform Identity Lifecycle Management.		
sec.ci. 008	Confidentiality	The Cloud Infrastructure **must** support tenant networks segregation.	RA-1 6.3.4 "Workload Security"	

Table 2-8: Reference Model Requirements: Confidentiality and Integrity Requirements

2.2.6.4. Workload Security (source RM7.9.4)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link

sec.wl.001	Workload	The Platform **must** support Workload placement policy.	RA-1 6.3.4 "Workload Security"	
sec.wl.002	Workload	The Cloud Infrastructure **must** provide methods to ensure the platform's trust status and integrity (e.g. remote attestation, Trusted Platform Module).		
sec.wl.003	Workload	The Platform **must** support secure provisioning of Workloads.	RA-1 6.3.4 "Workload Security"	
sec.wl.004	Workload	The Platform **must** support Location assertion (for mandated in-country or location requirements).	RA-1 6.3.4 "Workload Security"	
sec.wl.005	Workload	The Platform **must** support the separation of production and non-production Workloads.	This requirement's verification goes beyond Anuket testing scope	
sec.wl.006	Workload	The Platform **must** support the separation of Workloads based on their categorisation (for example, payment card information, healthcare, etc.)	RA-1 6.3.4 "Workload Security"	

Table 2-9: Reference Model Requirements: Workload Security Requirements

2.2.6.5. Image Security (source RM7.9.5)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec.img.001	Image	Images from untrusted sources **must not** be used.	RA-1 6.3.5 "Image Security"	
sec.img.002	Image	Images **must** be scanned to be maintained free from known vulnerabilities.	RA-1 6.3.5 "Image Security"	
sec.img.003	Image	Images **must not** be configured to run with privileges higher than the privileges of the actor authorized to run them.		
sec.img.004	Image	Images **must** only be accessible to authorized actors.	RA-1 6.3.3.2 "Confidentiality and Integrity of communications"	
sec.img.005	Image	Image Registries **must** only be accessible to authorized actors.	RA-1 6.3.3.2 "Confidentiality and Integrity of communications"	
sec.img.006	Image	Image Registries **must** only be accessible over networks that enforce authentication, integrity and confidentiality.	RA-1 6.3.3.2 "Confidentiality and Integrity of communications"	
sec.img.007	Image	Image registries **must** be clear of vulnerable and out of date versions.	RA-1 6.3.3.2 "Confidentiality and Integrity of communications", RA-1 6.3.5 "Image Security"	

Table 2-10: Reference Model Requirements: Image Security Requirements

2.2.6.6. Security LCM (source RM7.9.6)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec.lcm.001	LCM	The Platform **must** support Secure Provisioning, Availability, and Deprovisioning (Secure Clean-Up) of workload resources where Secure Clean-Up includes tear-down, defense against virus or other attacks.	RA-1 6.3.7 "Monitoring and Security Audit"	
sec.lcm.002	LCM	The Cloud Operator **must** use management protocols limiting security risk such as SNMPv3, SSH v2, ICMP, NTP, syslog and TLS v1.2 or higher.	RA-1 6.3.6 "Security LCM"	
sec.lcm.003	LCM	The Cloud Operator **must** implement and strictly follow change management processes for Cloud Infrastructure, Cloud Infrastructure Manager and other components of the cloud, and Platform change control on hardware.	RA-1 6.3.7 "Monitoring and Security Audit"	
sec.lcm.005	LCM	Platform **must** provide logs and these logs must be monitored for anomalous behavior.	RA-1 6.3.7 "Monitoring and Security Audit"	
sec.lcm.006	LCM	The Platform **must** verify the integrity of all Resource management requests.	RA-1 6.3.3.3 "Confidentiality and Integrity of tenant data"	

sec. lcm. 007	LCM	The Platform **must** be able to update newly instantiated, suspended, hibernated, migrated and restarted images with current time information.		
sec. lcm. 008	LCM	The Platform **must** be able to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant DNS information.		
sec. lcm. 009	LCM	The Platform **must** be able to update the tag of newly instantiated, suspended, hibernated, migrated and restarted images with relevant geolocation (geographical) information.		
sec. lcm. 010	LCM	The Platform **must** log all changes to geolocation along with the mechanisms and sources of location information (i.e. GPS, IP block, and timing).		
sec. lcm. 011	LCM	The Platform **must** implement Security life cycle management processes including the proactive update and patching of all deployed Cloud Infrastructure software.	RA-1 6.3.1.5 "Patches"	
sec. lcm. 012	LCM	The Platform **must** log any access privilege escalation.	RA-1 6.3.7.2 "What to Log"	

