LGC IaaS Operational Model

What is LGC IaaS ?

Infrastructure as a Service, commonly referred to as simply “IaaS,” is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, IaaS enables end users to scale and shrink resources on an as-needed basis, reducing the need for high, up-front capital expenditures or unnecessary “owned” infrastructure, especially in the case of “spiky” workloads.

LGC IaaS Platform and Architecture

LGC IaaS is made up of a collection of physical and virtualized resources that provide consumers with the basic building blocks needed to run applications and workloads in the LGC.

Physical data centers: LGC/ICTA co-located LGC on data centers that contain the physical machines required to power the various layers of abstraction on top of them and that are made available to end users over the LGC web console. In LGC IaaS models, end users do not interact directly with the physical infrastructure, but it is provided as a service to them.

Compute: IaaS is typically understood as virtualized compute resources, LGC manages the hypervisors and end users can then programmatically provision virtual “instances” with desired amounts of compute , memory and storage. LGC Cloud computer is planned to enable supporting services like auto scaling and load balancing that provide the scale and performance characteristics that make cloud desirable in the first place.

Network: Networking in the LGC is a form of Software Defined Networking in which traditional networking hardware, such as routers and switches, are made available programmatically, typically through APIs.

Storage: The primary types of cloud storage, block storage, and object storage are available on LGC. LGC block storage has multiple performance tiers , general tier to expansive tiers. Object storage has thus become the most common mode of storage in the cloud given that it is highly distributed (and thus resilient), it leverages commodity hardware, data can be accessed easily over HTTP, and scale is not only essentially limitless but performance scales linearly as the cluster grows.

LGC enables tenant consumers to have a private network or multiple private networks on the tenant and among multiple tenants. LGC provides control of subnet creation, IP address range selection, virtual firewalls, security groups, network ACLs, SSL VPN, load balancing and Web Application Firewall(WAF) service.

