Protecting IaaS Apps on Alibaba Cloud with VM-Series (Single VPC)

Kambiz Kazemi

Public Cloud Consulting Engineer

Agenda

- Before you begin
- Routing Considerations
- Load Balancer Considerations
- Supported designs
- Create Custom VM-Series Image for Alibaba Cloud
- Deploying VM-Series in Alibaba Cloud
- Building Outbound flow architecture with HA
- Building Inbound flow architecture – LB Sandwich

Before you begin

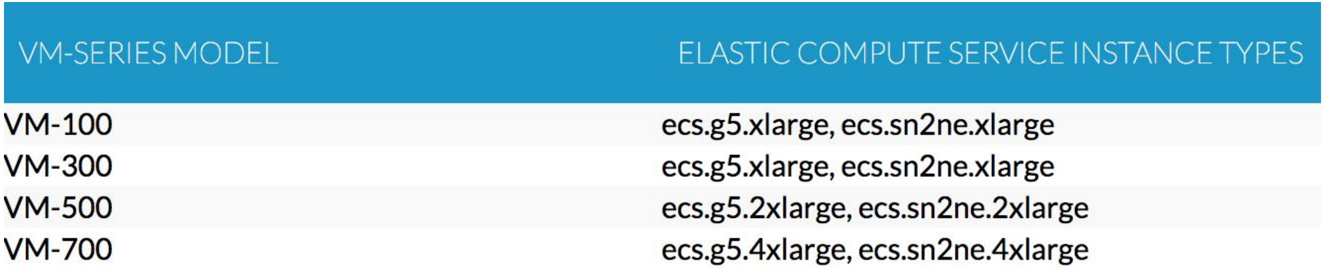
- As of April 2019, since VM-Series is not on Alibaba Cloud Marketplace yet, only BYOL and ELA deployments of VM-Series is available on Alibaba Cloud International Regions and Mainland China. In other words, no PAYG yet.

- You must first use a VM-Series firewall qcow2 image file (8.1.3 or higher) to create a Custom Image in the Alibaba Cloud Console and then create the VM-Series using that Custom Image.

- The VM-Series firewall on Alibaba Cloud runs on KVM and supports up to 8 network interfaces when you select an Alibaba Cloud instance with sufficient resources.

Before you begin

- Bootstrapping on Alibaba Cloud is not supported yet.
- Recommended Instance Types on Alibaba Cloud for VM-Series deployment:



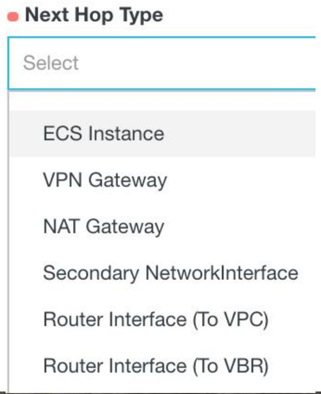
VM-SERIES MODEL	ELASTIC COMPUTE SERVICE INSTANCE TYPES
VM-100	ecs.g5.xlarge, ecs.sn2ne.xlarge
VM-300	ecs.g5.xlarge, ecs.sn2ne.xlarge
VM-500	ecs.g5.2xlarge, ecs.sn2ne.2xlarge
VM-700	ecs.g5.4xlarge, ecs.sn2ne.4xlarge

- I’ve tested with both g5 and sn2ne instance types and they worked fine. Do NOT use other instance types as you may see weird interface issues

Routing Considerations

- VPCs are Regionally scoped.
- vSwitches (subnets) are Zonally scoped. (You cannot extend a subnet across several Zones)
- Alibaba Cloud does not allow more specific routes at the VPC level, hence steering the subnet-to-subnet traffic inside a VPC is not possible yet.
- VPN GWs in Alibaba Cloud do not support BGP, hence there's no sense in creating Transit VPC architecture for Outbound and East-West between VPCs.
- Route Tables are assigned at the subnet (vSwitch) level.
- Next-Hop for a route entry can be one of these options:

This could be **ANY** of the firewall ENIs →



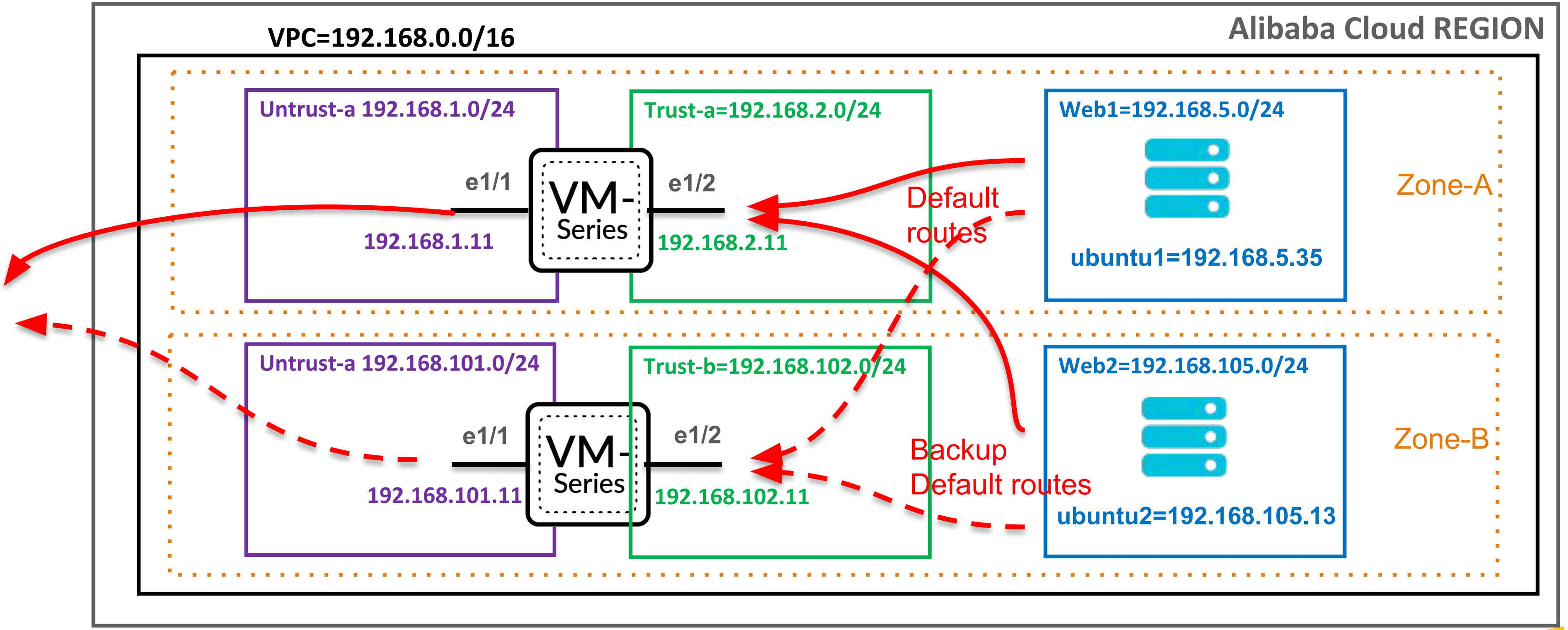
Next Hop Type
Select
ECS Instance
VPN Gateway
NAT Gateway
Secondary NetworkInterface
Router Interface (To VPC)
Router Interface (To VBR)

Load Balancer Considerations

- Load balancers can be public (Internet) or internal (Intranet).
- Load Balancer types are” TCP/UDP/HTTP/HTTPS
- Load Balancers can distribute traffic to instances in multiple zones.
- Internal Load balancer needs to be deployed in its own subnet.
- To configure the backend, you first need to place all instances behind the LB in a ‘VServer Group’
- Load balancers can deliver the traffic to ANY ENI, hence interface-swap is not required!
- SRC IP is preserved by default. You can see the actual client SRC IP on the firewall.

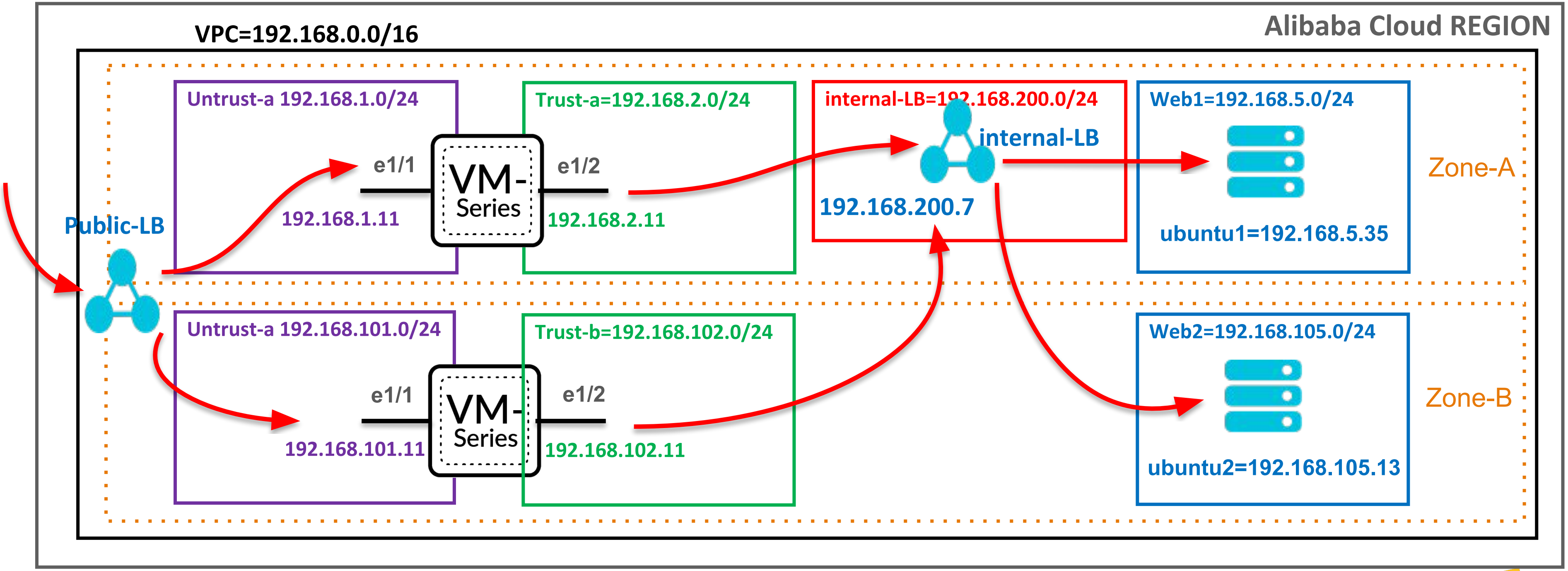
Supported designs – Outbound with HA

- Outbound flow architecture is based routing to one firewall ENI. The ha-script later provided in this deck can switch the outbound route between FW-a and FW-b, thus ensuring Outbound HA.



Supported designs – Inbound LB Sandwich

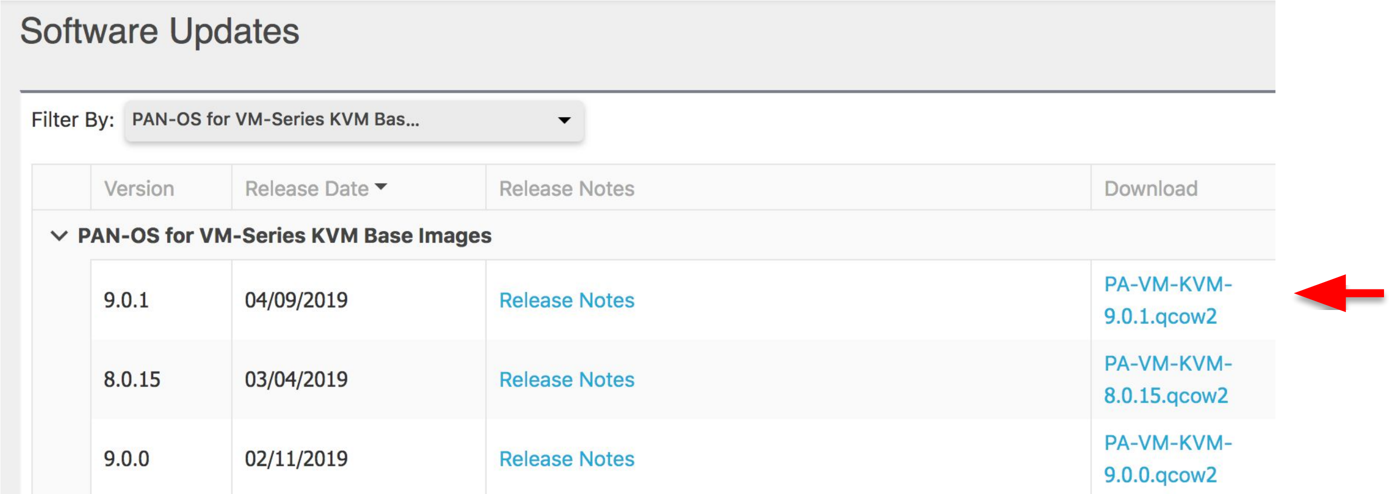
- Inbound flow architecture is based on the traditional LB Sandwich design



Create Custom VM-Series Image for Alibaba Cloud

- On the CSP, select **Updates > Software Updates** and from the **Filter By** drop-down menu, choose **Pan OS for VM-Series KVM Base Image** and locate the qcow2 file for the current version.

- Download the qcow2 file (For example, PA-VM-KVM-9.0.0.qcow2) to your laptop.



Software Updates

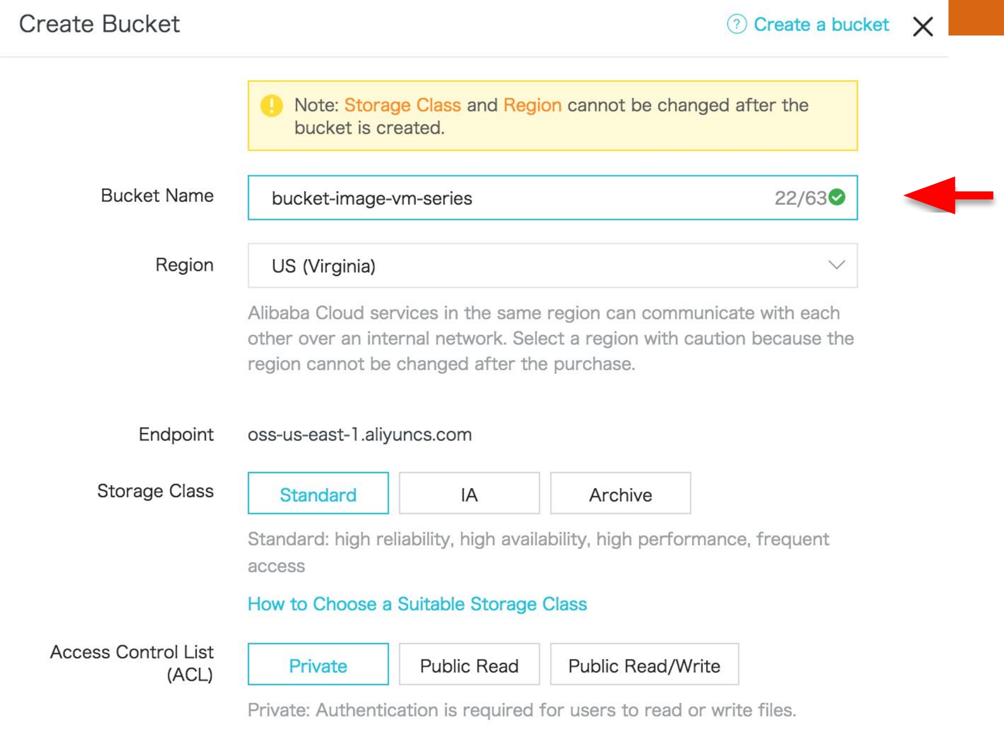
Filter By: PAN-OS for VM-Series KVM Bas...

