GETTING STARTED GUIDE

ALCATEL-LUCENT RAINBOW™

Rainbow Edge

TECHNICAL OVERVIEW Ed 08

DECEMBER 2021

Author: Operations - Cloud Services

Alcatel·Lucent Enterprise

Disclaimer

This documentation is provided for reference purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this documentation is provided “as is” without any warranty whatsoever and to the maximum extent permitted.

In the interest of continued product development, ALE International reserves the right to make improvements to this document and the products it describes at any time without notice or obligation.

Copyright

Contents

Glossary

ALE: Alcatel-Lucent Enterprise

CPE: Customer Premises Equipment

DC: Data Center

DMZ: Demilitarized Zone

FQDN: Fully Qualified Domain Name

GK: GateKeeper

HA: High-Availability

MPLS: Multiprotocol Label Switching

NAT: Network Address Translation

PBX: Private Branch Exchange

PoP: Point of Presence

QoS: Quality of Service

RTT: Round Time Trip

(S)DRS: (Storage) Distributed Resource Scheduler

SLA: Service Level Agreement

SSL: Secure Sockets Layer

TURN: Traversal Using Relays around NAT – RFC 5766

VPN: Virtual Private Network

1 History

Modifications	Date	Edition
Light version of the Edge Technical Overview	22/12/2021	ED08
Add Alfred, Kafka, Zookeeper and datalake, VIP for Gatekeeper, Local Git, Debian repo and NOC instance. Delete Connected Edge option	24/06/2021	ED07
Clarify the hardware footprint selection in a dedicated chapter.	20/08/2020	Ed 06
World map update (new ANZ region) and Swift requirement for standalone low-scale deployments.	30/06/2020	Ed 05
Renamed “Rainbow Spot” to “Rainbow Edge”. Added extra section related to extra “Rainbow Voice” features.	12/03/2020	Ed 04
Cosmetic changes, note related to Rainbow Voices features not being part of the Rainbow Edge scope.	13/02/2020	Ed 03
Reviewed, Extended Introduction, Smart Hands, Mail Server, Debian OS	10/02/2020	Ed 02
Initial Revision	04/02/2020	Ed 01

2 Introduction

This guide provides some technical overview of Rainbow Edge solution, detailed architecture will be shared under Non-Disclosure Agreement (NDA).

It aims to provide various inputs on what is Edge offer, summarize the global architecture, infrastructure and underlying network environments to be put in place.

Before moving forward with Rainbow Edge, Rainbow Public multi-tenant cloud service should be considered. The shared technology offers a secure solution while benefiting from a very competitive total cost of ownership.

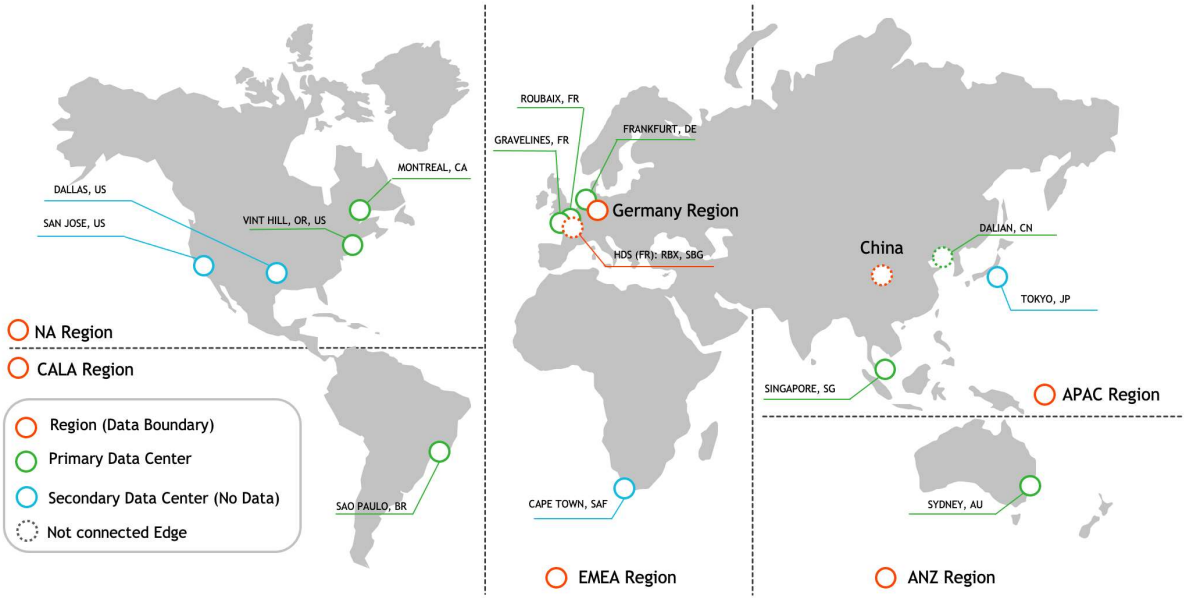
Rainbow manages several visibility profiles. See the complete description here https://support.openrainbow.com/hc/en-us/articles/115001397924-How-to-Change-the-Visibility-of-My-Company- . With an "isolated" company the End Customer can get a fully protected environment. And he could decide if certain selected employees could be connected to the open world.

