

Topics related to Cloud Computing - Standards

G.Narendra Nath

DDG(Security)

Dept. of Telecom, Govt. of India

Generic Requirements for Cloud Infrastructure (TEC/GR/IT/CLI-001/01/OCT-12)

- Functional Requirements for Cloud Infrastructure for Organizations
- Quality Requirements
- EMI/EMC Requirements
- Safety Requirements
- Security Requirements
- Other mandatory Requirements
- Desirable Requirements (Optional Specifications for Cloud Infrastructure for Organizations)

Functional Requirements for Cloud Infrastructure for Organizations

- General Framework of Cloud Infrastructure
- Functional Requirements for Computing Capability
 - CPU Virtualization
 - Memory virtualization
 - I/O device virtualization
 - Virtual machine Duplication and Migration
 - Multi-tenancy/User self-service

Functional Requirements for Cloud Infrastructure for Organizations

- Functional requirements for the cloud network
- Functional Requirements and Architecture for Storage Capability
- Requirements for Resource Management
- Cross Layer Functions

Requirements for Resource Management

- Functional Requirements for Resource Management
 - Resource encapsulation
 - Resource orchestration and provisioning
 - Assets management
 - Template management
 - Cloud service monitoring
 - Health monitoring
 - Performance monitoring
 - Capacity monitoring
 - Security and compliance monitoring
 - Monitoring and metering for charging and billing
 - Application and service monitoring
 - User resource environment management

- Cross Layer Functions
 - Cloud Operations Management
 - Cloud Performance Functions
 - Security and Privacy

Other Mandatory Requirements

- Engineering Requirements
- Operational Requirement
- Other Requirements
- Documentation
 - System description documents
 - System operation documents
 - Training Documents
 - Repair Manual
- Installation
- Software Maintenance

Other Mandatory Requirements

- Hardware and software requirement for the components of cloud infrastructure
 - Power Supply
 - Software Requirement
 - Man Machine Communication

Desirable Requirements

- Functional Requirements
 - Business Service Management Module
 - Dependency Discovery and Impact Analysis Module
 - IT service Management and IT asset Management
 - Monitoring and Event Management
 - Server and Application Monitoring
 - Network Monitoring System
 - Fault Management System

Desirable Requirements

- Hypervisor (Virtualization layer) Details
 - X86-64 architecture based Hypervisor (Virtualization Layer) Details
 - Unix (RISC) based Hypervisor (Virtualization Layer) Details
- Network Provisioning
- Cloud Service Automation

Security Requirements

- The cloud infrastructure shall have Security Administration and management function for administering security policies and managing security related information. These features shall be provided by NMS/EMS, if not indicated otherwise.

Security Requirements

- CSP should provide VPN/firewall security while the host/service specific authentication is controlled by the enterprise.
- CSP should provide 2-factor authentication to CSUs using SSH, HTTP or other procedures.
- CSP should associate the user's IP address with their enterprise identity which may need to be propagated to cloud entities that will enable the service.
- The CSP must integrate with security and privacy solutions.

Security Requirements

- CSP should provide or establish for security audit/certification by a third party and shall implement his own security policy by integrating the user security policy.
- Hypervisor used shall offer criteria to ensure protection for itself and hosted VMs, e.g. by moving antivirus and anti-spam processing from VM to hypervisor. This feature is relevant for X86 platforms, not for UNIX.
- VMs should be well isolated while sharing memory, CPU and storage capacity.

Security Requirements

- CSP should ensure the logical isolation of its storage systems without any constraint on the adopted solution.
- CSP should have flexible and strong network protection providing end to end logically secure domain for multiple tenants for dynamically sharing the same network infrastructure and ensuring both performance and QoS.
- The cloud system shall remain available to a user even in catastrophic situations and shall have the capability to recover to a safe mode.
- Service provider shall provide location of the data including tracing of the data to ascertain its source as per Government guidelines.

Security Requirements

- System should have capability for secure VM migration.
- CSP should encrypt data mandatorily at rest and optionally in transit.
- CSP should harden the VM so that exposure to attacks on the virtualization layer is minimized. This is an optional requirement.
- CSP shall also provision special virtual environments with a physical separation for cloud service users with special security requirements.
- As far as possible, CSP should implement the guidelines given by Cloud Security Alliance (CSA).

Security Requirements

- CSP shall make available the evidence of compliance with regional laws and regulations as per the applicable government guidelines prevailing from time to time.

Thank You