PAN-OS for VM-Series KVM Base Images

Version	Release Date	Release Notes	Download
9.0.1	04/09/2019	Release Notes	PA-VM-KVM-9.0.1.qcow2
8.0.15	03/04/2019	Release Notes	PA-VM-KVM-8.0.15.qcow2
9.0.0	02/11/2019	Release Notes	PA-VM-KVM-9.0.0.qcow2

Create Custom VM-Series Image for Alibaba Cloud

- Now we create a bucket on Alibaba Cloud to upload the qcow2 firewall image.
- This bucket should be in the same Region that you plan to deploy the firewalls.
- On Alibaba Cloud console, navigate to Object Storage Service (OSS) and create the bucket to hold the qcow2 image



Create Bucket

Note: Storage Class and Region cannot be changed after the bucket is created.

Bucket Name: bucket-image-vm-series 22/63

Region: US (Virginia)

Alibaba Cloud services in the same region can communicate with each other over an internal network. Select a region with caution because the region cannot be changed after the purchase.

Endpoint: oss-us-east-1.aliyuncs.com

Storage Class: Standard | IA | Archive

Standard: high reliability, high availability, high performance, frequent access

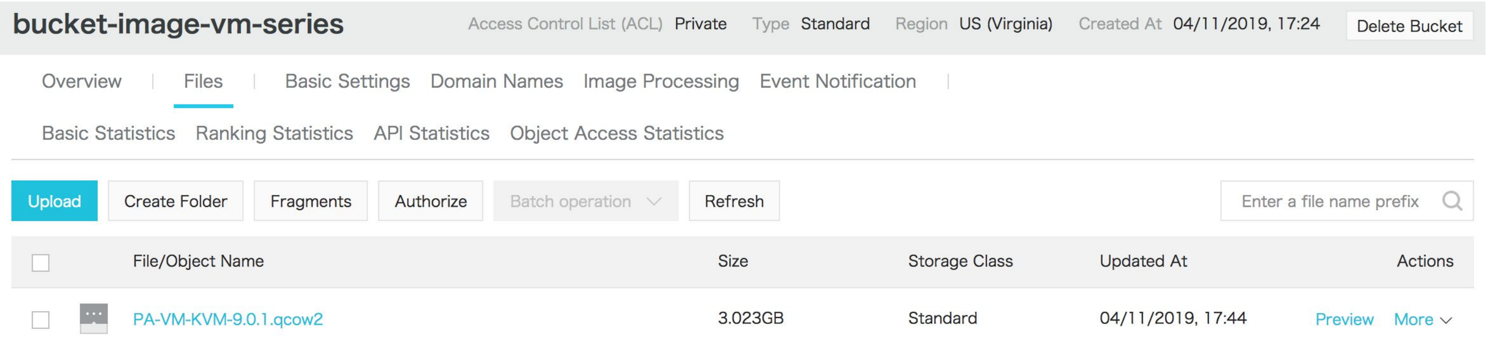
How to Choose a Suitable Storage Class

Access Control List (ACL): Private | Public Read | Public Read/Write

Private: Authentication is required for users to read or write files.

Create Custom VM-Series Image for Alibaba Cloud

- Next, upload the qcow2 image from your laptop to this bucket.



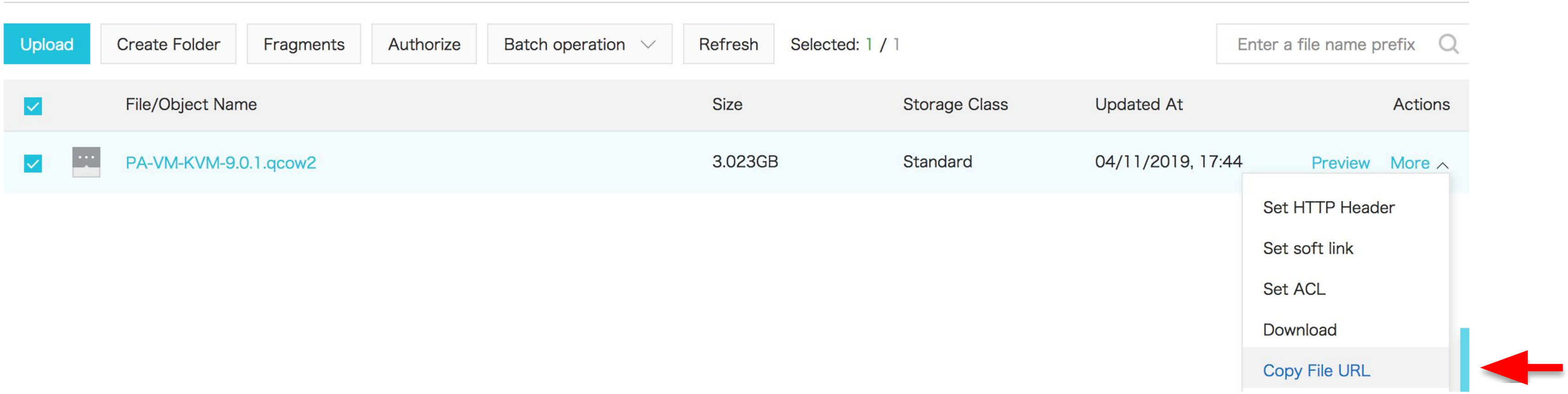
bucket-image-vm-series

Access Control List (ACL) Private   Type Standard   Region US (Virginia)   Created At 04/11/2019, 17:24

□	File/Object Name	Size	Storage Class	Updated At	Actions
□	PA-VM-KVM-9.0.1.qcow2	3.023GB	Standard	04/11/2019, 17:44	Preview More

Create Custom VM-Series Image for Alibaba Cloud

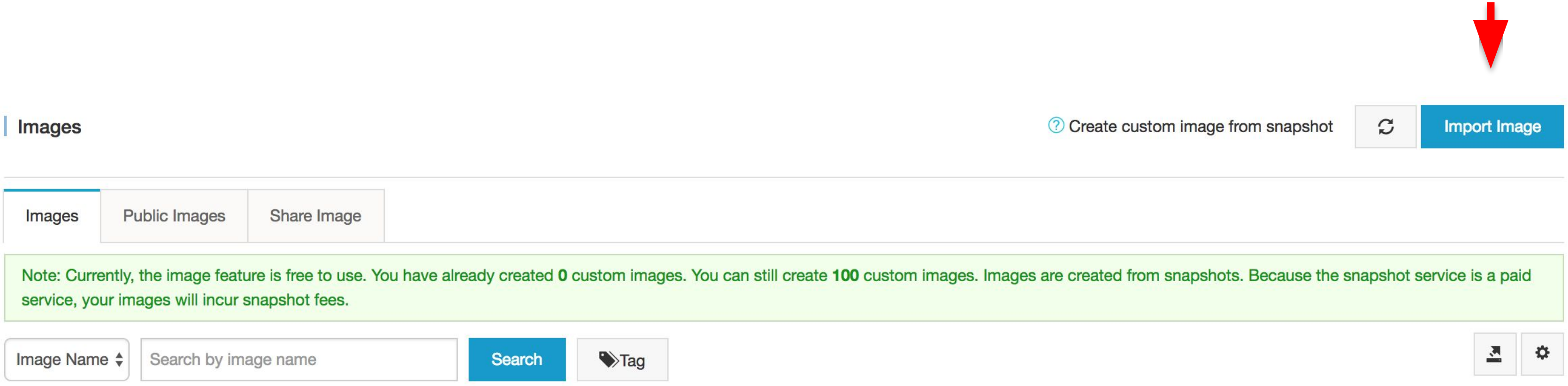
- Click on More > Copy File URL and copy the URL of the qcow2 image. You'll need this URL to create a custom vm-series image on Alibaba Cloud.



☑	File/Object Name	Size	Storage Class	Updated At	Actions
☑	PA-VM-KVM-9.0.1.qcow2	3.023GB	Standard	04/11/2019, 17:44	Preview More

Create Custom VM-Series Image for Alibaba Cloud

- Now navigate to ECS > Custom Images and click on “Import Image”

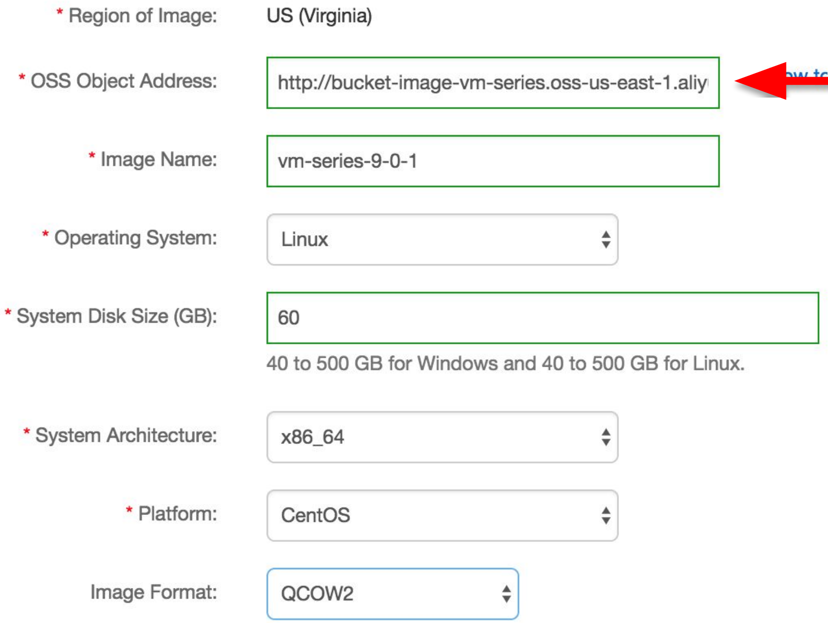


Images

Note: Currently, the image feature is free to use. You have already created **0** custom images. You can still create **100** custom images. Images are created from snapshots. Because the snapshot service is a paid service, your images will incur snapshot fees.

Create Custom VM-Series Image for Alibaba Cloud

- Fill out the required fields and specify the File URL to create the custom vm-series image for Alibaba Cloud

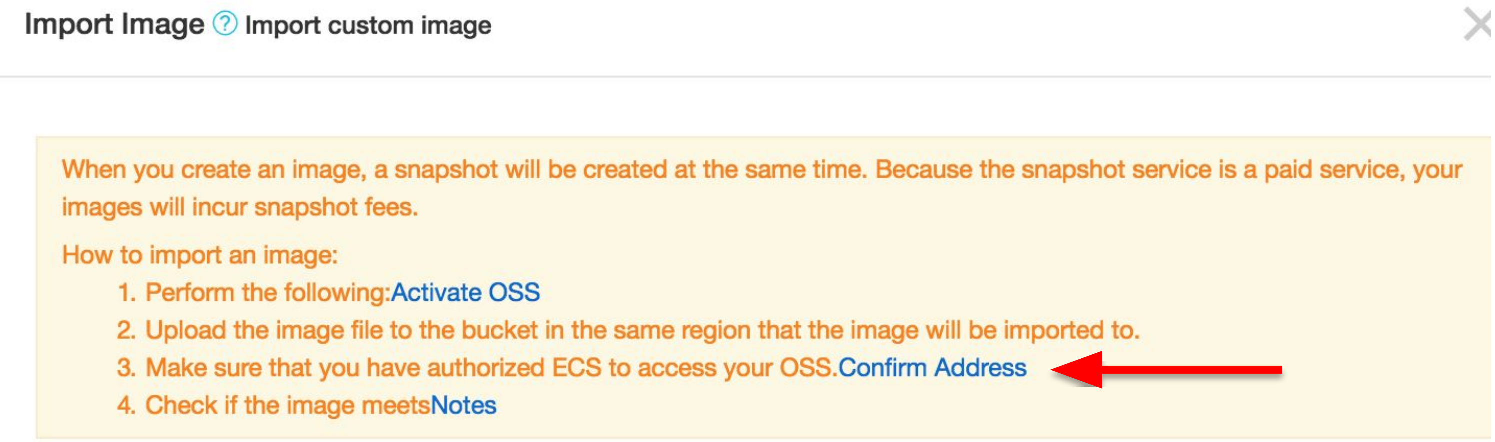


* Region of Image:	US (Virginia)
* OSS Object Address:	http://bucket-image-vm-series.oss-us-east-1.aliy
* Image Name:	vm-series-9-0-1
* Operating System:	Linux
* System Disk Size (GB):	60 40 to 500 GB for Windows and 40 to 500 GB for Linux.
* System Architecture:	x86_64
* Platform:	CentOS
Image Format:	QCOW2

File URL

Create Custom VM-Series Image for Alibaba Cloud

- Note: If you get a permission error, click on the link shown to Authorize ECS to access OSS (object store)



Import Image ⓘ Import custom image

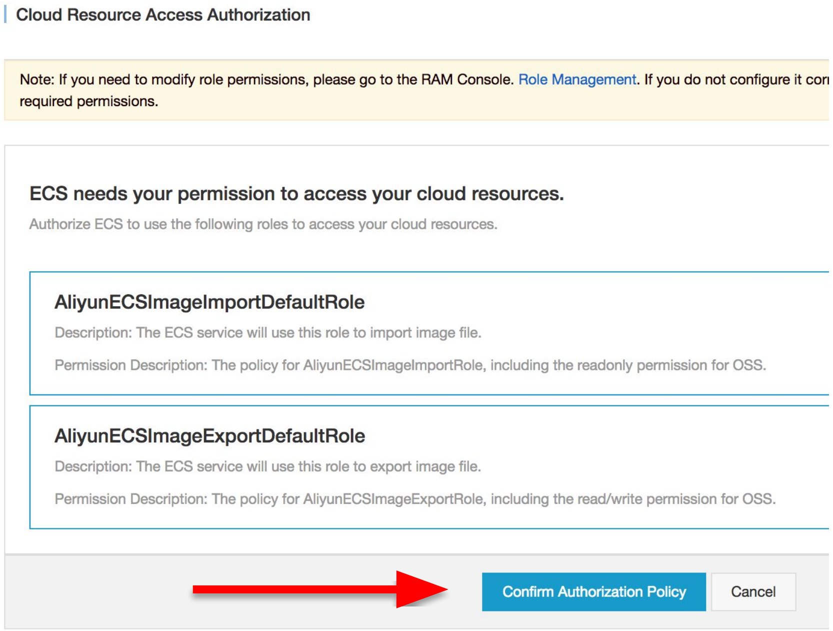
When you create an image, a snapshot will be created at the same time. Because the snapshot service is a paid service, your images will incur snapshot fees.