3 Overview

Alcatel-Lucent Enterprise (ALE) is offering Alcatel-Lucent Rainbow, an overlay cloud service operated by ALE. Rainbow offers contact management, presence, persistent messaging, audio/video, screen and file sharing, API openness to integrate with End Customer business applications, hybrid communication with existing customer PBXs.

Rainbow is a global Cloud services available in many countries with hardened methods implemented to ensure data privacy and geographical data isolation and segregation. For specific use cases, Rainbow features an extended variant called “Rainbow Edge”, allowing for Rainbow services and data to be hosted in a customer-based or partner-based datacenter.

Rainbow Public is a global UCaaS and CPaaS Services, sustained by datacenters in multiple regions around the globe, as described in the diagram below. Rainbow Public is updated every few weeks to increase customer experience without concessions to reliability.



Doing so, Rainbow guarantees:

- Performances to end users, ensuring high availability and scalability as close as possible from its users, as to minimize global latency.
- Data privacy and data geographical isolation, ensuring that user data are stored in the region of users’ belonging and not replicated globally.

4 Related Documents

- Rainbow – Solution Brief – Infrastructure Abstract
- Rainbow – Solution Brief – Security Abstract
- Rainbow - Network Requirements

5 Rainbow Edge Variant

For specific use cases, Rainbow Edge Extensions can be offered to provide more data isolation. **Rainbow Standalone Edge**, a partner or customer hosted datacenter, operated by ALE, offering private on-premises data storage and standalone applicative infrastructure.

	Region/Country Local DC	Standalone Edge
Rainbow Relationship Engine & Services	Global	Restricted to partner's scope
Coverage (Perfs, Latency, Mobility)	Global Worldwide	Edge-Local Only Access
Runtime Operations	ALE 24x7x365	ALE 24x7x365
Availability	HA, Guaranteed by ALE	Limited, Shared with Partner
Infrastructure Resources	Mutualized	Dedicated
Access, Security, Logs	Mutualized	Dedicated
Data Location	Region-Bound	Edge-Bound
Data Storage	Mutualized / Segregated	Dedicated / Private
Infrastructure & Network Costs	ALE Mutualized	Partner-Supported (>TCO)

Standalone Edge will provide customers with a private Cloud Rainbow instances (with or without public Internet connectivity) with no possible interaction with the global Rainbow network.

