# Lakelse RA2 Review

Reviewers:  please add notes and GitHub issue links in the right-hand column

## 2.2.1 Cloud Infrastructure Software Profile Capabilities

| Reference Model Section | Reference | Description | Requirement for Basic Profile | Requirement for Network Intensive Profile | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|---|---|
| 4.2.5 | e.cap.001 | Max number of vCPU that can be assigned to a single Pod by the Cloud Infrastructure | At least 16 (1) | At least 16 (1) | ra2.ch.011 | |
| 4.2.5 | e.cap.002 | Max memory in MB that can be assigned to a single Pod by the Cloud Infrastructure | at least 32 GB(1) | at least 32 GB(1) | ra2.ch.012 | |
| 4.2.5 | e.cap.003 | Max storage in GB that can be assigned to a single Pod by the Cloud Infrastructure | at least 320 GB(1) | at least 320 GB(1) | ra2.ch.010 | |
| 4.2.5 | e.cap.004 | Max number of connection points that can be assigned to a single Pod by the Cloud Infrastructure | 6 | 6 | ra2.ntw.003 | |
| 4.2.5 | e.cap.005 | Max storage in GB that can be attached / mounted to Pod by the Cloud Infrastructure | Up to 16TB(2) | Up to 16TB(2) | | |
| 4.2.5 | e.cap.006 | CPU pinning support | Not required | Must support | ra2.k8s.009 | |
| 4.2.5 | e.cap.007 | NUMA support | Not required | Must support | ra2.k8s.006 | |
| 4.2.5 | e.cap.008 | IPSec Acceleration using the virtio-ipsec interface | Not required | Optional | | |
| 4.2.5 | e.cap.009 | Crypto Acceleration using the virtio-crypto interface | Not required | Optional | | |
| 4.2.5 | e.cap.010 | Transcoding Acceleration | Not required | Not required | | |
| 4.2.5 | e.cap.011 | Programmable Acceleration | Not required | Not required | | |
| 4.2.5 | e.cap.012 | Enhanced Cache Management: L=Lean; E=Equal; X=eXpanded | E | E | | |
| 4.2.5 | e.cap.013 | SR-IOV over PCI-PT | Not required | Must support | ra2.ch.002<br>ra2.ch.003<br>ra2.k8s.007<br>ra2.ntw.004<br>ra2.ntw.008 | |
| 4.2.5 | e.cap.014 | Hardware coprocessor support (GPU/NPU) | Not required | Not required | N/A | |
| 4.2.5 | e.cap.015 | SmartNICs | Not required | Optional | | |
| 4.2.5 | e.cap.016 | FPGA/other Acceleration H/W | Not required | Optional | ra2.k8s.007<br>ra2.ntw.012 | |
| 4.2.5 | *e.cap.017* | *Ability to monitor L2-L7 data from workload* | *n/a(3)* | *n/a(3)* | | |
| 4.2.5 | i.cap.014 | Specifies the proportion of CPU cores consumed by the Cloud Infrastructure system on the worker nodes. If SMT is used, it indicates the number of consumed SMT threads. | 2 | 2 | ra2.k8s.008 | |
| 4.2.5 | i.cap.015 | Indicates the memory consumed by Cloud Infrastructure on the worker nodes | 16 GB | 16GB | | |
| 4.2.5 | i.cap.016 | Number of virtual cores per physical core; also known as CPU overbooking ratio that is required | 1:1 | 1:1 | ra2.ch.004<br>ra2.ch.005 | |
| 4.2.5 | i.cap.017 | QoS enablement of the connection point (vNIC or interface) | Not required | Must support | | |
| 4.2.5 | i.cap.018 | Support for huge pages | Not required | Must support | ra2.ch.001 | |
| 4.2.5 | i.pm.001 | Monitor worker node CPU usage, per nanosecond | Must support | Must support | | |
| 4.2.5 | i.pm.002 | Monitor pod CPU usage, per nanosecond | Must support | Must support | | |
| 4.2.5 | i.pm.003 | Monitor worker node CPU utilisation (%) | Must support | Must support | | |
| 4.2.5 | i.pm.004 | Monitor pod CPU utilisation | Must support | Must support | | |
| 4.2.5 | i.pm.005 | Measure external storage IOPs | Must support | Must support | | |
| 4.2.5 | i.pm.006 | Measure external storage throughput | Must support | Must support | | |
| 4.2.5 | i.pm.007 | Measure external storage capacity | Must support | Must support | | |

