# SAP CP @ Alibaba Cloud

Nicole Zhou, SAP
04/11, 2019

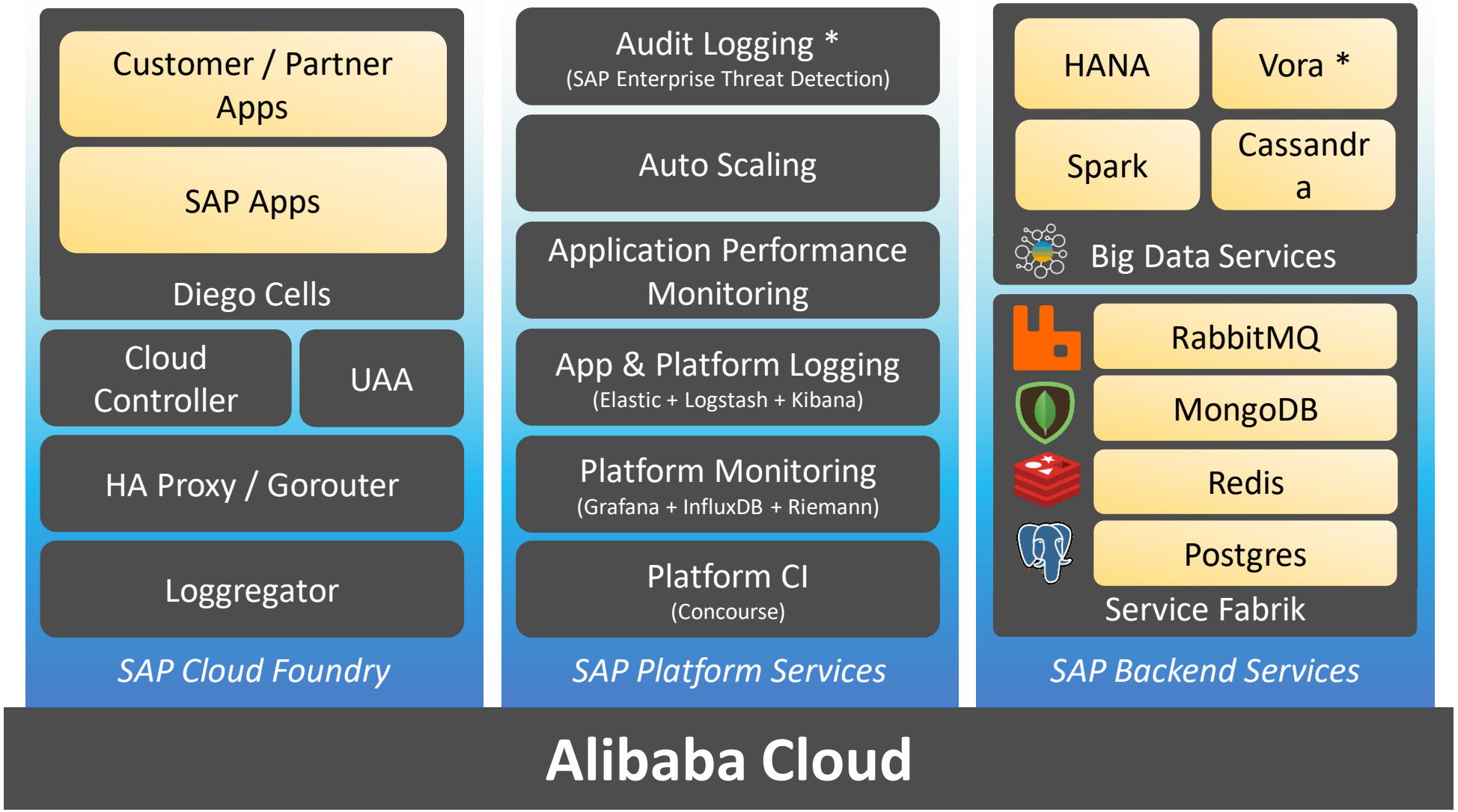
# Agenda

- Alicloud Overview
- China Deployment
- SCP Components

# Alicloud Overview

# SAP Cloud Platform

* - Work in progress/future



# VM Types - High-Level Overview

- Alibaba Cloud ECS and Amazon EC2 employ the same method to categorize VM instances by specifications and types, but the categorization differs in terms of CPU, memory, storage performance, and network capability.
- Each family is composed of different instance types.

| Target | Scenario | Alicloud |
|---|---|---|
| Entry level | General type | t5 |
| Enterprise level | General type | g5 |
| | Computing instance | c5 |
| | High-frequency computing instance | c4, cm4, ce4, hfc5 |
| | Memory instance | r5, re4 |
| | | se1 |
| | Big data | d1, d1ne |
| | Local SSD | i1, i2 |
| | High capability packet forwarding | sn1ne, sn2ne, se1ne |
| | GPU visualization | ga1 |
| | GPU computing | gn4, gn5 |
| | FPGA | f1, f2 |

# VM Types - Definitions

- The VM resources offered in Alibaba Cloud are not equally available in all regions. Some resources are available in some regions and not available in other regions.