How to import an image:

1. Perform the following:Activate OSS
2. Upload the image file to the bucket in the same region that the image will be imported to.
3. Make sure that you have authorized ECS to access your OSS.Confirm Address
4. Check if the image meetsNotes

Create Custom VM-Series Image for Alibaba Cloud

- Authorizing ECS to access OSS



Cloud Resource Access Authorization

Note: If you need to modify role permissions, please go to the RAM Console. Role Management. If you do not configure it corr
required permissions.

ECS needs your permission to access your cloud resources.

Authorize ECS to use the following roles to access your cloud resources.

AliyunECSImageImportDefaultRole

Description: The ECS service will use this role to import image file.

Permission Description: The policy for AliyunECSImageImportRole, including the readonly permission for OSS.

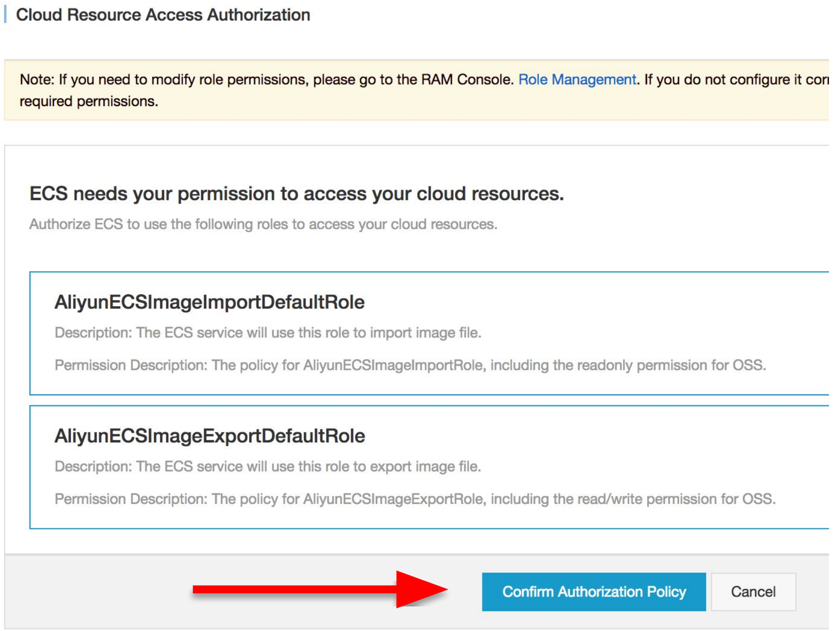
AliyunECSImageExportDefaultRole

Description: The ECS service will use this role to export image file.

Permission Description: The policy for AliyunECSImageExportRole, including the read/write permission for OSS.

Create Custom VM-Series Image for Alibaba Cloud

- Authorizing ECS to access OSS



Cloud Resource Access Authorization

Note: If you need to modify role permissions, please go to the RAM Console. Role Management. If you do not configure it cor
required permissions.

ECS needs your permission to access your cloud resources.

Authorize ECS to use the following roles to access your cloud resources.

AliyunECSImageImportDefaultRole

Description: The ECS service will use this role to import image file.

Permission Description: The policy for AliyunECSImageImportRole, including the readonly permission for OSS.

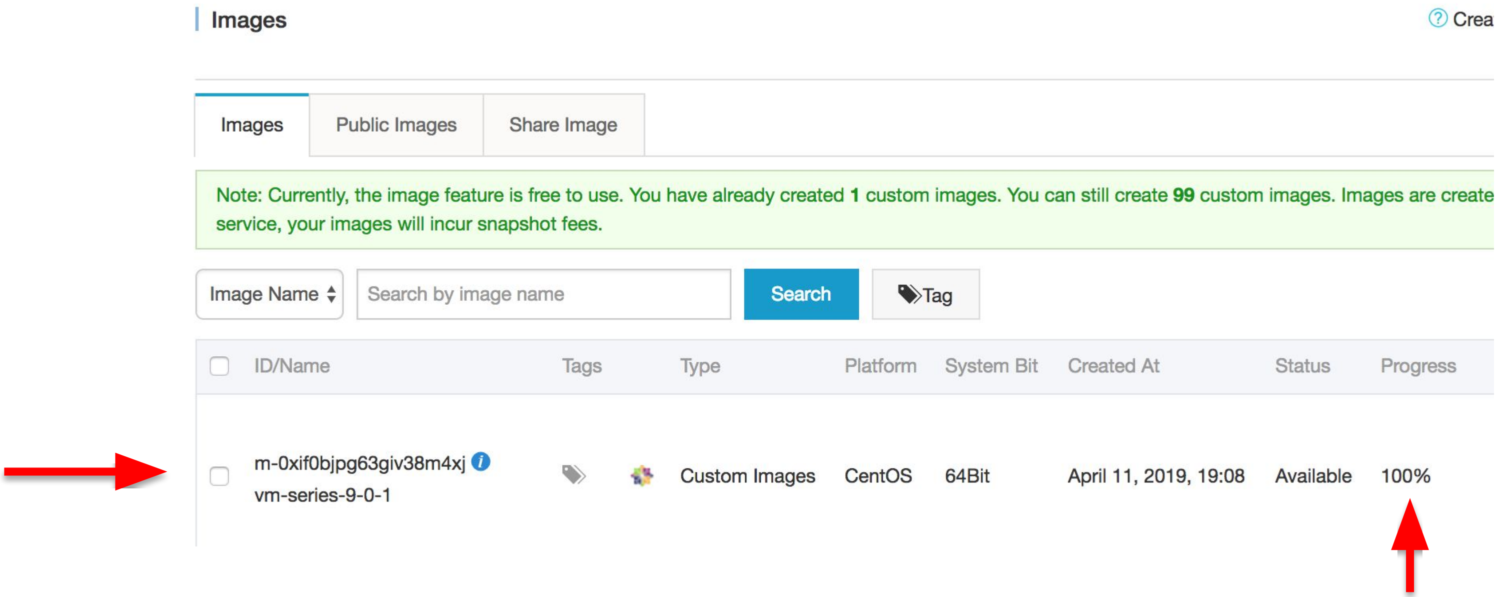
AliyunECSImageExportDefaultRole

Description: The ECS service will use this role to export image file.

Permission Description: The policy for AliyunECSImageExportRole, including the read/write permission for OSS.

Create Custom VM-Series Image for Alibaba Cloud

- Image creation can take a substantial amount of time so be patient.



Images

? Crea

Images | Public Images | Share Image

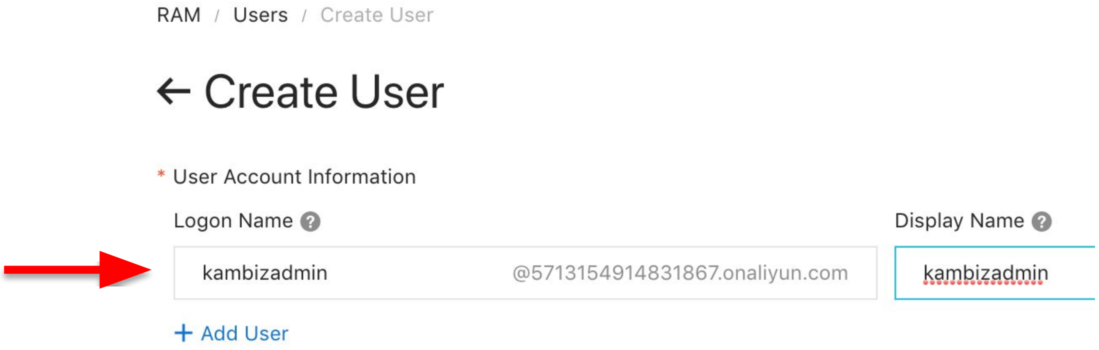
Note: Currently, the image feature is free to use. You have already created **1** custom images. You can still create **99** custom images. Images are create service, your images will incur snapshot fees.

Image Name ⇕ | Search by image name | Search | Tag

□	ID/Name	Tags	Type	Platform	System Bit	Created At	Status	Progress
□	m-0xif0bjpg63giv38m4xj vm-series-9-0-1		Custom Images	CentOS	64Bit	April 11, 2019, 19:08	Available	100%

Create Custom VM-Series Image for Alibaba Cloud

- We need to perform some of the actions later via Alibaba Cloud CLI (Aliyun), so let’s get out CLI set up.
- First we need to create an Access Key. Access Keys are used to directly call APIs.
- Navigate to RAM (Resource Access Management) > Users and create a User



RAM / Users / Create User

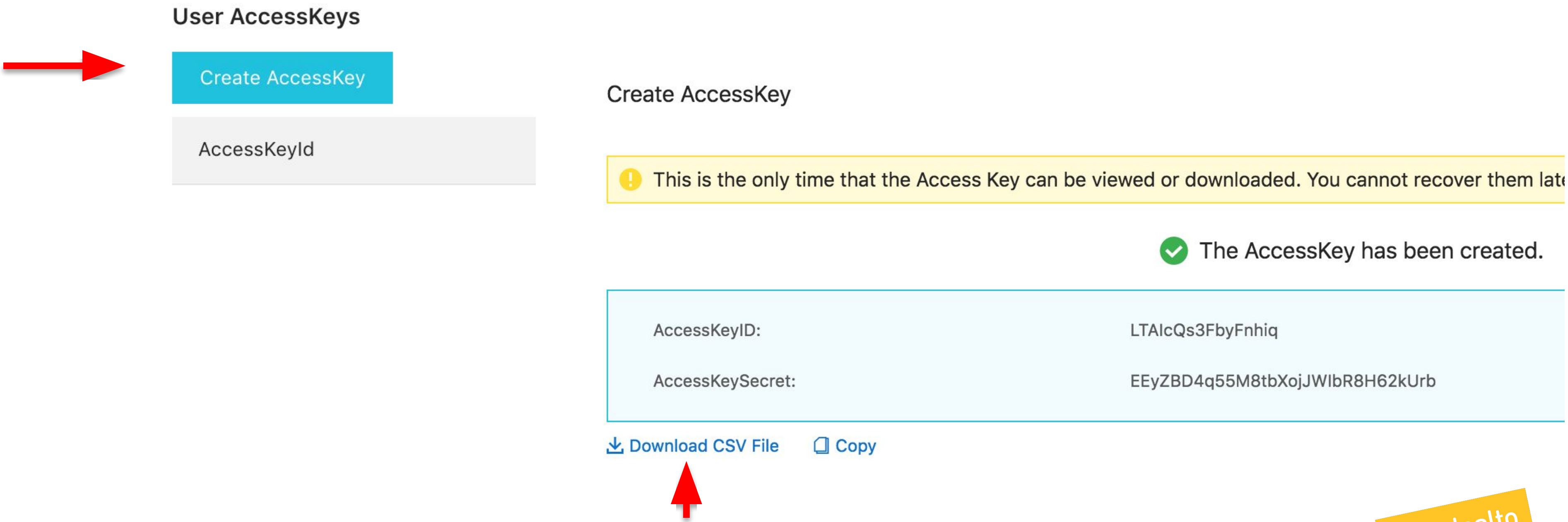
← Create User

* User Account Information

Logon Name	kambizadmin @5713154914831867.onaliyun.com
Display Name	kambizadmin

Create Custom VM-Series Image for Alibaba Cloud

- Click on the User you just created, go to the bottom of page and create an Access Key and download the CSV file to your laptop



User AccessKeys

Create AccessKey

AccessKeyId

Create AccessKey

This is the only time that the Access Key can be viewed or downloaded. You cannot recover them late

The AccessKey has been created.

AccessKeyID: LTAIcQs3FbyFnhiq

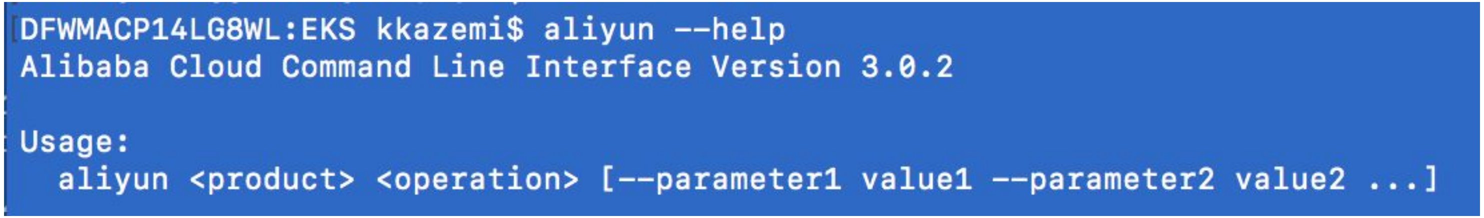
AccessKeySecret: EEyZBD4q55M8tbXojJWlbR8H62kUrb

Download CSV File   Copy

Create Custom VM-Series Image for Alibaba Cloud

- Follow the instructions from https://www.alibabacloud.com/help/doc-detail/90765.html to download and install the aliyun for your laptop OS.

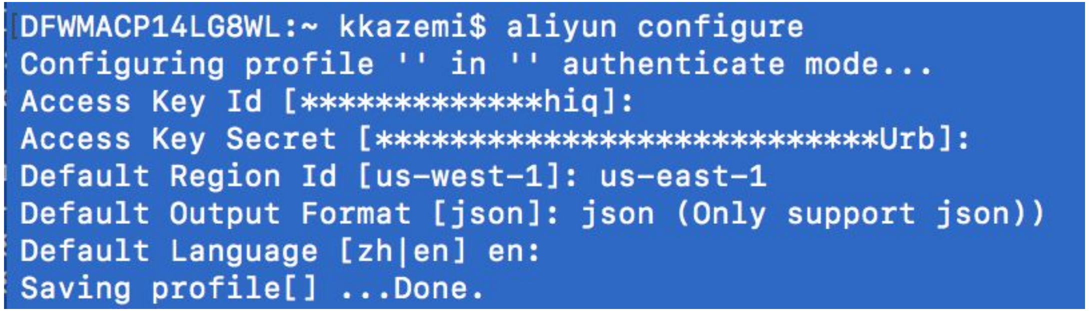
- Make sure you can execute aliyun commands from your laptop:



```
[DFWMACP14LG8WL:EKS kkazemi$ aliyun --help
Alibaba Cloud Command Line Interface Version 3.0.2

Usage:
  aliyun <product> <operation> [--parameter1 value1 --parameter2 value2 ...]
```

Create Custom VM-Series Image for Alibaba Cloud

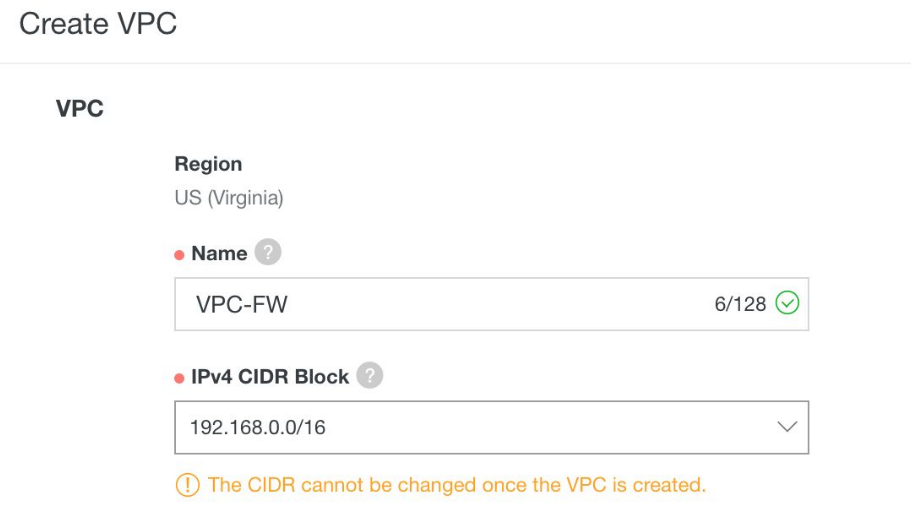
- Lastly we have to configure aliyun by typing ‘aliyun configure’. You’ll need to enter your ‘Access Key Id’ and ‘Access Key Secret’



```
DFWMACP14LG8WL:~ kkazemi$ aliyun configure
Configuring profile '' in '' authenticate mode...
Access Key Id [*************hiq]:
Access Key Secret [***************************Urb]:
Default Region Id [us-west-1]: us-east-1
Default Output Format [json]: json (Only support json))
Default Language [zh|en] en:
Saving profile[] ...Done.
```