## 2.2.2 Virtual Network Interface Specifications

The required number of connection points to a Pod is described in `e.cap.004` above. This section describes the required bandwidth of those connection points.

| Reference Model Section | Reference | Description | Requirement for Basic Profile | Requirement for Network Intensive Profile | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|---|---|
| 4.2.2 | n1, n2, n3, n4, n5, n6 | 1, 2, 3, 4, 5, 6 Gbps | Must support | Must support | | |
| 4.2.2 | nn10, n20, n30, n40, n50, n60 | 10, 20, 30, 40, 50, 60 Gbps | Must support | Must support | | |
| 4.2.2 | n25, n50, n75, n100, n125, n150 | 25, 50, 75, 100, 125, 150 Gbps | Must support | Must support | | |
| 4.2.2 | nn50, n100, n150, n200, n250, n300 | 50, 100, 150, 200, 250, 300 Gbps | Must support | Must support | | |
| 4.2.2 | n100, n200, n300, n400, n500, n600 | 100, 200, 300, 400, 500, 600 Gbps | Must support | Must support | | |

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

## 2.2.3 Cloud Infrastructure Software Profile Requirements

| Reference Model Section | Reference | Description | Requirement for Basic Profile | Requirement for Network Intensive Profile | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|---|---|
| 5.2.1 | infra.com.cfg.001 | CPU allocation ratio | 1:1 | 1:1 | ra2.ch.005<br>ra2.ch.006 | |
| 5.2.1 | infra.com.cfg.002 | NUMA awareness | Must support | Must support | ra2.k8s.006 | |
| 5.2.1 | infra.com.cfg.003 | CPU pinning capability | Not required | Must support | ra2.k8s.009 | |
| 5.2.1 | infra.com.cfg.004 | Huge Pages | Must support | Must support | ra2.ch.001 | |
| 5.2.2 | infra.stg.cfg.002 | Storage Block | Must support | Must support | ra2.stg.004 | |
| 5.2.2 | infra.stg.cfg.003 | Storage with replication | Not required | Must support | | |
| 5.2.2 | infra.stg.cfg.004 | Storage with encryption | Must support | Must support | | |
| 5.2.2 | infra.stg.acc.cfg.001 | Storage IOPS oriented | Not required | Must support | | |
| 5.2.2 | infra.stg.acc.cfg.002 | Storage capacity oriented | Not required | Not required | | |
| 5.2.3 | infra.net.cfg.001 | IO virtualisation using virtio1.1 | Must support(1) | Must support(1) | | |
| 5.2.3 | 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.(2) | Must support VXLAN, MPLSoUDP, GENEVE, other | *No requirement specified* | | |
| 5.2.3 | infra.net.cfg.003 | Network Address Translation | Must support | Must support | | |
| 5.2.3 | infra.net.cfg.004 | Security Groups | Must support | Must support | | |
| 5.2.3 | infra.net.cfg.005 | SFC support | Not required | Must support | | |
| 5.2.3 | infra.net.cfg.006 | Traffic patterns symmetry | Must support | Must support | | |
| 5.2.3 | infra.net.acc.cfg.001 | vSwitch optimisation | Not required | Must support DPDK(3) | ra2.ntw.010 | |
| 5.2.3 | infra.net.acc.cfg.002 | Support of HW offload | Not required | Must support SmartNic | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5.2.3 | infra.net.acc.cfg.003 | Crypto acceleration | Not required | Must support | | |
| 5.2.3 | infra.net.acc.cfg.004 | Crypto Acceleration Interface | Not required | Must support | | |