- In addition, even within the same region the resources might not be available in all availability zones.

- To enable SAP CP deployment on Alibaba Cloud, the set of VM types is defined per deployment region.

# Instance Images

- Instance image refers to the running environment template for virtual machine instances.
- To create a VM instance the image should be specified to provide base operation system environment.
- Alibaba Cloud has 4 types of images available:
  – Public images (officially templates)
  – Marketplace images (provided by third-party), the OS may come with preinstalled services of software.
  – User-shared images
  – Custom images
- Alibaba Cloud instance images are a regional resource. To use the image in another region, it should first be replicated.

# Disk Types

- Alibaba Cloud provides several types of disk storage that can be attached to a VM.

| Category | Alicloud |
| --- | --- |
| Basic | Basic Cloud Disk |
| Intermediate | Ultra Cloud Disk |
| I/O Optimized * | SSD Cloud Disk |

- Additionally, Alibaba Cloud provides VMs with a local disk, which features low latency and high IOPS:
  - local NVMe SSD
  - SATA HDD
- The latest Alibaba Cloud ESSD supports up to 1M random IOPS.

- Performance comparison can be found at https://www.alibabacloud.com/help/doc-detail/25382.htm

- By default, the ultra cloud disk is used for SAP CP @ Alibaba Cloud deployment.

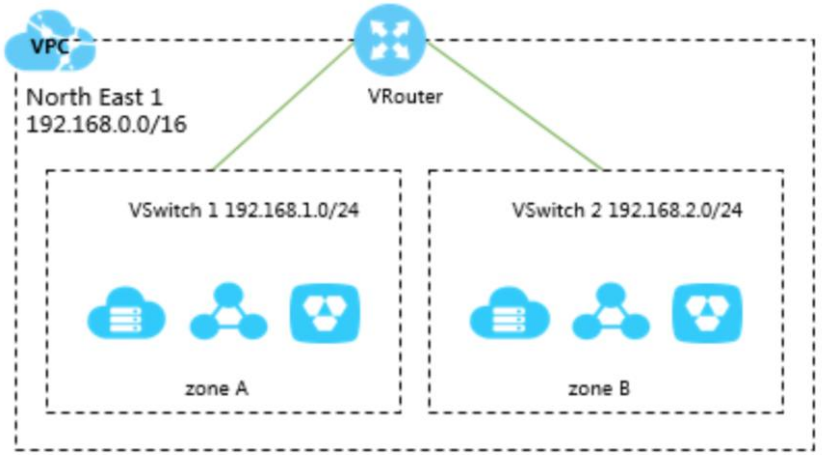
# Blob Storage

- In Alibaba Cloud, object storage is a type of data storage where data is managed as objects, instead of blocks of files. Typically, object storage is used to store large files that are dominated by read operations.

- Alibaba Cloud OSS offers three storage types: standard, low-frequency access, and archiving, supporting different storage prices, read speeds and availability.

| Feature | Alicloud |
|---|---|
| Deployment unit | Storage space |
| Object identifier | Key |
| Object metadata | Object meta |
| Version control | Not supported (In progress) |
| File size | Up to 48.8TB |
| Deployment location | Region |

# VPC




- VPC is a dedicated private network in Alibaba Cloud.
- VRouter and VSwitch are two basic components of VPC.
- VSwitch is used to connect different cloud product instances.
  - It is used to segment VPC to one or more subnets by creating VSwitches.
  - Applications can be deployed to different VSwitches that are located in different zones to improve the service availability.
  - VSwitches in different zones of a VPC can communicate with each other through the intranet by default.
- VRouter serves as the gateway connecting the VPC with other networks.
  - A VRouter is automatically created after a VPC is created.
  - Each VRouter associates with a route table.

The first and last three IP addresses of a VSwitch are reserved by the system.
For example, if the CIDR block of a VSwitch is 192.168.1.0/24,
IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.

# Security Groups

- VPC doesn’t come with an independent access control policy. Access control in the VPC relies on the access control capabilities of each cloud product. For example, ECS instances use security groups to achieve access control, while SLB and RDS use whitelists to achieve access control.

- **ECS security group**
  - A security group is a virtual firewall that provides the stateful packet inspection feature.
  - Security groups are used to set network access control for one or more ECS instances. As an important measure to isolate networks, security groups are used to divide security domains in the cloud.

- **RDS whitelist**
  - ApsaraDB for RDS uses a set of IP addresses that are allowed to access the RDS instances. Access from other IP addresses is denied.