Deploying VM-Series in Alibaba Cloud

- Next we create out VPC Infrastructure.
- Navigate to VPC and create a VPC=VPC-FW=192.168.0.0/16
- For now just create a subnet=vSwitch=Mgmt-a in Zone-a



Create VPC

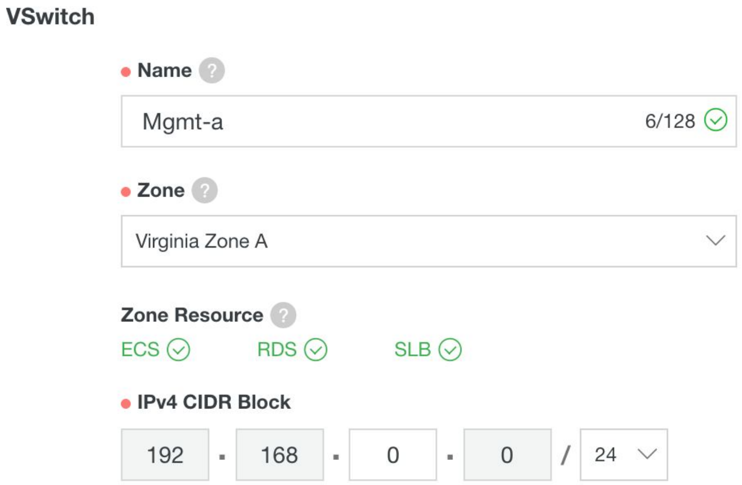
VPC

Region
US (Virginia)

● **Name** ?
VPC-FW 6/128 ✓

● **IPv4 CIDR Block** ?
192.168.0.0/16

(!) The CIDR cannot be changed once the VPC is created.



VSwitch

● **Name** ?
Mgmt-a 6/128 ✓

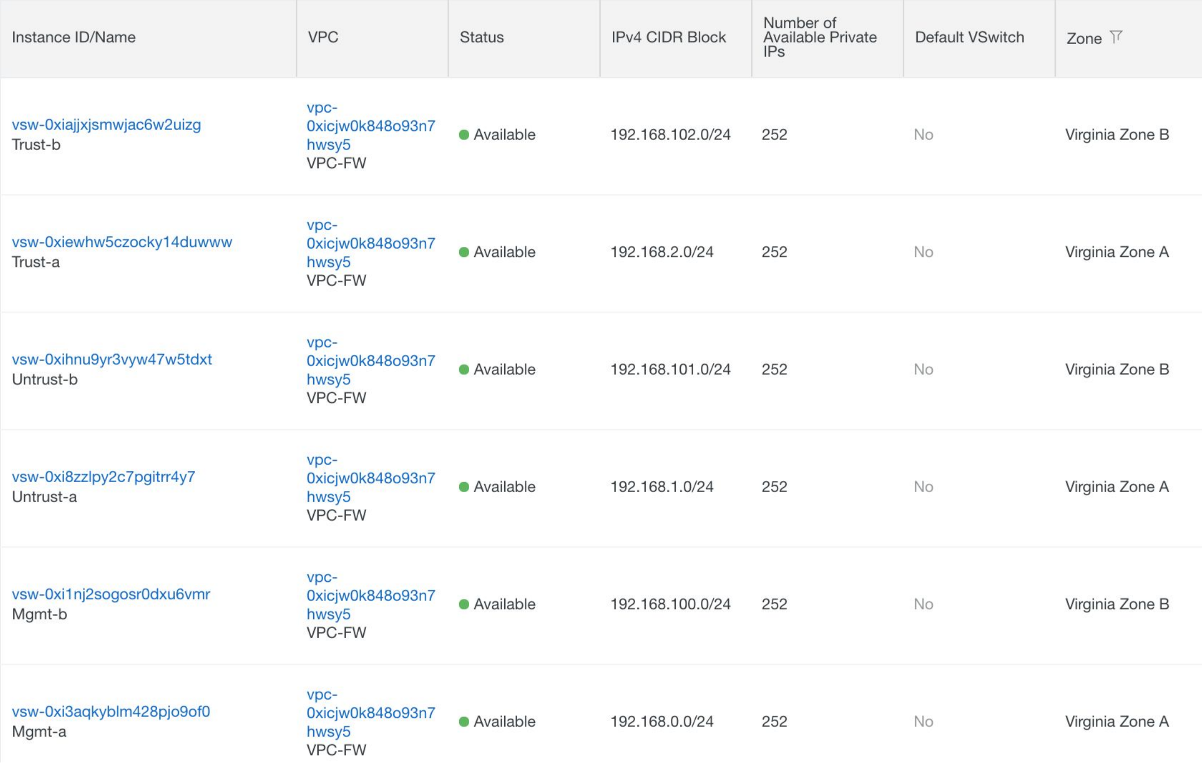
● **Zone** ?
Virginia Zone A

Zone Resource ?
ECS ✓ RDS ✓ SLB ✓

● **IPv4 CIDR Block**
192 . 168 . 0 . 0 / 24

Deploying VM-Series in Alibaba Cloud

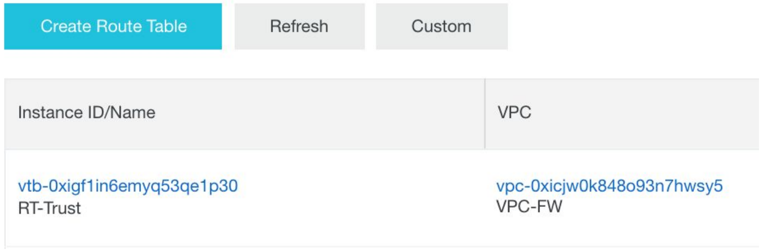
- Create 5 additional vSwitches so that we have Mgmt-a, Mgmt-b, Untrust-a, Untrust-b, Trust-a, Trust-b



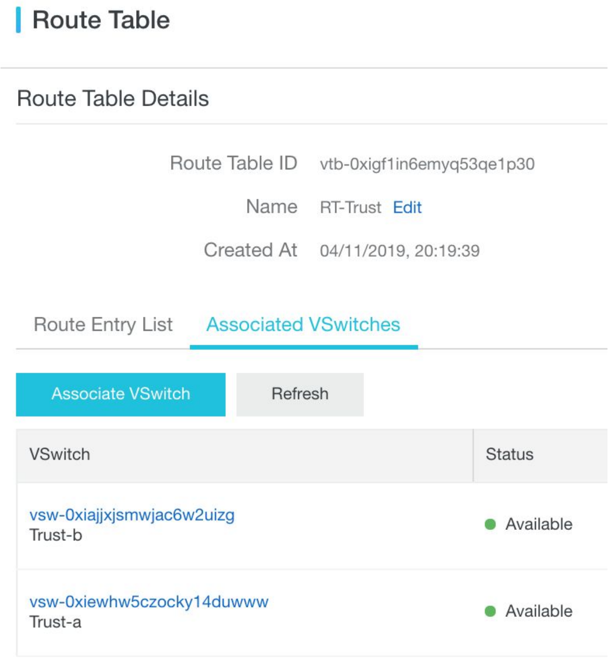
Instance ID/Name	VPC	Status	IPv4 CIDR Block	Number of Available Private IPs	Default VSwitch	Zone
vsw-0xiajjxjsmwjac6w2uizg Trust-b	vpc-0xicjw0k848o93n7hwsy5 VPC-FW	● Available	192.168.102.0/24	252	No	Virginia Zone B
vsw-0xiewhw5czocky14duwww Trust-a	vpc-0xicjw0k848o93n7hwsy5 VPC-FW	● Available	192.168.2.0/24	252	No	Virginia Zone A
vsw-0xihnu9yr3vyw47w5tdxt Untrust-b	vpc-0xicjw0k848o93n7hwsy5 VPC-FW	● Available	192.168.101.0/24	252	No	Virginia Zone B
vsw-0xi8zzlpy2c7pgitrr4y7 Untrust-a	vpc-0xicjw0k848o93n7hwsy5 VPC-FW	● Available	192.168.1.0/24	252	No	Virginia Zone A
vsw-0xi1nj2sogosr0dxu6vmr Mgmt-b	vpc-0xicjw0k848o93n7hwsy5 VPC-FW	● Available	192.168.100.0/24	252	No	Virginia Zone B
vsw-0xi3aqkyblm428pjo9of0 Mgmt-a	vpc-0xicjw0k848o93n7hwsy5 VPC-FW	● Available	192.168.0.0/24	252	No	Virginia Zone A

Deploying VM-Series in Alibaba Cloud

- Next, create a RT called RT-Trust. Just leave the system routes inside of it and then associate it with vSwitch Trust-a and Trust-b



Instance ID/Name	VPC
vtb-0xigf1in6emyq53qe1p30 RT-Trust	vpc-0xicjw0k848o93n7hwsy5 VPC-FW



Route Table

Route Table Details

Route Table ID vtb-0xigf1in6emyq53qe1p30

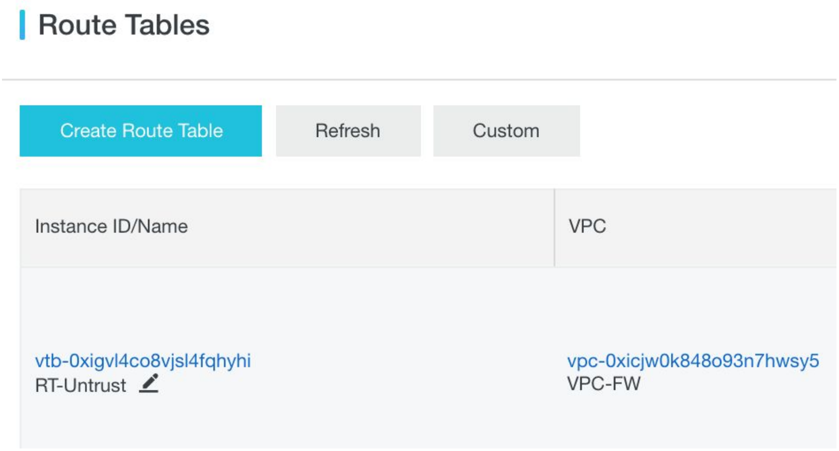
Name RT-Trust Edit

Created At 04/11/2019, 20:19:39

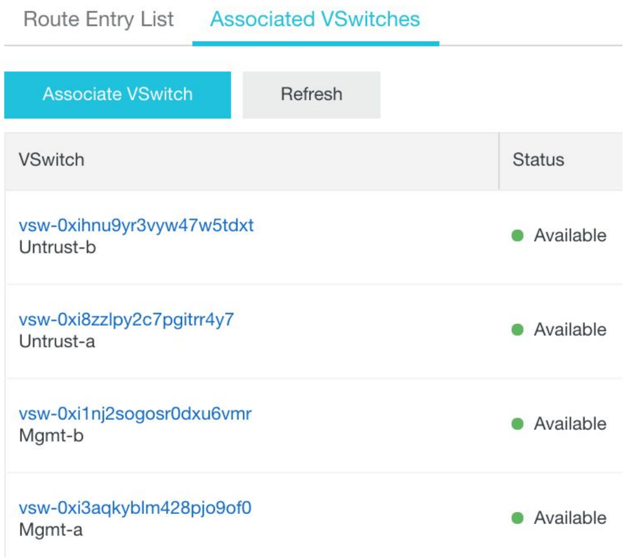
VSwitch	Status
vsw-0xiajjxjsmwjac6w2uizg Trust-b	● Available
vsw-0xiewhw5czocky14duwww Trust-a	● Available

Deploying VM-Series in Alibaba Cloud

- Similarly, create a RT called RT-Unrust. Just leave the system routes inside of it for now and then associate it with vSwitch Mgmt-a, Mgmt-b, Untrust-a, Untrust-b



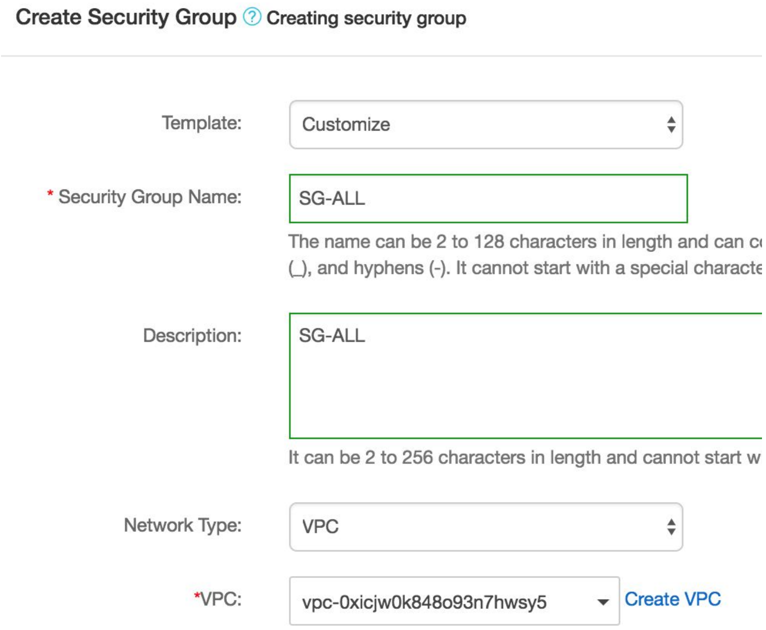
Instance ID/Name	VPC
vtb-0xigvl4co8vjsl4fqhyhi RT-Untrust	vpc-0xicjw0k848o93n7hwsy5 VPC-FW



VSwitch	Status
vsw-0xihnu9yr3vyw47w5tdxt Untrust-b	● Available
vsw-0xi8zzlpy2c7pgitrr4y7 Untrust-a	● Available
vsw-0xi1nj2sogosr0dxu6vmr Mgmt-b	● Available
vsw-0xi3aqkyblm428pjo9of0 Mgmt-a	● Available

Deploying VM-Series in Alibaba Cloud

- Create a SG and create inbound rules for it (Outbound is allowed by default)