Table 2-11: Reference Model Requirements: Security LCM Requirements

2.2.6.7. Monitoring and Security Audit (source RM7.9.7)

The Platform is assumed to provide configurable alerting and notification capability and the operator is assumed to have automated systems, policies and procedures to act on alerts and notifications in a timely fashion. In the following the monitoring and logging capabilities can trigger alerts and notifications for appropriate action.

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. mon. 001	Monitoring /Audit	Platform **must** provide logs and these logs must be regularly monitored for events of interest. The logs **must** contain the following fields: event type, date/time, protocol, service or program used for access, success/failure, login ID or process ID, IP address and ports (source and destination) involved.	RA-1 6.3.7.1 "Creating logs", RA-1 6.3.7.4 "Required Fields"	
sec. mon. 002	Monitoring	Security logs **must** be time synchronised.	RA-1 6.3.7.6 "Security Logs Time Synchronisation"	
sec. mon. 003	Monitoring	The Platform **must** log all changes to time server source, time, date and time zones.	RA-1 6.3.7.6 "Security Logs Time Synchronisation"	
sec. mon. 004	Audit	The Platform **must** secure and protect Audit logs (containing sensitive information) both in-transit and at rest.	RA-1 6.3.6 "Security LCM"	
sec. mon. 005	Monitoring /Audit	The Platform **must** Monitor and Audit various behaviours of connection and login attempts to detect access attacks and potential access attempts and take corrective actions accordingly	RA-1 6.3.3.2 "Confidentiality and Integrity of communications", RA-1 6.3.7.2 "What to log, what not to log"	
sec. mon. 006	Monitoring /Audit	The Platform **must** Monitor and Audit operations by authorized account access after login to detect malicious operational activity and take corrective actions.	RA-1 6.3.3.2 "Integrity of OpenStack components configuration", RA-1 6.3.7 "Monitoring and Security Audit"	
sec. mon. 007	Monitoring /Audit	The Platform **must** Monitor and Audit security parameter configurations for compliance with defined security policies.	RA-1 6.3.3.2 "Integrity of OpenStack components configuration"	
sec. mon. 008	Monitoring /Audit	The Platform **must** Monitor and Audit externally exposed interfaces for illegal access (attacks) and take corrective security hardening measures.	RA-1 6.3.3.1 "Confidentiality and Integrity of communications"	
sec. mon. 009	Monitoring /Audit	The Platform **must** Monitor and Audit service for various attacks (malformed messages, signalling flooding and replaying, etc.) and take corrective actions accordingly.	RA-1 6.3.3.2 "Confidentiality and Integrity of communications", RA-1 6.3.7 "Monitoring and Security Audit"	
sec. mon. 010	Monitoring /Audit	The Platform **must** Monitor and Audit running processes to detect unexpected or unauthorized processes and take corrective actions accordingly.	RA-1 6.3.7 "Monitoring and Security Audit"	
sec. mon. 011	Monitoring /Audit	The Platform **must** Monitor and Audit logs from infrastructure elements and workloads to detected anomalies in the system components and take corrective actions accordingly.	RA-1 6.3.7.1 "Creating logs"	