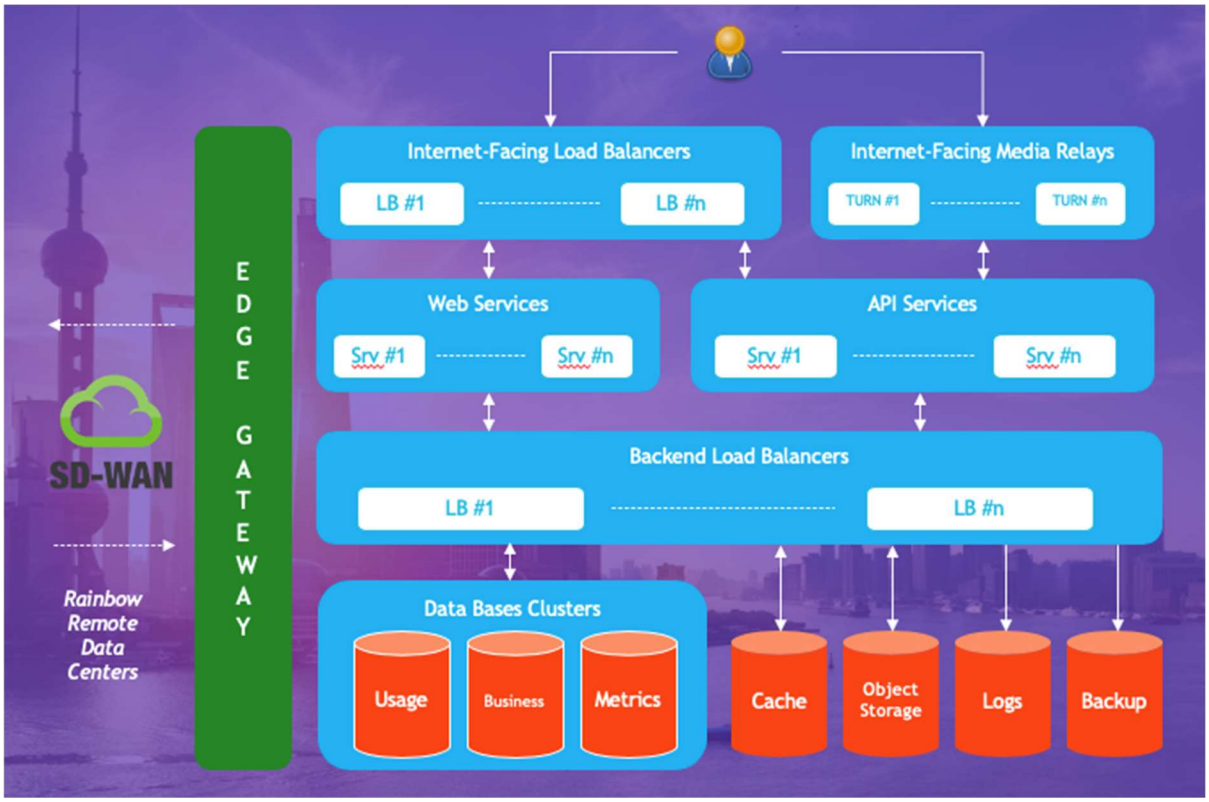
The underlying infrastructure will be selected and provided by the customer, who will be in charge of its well behavior. Both the network and application setup, upgrades rollout and day to day runtime operations will remain held by ALE Cloud Operations team.

Please bear in mind that at least partial Internet connectivity is required by ALE Operations team to handle 24x7x365 support. Shall the Internet connection be not permanent, it will impact the SLA of the Operation Service.

6 Rainbow Edge Global Architecture

6.1 Highly Available Infrastructure

Rainbow internal datacenter's architecture comes with a generic "Frontend / Backend / Data" architecture, with infinite horizontal and vertical scalability and high availability, as described in the diagram below:



Various kind of databases co-exist as to handle infrastructure metrics (used for monitoring and serviceability), object storage (for file transfer features), logs (for application debugging and/or legal compliance) and backup (for resilience).

Note that regardless of the data type and underlying storage technology, all data are encrypted at rest using AES256 mechanisms.

6.2 GateKeeper Edge Gateway

The GateKeeper (GK) component acts as Rainbow datacenters' edge gateway. It's a full software-based network equipment that provides the following features:

- Local (Edge) VLANs manager
- Local (Edge) router
- Local (Edge) firewall
- Local (Edge) DHCP / DNS server
- Local (Edge) software packages repository / mirror.
- Local (Edge) backup
- Global SD-WAN like encrypted VPN tunnel for remote GK mesh and connectivity.

As stated, the GateKeeper components provides the basic networking services to all software components within the Edge.

It also provides network connectivity to Rainbow NOC platform through a WireGuard-based secure tunnel.

In the Rainbow Standalone Edge configuration, the sole usage of the tunnel will be to provide connectivity to remote operation tools and will require a limited bandwidth.

Network requirements and recommendation are to:

- Allow unrestricted outbound traffic to the Internet (to allow NTP / DHCP Relay / Packages Mirroring … to work)
- Block everything but WireGuard for inbound traffic from the Internet (UDP port to be chosen).

It is strongly advised to have GateKeeper redounded (as any other parts of the application are) as to ensure connectivity in case of failure.