Create Security Group ? Creating security group

Template: Customize

* Security Group Name: SG-ALL

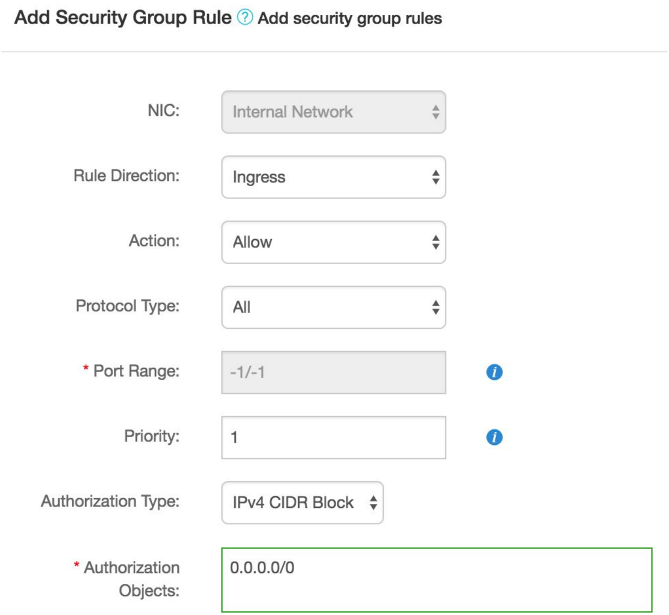
The name can be 2 to 128 characters in length and can c
(_), and hyphens (-). It cannot start with a special characte

Description: SG-ALL

It can be 2 to 256 characters in length and cannot start w

Network Type: VPC

*VPC: vpc-0xicjw0k848o93n7hwsy5



Add Security Group Rule ? Add security group rules

NIC: Internal Network

Rule Direction: Ingress

Action: Allow

Protocol Type: All

* Port Range: -1/-1

Priority: 1

Authorization Type: IPv4 CIDR Block

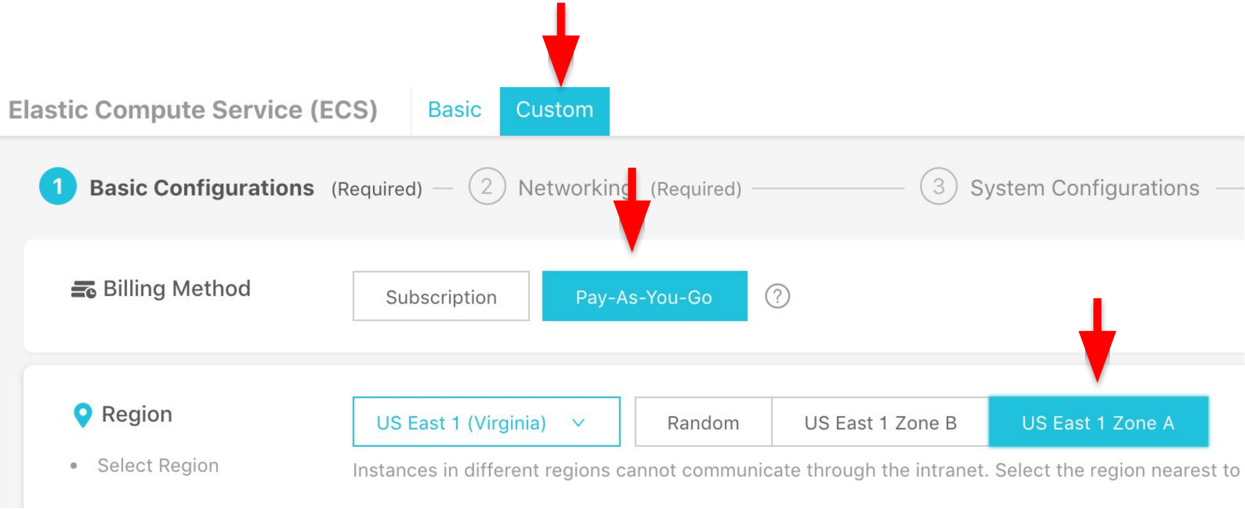
* Authorization Objects: 0.0.0.0/0

Deploying VM-Series in Alibaba Cloud

- Now we create FW-a from the Custom Image we created earlier. We will create the firewall with Mgmt interface only and later attach the Untrust and Trust ENIs

- Navigate to ECS > Instances > Create Instance

- Choose custom, PAYG and choose Zone-a in us-east-1 Region



Elastic Compute Service (ECS) Basic Custom

1 Basic Configurations (Required) — 2 Networking (Required) — 3 System Configurations

Billing Method: Subscription | Pay-As-You-Go (selected)

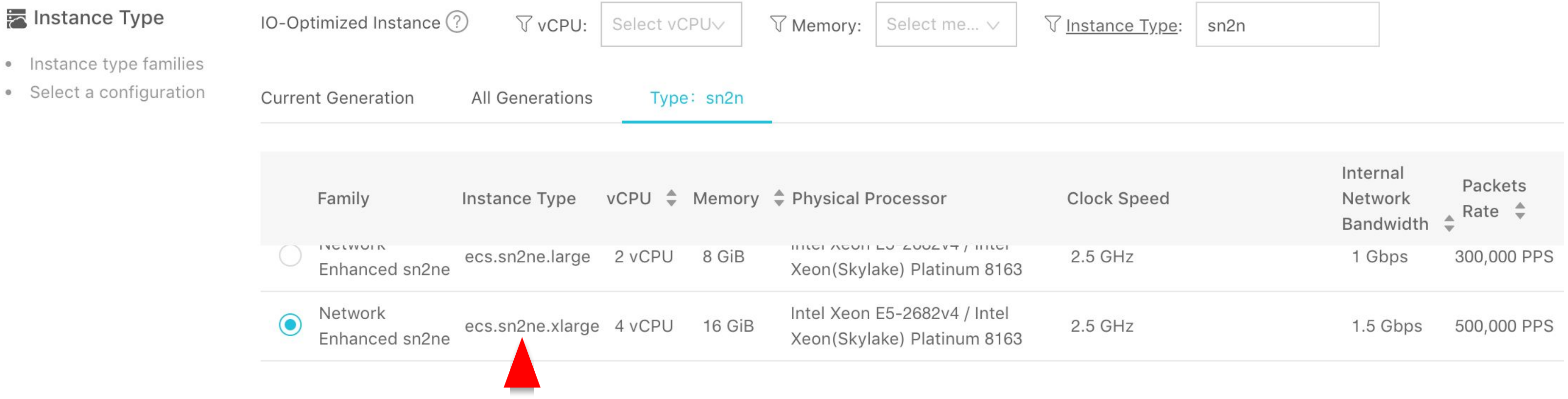
Region: US East 1 (Virginia) | Random | US East 1 Zone B | US East 1 Zone A (selected)

- Select Region

Instances in different regions cannot communicate through the intranet. Select the region nearest to

Deploying VM-Series in Alibaba Cloud

- If you’re deploying a VM-300, choose Instance Type=sn2.large



Instance Type

- Instance type families
- Select a configuration

IO-Optimized Instance ? vCPU: Select vCPU Memory: Select me... Instance Type: sn2n

Current Generation | All Generations | Type：sn2n

	Family	Instance Type	vCPU	Memory	Physical Processor	Clock Speed	Internal Network Bandwidth	Packets Rate
○	Network Enhanced sn2ne	ecs.sn2ne.large	2 vCPU	8 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1 Gbps	300,000 PPS
●	Network Enhanced sn2ne	ecs.sn2ne.xlarge	4 vCPU	16 GiB	Intel Xeon E5-2682v4 / Intel Xeon(Skylake) Platinum 8163	2.5 GHz	1.5 Gbps	500,000 PPS

- For other VM flavors use:

VM-Series Model	Elastic Compute Service Instance Types
VM-100	ecs.g5.xlarge, ecs.sn2ne.xlarge
VM-300	ecs.g5.xlarge, ecs.sn2ne.xlarge
VM-500	ecs.g5.2xlarge, ecs.sn2ne.2xlarge
VM-700	ecs.g5.4xlarge, ecs.sn2ne.4xlarge

DO NOT use arbitrary instance types!
Use either sn2ne or g5 types otherwise you’ll see weird interface issues

Deploying VM-Series in Alibaba Cloud

- For image, choose the custom image you created earlier. Leave the storage to 60GB

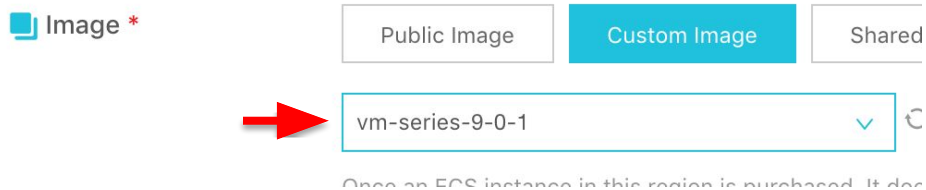
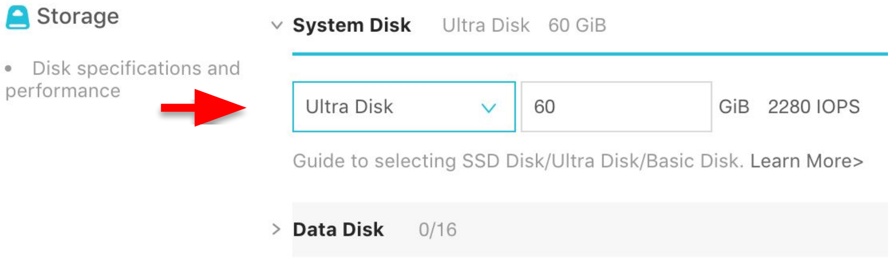


Image *

vm-series-9-0-1

Once an ECS instance in this region is purchased. It doe



Storage

- Disk specifications and performance

System Disk Ultra Disk 60 GiB

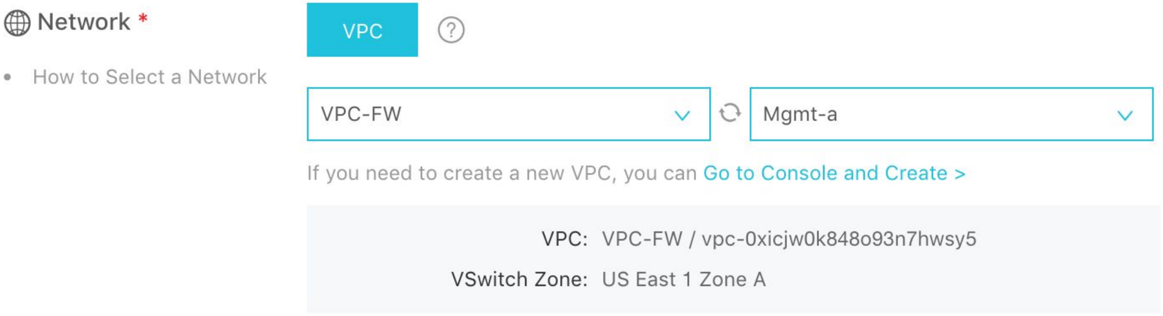
Ultra Disk 60 GiB 2280 IOPS

Guide to selecting SSD Disk/Ultra Disk/Basic Disk. Learn More>

Data Disk 0/16

Deploying VM-Series in Alibaba Cloud

- Choose VPC=VPC-FW and vSwitch=Mgmt-a



Network *

- How to Select a Network

VPC

VPC-FW

Mgmt-a

If you need to create a new VPC, you can Go to Console and Create >

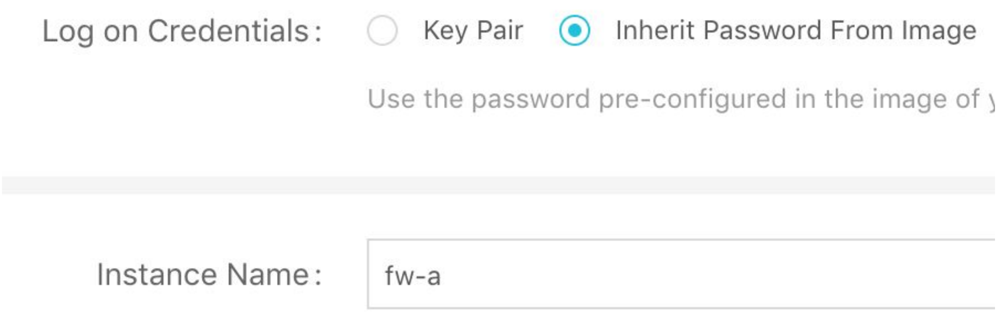
VPC: VPC-FW / vpc-0xicjw0k848o93n7hwsy5

VSwitch Zone: US East 1 Zone A

- Do NOT assign a Public IP for now.

Deploying VM-Series in Alibaba Cloud

- For Log on credentials, choose inherit from Image.
- Give the instance a name (fw-a)
- Finish creating the Instance.



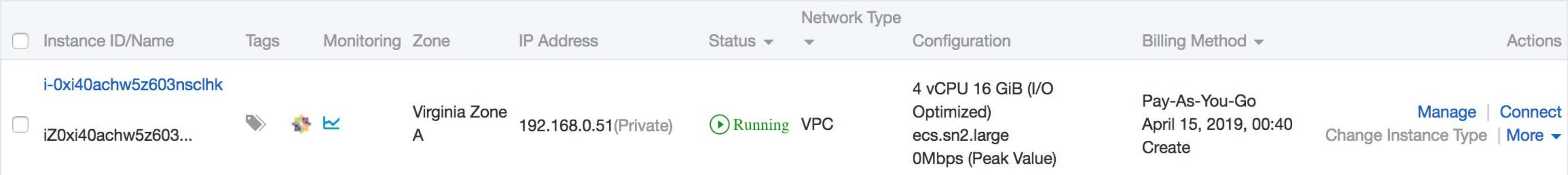
Log on Credentials: ○ Key Pair ● Inherit Password From Image

Use the password pre-configured in the image of

Instance Name: fw-a

Deploying VM-Series in Alibaba Cloud

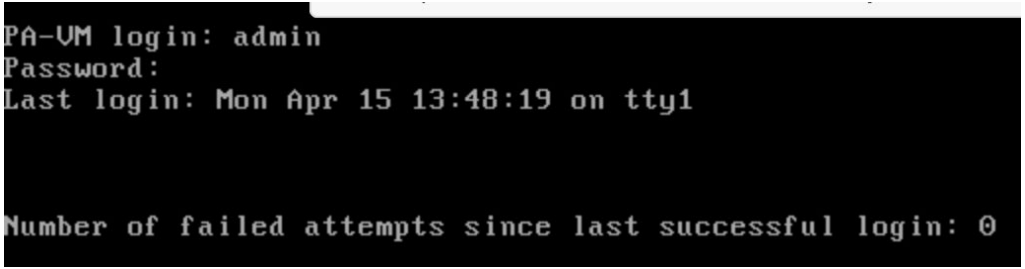
- After the Instance is created, on the right side click on ‘connect’



□	Instance ID/Name	Tags	Monitoring	Zone	IP Address	Status ▾	Network Type ▾	Configuration	Billing Method ▾	Actions
□	i-0xi40achw5z603nsclhk iZ0xi40achw5z603...			Virginia Zone A	192.168.0.51(Private)	Running	VPC	4 vCPU 16 GiB (I/O Optimized) ecs.sn2.large 0Mbps (Peak Value)	Pay-As-You-Go April 15, 2019, 00:40 Create	Manage | Connect Change Instance Type | More ▾

- Note: The VNC password is shown only once. Copy it somewhere.