## 2.2.4 Cloud Infrastructure Hardware Profile Requirements

| Reference Model Section | Reference | Description | Requirement for Basic Profile | Requirement for Network Intensive Profile | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|---|---|
| 5.4.1 | infra.hw.cpu.cfg.001 | Minimum number of CPU sockets | 2 | 2 | ra2.ch.008 | |
| 5.4.1 | infra.hw.cpu.cfg.002 | Minimum number of Cores per CPU | 20 | 20 | ra2.ch.008 | |
| 5.4.1 | infra.hw.cpu.cfg.003 | NUMA | Not required | Must support | ra2.k8s.006 | |
| 5.4.1 | infra.hw.cpu.cfg.004 | Simultaneous Multithreading/Symmetric Multiprocessing (SMT/SMP) | Must support | Must support | ra2.ch.004 | |
| 5.4.1 | infra.hw.cac.cfg.001 | GPU | Not required | Not required | | |
| 5.4.2 | infra.hw.stg.hdd.cfg.001 | Local Storage HDD | *No requirement specified* | *No requirement specified* | | |
| 5.4.2 | infra.hw.stg.ssd.cfg.002 | Local Storage SSD | Should support | Should support | ra2.ch.009 | |
| 5.4.3 | infra.hw.nic.cfg.001 | Total Number of NIC Ports available in the host | 4 | 4 | ra2.ch.013 | |
| 5.4.3 | infra.hw.nic.cfg.002 | Port speed specified in Gbps (minimum values) | 10 | 25 | ra2.ch.014<br>ra2.ch.015 | |
| 5.4.3 | infra.hw.pci.cfg.001 | Number of PCIe slots available in the host | 8 | 8 | ra2.ch.016 | |
| 5.4.3 | infra.hw.pci.cfg.002 | PCIe speed | Gen 3 | Gen 3 | ra2.ch.016 | |
| 5.4.3 | infra.hw.pci.cfg.003 | PCIe Lanes | 8 | 8 | ra2.ch.016 | |
| 5.4.3 | infra.hw.nac.cfg.001 | Cryptographic Acceleration | Not required | Optional | | |
| 5.4.3 | infra.hw.nac.cfg.002 | A SmartNIC that is used to offload vSwitch functionality to hardware | Not required | Optional[(1)] | | |
| 5.4.3 | infra.hw.nac.cfg.003 | Compression | *No requirement specified* | *No requirement specified* | | |

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

**(1)** There is no vSwitch in case of containers, but a SmartNIC can be used to offload any other network processing.

## 2.2.5 Cloud Infrastructure Management Requirements

| Reference Model Section | Reference | Description | Requirement (common to all Profiles) | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|---|
| 4.1.5 | e.man.001 | Capability to allocate virtual compute resources to a workload | Must support | | |
| 4.1.5 | e.man.002 | Capability to allocate virtual storage resources to a workload | Must support | | |
| 4.1.5 | e.man.003 | Capability to allocate virtual networking resources to a workload | Must support | | |
| 4.1.5 | e.man.004 | Capability to isolate resources between tenants | Must support | | |
| 4.1.5 | e.man.005 | Capability to manage workload software images | Must support | | |
| 4.1.5 | e.man.006 | Capability to provide information related to allocated virtualised resources per tenant | Must support | | |
| 4.1.5 | e.man.007 | Capability to notify state changes of allocated resources | Must support | | |

| | | | | | |
|---|---|---|---|---|---|
| 4.1.5 | e.man.008 | Capability to collect and expose performance information on virtualised resources allocated | Must support | | |
| 4.1.5 | 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

| Reference Model Section | Reference | Requirement (common to all Profiles) | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|
| 7.9.1 | sec.gen.001 | The Platform **must** maintain the specified configuration. | | |
| 7.9.1 | sec.gen.002 | All systems part of Cloud Infrastructure **must** support password hardening as defined in CIS Password Policy Guide. Hardening: CIS Password Policy Guide | | |
| 7.9.1 | sec.gen.003 | All servers part of Cloud Infrastructure **must** support a root of trust and secure boot. | | |
| 7.9.1 | sec.gen.004 | 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) | | |
| 7.9.1 | sec.gen.005 | The Platform **must** support Operating System level access control | | |
| 7.9.1 | sec.gen.006 | The Platform **must** support Secure logging. Logging with root account must be prohibited when root privileges are not required. | | |
| 7.9.1 | sec.gen.007 | All servers part of Cloud Infrastructure **must** be Time synchronized with authenticated Time service. | | |
| 7.9.1 | sec.gen.008 | All servers part of Cloud Infrastructure **must** be regularly updated to address security vulnerabilities. | | |
| 7.9.1 | sec.gen.009 | The Platform **must** support Software integrity protection and verification and **must**scan source code and manifests. | | |
| 7.9.1 | sec.gen.010 | 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 | | |
| 7.9.1 | sec.gen.011 | The Cloud Infrastructure **should** support Read and Write only storage partitions (write only permission to one or more authorized actors). | | |
| 7.9.1 | sec.gen.012 | The Operator **must** ensure that only authorized actors have physical access to the underlying infrastructure. | | |
| 7.9.1 | sec.gen.013 | The Platform **must** ensure that only authorized actors have logical access to the underlying infrastructure. | | |
| 7.9.1 | sec.gen.014 | All servers part of Cloud Infrastructure **should** support measured boot and an attestation server that monitors the measurements of the servers. | | |
| 7.9.1 | sec.gen.015 | 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. | | |
| 7.9.2 | sec.sys.001 | The Platform **must** support authenticated and secure access to API, GUI and command line interfaces. | | |
| 7.9.2 | sec.sys.002 | The Platform **must** support Traffic Filtering for workloads (for example, Fire Wall). | | |
| 7.9.2 | sec.sys.003 | The Platform **must** support Secure and encrypted communications, and confidentiality and integrity of network traffic. | | |
| 7.9.2 | sec.sys.004 | The Cloud Infrastructure **must** support authentication, integrity and confidentiality on all network channels. | | |
| 7.9.2 | sec.sys.005 | The Cloud Infrastructure **must** segregate the underlay and overlay networks. | | |
| 7.9.2 | sec.sys.006 | The Cloud Infrastructure must be able to utilize the Cloud Infrastructure Manager identity lifecycle management capabilities. | | |
| 7.9.2 | sec.sys.007 | The Platform **must** implement controls enforcing separation of duties and privileges, least privilege use and least common mechanism (Role-Based Access Control). | | |
| 7.9.2 | sec.sys.008 | The Platform **must** be able to assign the Entities that comprise the tenant networks to different trust domains. | | |
| 7.9.2 | sec.sys.009 | The Platform **must** support creation of Trust Relationships between trust domains. | | |
| 7.9.2 | sec.sys.010 | 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. | | |
| 7.9.2 | sec.sys.011 | The Platform **must not** reuse the same authentication credential (e.g., key-pair) on different Platform components (e.g., on different hosts, or different services). | | |