LGC IaaS Shared Responsibility Schematic

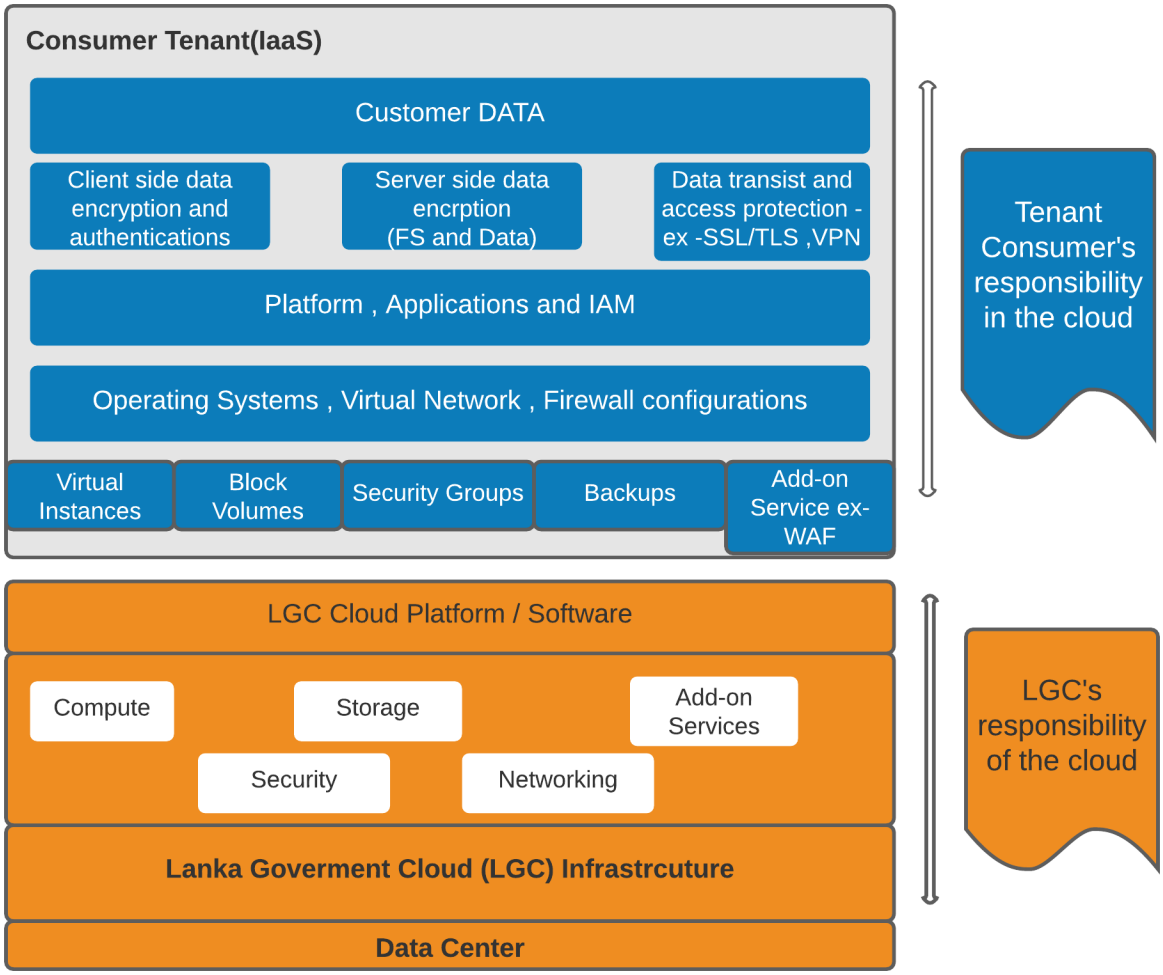

Figure1 : LGC IaaS Shared Responsibility schematic

How LGC IaaS security responsibilities divided

1. **Security of the cloud** = everything the Cloud provider does, including:

    a. Securing LGC infrastructure, including physical access to data center facilities where your IT resources are housed

    b. Protecting the physical networking, compute, and storage resources, so you don't have to worry about setting up servers or storage hardware, patching firmware, or installing and properly disposing of drives, etc.

    c. Securing Hypervisors and underlying technology stack that host and manage consumers VMs running on cloud infrastructure

2. **Security in the cloud** = everything Consumers responsible for, including:

    a. Securing and guarding data generated or collected by your applications

    b. Maintaining secure operating system, virtual network, and virtual firewall configurations ,
        i. Security updates and patching for system software, middleware and tools
        ii. System updates and maintenance for system software, middleware and tools

    c. Identifying and accessing control mechanisms tied to any platforms or applications you manage
        i. System administration security models, best practices, professionalism and ethics
        ii. Ensuring the use of non-super user account with just the right amount of privileges to deploy applications, manage applications, manage databases and file systems

    d. Protecting information by ensuring data integrity, using encryption, and properly using identity management technologies

    e. Code security - Fix issues highlighted by static code analyzer

    f. API security - API should be secured using standard API security mechanism

    g. Application security -

    h. Security Audit -

i. Scan - Throughout the development lifecycle, prior to final production deployment and regular post production intervals security audit of the deployed system should be carried out with the help of recognized security certifying body such as Sri Lanka CERT

ii. Penetration Testing : Periodic pen-testing should be carried out for applications

i. Security of backups (Details in below section)

Backup and Disaster Recovery

IaaS Tenant Consumer's(Customer) responsibility to implement backup and recovery strategy for hosting applications/systems, Consumer may consider following aspects ,

- ☐ What data or systems should be backed up
- ☐ Where the backup should be located – offsite, or in the cloud
- ☐ When and how often data or systems should be backed up. Data with no paper record must be backed up more frequently, while data that changes infrequently or is easily created can be backed up less frequently.
- ☐ How the backup files will be protected. For example, and do only authorized users have access?
- ☐ How long the backup files will be kept. For critical backups, you might want an additional copy maintained offsite to protect the data in the event of a disaster or ransomware.

LGC IaaS Operational Scope

- LGC IaaS Provider DO NOT have

  - Access to instances and volumes
  - Access to the operating system
  - Access to the file system
  - Access to the databases

    - Access to the application software

- In case of a system crash, LGC can
    - Help restore the instances if consumer has working backup of instance or volume
    - But not the operating system, files, databases or software

- In case tenant consumer want to restore
    - Bit stream of instance– needs to be done by the consumer using the operating system access
    - File system – needs to be done by the consumer using the operating system access

- How to restore a crashed software system in IaaS
    - Consumer needs to restore access to the machine instance
    - Get into the operating system
    - Use the operating system utilities and other tools to restore
    -
    - Or restore entire instance from previously backuped snapshot

- How to get a replica of a system in question
    - We can allocate a tenant space
    - Consumer will have to instantiate instances and transfer files / data and software needed

Backup and Recovery References

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_backup.html
https://sao.wa.gov/wp-content/uploads/2020/06/Backup_Recovery_Best-Practices_Leadership_Planning_6_5_20.pdf

https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en
https://www.iso.org/obp/ui/#iso:std:iso-iec:24762:ed-1:v1:en