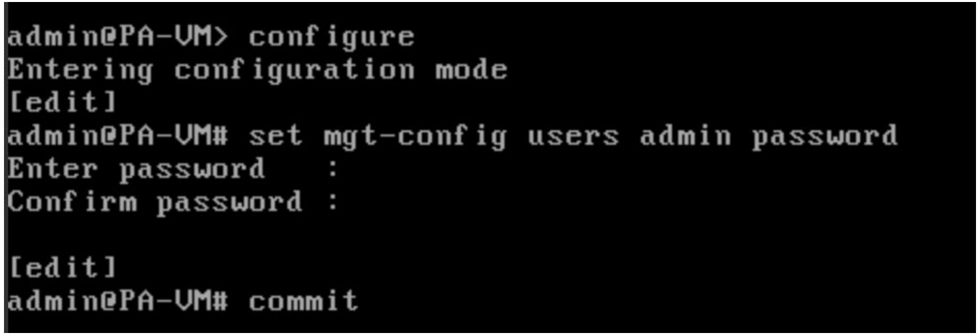
- Paste the VNC password to see the console. Then login with admin/admin



```
PA-VM login: admin
Password:
Last login: Mon Apr 15 13:48:19 on tty1


Number of failed attempts since last successful login: 0
```

Deploying VM-Series in Alibaba Cloud

- Immediately change the admin password



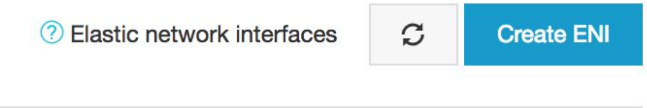
```
admin@PA-VM> configure
Entering configuration mode
[edit]
admin@PA-VM# set mgt-config users admin password
Enter password   :
Confirm password :

[edit]
admin@PA-VM# commit
```

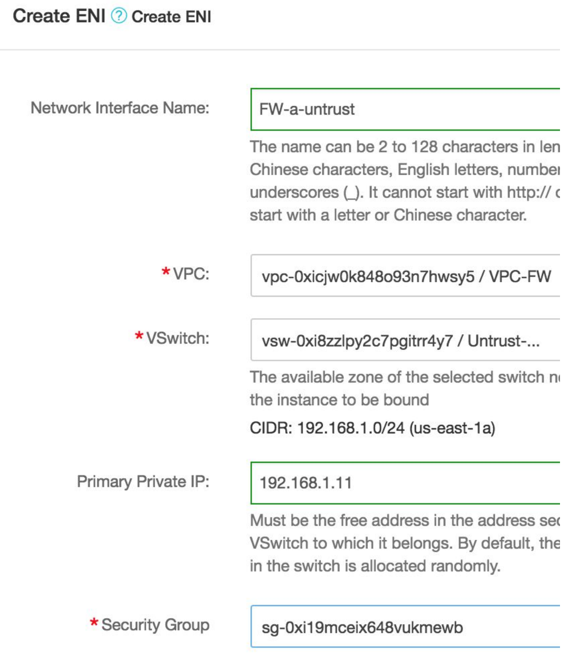
- DO NOT disable DPDK!

Deploying VM-Series in Alibaba Cloud

- Next we will create the untrust and trust ENIs and bind them to to FW-a. Make sure you shut down FW-a before doing the ENI creation/binding.

- Create an ENI for Untrust interface of FW-a in vSwitch=untrust-a





Create ENI ⓘ Create ENI

Network Interface Name: FW-a-untrust

The name can be 2 to 128 characters in len Chinese characters, English letters, numbe underscores (_). It cannot start with http:// c start with a letter or Chinese character.

*VPC: vpc-0xicjw0k848o93n7hwsy5 / VPC-FW

*VSwitch: vsw-0xi8zzlpy2c7pgitrr4y7 / Untrust-...

The available zone of the selected switch n the instance to be bound

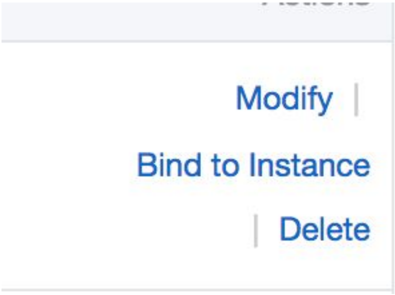
CIDR: 192.168.1.0/24 (us-east-1a)

Primary Private IP: 192.168.1.11

Must be the free address in the address se VSwitch to which it belongs. By default, the in the switch is allocated randomly.

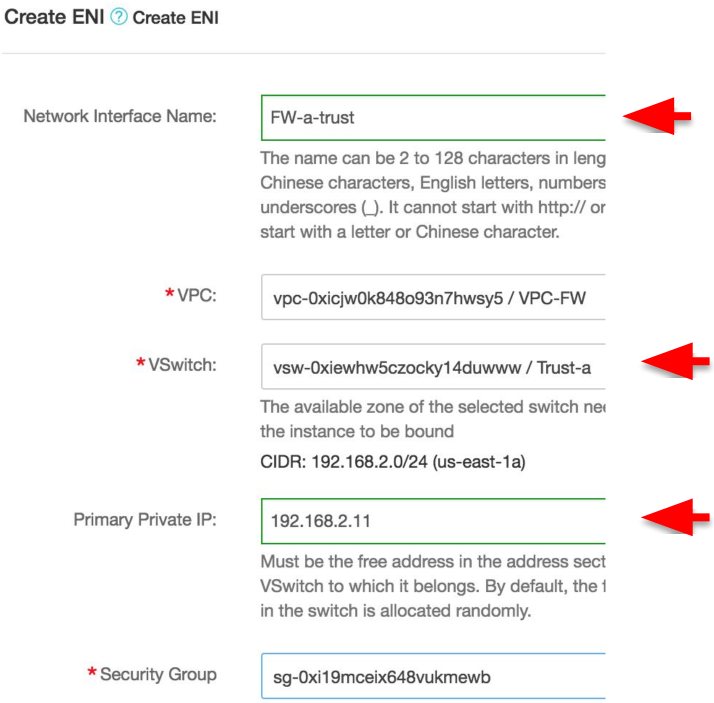
*Security Group sg-0xi19mceix648vukmewb

- Lastly bind this ENI to FW-1



Deploying VM-Series in Alibaba Cloud

- Similarly, create an ENI for Trust interface of FW-a in vSwitch=trust-a and bind it to FW-a

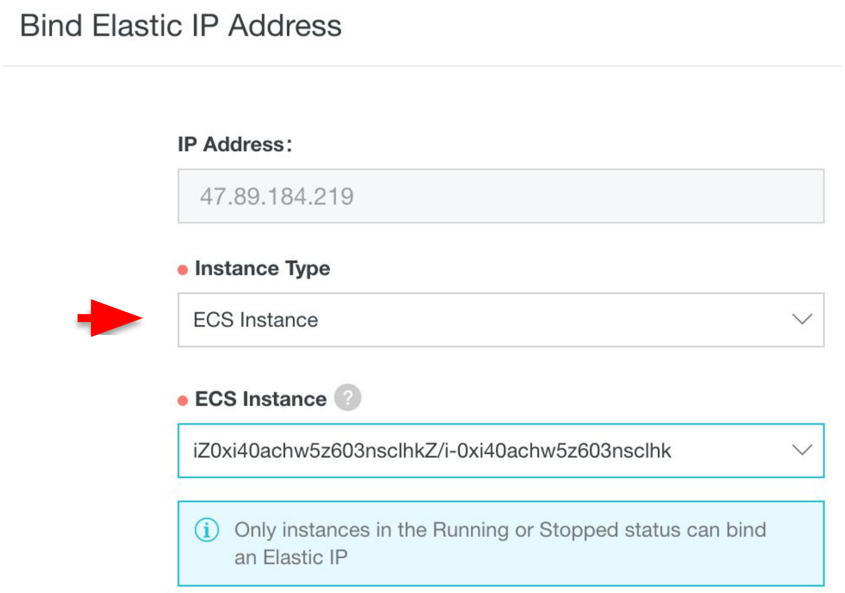


Create ENI Create ENI

Network Interface Name:	FW-a-trust The name can be 2 to 128 characters in leng Chinese characters, English letters, numbers underscores (_). It cannot start with http:// or start with a letter or Chinese character.
* VPC:	vpc-0xicjw0k848o93n7hwsy5 / VPC-FW
* VSwitch:	vsw-0xiewhw5czocky14duwww / Trust-a The available zone of the selected switch ne the instance to be bound CIDR: 192.168.2.0/24 (us-east-1a)
Primary Private IP:	192.168.2.11 Must be the free address in the address sect VSwitch to which it belongs. By default, the in the switch is allocated randomly.
* Security Group	sg-0xi19mceix648vukmewb

Deploying VM-Series in Alibaba Cloud

- Create an EIP for FW-a-mgmt and an EIP for FW-a-untrust
- Bind the first EIP to FW-a-mgmt (by ECS Instance) and bind the second EIP to FW-a-untrust (by secondary ENI)



Bind Elastic IP Address

IP Address:

47.89.184.219

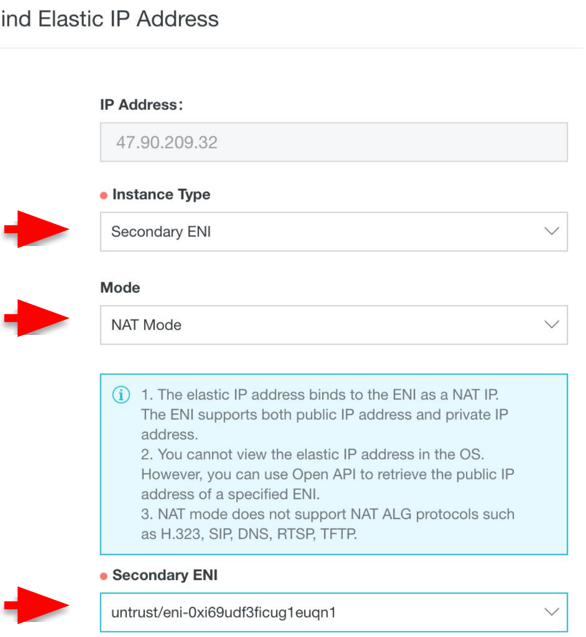
● Instance Type

ECS Instance

● ECS Instance

iZ0xi40achw5z603nsclhkZ/i-0xi40achw5z603nsclhk

Only instances in the Running or Stopped status can bind an Elastic IP



Bind Elastic IP Address

IP Address:

47.90.209.32

● Instance Type

Secondary ENI

Mode

NAT Mode

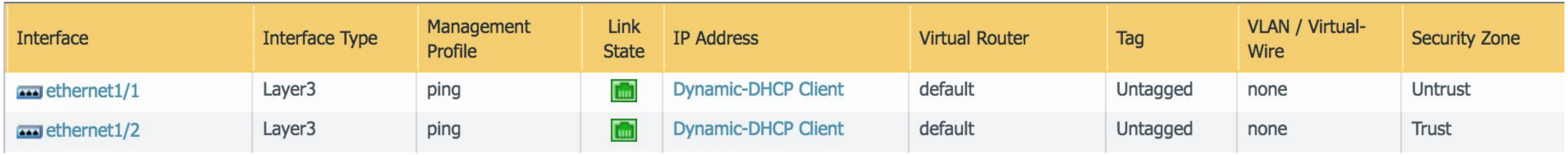
1. The elastic IP address binds to the ENI as a NAT IP. The ENI supports both public IP address and private IP address.
2. You cannot view the elastic IP address in the OS. However, you can use Open API to retrieve the public IP address of a specified ENI.
3. NAT mode does not support NAT ALG protocols such as H.323, SIP, DNS, RTSP, TFTP.

● Secondary ENI

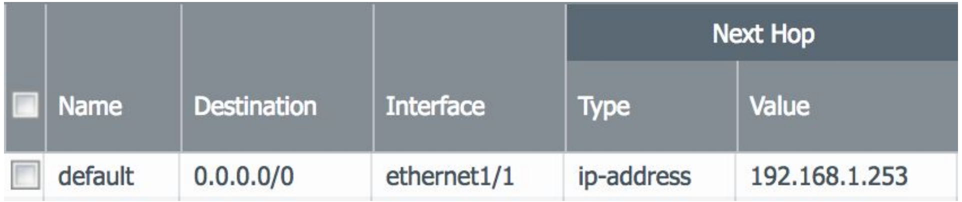
untrust/eni-0xi69udf3ficug1euqn1

Deploying VM-Series in Alibaba Cloud

- At this point, go ahead and start FW-a from Alibaba Cloud console so it recognizes the newly attached ENIs
- From your laptop, open a browser to the EIP you just assigned to FW-a-mgmt.
- Configure FW interfaces and a default route per below



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Layer3	ping	🟩	Dynamic-DHCP Client	default	Untagged	none	Untrust
ethernet1/2	Layer3	ping	🟩	Dynamic-DHCP Client	default	Untagged	none	Trust

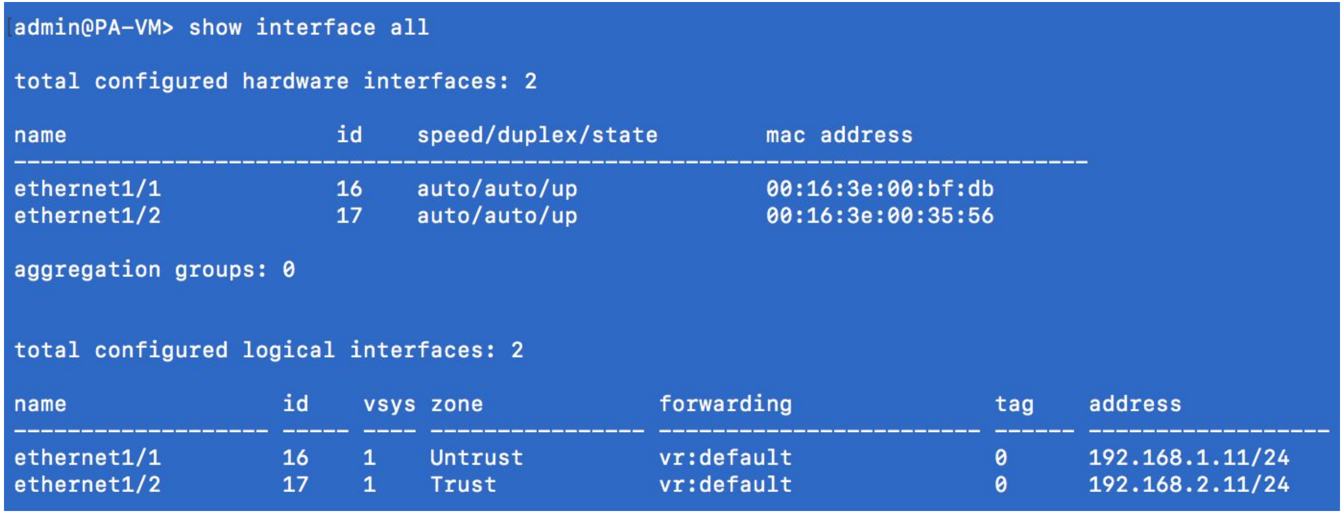


				Next Hop	
□	Name	Destination	Interface	Type	Value
□	default	0.0.0.0/0	ethernet1/1	ip-address	192.168.1.253