| | | | | |
|---|---|---|---|---|
| 7.9.2 | sec.sys.012 | 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). | |
| 7.9.2 | sec.sys.013 | The Platform **must** provide secrets dynamically as and when needed. | | |
| 7.9.2 | sec.sys.014 | The Platform **should** use Linux Security Modules such as SELinux to control access to resources. | | |
| 7.9.2 | sec.sys.015 | The Platform **must not** contain back door entries (unpublished access points, APIs, etc.). | | |
| 7.9.2 | sec.sys.016 | 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 | | |
| 7.9.2 | sec.sys.017 | The Platform **must** provide the capability of using digital certificates that comply with X.509 standards issued by a trusted Certification Authority. | | |
| 7.9.2 | sec.sys.018 | The Platform **must** provide the capability of allowing certificate renewal and revocation. | | |
| 7.9.2 | sec.sys.019 | The Platform **must** provide the capability of testing the validity of a digital certificate (CA signature, validity period, non revocation, identity). | | |
| 7.9.3 | sec.ci.001 | The Platform **must** support Confidentiality and Integrity of data at rest and in-transit. | | |
| 7.9.3 | sec.ci.002 | The Platform **should** support self-encrypting storage devices. | | |
| 7.9.3 | sec.ci.003 | The Platform **must** support Confidentiality and Integrity of data related metadata. | | |
| 7.9.3 | sec.ci.004 | The Platform **must** support Confidentiality of processes and restrict information sharing with only the process owner (e.g., tenant). | | |
| 7.9.3 | sec.ci.005 | The Platform **must** support Confidentiality and Integrity of process-related metadata and restrict information sharing with only the process owner (e.g., tenant). | | |
| 7.9.3 | sec.ci.006 | 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). | | |
| 7.9.3 | sec.ci.007 | 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 by secure monitoring services. | | |
| 7.9.3 | sec.ci.008 | The Cloud Infrastructure **must** support tenant networks segregation. | | |
| 7.9.4 | sec.wl.001 | The Platform **must** support Workload placement policy. | | |
| 7.9.4 | sec.wl.002 | The Cloud Infrastructure **must** provide methods to ensure the platform's trust status and integrity (e.g. remote attestation, Trusted Platform Module). | | |
| 7.9.4 | sec.wl.003 | The Platform **must** support secure provisioning of workloads. | | |
| 7.9.4 | sec.wl.004 | The Platform **must** support Location assertion (for mandated in-country or location requirements). | | |
| 7.9.4 | sec.wl.005 | The Platform **must** support the separation of production and non-production Workloads. | | |
| 7.9.4 | sec.wl.006 | The Platform **must** support the separation of Workloads based on their categorisation (for example, payment card information, healthcare, etc.). | | |
| 7.9.4 | sec.wl.007 | The Operator **should** implement processes and tools to verify VNF authenticity and integrity. | | |
| 7.9.5 | sec.img.001 | Images from untrusted sources **must not** be used. | | |
| 7.9.5 | sec.img.002 | Images **must** be scanned to be maintained free from known vulnerabilities. | | |
| 7.9.5 | sec.img.003 | Images **must not** be configured to run with privileges higher than the privileges of the actor authorized to run them. | | |
| 7.9.5 | sec.img.004 | Images **must** only be accessible to authorized actors. | | |
| 7.9.5 | sec.img.005 | Image Registries **must** only be accessible to authorized actors. | | |
| 7.9.5 | sec.img.006 | Image Registries **must** only be accessible over secure networks that enforce authentication, integrity and confidentiality. | | |
| 7.9.5 | sec.img.007 | Image registries **must** be clear of vulnerable and stale (out of date) versions. | | |
| 7.9.6 | sec.lcm.001 | 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. | | |
| 7.9.6 | sec.lcm.002 | Cloud operations staff and systems **must** use management protocols limiting security risk such as SNMPv3, SSH v2, ICMP, NTP, syslog and TLS v1.2 or higher. | | |
| 7.9.6 | sec.lcm.003 | 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. | | |
| 7.9.6 | sec.lcm.004 | The Cloud Operator **should** support automated templated approved changes. | | |
| 7.9.6 | sec.lcm.005 | Platform **must** provide logs and these logs must be regularly monitored for anomalous behavior. | | |
| 7.9.6 | sec.lcm.006 | The Platform **must** verify the integrity of all Resource management requests. | | |