sec. mon. 012	Monitoring /Audit	The Platform **must** Monitor and Audit Traffic patterns and volumes to prevent malware download attempts.	RA-1 6.3.3.3 "Confidentiality and Integrity of tenant data"	
sec. mon. 013	Monitoring	The monitoring system **must not** affect the security (integrity and confidentiality) of the infrastructure, workloads, or the user data (through back door entries).		
sec. mon. 015	Monitoring	The Platform **must** ensure that the Monitoring systems are never starved of resources and **must** activate alarms when resource utilisation exceeds a configurable threshold.	RA-1 6.3.7 "Monitoring and Security Audit"	
sec. mon. 017	Audit	The Platform **must** audit systems for any missing security patches and take appropriate actions.	RA-1 6.3.1.5 "Patches"	
sec. mon. 018	Monitoring	The Platform, starting from initialization, **must** collect and analyze logs to identify security events, and store these events in an external system.	RA-1 6.3.7.3 "Where to Log"	
sec. mon. 019	Monitoring	The Platform's components **must not** include an authentication credential, e.g., password, in any logs, even if encrypted.	RA-1 6.3.7.2 "What to Log"	
sec. mon. 020	Monitoring /Audit	The Platform's logging system **must** support the storage of security audit logs for a configurable period of time.	RA-1 6.3.7.5 "Data Retention	
sec. mon. 021	Monitoring	The Platform **must** store security events locally if the external logging system is unavailable and shall periodically attempt to send these to the external logging system until successful.	RA-1 6.3.7.3 "Where to Log"	

Table 2-12: Reference Model Requirements: Monitoring and Security Audit Requirements

2.2.6.9. Open Source Software (source RM7.9.8)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. oss. 001	Software	Open source code **must** be inspected by tools with various capabilities for static and dynamic code analysis.		
sec. oss. 002	Software	The CVE(Common Vulnerabilities and Exposures) **must** be used to identify vulnerabilities and their severity rating for open source code part of Cloud Infrastructure and workloads software, https://cve.mitre.org/		
sec. oss. 003	Software	High severity rated vulnerabilities **must** be fixed. Refer to the CVSS (Common Vulnerability Scoring System) to know a vulnerability score.		
sec. oss. 004	Software	A dedicated internal isolated repository separated from the production environment **must**be used to store vetted open source content.		

Table 2-13: Reference Model Requirements: Open Source Software Security Requirements

2.2.6.9. IaaC security (source RM7.9.9)

Secure Code Stage Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. code. 001	IaaC	SAST -Static Application Security Testing **must** be applied during Secure Coding stage triggered by Pull, Clone or Comment trigger. Security testing that analyses application source code for software vulnerabilities and gaps against best practices. Example: open source OWASP range of tools.		

Table 2-14: Reference Model Requirements: IaaC Security Requirements, Secure Code Stage

Continuous Build, Integration and Testing Stage Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. bld. 003	IaaC	Container and Image Scan **must** be applied during the Continuous Build, Integration and Testing stage triggered by Package trigger. Example: A push of a container image to a container registry may trigger a vulnerability scan before the image becomes available in the registry.		

Table 2-15: Reference Model Requirements: IaaC Security Requirements, Continuous Build, Integration and Testing Stage

Continuous Delivery and Deployment Stage Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. del. 001	IaaC	Image Scan **must** be applied during the Continuous Delivery and Deployment stage triggered by Publish to Artifact and Image Repository trigger. Example: GitLab uses the open source Clair engine for container image scanning.		
sec. del. 002	IaaC	Code Signing **must** be applied during the Continuous Delivery and Deployment stage triggered by Publish to Artifact and Image Repository trigger. Code Signing provides authentication to assure that downloaded files are form the publisher named on the certificate.		
sec. del. 004	IaaC	Component Vulnerability Scan **must** be applied during the Continuous Delivery and Deployment stage triggered by Instantiate Infrastructure trigger. The vulnerability scanning system is deployed on the cloud platform to detect security vulnerabilities of specified components through scanning and to provide timely security protection. Example: OWASP Zed Attack Proxy (ZAP).		

Table 2-16: Reference Model Requirements: IaaC Security Requirements, Continuous Delivery and Deployment Stage

Runtime Defence and Monitoring Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. run. 001	IaaC	Component Vulnerability Monitoring **must** be continuously applied during the Runtime Defence and Monitoring stage. Security technology that monitors components like virtual servers and assesses data, applications, and infrastructure for security risks.		

Table 2-17: Reference Model Requirements: IaaC Security Requirements, Runtime Defence and Monitoring Stage

2.2.6.10. Compliance with Standards (source RM7.9.10)

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
sec. std. 012	Standards	The Public Cloud Operator **must**, and the Private Cloud Operator **may** be certified to be compliant with the International Standard on Awareness Engagements (ISAE) 3402 (in the US: SSAE 16); International Standard on Awareness Engagements (ISAE) 3402. US Equivalent: SSAE16.		