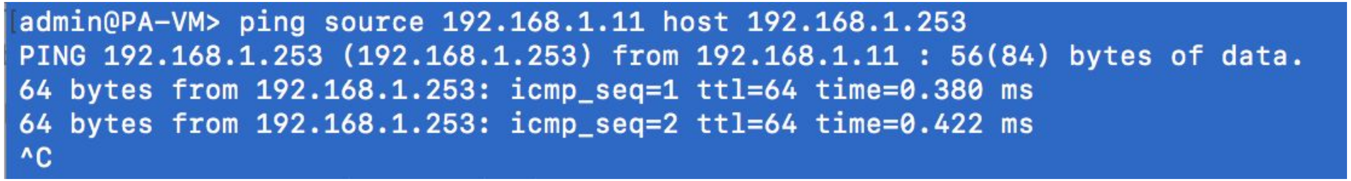
Default Gateway in an Alibaba Cloud subnet is always the broadcast IP of the subnet minus 2

Deploying VM-Series in Alibaba Cloud

- Make sure from untrust interface of FW-a you can ping to Internet before proceeding.
- Note: in Alibaba Cloud there is not concept of an IGW. Any VM with a public IP, can reach out to Internet.



```
admin@PA-VM> show interface all

total configured hardware interfaces: 2

name                    id    speed/duplex/state        mac address
--------------------------------------------------------------------------------
ethernet1/1             16    auto/auto/up              00:16:3e:00:bf:db
ethernet1/2             17    auto/auto/up              00:16:3e:00:35:56

aggregation groups: 0


total configured logical interfaces: 2

name                id     vsys zone             forwarding               tag    address
------------------- ------ ---- ---------------- ------------------------ ------ ------------------
ethernet1/1         16     1    Untrust          vr:default               0      192.168.1.11/24
ethernet1/2         17     1    Trust            vr:default               0      192.168.2.11/24
```

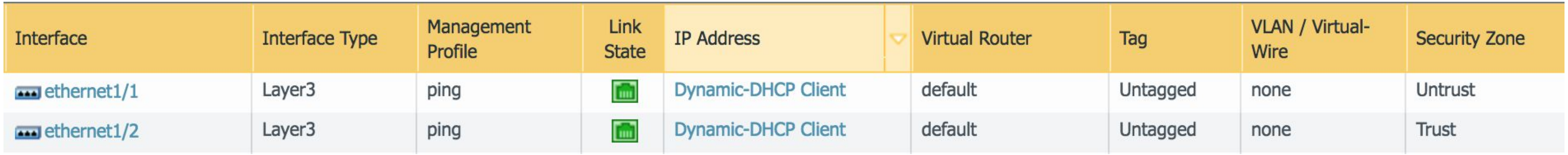


```
admin@PA-VM> ping source 192.168.1.11 host 192.168.1.253
PING 192.168.1.253 (192.168.1.253) from 192.168.1.11 : 56(84) bytes of data.
64 bytes from 192.168.1.253: icmp_seq=1 ttl=64 time=0.380 ms
64 bytes from 192.168.1.253: icmp_seq=2 ttl=64 time=0.422 ms
^C
```

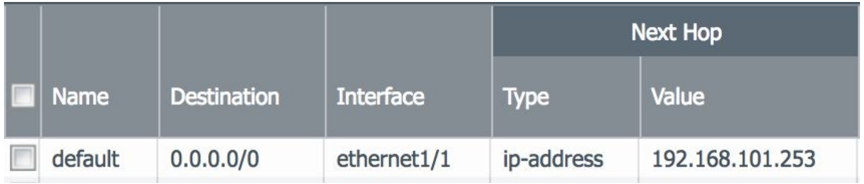
Deploying VM-Series in Alibaba Cloud

- Repeat the previous steps to create FW-b (in AZ-b) with interfaces in Mgmt-b, untrust-b and trust-b. Fw-b configuration should look like this.

- License both firewalls at this time



Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/1	Layer3	ping	🟩	Dynamic-DHCP Client	default	Untagged	none	Untrust
ethernet1/2	Layer3	ping	🟩	Dynamic-DHCP Client	default	Untagged	none	Trust

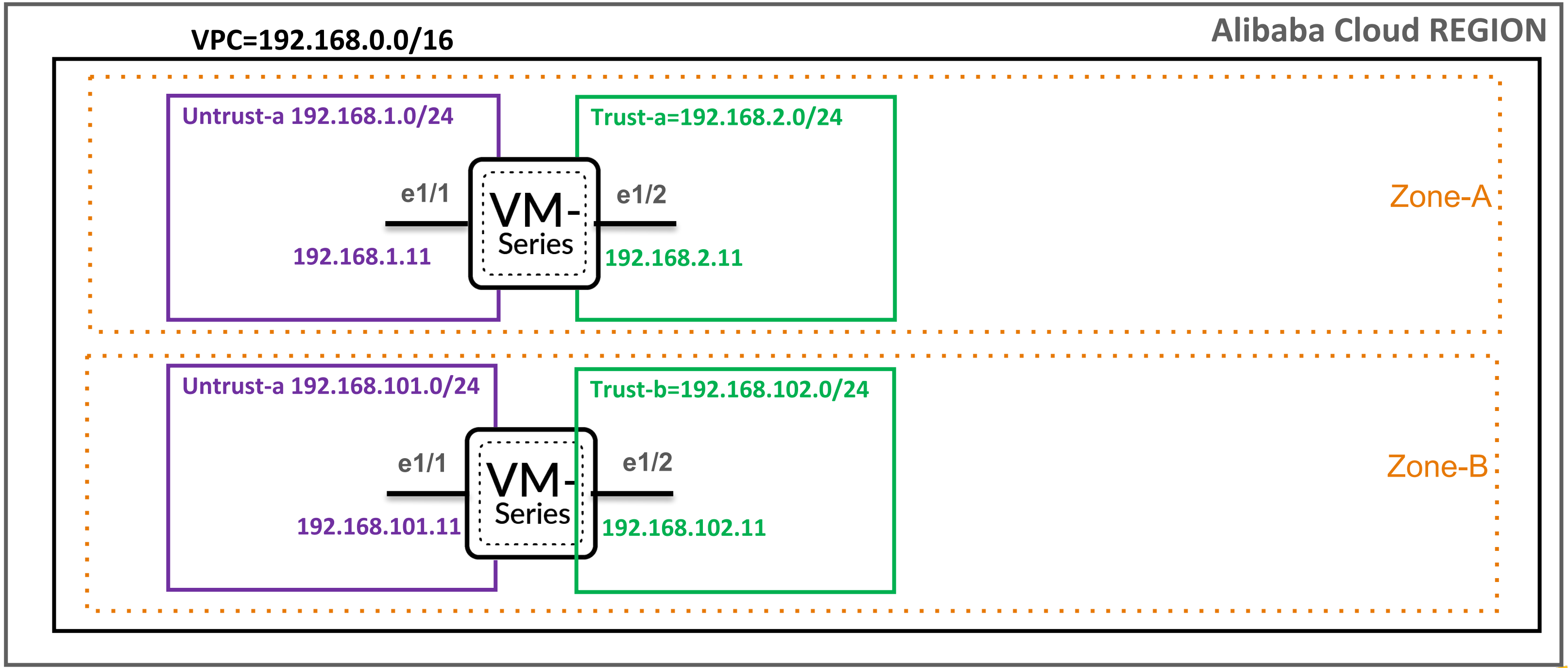


				Next Hop	
□	Name	Destination	Interface	Type	Value
□	default	0.0.0.0/0	ethernet1/1	ip-address	192.168.101.253

Default Gateway in an Alibaba Cloud subnet is always the broadcast IP of the subnet minus 2

Deploying VM-Series in Alibaba Cloud

- This is the base architecture we have built so far



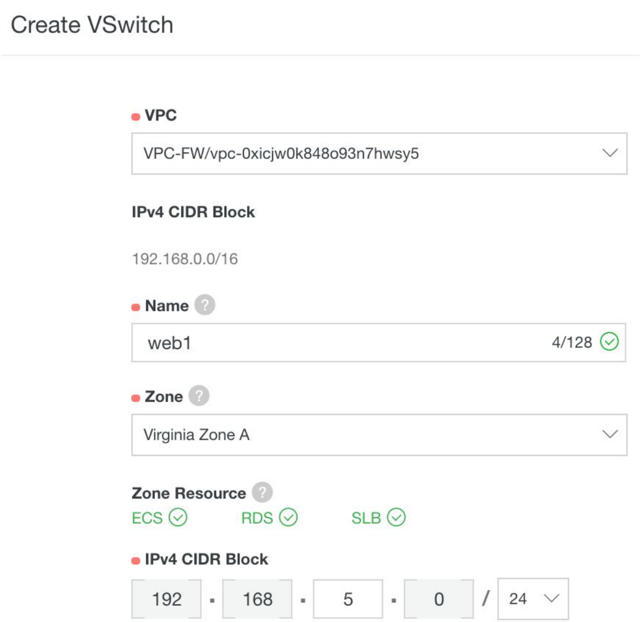
Deploying VM-Series in Alibaba Cloud

- Next, we will focus on creating:
  - Inbound flow architecture
  - Outbound flow architecture

- Note: In Alibaba Cloud you cannot hide the VPC route (you can not define a custom route more specific than the VPC route), which means that inside a VPC, you cannot steer the subnet-to-subnet traffic to a firewalls, thus East-West flow inside a VPC is not a use case!

Building Outbound flow architecture with HA

- We will create 2 subnets to host our web servers behind the firewall
  - web1=192.168.5.0/24 in Zone-A
  - web2=192.168.105.0/24 in Zone-b



Create VSwitch

VPC
VPC-FW/vpc-0xicjw0k848o93n7hwsy5

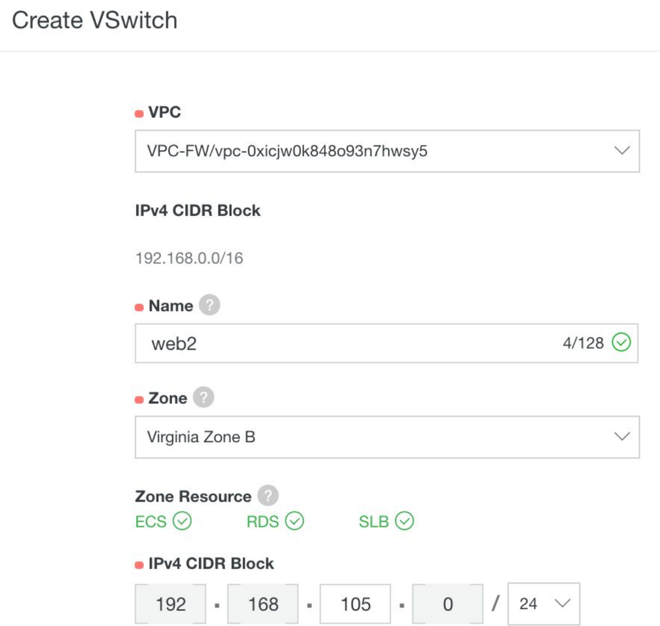
IPv4 CIDR Block
192.168.0.0/16

Name ?
web1 4/128 ✓

Zone ?
Virginia Zone A

Zone Resource ?
ECS ✓ RDS ✓ SLB ✓

IPv4 CIDR Block
192 . 168 . 5 . 0 / 24



Create VSwitch

VPC
VPC-FW/vpc-0xicjw0k848o93n7hwsy5

IPv4 CIDR Block
192.168.0.0/16

Name ?
web2 4/128 ✓

Zone ?
Virginia Zone B

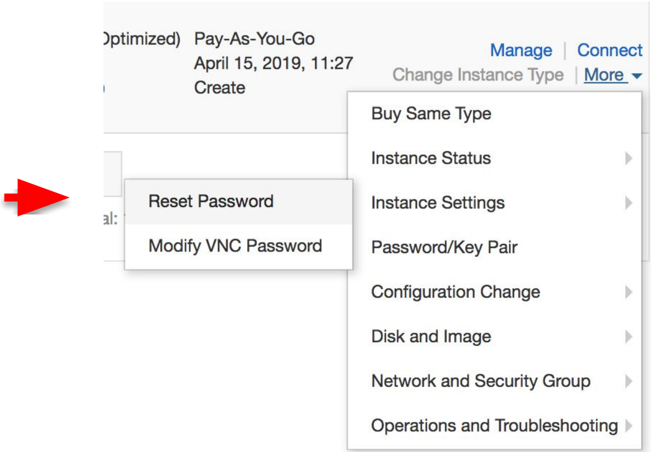
Zone Resource ?
ECS ✓ RDS ✓ SLB ✓

IPv4 CIDR Block
192 . 168 . 105 . 0 / 24

Building Outbound flow architecture with HA

- Create two VMs: ubuntu1 in web1 subnet and ubuntu2 in web2 subnet.

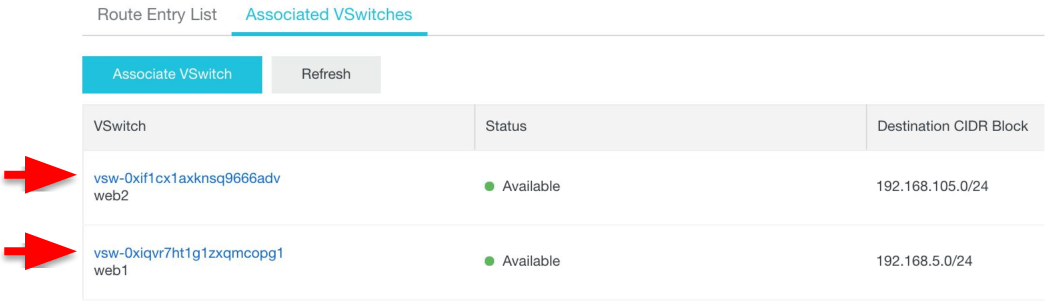
- Note: You can set the VM password at the time of creation, or if you forget, after VMs are created, click on more > reset password and place your desired password (reboot the instance to take effect)



- Next, from VNC, connect to the ubuntu VMs using user=root and the password you just set.