| | | | | |
|---|---|---|---|---|
| 7.9.6 | sec.lcm.007 | The Platform **must** be able to update newly instantiated, suspended, hibernated, migrated and restarted images with current time information. | | |
| 7.9.6 | sec.lcm.008 | The Platform **must** be able to update newly instantiated, suspended, hibernated, migrated and restarted images with relevant DNS information. | | |
| 7.9.6 | sec.lcm.009 | The Platform **must** be able to update the tag of newly instantiated, suspended, hibernated, migrated and restarted images with relevant geolocation (geographical) information. | | |
| 7.9.6 | sec.lcm.010 | The Platform **must** log all changes to geolocation along with the mechanisms and sources of location information (i.e. GPS, IP block, and timing). | | |
| 7.9.6 | sec.lcm.011 | The Platform **must** implement Security life cycle management processes including the proactive update and patching of all deployed Cloud Infrastructure software. | | |
| 7.9.6 | sec.lcm.012 | The Platform **must** log any access privilege escalation. | | |
| 7.9.7 | sec.mon.001 | 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. | | |
| 7.9.7 | sec.mon.002 | Security logs **must** be time synchronised. | | |
| 7.9.7 | sec.mon.003 | The Platform **must** log all changes to time server source, time, date and time zones. | | |
| 7.9.7 | sec.mon.004 | The Platform **must** secure and protect Audit logs (containing sensitive information) both in-transit and at rest. | | |
| 7.9.7 | sec.mon.005 | 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. | | |
| 7.9.7 | sec.mon.006 | The Platform **must** Monitor and Audit operations by authorized account access after login to detect malicious operational activity and take corrective actions accordingly. | | |
| 7.9.7 | sec.mon.007 | The Platform **must** Monitor and Audit security parameter configurations for compliance with defined security policies. | | |
| 7.9.7 | sec.mon.008 | The Platform **must** Monitor and Audit externally exposed interfaces for illegal access (attacks) and take corrective security hardening measures. | | |
| 7.9.7 | sec.mon.009 | The Platform **must** Monitor and Audit service handling for various attacks (malformed messages, signalling flooding and replaying, etc.) and take corrective actions accordingly. | | |
| 7.9.7 | sec.mon.010 | The Platform **must** Monitor and Audit running processes to detect unexpected or unauthorized processes and take corrective actions accordingly. | | |
| 7.9.7 | sec.mon.011 | The Platform **must** Monitor and Audit logs from infrastructure elements and workloads to detected anomalies in the system components and take corrective actions accordingly. | | |
| 7.9.7 | sec.mon.012 | The Platform **must** Monitor and Audit Traffic patterns and volumes to prevent malware download attempts. | | |
| 7.9.7 | sec.mon.013 | The monitoring system **must not** affect the security (integrity and confidentiality) of the infrastructure, workloads, or the user data (through back door entries). | | |
| 7.9.7 | sec.mon.014 | The Monitoring systems **should not** impact IAAS, PAAS, and SAAS SLAs including availability SLAs. | | |
| 7.9.7 | sec.mon.015 | The Platform **must** ensure that the Monitoring systems are never starved of resources and **must** activate alarms when resource utilisation exceeds a configurable threshold. | | |
| 7.9.7 | sec.mon.016 | The Platform Monitoring components **should** follow security best practices for auditing, including secure logging and tracing. | | |
| 7.9.7 | sec.mon.017 | The Platform **must** audit systems for any missing security patches and take appropriate actions. | | |
| 7.9.7 | sec.mon.018 | The Platform, starting from initialization, **must** collect and analyze logs to identify security events, and store these events in an external system. | | |
| 7.9.7 | sec.mon.019 | The Platform's components **must not** include an authentication credential, e.g., password, in any logs, even if encrypted. | | |
| 7.9.7 | sec.mon.020 | The Platform's logging system **must** support the storage of security audit logs for a configurable period of time. | | |
| 7.9.7 | sec.mon.021 | 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. | | |
| 7.9.8 | sec.std.001 | The Cloud Operator **should** comply with Center for Internet Security CIS Controls (https://www.cisecurity.org/) | | |
| 7.9.8 | sec.std.002 | The Cloud Operator, Platform and Workloads **should** follow the guidance in the CSA Security Guidance for Critical Areas of Focus in Cloud Computing (latest version) https://cloudsecurityalliance.org/ | | |
| 7.9.8 | sec.std.003 | The Platform and Workloads **should** follow the guidance in the OWASP Cheat Sheet Series (OCSS) https://github.com/OWASP/CheatSheetSeries | | |
| 7.9.8 | sec.std.004 | The Cloud Operator, Platform and Workloads **should** ensure that their code is not vulnerable to the OWASP Top Ten Security Risks https://owasp.org/www-project-top-ten/ | | |