For performances, QoS, quality and security reasons, GateKeeper inter-connected can be achieved through public Internet routing (default) or private segments (dedicated MPLS, mutualized or dedicated cross-connections through various PoPs like Equinix / Megaport …).

6.3 Software Licenses

Rainbow service is made out of multiple Open Source software and ALE proprietary applications. It does not involve any third-party software requiring any proprietary license to be purchased.

All servers make use of Debian GNU/Linux stable distribution as their native operating system.

The customer use of proprietary software solution for infrastructure hosting (e.g. VMware …) is however subject to license and is the sole responsibility of the customer.

7 Rainbow Edge Requirements

7.1 Generic Hardware Requirements

Rainbow services are hardware-agnostic and can be deployed on multiple IaaS providers:

- Bare Metal servers
- Virtual Machines on VMware vSphere
- Virtual Machines on Linux KVM
- Other environment (feasibility study might be required)

As a rule of thumb, it is recommended for high-availability considerations to use (when technically and financially possible) two to three geographically distinct datacenters, yet inter-connected, and deploy the various servers' instances on each datacenter. When considering such an option, services are deployed in an active-active state, meaning that both datacenters will be actively used (by opposition to active-passive scenarios) and resources usage should not exceed half of the processing capabilities as to cope with failover mechanisms and high load.

The IaaS selection is bound to the customer and can even be a mix of both technologies providing that network requirements are met. The customer is responsible from the IaaS infrastructure, both from setup and runtime phases and must deal with any issues related to hardware or network layers.

Should the customer opt for virtualization technology, ALE recommends the following to be put in place. This relates to VMware's terminology, but equivalent exists for other providers:

- Virtual Machines should run on modern hypervisors (minimum recommended is vSphere 6.5)
- VM and Storage High-Availability should be provided by vSphere DRS / SDRS technology.
- ALE recommends running at least 2 ESX hypervisors for High-Availability DRS support
- ALE recommends using distinct datastores: "standard-perf" and "high-perf" ones, with High-Availability SDRS support.
- Low-Level (Physical resources, i.e. hardware, disks, network connectivity, Internet bandwidth, power …) fully managed by Customer.

7.2 Generic Network Requirements

As for hardware requirements, Rainbow Edges come with some network specific requirements (or at least recommendations), namely:

- Should the customer host the service on multiple distinct datacenters, it is mandatory that the DCs share the same L2 segment for the different services to be part of the same private network and VLAN.
- Should the customer host the service on multiple distinct datacenters, it is mandatory that the round time trip (RTT) between the different DCs never goes above 5ms.

- ALE requires private -LAN addressing usually on 10.20/24 subnet (might be accommodated according Customer context).
- Customer has to provide public IPv4 on WAN (Internet facing) and WAN connectivity to the various servers. It is highly recommended that WAN IPv4 addresses are directly associated to the various servers and not mapped through NAT.
- When Internet-facing services are expected, it is recommended to have a /28 subnet (16 IPs).
- All servers are expected to provide at least 1 Gbps NICs. For servers requiring both LAN and WAN network access, it is highly recommended that 2 distinct NICs are being used.
- For large scale deployments, when a complete service redundancy and clustering support is expected, it is recommended that data hosting services (databases, object storage, logs and backups) feature a 10 Gbps NIC on LAN. While not being mandatory, it is highly recommended in case of hardware failure, to allow service restoration as fast as possible.

7.3 Operational Requirements

Due to the nature of Edges, service operations will feature a split responsibility:

- Customer will remain in charge of the functional state of the underlying infrastructure (hardware or virtual environments well-being) and associated network (both LAN/WAN) connectivity. ALE's contractual SLA won't apply if the root cause is verified to be low-level infrastructure related. See section 7.5 ("Smart Hands") for additional details.

- ALE will remain in charge of Rainbow back-end components (virtual machines, OS, network configuration, applications, monitoring …). This will be fully managed by ALE. As to manage and reach our commitments, no logical access to the servers will be authorized to customer's or partner's IT staff, as to prevent any possible failure cause due to external interaction with Rainbow core services.

- Note that due to the complex nature of the Rainbow Edge, ALE provides a 24x7x365 Operational support and coverage. The Operation service SLA is linked to a permanent remote access to the Edge platform. In case the remote access is only established on demand, this make the monitoring of the platform not be part of the provided Operation service.