- **SLB whitelist**
  - Server Load Balancer listeners can be configured to allow access only from certain IP addresses.

# Security Group Limitations

By default, each account can create a maximum of 100 security groups in a region. To raise the limit, you can open a ticket.

Each Elastic Network Interface (ENI) of an instance can join up to 5 security groups by default. You can open a ticket to raise the upper limit to a maximum of 10 or 16.

VPC instances can join security groups on the same VPC. A single security group on a VPC cannot contain more than 2,000 private IP addresses (shared by the primary and secondary ENIs). If more than 2,000 private IP addresses need to access each other over the intranet, you can allocate the relevant instances to different security groups and authorize mutual access among the security groups.

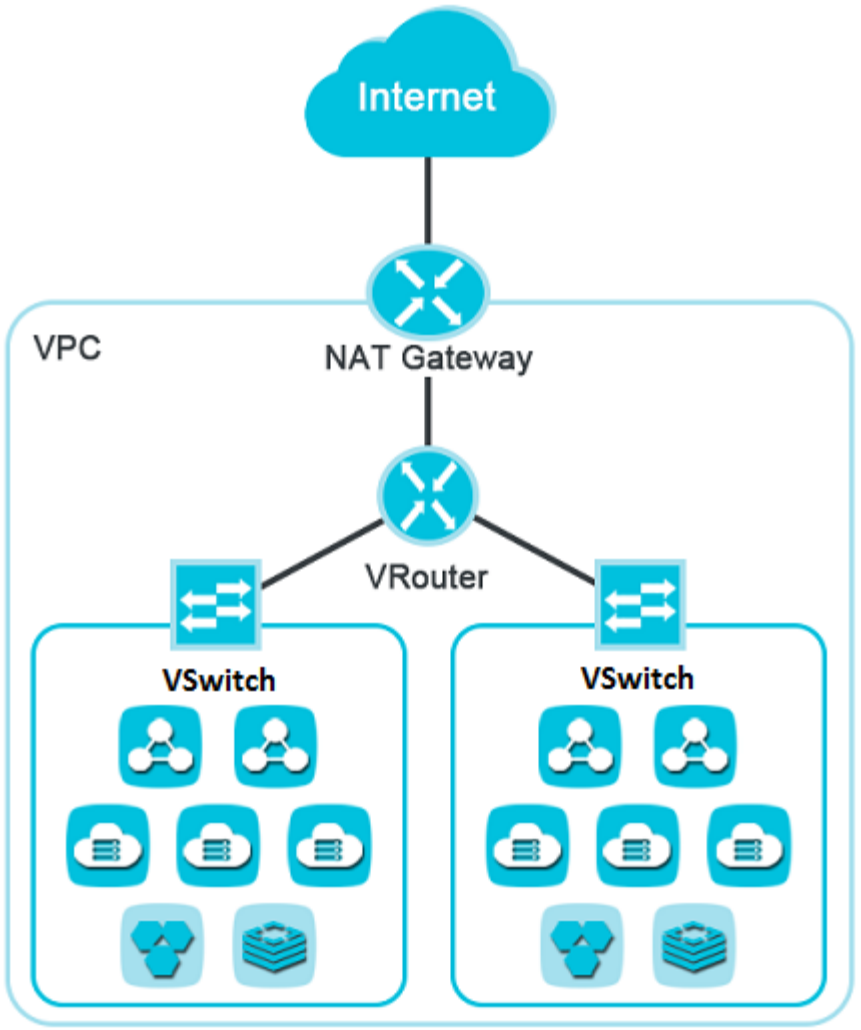
Maximum number of security group rules per ENI = number of security groups that the subject instance can join × maximum number of rules per security group.

Each ENI of an instance can have a maximum of 500 security group rules.
Where: The number of rules per security group can be 100, 50, or 30, depending on the quota of security groups.
The number of rules per security group varies according to the number of security groups that an ENI can join. However, the total number cannot exceed 100 collectively (that is, the inbound and outbound rules are not counted separately).

# NAT

- Alibaba Cloud provides a NAT gateway for VPC networks.

- In Alibaba Cloud, the NAT gateway can reach the internet only via an associated public network IP.



# NAT

- It allows the flexibility of IP management and instance switching.
- Up to 10 EIP can be associated to NAT GW (soft-limit).
- Each EIP limited up to 200 Mbps bandwidth.

| Functionality | Scenario |
| --- | --- |
| Support for multiple SNAT (source) and DNAT (destination) entries, easy to manage, simple billing. No need to configure routing separately after the instance is created. | ECS access to the internet from VPC, or serve internet facing external requests. |
| SNAT supports VPC, subnet, ECS, and SNAT for any CIDR segment within VPC.<br>DNAT supports mapping of ECS NIC and elastic NICs and it can support multiple public IP addresses for ECS | |

| Specification | Small | Medium | Large | Super Large |
| --- | --- | --- | --- | --- |
| Max SNAT connections | 10,000 | 50,000 | 200,000 | 1,000,000 |
| Max new SNAT connections established per second | 1,000 | 5,000 | 10,000 | 30,000 |

# Express Connect

- Alibaba Cloud can establish a dedicated network connection from an on premise-environment to cloud services and also between cross-regional VPCs and between cross-account VPCs using Express Connect.