2.3 Architecture and OpenStack Requirements

"Architecture" in this chapter refers to Cloud infrastructure (referred to as NFVI by ETSI) + VIM (as specified in Reference Model Chapter 3).

2.3.1 General Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
gen. ost.01	Open source	The Architecture **must** use OpenStack APIs.	RA-1 5.3	

gen. ost.02	Open source	The Architecture **must** support dynamic request and configuration of virtual resources (compute, network, storage) through OpenStack APIs.	RA-1 5.3	
gen. rsl.01	Resiliency	The Architecture **must** support resilient OpenStack components that are required for the continued availability of running workloads.		
gen. avl.01	Availability	The Architecture **must** provide High Availability for OpenStack components.	RA-1 4.2 "Underlying Resources"	

Table 2-19: General Requirements

2.3.2 Infrastructure Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
inf. com. 01	Compute	The Architecture **must** provide compute resources for VM instances.	RA-1 3.3.1.4 "Cloud Workload Services"	
inf. com. 04	Compute	The Architecture **must** be able to support multiple CPU type options to support various infrastructure profiles (Basic and High Performance).	RA-1 4.4.1. "Support for Cloud Infrastructure Profiles and flavors"	
inf. com. 05	Compute	The Architecture **must** support Hardware Platforms with NUMA capabilities.	RA-1 4.4.1. "Support for Cloud Infrastructure Profiles and flavors"	
inf. com. 06	Compute	The Architecture **must** support CPU Pinning of the vCPUs of VM instance.	RA-1 4.4.1. "Support for Cloud Infrastructure Profiles and flavors"	
inf. com. 07	Compute	The Architecture **must** support different hardware configurations to support various infrastructure profiles (Basic and High Performance).	RA-1 3.3.3. "Host aggregates providing resource pooling"	
inf. com. 08	Compute	The Architecture **must** support allocating certain number of host cores for all non-tenant workloads such as for OpenStack services. SMT threads can be allocated to individual OpenStack services or their components.	Dedicating host cores to certain workloads (e. g., OpenStack services). Please see example, " Configuring libvirt compute nodes for CPU pinning"	
inf. com. 09	Compute	The Architecture **must** ensure that the host cores assigned to non-tenant and tenant workloads are SMT aware: that is, a host core and its associated SMT threads are either all assigned to non-tenant workloads or all assigned to tenant workloads.	Achieved through configuring the "cpu_dedicated_set" and "cpu_shared_set" parameters in nova.conf correctly.	
inf.stg. 01	Storage	The Architecture **must** provide remote (not directly attached to the host) Block storage for VM Instances.	RA-1 3.4.2.3. "Storage"	
inf.stg. 02	Storage	The Architecture **must** provide Object storage for VM Instances. Operators **may** choose not to implement Object Storage but must be cognizant of the risk of "Compliant VNFs" failing in their environment.	OpenStack Swift Service (RA-1 4.3.1.4 "Swift")	
inf.ntw. 01	Network	The Architecture **must** provide virtual network interfaces to VM instances.	RA-1 5.2.5. "Neutron"	
inf.ntw. 02	Network	The Architecture **must** include capabilities for integrating SDN controllers to support provisioning of network services, from the OpenStack Neutron service, such as networking of VTEPs to the Border Edge based VRFs.	RA-1 3.2.5. "Virtual Networking – 3rd party SDN solution"	
inf.ntw. 03	Network	The Architecture **must** support low latency and high throughput traffic needs.	RA-1 4.2.3. "Network Fabric"	
inf.ntw. 05	Network	The Architecture **must** allow for East/West tenant traffic within the cloud (via tunnelled encapsulation overlay such as VXLAN or Geneve).	RA-1 4.2.3. "Network Fabric"	
inf.ntw. 07	Network	The Architecture **must** support network resiliency.	RA-1 3.4.2.2. "Network"	
inf.ntw. 10	Network	The Cloud Infrastructure Network Fabric **must** be capable of enabling highly available (Five 9's or better) Cloud Infrastructure.	RA-1 3.4.2.2. "Network"	
inf.ntw. 15	Network	The Architecture **must** support multiple networking options for Cloud Infrastructure to support various infrastructure profiles (Basic and High Performance).	RA-1 4.2.3.4. "Neutron ML2-plugin Integration" and "OpenStack Neutron Plugins"	
inf.ntw. 16	Network	The Architecture **must** support dual stack IPv4 and IPv6 for tenant networks and workloads.		