7.4 Hardware Footprint

Rainbow Edges hardware requirements are highly dependent on:

- The expected volume of users (total and concurrent)
- The expected scalability and redundancy, being mono DC or multi DC

That being said, various software components and services are either required, optional or disabled depending on the chosen configuration. Please refer to chapter related to hardware footprint for details.

7.5 Local “Smart Hands”

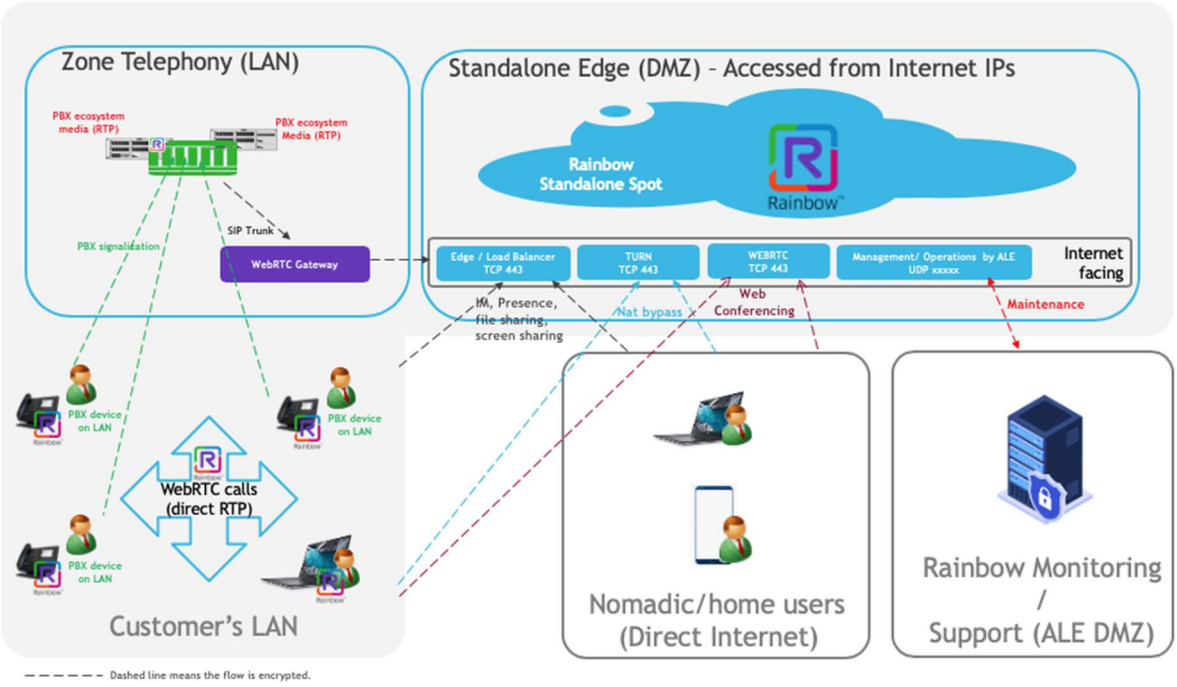
Due to the shared service responsibility (partner providing infrastructure vs. ALE providing over the top service), ALE Operations team require local “Smart Hands” from partner. “Smart Hands” are an around-the-clock, on-site, operational support service for remote management, installation and troubleshooting of the data center’s equipment. This is absolutely key for ALE Ops team to be able to maintain the global expected SLA.

8 Standalone Edge

8.1 Network Topology

A Rainbow “Standalone Edge” is meant to provide customer with a completely isolated Rainbow service instance, with data storage within customers premises as well as application servers. It can be seen as private Cloud service, dedicated to customer with no possible interaction with the global Rainbow network.

The standalone Edge still behaves like a Cloud service, being accessible from public Internet, allowing user connection from both enterprise LAN and public Internet. Should the service be bound to enterprise’s LAN only, it will require the various nomadic/home users (desktop or mobile) to always connect to enterprise’s corporate network first, through a dedicated VPN. This is customer’s responsibility and out of the scope of this document.



8.2 Network Requirements

Rainbow “Standalone Edge” is still considered as Cloud service; yet being private to customer. This allows nomadic/home users to reach their private Cloud service from virtually anywhere.