- The data on Express Connect is transmitted only inside Alibaba Cloud datacenters or over leased lines and does not pass to the internet. This avoids data leakage during transmission and provides better network quality.

- The Express Connect data rate can be upgraded or downgraded at any time and the change will be applied immediately.

- If Express Connect is established then the following communication between resources can be done:
  – ECS instances on both sides can access ECS instances, Load Balancer, and RDS on the other side.
  – SLB cannot use ECS instances from the other side as backend servers.

# Load Balancing

- A load balancing service distributes traffic across multiple cloud servers to improve the servicing capabilities of the applications.
- Alibaba Cloud Load Balancing service supports L4 and L7 balancing services.

| Functionality | Alibaba Cloud SLB |
|---|---|
| Supported protocols | TCP, UDP, HTTP/HTTPs |
| HTTP 2.0 | Not supported (in progress) |
| Forward of domain names and URLS | Supported |
| Active/Standby server | Supported |
| Whitelist | Supported |
| Security | Security groups can be associated to the load balancer.<br>Includes DDoS protection |

# RDS

- Alibaba Cloud supports the RDS services of MySQL, Postgres, and many others.
- RDS is provided in 18 regions across the world.
- Each RDS has two physical nodes for master-slave hot standby.
  - When the master instance is unavailable, the RDS will be automatically migrated to the backup instance or slave instance.
  - When multi-zone configuration is enabled, RDS synchronously replicates the data to backup instances in other zones.

# Monitoring Service

- Alibaba Cloud Monitor is a service that monitors cloud resources and applications. It can be used to collect monitoring metrics to detect service availability and to set alerts for these metrics.

| Functionality | Alibaba Cloud Monitor |
| --- | --- |
| Host monitoring | Supported |
| Alarm mode | Email, SMS, Phone, Aliwangwang + DingTalk |
| Cloud Service monitoring | Supported |
| Log monitoring | Supported (not available in international site) |
| Overview | Supported of all cloud resource statistics, alerts, events and resource count. |

# Email Blocked Ports

TCP port 25 is the port that is open to the SMTP service that is used for sending mails.

Based on security concerns, ECS instance port 25 is restricted by default.

See apply to open TCP port 25 (https://www.alibabacloud.com/help/doc-detail/56130.htm) to remove the limit.

# Server Time Zone

- The current default time zone for Alibaba Cloud ECS instances across all regions is CST (China Standard Time).
- In addition, the NTP (Network Time Protocol) service guarantees that your instances are synchronized with the standard time.

| Classic network intranet | VPC intranet | Internet |
|---|---|---|
| ntp.cloud.aliyuncs.com | | ntp1.aliyun.com |
| ntp1.cloud.aliyuncs.com | ntp7.cloud.aliyuncs.com | ntp2.aliyun.com |
| ntp2.cloud.aliyuncs.com | ntp8.cloud.aliyuncs.com | ntp3.aliyun.com |
| ntp3.cloud.aliyuncs.com | ntp9.cloud.aliyuncs.com | ntp4.aliyun.com |
| ntp4.cloud.aliyuncs.com | ntp10.cloud.aliyuncs.com | ntp5.aliyun.com |
| ntp5.cloud.aliyuncs.com | ntp11.cloud.aliyuncs.com | ntp6.aliyun.com |
| ntp6.cloud.aliyuncs.com | ntp12.cloud.aliyuncs.com | ntp7.aliyun.com |

# Instance Metadata & DNS

ECS Instances access the metadata service at http://100.100.100.200/.