| | | | | | |
|---|---|---|---|---|---|
| 7.9.8 | sec.std.005 | The Cloud Operator, Platform and Workloads **should** strive to improve their maturity on the OWASP Software Maturity Model (SAMM) https://owaspsamm.org/blog/2019/12/20/version2-community-release/ | | |
| 7.9.8 | sec.std.006 | The Cloud Operator, Platform and Workloads **should** utilize the OWASP Web Security Testing Guide https://github.com/OWASP/wstg/tree/master/document | | |
| 7.9.8 | sec.std.007 | The Cloud Operator, and Platform **should** satisfy the requirements for Information Management Systems specified in ISO/IEC 27001 https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. ISO/IEC 27002:2013 - ISO/IEC 27001 is the international Standard for best-practice information security management systems (ISMSs). | | |
| 7.9.8 | sec.std.008 | The Cloud Operator, and Platform **should** implement the Code of practice for Security Controls specified ISO/IEC 27002:2013 (or latest) https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en | | |
| 7.9.8 | sec.std.009 | The Cloud Operator, and Platform **should** implement the ISO/IEC 27032:2012 (or latest) Guidelines for Cybersecurity techniques https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. ISO/IEC 27032 - ISO/IEC 27032is the international Standard focusing explicitly on cybersecurity. | | |
| 7.9.8 | sec.std.010 | The Cloud Operator **should** conform to the ISO/IEC 27035 standard for incidence management. ISO/IEC 27035 - ISO/IEC 27035 is the international Standard for incident management. | | |
| 7.9.8 | sec.std.011 | The Cloud Operator **should** conform to the ISO/IEC 27031 standard for business continuity. ISO/IEC 27031 - ISO/IEC 27031 is the international Standard for ICT readiness for business continuity. | | |
| 7.9.8 | sec.std.012 | 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. | | |

**Table 2-6:** Reference Model Requirements: Cloud Infrastructure Security Requirements

## 2.3 Kubernetes Architecture Requirements

The Reference Model (RM) defines the Cloud Infrastructure, which consists of the physical resources, virtualised resources and a software management system. In the virtualised world, the Cloud Infrastructure consists of the Guest Operating System, Hypervisor and, if needed, other software such as libvirt. The Cloud Infrastructure Management component is responsible for, among others, tenant management, resources management, inventory, scheduling, and access management.

Now consider the containerisation equivalent, references to "Architecture" in this chapter refer to the Cloud Infrastructure Hardware (e.g. physical resources), Cloud Infrastructure Software (e.g. Hypervisor (optional), Container Runtime, virtual or container Orchestrator(s), Operating System), and infrastructure resources consumed by virtual machines or containers.