The direct consequences of this private Cloud are:

- The Edge will be Internet-facing. Servers parts of the customer’s DMZ will then have services exposed to Internet and will potentially be subjects to network threats. ALE Cloud Operations team has developed all the necessary toolkits that ensure the global security of the infrastructure. The network requirements exposed in the

"Rainbow Network Requirements" document then need to be addressed, but from an inbound perspective (server-side instead of client-side).

- The Edge will be made available through its very own DNS and FQDN. Global Rainbow platform is accessible through openrainbow.com (and its associated subdomains). Customer will be requested by ALE to provide a domain for its service. It can be a standalone dedicated domain (e.g. customer-brand-new-service.com) or part of an existing corporate domain (e.g. service.customer-brand.com, where customer-brand.com is the customer's existing domain name). Be aware that ALE will not be held responsible for any legal copyright infringement associated with the selected domain and will be the sole responsibility of the customer. The requirement for ALE Cloud operations team is to be able to administrate the public DNS accordingly. ALE Ops team can either:
    - Provide the customer with the necessary technical information.
    - Buy and manage the domain for the customer.
    - Let the customer buy the domain and do the technical administration part.
- The Edge being publicly available over the Internet with its new unique domain name, it is up to the customer to provide associated SSL certificates to ensure encrypted traffic. Rainbow uses wildcard SSL certificates, signed by recognized Certificate of Authority using SHA256. ALE Ops can either:
    - Provide the customer with the necessary technical information and install the provided certificates back in return.
    - Buy and manage the certificates for the customer (transaction will still require domain owner's approval)
- In order to seamless connect the end users to the Edge environment using Rainbow official mobile applications, the partner should either:
    - Use an MDM service to configure each mobile app to use specific edge
    - Allow the mobile applications to connect to Rainbow Public: Edge location API, ie allow access to openrainbow.com on each mobile

8.3 Hardware Footprint (Small Scale Deployments)

Small scale deployments (500-1000 concurrent users, 5000 registered users) may not require a full blown highly available and scalable infrastructure. Most of Rainbow services can then be mutualized within one single server instance codenamed AiO (All-In-One), where HA is covered through infrastructure's virtualization capabilities. Please refer to "Hardware footprint" chapter for exhaustive hardware footprint requirements.

8.4 Hardware Footprint (Large Scale Deployments)

For large scale deployments (more than 1000 concurrent users, 5000 registered), expected to scale up, for multi DC load balancing, for redundancy at application layer, a more exhaustive infrastructure is foreseen, as to allow further seamless scalability and benefit of the nature of the native Rainbow cloud architecture.

8.5 Mail Server

Please note that in case of standalone Edge, Rainbow will require a valid SMTP server to be used to send email notification, passwords recovery and so on. Different possibilities are offered:

- Using company's corporate mailing services if available
- Using external mail service provided by partner.
- Extending the Rainbow standalone infrastructure with a couple of instances, secured and dedicated to send emails using the appropriate Edge's domain (recommended scenario).

8.6 Backup

Please note that in case of standalone Edge, Rainbow operations team enforces the usage of an external secondary backup solution out of the primary datacenter premises/location.

9 Hardware Footprint

Option 1 : Large scale requirement, multi-DC architecture, redundancy handled natively at Rainbow application layer

		Technical Characteristics (per server)								
	Name	Qty	HA	CPU	Memory	Disk		Network		Standalone
		#VMs	Mode	vCPUs	Size (GB)	Size (GB)	IOPS	NIC type	#IPv4	Large
Rainbow Base / Tools	Edge GW	2	M/S	2	2	64	Standard	WAN	1	Y
						256	Standard	LAN	1+ VIP	
	Logs	1	*	4	32	1024+	Premium	LAN	1	Y
	Backup	1	*	1	2	64	Standard	LAN	1	Y
						2048+	Standard			
	Metrics & Monitoring	1	*	2	4	64	Standard	LAN	1	Y
						512	Standard			
	Datalake	1	*	1	4	64	Standard	LAN	1	option
	Admin message bus	1	*	2	8	64	Standard	LAN	1	option
	Repository + NOC	1	*	2	4	256	Standard	LAN	1	option
	Mailer	1	*	1	1	64	Standard	LAN	1 +VIP	option
								WAN	1	
Rainbow Core	Core Server	2	M/S	4	16	64	Standard	LAN	1	Y
	Messages DB	2	M/S	4	64	64	Standard	LAN	1	Y
						256+	Premium			
						256+	Premium			
	Business DB	3	M/S	4	64	64	Standard	LAN	1	Y
						256+	Premium			