**Retrieve latest metadata:**
$ curl http://100.100.100.200/latest/meta-data/

**Retrieve ECS hostname:**

$ curl http://100.100.100.200/latest/meta-data/hostname

> webserver-01

**Retrieve public EIP of the ECS instance**

$ curl http://100.100.100.200/latest/meta-data/eipv4

> 47.88.57.195

**Retrieve DNS server information of the ECS instance:**

$ curl http://100.100.100.200/latest/meta-data/dns-conf/nameservers

> 100.100.2.136 1

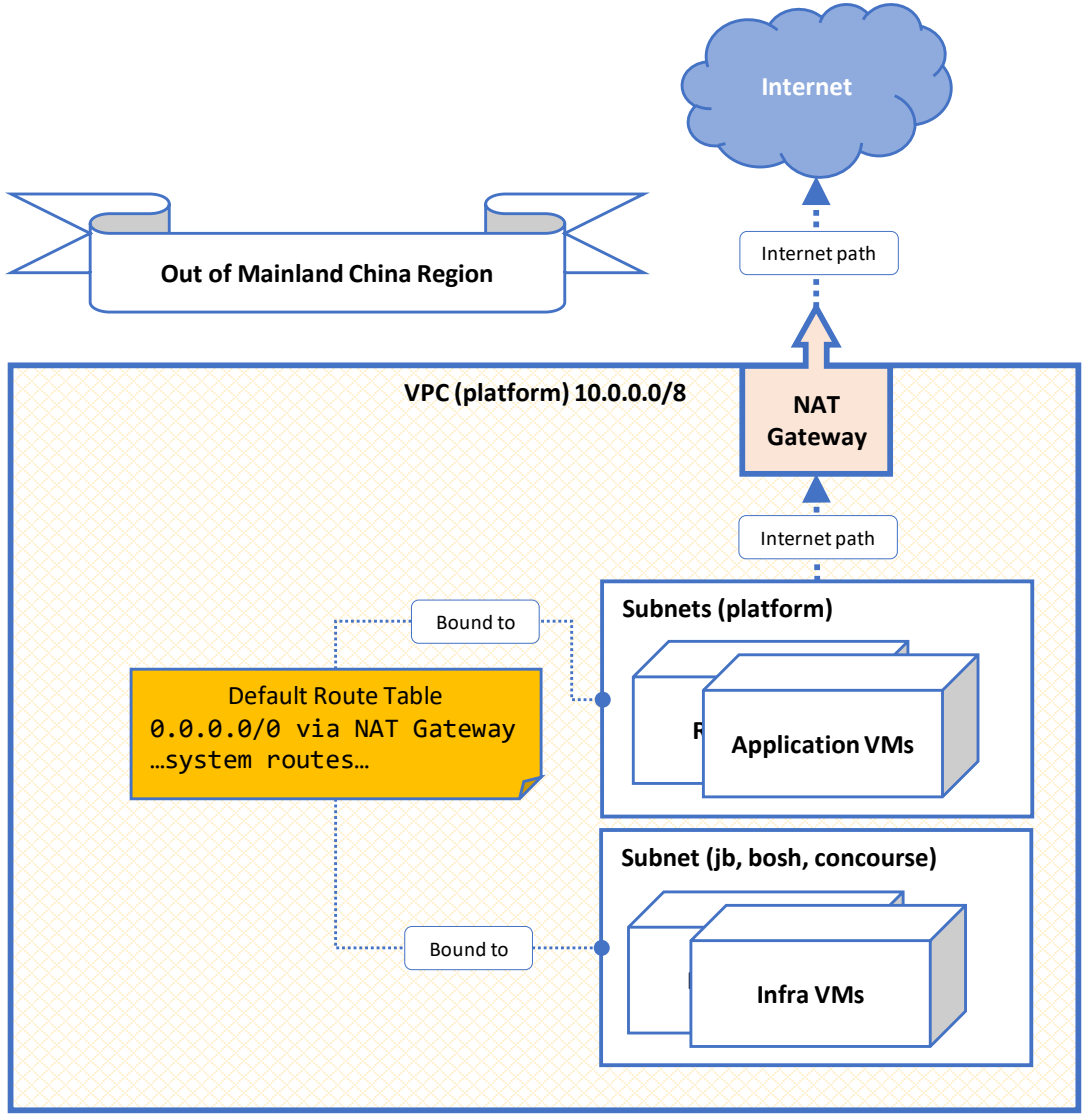
> 100.100.2.138

# China Deployment

# NAT Gateway / SAP Infra Connectivity In-Out of Mainland China Regions

## Frankfurt region deployment option:

In the Frankfurt region, there are no extra internet connectivity limitations, except the boundaries of the NAT Gateway / EIP bandwidth capabilities.