The requirements in this section are to be delivered in addition to those in section 2.2, and have been created to support the Principles defined in Chapter 1 of this Reference Architecture.

| Ref # | Category | Sub-category | Description | Specification Reference | Notes and GitHub Issue link |
|---|---|---|---|---|---|
| req.gen.cnt.02 | General | Cloud nativeness | The Architecture **must** support immutable infrastructure. | ra2.ch.017 | Need Kubernetes reference to definition of immutable<br><br>Essentially, configuration is not changed once deployed<br><br>What does this apply to? Workloads?<br><br>Are there test cases for this?<br><br>**OK** |
| req.gen.cnt.03 | General | Cloud nativeness | The Architecture **must** run conformant Kubernetes as defined by the CNCF. | ra2.k8s.001 | **OK** |
| req.gen.cnt.04 | General | Cloud nativeness | The Architecture **must** support clearly defined abstraction layers. | | Seems vague. What does "abstraction layer" mean specifically? Hardware abstraction?<br><br>☑ Rihab Bandayto create GitHub issue and add link<br><br>Link to the GitHub issue: https://github.com/cntt-n/CNTT/issues/2551<br><br>**NO** |
| req.gen.cnt.05 | General | Cloud nativeness | The Architecture **should** support configuration of all components in an automated manner using openly published API definitions. | | |

| | | | | | |
|---|---|---|---|---|---|
| req.gen.scl.01 | General | Scalability | The Architecture **should** support policy driven horizontal auto-scaling of workloads. | | |
| req.gen.rsl.01 | General | Resiliency | The Architecture **must** support resilient Kubernetes components that are required for the continued availability of running workloads. | ra2.k8s.004 | Note: additional detail in link. |
| req.gen.rsl.02 | General | Resiliency | The Architecture **should** support resilient Kubernetes service components that are not subject to `req.gen.rsl.01`. | ra2.k8s.002<br>ra2.k8s.003 | **OK** |
| req.gen.avl.01 | General | Availability | The Architecture **must** provide High Availability for Kubernetes components. | ra2.k8s.002<br>ra2.k8s.003<br>ra2.k8s.004 | **OK** |
| req.gen.ost.01 | General | Openness | The Architecture **should** embrace open-based standards and technologies. | ra2.crt.001<br>ra2.crt.002<br>ra2.ntw.002<br>ra2.ntw.006<br>ra2.ntw.007 | |
| req.inf.com.01 | Infrastructure | Compute | The Architecture **must** provide compute resources for Pods. | ra2.k8s.004 | **OK** |
| req.inf.stg.01 | Infrastructure | Storage | The Architecture **must** support the ability for an operator to choose whether or not to deploy persistent storage for Pods. | ra2.stg.004 | **OK** |
| req.inf.ntw.01 | Infrastructure | Network | The Architecture **must** support network resiliency on the Kubernetes nodes. | | No link for additional detail. What does "network resiliency mean, specifially?". What is the configuration? How many nodes, etc.<br><br>☑ Sandra Jacksoncreate GitHub issue and add link<br><br>☑ https://github.com/cntt-n/CNTT/issues/2547<br><br>**NO** |
| req.inf.ntw.02 | Infrastructure | Network | The Architecture **must** support fully redundant network connectivity to the Kubernetes nodes, leveraging multiple network connections. | | Seems vague. Need more definition. Possibly redundant to HA requirement. No link.<br><br>Pankaj says that there is a reference that provides additional detail (ra2.ch.013 Sect 4.2 of the RA-2 document)<br><br>☑ Emma Foleycreate GitHub issue and add link<br><br>https://github.com/cntt-n/CNTT/issues/2548<br><br>**NO** |
| req.inf.ntw.03 | Infrastructure | Network | The networking solution **should** be able to be centrally administrated and configured. | ra2.ntw.001<br>ra2.ntw.004 | |
| req.inf.ntw.04 | Infrastructure | Network | The Architecture **must** support dual stack IPv4 and IPv6 for Kubernetes workloads. | ra2.ch.007<br>ra2.k8s.010 | **OK** |
| req.inf.ntw.05 | Infrastructure | Network | The Architecture **must** support capabilities for integrating SDN controllers. | | **OK** |
| req.inf.ntw.06 | Infrastructure | Network | The Architecture **must** support more than one networking solution. | ra2.ntw.005<br>ra2.ntw.007 | **OK** |