Table 2-20: Infrastructure Requirements

2.3.3 VIM Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
vim.01	General	The Architecture **must** allow infrastructure resource sharing.	RA-1 3.2. "Consumable Infrastructure Resources and Services"	
vim.03	General	The Architecture **must** allow VIM to discover and manage Cloud Infrastructure resources.	RA-1 5.2.7. "Placement"	
vim.05	General	The Architecture **must** include image repository management.	RA-1 4.3.1.2. "Glance"	
vim.07	General	The Architecture **must** support multi-tenancy.	RA-1 3.2.1. "Multi-Tenancy"	
vim.08	General	The Architecture **must** support resource tagging.	"OpenStack Resource Tags"	

Table 2-21: VIM Requirements

2.3.4 Interfaces & APIs Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
int.api.01	API	The Architecture **must** provide APIs to access the authentication service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.1 "Keystone"	
int.api.02	API	The Architecture **must** provide APIs to access the image management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.2 "Glance"	
int.api.03	API	The Architecture **must** provide APIs to access the block storage management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.3 "Cinder"	
int.api	API	The Architecture **must** provide APIs to access the object storage management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.4 "Swift"	
int.api.05	API	The Architecture **must** provide APIs to access the network management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.5 "Neutron"	
int.api.06	API	The Architecture **must** provide APIs to access the compute resources management service and the associated mandatory features detailed in chapter 5.	RA-1 5.2.6 "Nova"	
int.api.07	API	The Architecture **must** provide GUI access to tenant facing cloud platform core services except at Edge/Far Edge clouds.	RA-1 4.3.1.9 "Horizon"	
int.api.08	API	The Architecture **must** provide APIs needed to discover and manage Cloud Infrastructure resources.	RA-1 5.2.7. "Placement"	
int.api.09	API	The Architecture **must** provide APIs to access the orchestration service.	RA-1 5.2.8 "Heat"	
int.api.10	API	The Architecture must expose the latest version and microversion of the APIs for the given Anuket OpenStack release for each of the OpenStack core services.	RA-1 5.2 Core OpenStack Services APIs	

Table 2-22: Interfaces and APIs Requirements

2.3.5 Tenant Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
tnt.gen.01	General	The Architecture **must** support multi-tenancy.	**duplicate of vim.07**	
tnt.gen.02	General	The Architecture **must** support self-service dashboard (GUI) and APIs for users to deploy, configure and manage their workloads.	RA-1 4.3.1.9 "Horizon" and 3.3.1.4 Cloud Workload Services	

Table 2-23: Tenant Requirements

2.3.6 Operations and LCM

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
lcm.gen.01	General	The Architecture must support zero downtime of running workloads when the number of compute hosts and/or the storage capacity is being expanded or unused capacity is being removed.		
lcm.adp.02	Automated deployment	The Architecture must support upgrades of software, provided by the cloud provider, so that the running workloads are not impacted (viz., hitless upgrades). Please note that this means that the existing data plane services should not fail (go down).		

Table 2-24: LCM Requirements

2.3.7 Assurance Requirements

Ref #	sub-category	Description	Traceability	Notes and GitHub Issue link
asr.mon.01	Integration	The Architecture **must** include integration with various infrastructure components to support collection of telemetry for assurance monitoring and network intelligence.		
asr.mon.03	Monitoring	The Architecture **must** allow for the collection and dissemination of performance and fault information.		
asr.mon.04	Network	The Cloud Infrastructure Network Fabric and Network Operating System **must** provide network operational visibility through alarming and streaming telemetry services for operational management, engineering planning, troubleshooting, and network performance optimisation.		

Table 2-25: Assurance Requirements

Table 2-18: Refere