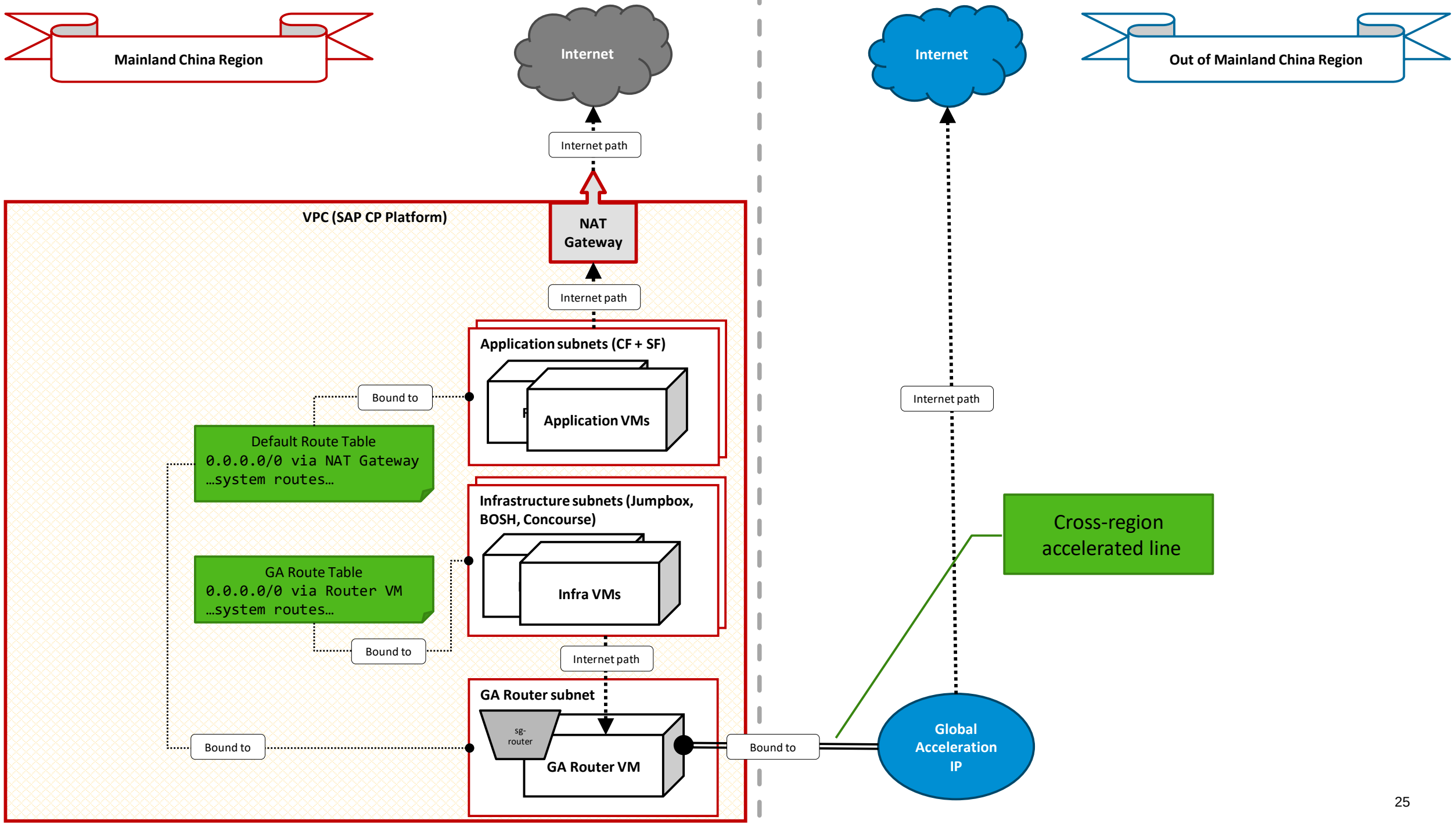
# NAT Gateway / SAP Infra Connectivity in China Regions

The deployment in China region should provide a China exit point (NAT Gateway) for application deployments (Cloud Foundry, Service Fabrik, Customer Applications, etc.), while the infrastructure services (such as BOSH, Jumpbox, Concourse) should get accelerated access to the Internet resources outside of the Mainland China region.

Global Acceleration enables this scenario by providing accelerated access to the Internet from point of presence located in-out of the Mainland China region. On a network level, global acceleration is a network interface (in China region) that can be bound to the ECS instance and provide the accelerated access to the Internet. The public IP of this network interface is located outside the China region.

A dedicated route table is used to enable different Internet path for infrastructure subnets.

The diagram in the next slide provides the details…


Mainland China Region
Internet
Internet path
VPC (SAP CP Platform)
NAT Gateway
Internet path
Application subnets (CF + SF)
Application VMs
Bound to
Default Route Table
0.0.0.0/0 via NAT Gateway
…system routes…
Infrastructure subnets (Jumpbox, BOSH, Concourse)
Infra VMs
GA Route Table
0.0.0.0/0 via Router VM
…system routes…
Bound to
Internet path
GA Router subnet
sg-router
GA Router VM
Bound to
Bound to
Internet
Internet path
Out of Mainland China Region
Cross-region accelerated line
Global Acceleration IP