| | | | | | |
|---|---|---|---|---|---|
| req.inf.ntw.07 | Infrastructure | Network | The Architecture **must** support the ability for an operator to choose whether or not to deploy more than one networking solution. | ra2.ntw.005 | **OK** |
| req.inf.ntw.08 | Infrastructure | Network | The Architecture **must** provide a default network which implements the Kubernetes network model. | ra2.ntw.002 | **OK** |
| req.inf.ntw.09 | Infrastructure | Network | The networking solution **must not** interfere with or cause interference to any interface or network it does not own. | | **OK** |
| req.inf.ntw.10 | Infrastructure | Network | The Architecture **must** support Cluster wide coordination of IP address assignment. | | Need a link with more detail.<br><br>☑ Pankaj Goyalcreate GitHub issue and add link<br>☐ Existing Issue Number 2275 – added question related to this requirement |
| req.inf.ntw.13 | Infrastructure | Network | The platform **must** allow specifying multiple separate IP pools. Tenants are required to select at least one IP pool that is different from the control infrastructure IP pool or other tenant IP pools. | | More specifics are being developed as a PR. Requires an IPAM CNI<br><br>Testability is dependent on API.<br><br>2 step process<br><br>1. Verify existence of the CNI (optional)<br><br>2. Test CNI APIs<br><br>This is ok if there is a common way to test this. OR if the reqs specify a specific implementation.<br><br>If someone brings another CNI, they must also bring sufficient test cases - i.e. test coverage is a requirement for CNIs to be considered for inclusion in RI/to be "Anuket compliant".<br><br>**OK - Once PR is complete.** |
| req.inf.ntw.14 | Infrastructure | Network | The platform **must** allow NATless traffic (i.e. exposing the pod IP address directly to the outside), allowing source and destination IP addresses to be preserved in the traffic headers from workloads to external networks. This is needed e.g. for signaling applications, using SIP and Diameter protocols. | ra2.ntw.011 | ☐ To Do: Verify for next Session<br><br>Cedric to verify and Update this cell. |
| req.inf.vir.01 | Infrastructure | Virtual Infrastructure | The Architecture **must** support the capability for Containers to consume infrastructure resources abstracted by Host Operating Systems that are running within a virtual machine. | ra2.ch.005<br>ra2.ch.011 | **OK** |
| req.inf.phy.01 | Infrastructure | Physical Infrastructure | The Architecture **must** support the capability for Containers to consume infrastructure resources abstracted by Host Operating Systems that are running within a physical server. | | Bare metal<br><br>☐ Issue: add the Ref to the Table: ra2.ch.008 in (Assignment Pankaj Goyal )<br><br>Opened an Issue # 2557 and PR #2561 for the missing spec for "Bare Metal" add ra2.ch.008 spec to the reqt<br><br>Per Specification: The physical machines on which the Kubernetes Nodes run must be equipped with at least 2 physical sockets, each of at least 20 CPU cores. |

| | | | | | |
|---|---|---|---|---|---|
| req.kcm.gen.01 | Kubernetes Cluster | General | The Architecture **must** support policy driven horizontal auto-scaling of Kubernetes Cluster. | | ☑ Issue: missing requirement: Rihab Banday assigned<br><br>Link to the GitHub issue - https://github.com/cntt-n/CNTT/issues/2563 |
| req.kcm.gen.02 | Kubernetes Cluster | General | The Architecture **must** enable workload resiliency. | ra2.k8s.004 | 2 Votes OK<br><br>**OK** |
| req.int.api.01 | API | General | The Architecture **must** leverage the Kubernetes APIs to discover and declaratively manage compute (virtual and bare metal resources), network, and storage. | For Networking:<br>• ra2.ntw.001<br>• ra2.ntw.008<br>• ra2.app.006<br><br>Compute /storage not yet met. | An Issue is already opened regarding defining/listing Storage types<br><br>Active PR being worked/not yet approved (2480)<br><br>John Hartley is working on RM storage Spec and will then work RA1/RA2 |
| req.int.api.02 | API | General | The Architecture **must** support the usage of a Kubernetes Application package manager using the Kubernetes API, like Helm v3. | ra2.pkg.001 | Already part of RC-2 in Functest VIMS<br><br>**1 line change will be incorporate in RC-2 if the test cases is not disruptive /destructive.**<br><br>**OK** |
| req.int.api.03 | API | General | The Architecture **must** support stable features in its APIs. | | Not Testable.<br><br>Need to specific a set of stable features/APIs and define what stable means for each API /Feature<br><br>**Consider Removal** |
| req.int.api.03 | API | General | The Architecture **must** support limited backward compatibility in its APIs. Support for the whole API must not be dropped, but the schema or other details can change. | | Requirement needs to be rewritten. Vague. May be what K8s would have developed as part of their goals.<br><br>This is a requirement for the projects.<br><br>if is a default for K8s why are we specifying it in Anuket.<br><br>Need a broader audience for context.<br><br>Next session? |

Depends on Definition of Wrkld Rel