						256+	Premium			
	Private Load Balancer	2	M/M	4	4	64	Standard	LAN	1+2VIP	Y
	Public Load Balancer	2	M/M	4	4	64	Standard	LAN	1	Y
								WAN	2	
	Files Storage	3	M/M	6	16	64	Standard	LAN	1	Y
						1024+	Standard			
						1024+	Standard			
						1024+	Standard			
	WebRTC STUN/TURN	2	M/M	1	4	64	Standard	LAN	1	Y
								WAN	1	
	WebRTC Conferencing*	2	M/M	8	8	64	Standard	LAN	1	Y
								WAN	1	
	API Server	2	M/M	4	16	64	Standard	LAN	1	Y
	Cloud PBX Gateway	2	M/M	4	4	128	Standard	LAN	1	Y

Rainbow Core Services

These are the minimum footprint requirements that can accommodate up to:

- 20k active users
- 100k registered users
- WebRTC Conferencing VMs requirements are related to the number of simultaneous users in conference, according the expected traffic additional servers might be required
- usable for multi DC deployment
- redundancy at application layer (machine sizing need to be reconsidered in case one site need to support 100% of the traffic)

note :

- M stands for Master (or Primary)
- S stands for Slave (or Secondary)
- VIP stands for “Virtual IP”, a floating IP shared through VRPP.
- “+” sign indicates a minimum value, that may need to grow over time and usage.

Option 2 : Small scale requirement, mono DC, fix sizing (no scale up, maxi 1000 active users), redundancy handle at virtualization layer (limited)

		Technical Characteristics (per server)								
	Name	Qty	HA	CPU	Memory	Disk		Network		Standalone
		#VMs	Mode	vCPUs	Size (GB)	Size (GB)	IOPS	NIC type	#IPv4	Small
Rainbow Base / Tools	Edge GW	2	M/S	2	2	64	Standard	WAN	1	Y
						256	Standard	LAN	1+ VIP	
	Logs	1	*	4	32	1024+	Premium	LAN	1	Y
	Backup	1	*	1	2	64	Standard	LAN	1	Y
						2048+	Standard			
	Metrics & Monitoring	1	*	2	4	64	Standard	LAN	1	Y
						512	Standard			
	Datalake	1	*	1	4	64	Standard	LAN	1	option
	Admin message bus	1	*	2	8	64	Standard	LAN	1	option
	Repository + NOC	1	*	2	4	256	Standard	LAN	1	option
	Mailer	1	*	1	1	64	Standard	LAN	1 +VIP	option
								WAN	1	
Rainbow Core	All-in-One	1	*	8	32	64	Standard	LAN	1	Y
						512+	Premium	WAN	2	
						512+	Premium			
	SWIFT Object Storage	3	M/M	6	16	64	Standard	LAN	1	*1 only
						1024+	Standard			
						1024+	Standard			
						1024+	Standard			
	WebRTC STUN/TURN	2*	M/M	1	4	64	Standard	LAN	1	*1 only

								WAN	1	
	WebRTC Conferencing*	2*	M/M	8	8	64	Standard	LAN	1	*1 only
								WAN	1	

Rainbow Core Services

These are the minimum footprint requirements that can accommodate up to :

- 1k active users
- 5k registered users.
- WebRTC Conferencing VMs requirements are related to the number of simultaneous users in conference, according the expected traffic additional servers might be required
- not relevant for multi DC split (refer to option 1 for this architecture requirement).
- redundancy handle at virtualisation layer (Vmware HA for instance).

note :

- M stands for Master (or Primary)
- S stands for Slave (or Secondary)
- VIP stands for “Virtual IP”, a floating IP shared through VRPP.
- “+” sign indicates a minimum value, that may need to grow over time and usage.

9.1 Rainbow Core Services

It is important to note that these requirements are likely to scale up, should time go on (and so will the usage), or user base grow.

Going above this footprint is possible and recommended as to increase performances or “be ready for the future”.

Should the usage scale up, so will the required footprint. Rainbow core services have been designed to scale up both horizontally and vertically, making things easier for upgrades. As a rule of thumb, it is recommended to double up the footprint for every 20k active users (100-200k registers users). The most adequate scale up strategy (horizontal / vertical) is to be discussed between customer and ALE Cloud Operations.

End of Document