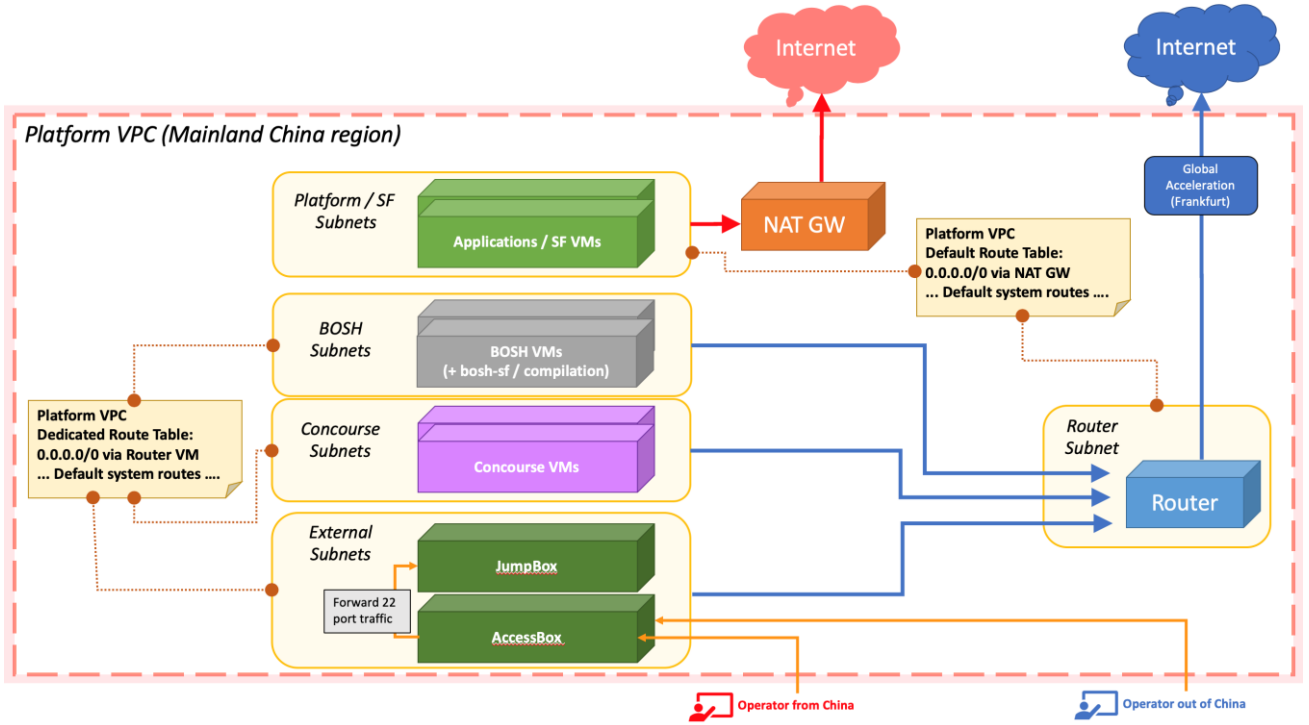
# AccessBox

In SAP CP deployment using Global Acceleration, the Jumpbox machine cannot be deployed with the association to its own public IP because it breaks the accelerated internet connectivity path.

To work around this issue, the additional VM (AccessBox) is created and associated with the Jumpbox public IP.

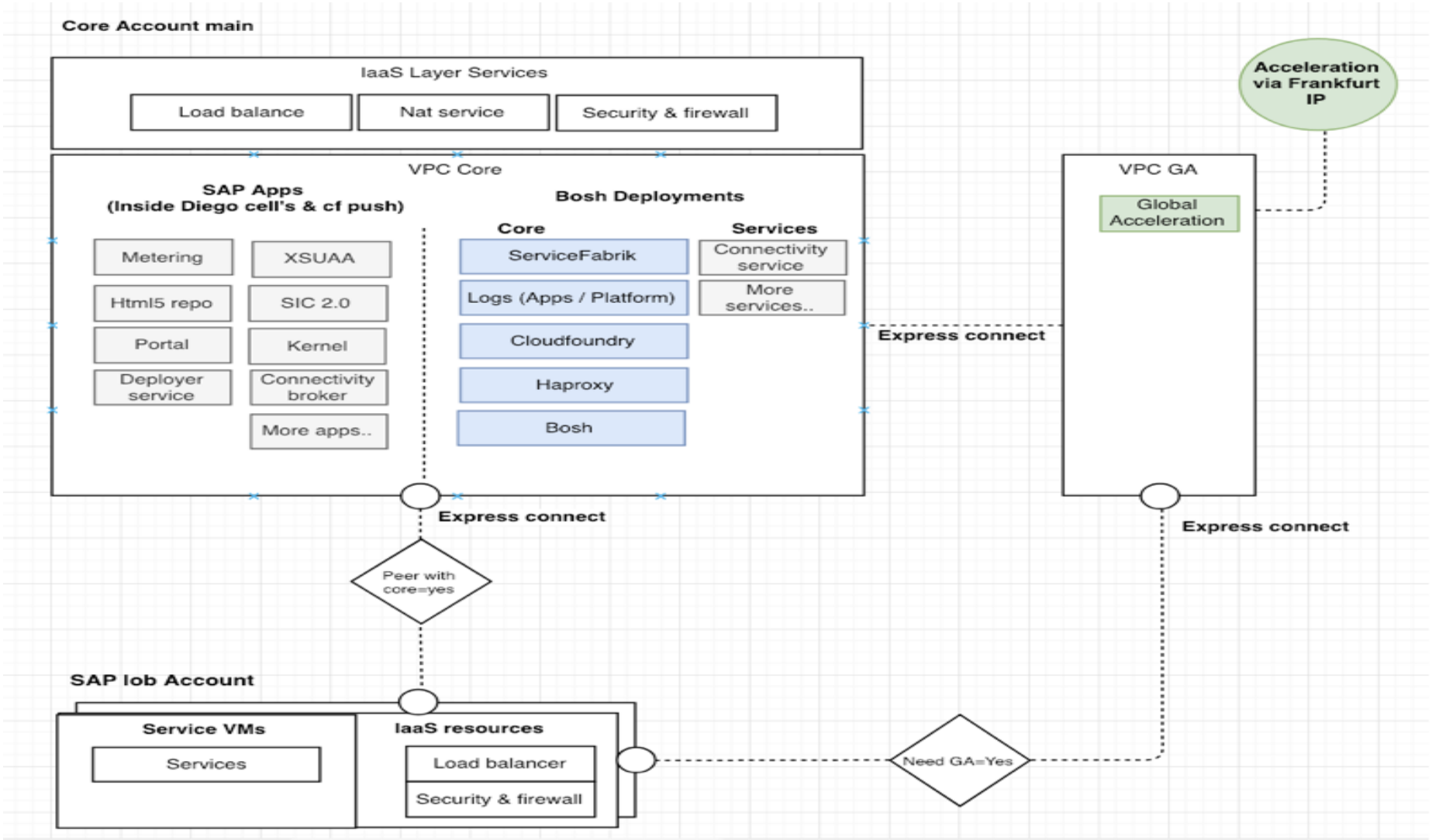
The AccessBox VM comes with a configuration that forwards all the packets sent to port 22 to the Jumpbox VM using a private IP.

This allows the operator to connect to Jumpbox using public IP, while the Jumpbox can continue to use accelerated internet connectivity.




*Operator path for connecting into Jumpbox*

# Cross-Account Peering and Global Acceleration Drawing



# SCP Components

# Component: IaaS Provider

It uses terraform to deploy the following resources:

- VPC including CIDR_BLOCK and route table configured

# Component: IaaS-routing

It uses terraform to deploy the following resources:

- NAT Gateway + SNAT table
- EIPs + EIPs associated with NAT Gateway
- Haproxy’s security group + 2 security group rules
- SLB(Server Load Balance)+ 3 listening ports(http/80, https/443, ssh/2222)
- GA instance + GA vswitch + GA route table + GA disks + GA key pair + GA security group + GA security group rule

# Component: IaaS network

It uses terraform to deploy the following resources:

- Vswitches + SNAT for these Vswitches
- GA route table attachment to infrastructure services(bosh, concourse, sf, ext)

# Component: IaaS-securitygroup

It uses terraform to deploy the following resources:

- Security groups
- Security groups’ rules

# Component: iaas/ali/infra

It uses terraform to deploy the following resources:

- Key pairs for bosh and jumpbox
- OSS buckets for cf, cf-buildpacks, cf-droplets, cf-packages, cf-resources

# Component: jumpbox

It uses terraform to deploy the following resources:

- 2 ECS: Jumpbox and accessbox
- Public IP for accessbox
- Key pair
- Route entry to AB’s eip via AB
- Security groups and their rules

# Component: bootstrap-bosh, bosh , bosh-sf

It uses bosh-cli/bosh director to deploy the following resources:

- Image : stemcell
- Disk
- ECS: bootstrap-bosh, bosh, bosh-sf

# Component: cf-persistence

It uses terraform to deploy the following resources:

- RDS : ccdb, credhubdb, diegodb, locketdb, networkpolicydb, silkdb and uaadb
- DB accounts and backup policies

# Component: Concourse

It uses bosh to deploy the following resources:

- ECS instances

It uses terraform to deploy the following resources:

- Alarm policies
- DB instance , DB account & backup policy

# Referrence

AliCloud Docs : https://help.aliyun.com/?spm=a2c4g.11174283.6.538.7d2f52fenzAgtU

ECS instances metadata: https://www.alibabacloud.com/blog/594351

# Q&A

# Thank you.

Contact information:

**Nicole Zhou**
**DevOPS**