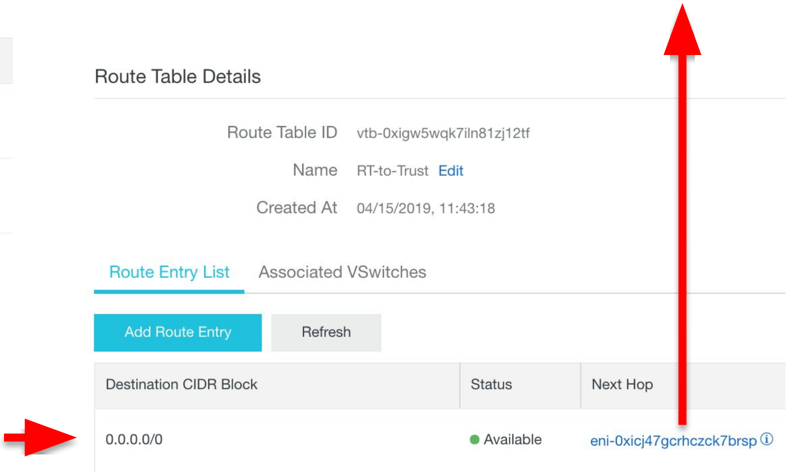
Building Outbound flow architecture with HA

- Create a RT called RT-to-Trust, associate it to web1 and web2 subnets and create the following route entry inside of it (default route to FW-a-trust ENI)



VSwitch	Status	Destination CIDR Block
vsw-0xif1cx1axknsq9666adv web2	● Available	192.168.105.0/24
vsw-0xiqvr7ht1g1zxqmcopg1 web1	● Available	192.168.5.0/24

N-H=FW1-trust-EIP


Route Table Details

Route Table ID vtb-0xigw5wqk7iln81zj12tf

Name RT-to-Trust Edit

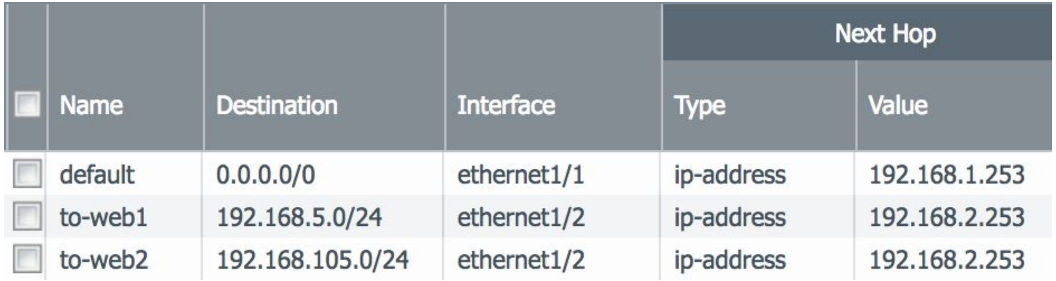
Created At 04/15/2019, 11:43:18

Destination CIDR Block	Status	Next Hop
0.0.0.0/0	● Available	eni-0xicj47gcrhczck7brsp ⓘ

Building Outbound flow architecture with HA

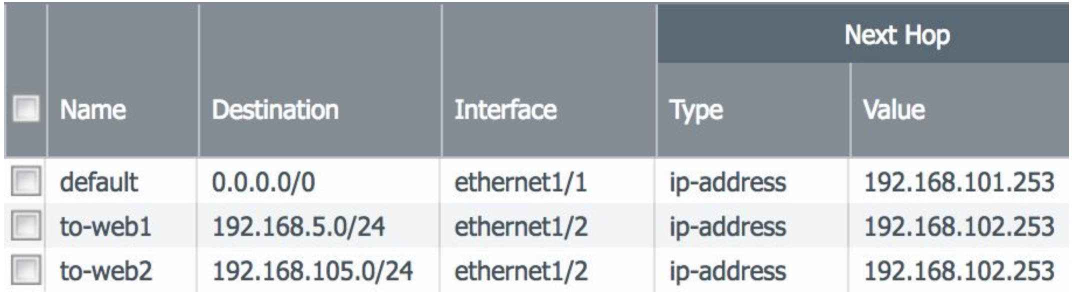
- On FW-a/FW-b define routes to get back to web1/web2 subnets

FW-a



				Next Hop	
□	Name	Destination	Interface	Type	Value
□	default	0.0.0.0/0	ethernet1/1	ip-address	192.168.1.253
□	to-web1	192.168.5.0/24	ethernet1/2	ip-address	192.168.2.253
□	to-web2	192.168.105.0/24	ethernet1/2	ip-address	192.168.2.253

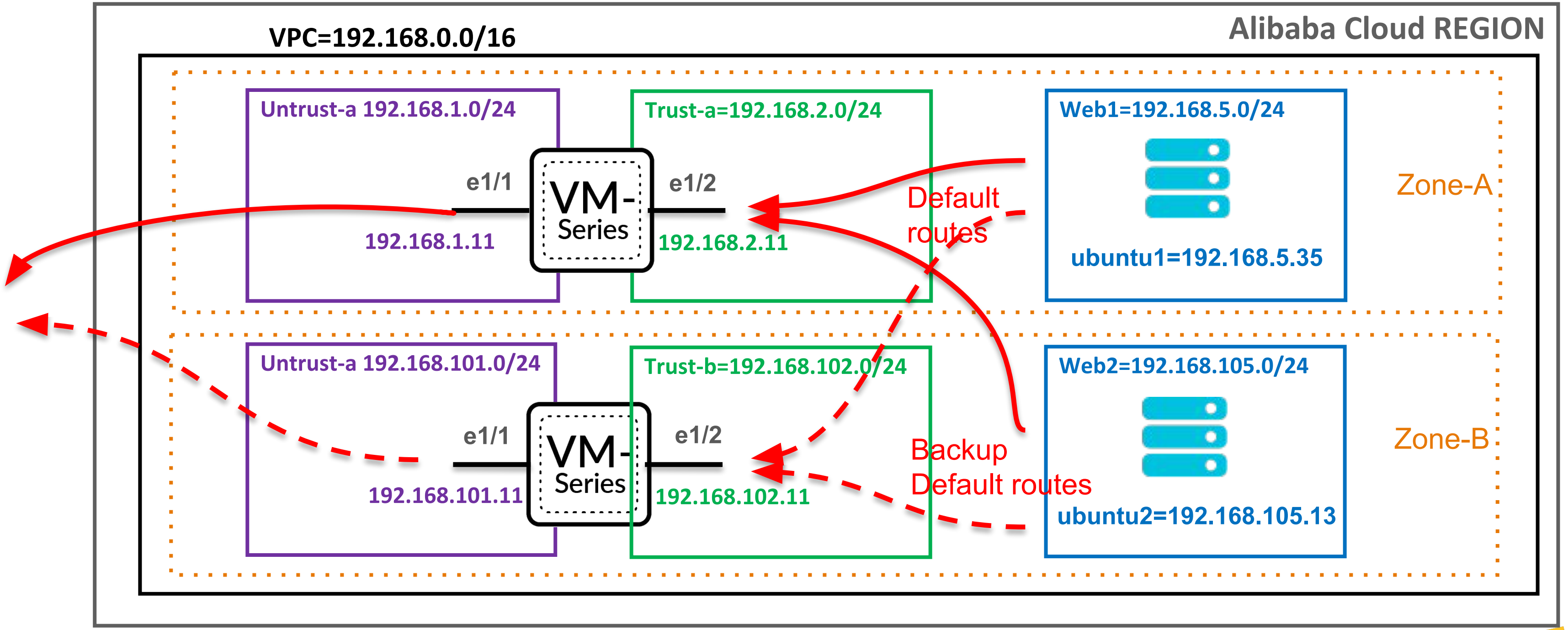
FW-b



				Next Hop	
□	Name	Destination	Interface	Type	Value
□	default	0.0.0.0/0	ethernet1/1	ip-address	192.168.101.253
□	to-web1	192.168.5.0/24	ethernet1/2	ip-address	192.168.102.253
□	to-web2	192.168.105.0/24	ethernet1/2	ip-address	192.168.102.253

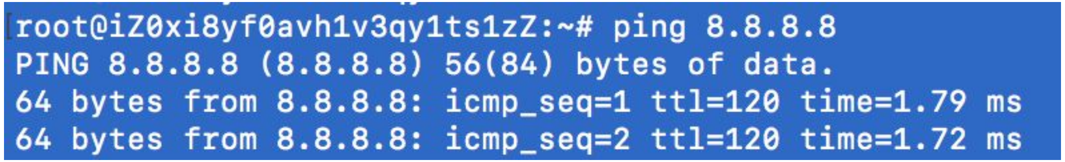
Building Outbound flow architecture with HA

- This is the base architecture we have built so far

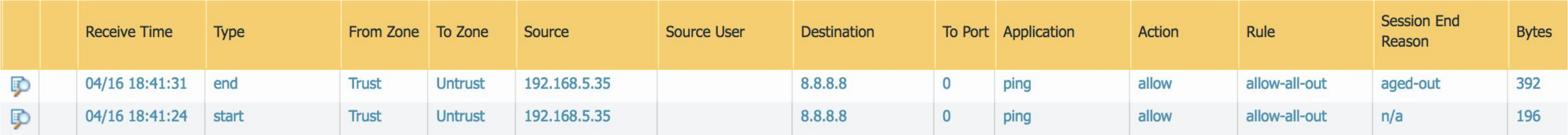


Building Outbound flow architecture with HA

- From console VNC (or by SSHing from FW-a as a jumpbox), connect to ubuntu1 and verify that you can reach out to Internet through FW-a and that you can see the sessions on FW-a



```
root@iZ0xi8yf0avh1v3qy1ts1zZ:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=120 time=1.79 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=120 time=1.72 ms
```



		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
		04/16 18:41:31	end	Trust	Untrust	192.168.5.35		8.8.8.8	0	ping	allow	allow-all-out	aged-out	392
		04/16 18:41:24	start	Trust	Untrust	192.168.5.35		8.8.8.8	0	ping	allow	allow-all-out	n/a	196

ubuntu1

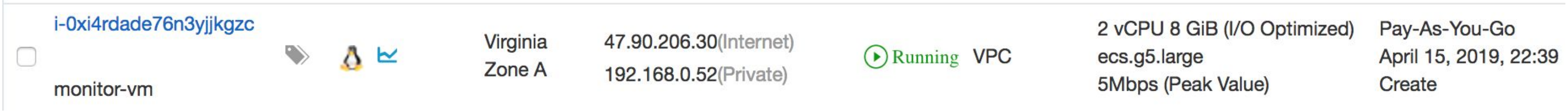
Building Outbound flow architecture with HA

- Right now, all outbound traffic from web1/web2 subnets is routed through FW-a. If FW-a goes down, outbound traffic will be blackholed.

- In order to address this issue and have a highly available setup for outbound traffic, we will use a bash ha-script that will be running on a monitoring VM that will monitor the health of firewalls and make API calls to change the route between FW-a and FW-b if needed. **Note: ha-script is NOT officially supported by Palo Alto Networks. Please use or modify it at your own discretion and after sufficient testing..**

- For this setup, first spin up a monitor-vm in a publicly accessible subnet in your VPC. It also needa. apublic IP assigned to it. The reason is that the API calls from this monitor-vm needs to publicly routed over Internet.

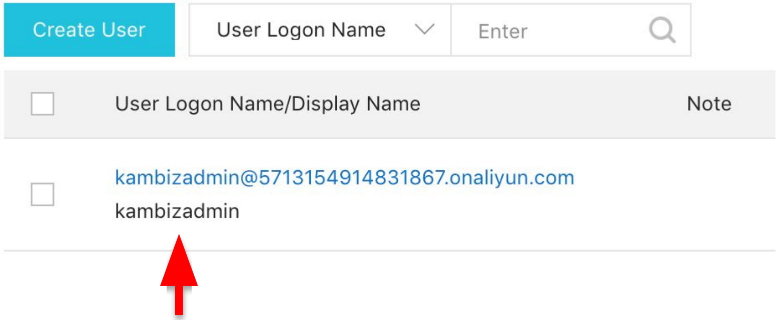
- In my case, I spun up the monitor-cm in Mgmt-a subnet.



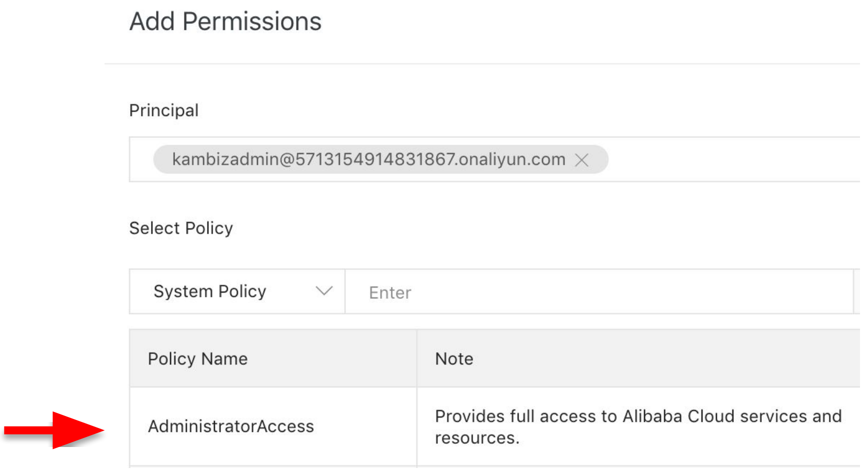
□	i-0xi4rdade76n3yjjkgzc
	monitor-vm
		Virginia
		Zone A
			47.90.206.30(Internet)
			192.168.0.52(Private)
				Running	VPC	2 vCPU 8 GiB (I/O Optimized)
						ecs.g5.large
						5Mbps (Peak Value)
							Pay-As-You-Go
							April 15, 2019, 22:39
							Create

Building Outbound flow architecture with HA

- From your laptop, SSH into the monitor-vm and install aliyun CLI. Instructions can be found here:
- https://www.alibabacloud.com/help/doc-detail/90765.htm
- Next, on Alibaba Cloud console, create a user and give them “AdministratorAccess” permission.



□	User Logon Name/Display Name	Note
□	kambizadmin@5713154914831867.onaliyun.com kambizadmin	



Add Permissions

Principal

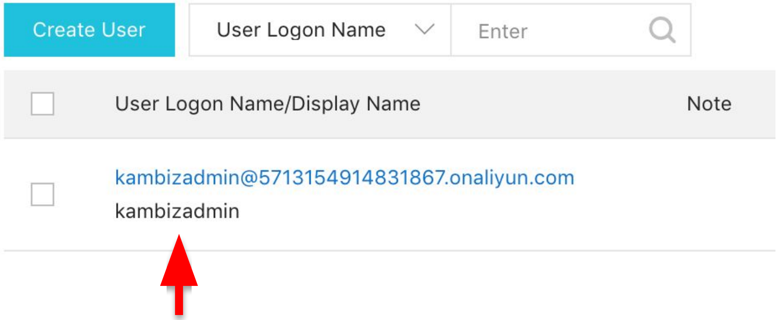
kambizadmin@5713154914831867.onaliyun.com ×

Select Policy

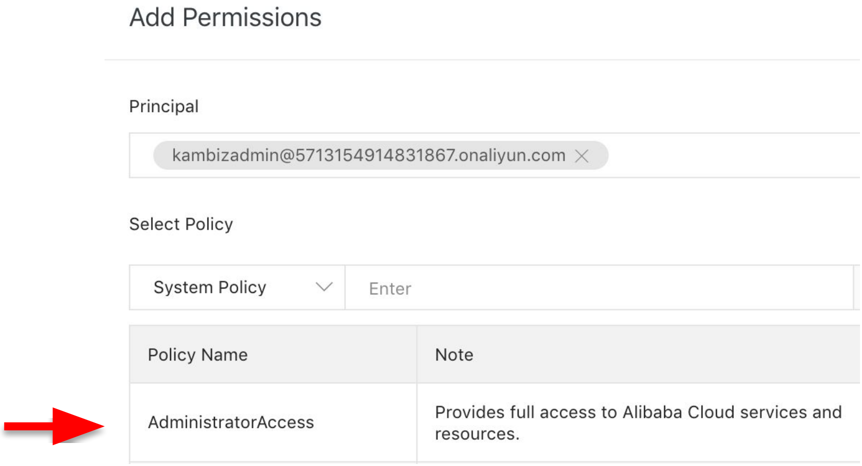
Policy Name	Note
AdministratorAccess	Provides full access to Alibaba Cloud services and resources.

Building Outbound flow architecture with HA

- From your laptop, SSH into the monitor-vm and install aliyun CLI. Instructions can be found here:
- https://www.alibabacloud.com/help/doc-detail/90765.htm
- Next, on Alibaba Cloud console, create a user and give them “AdministratorAccess” permission.



□	User Logon Name/Display Name	Note
□	kambizadmin@5713154914831867.onaliyun.com kambizadmin	


Add Permissions

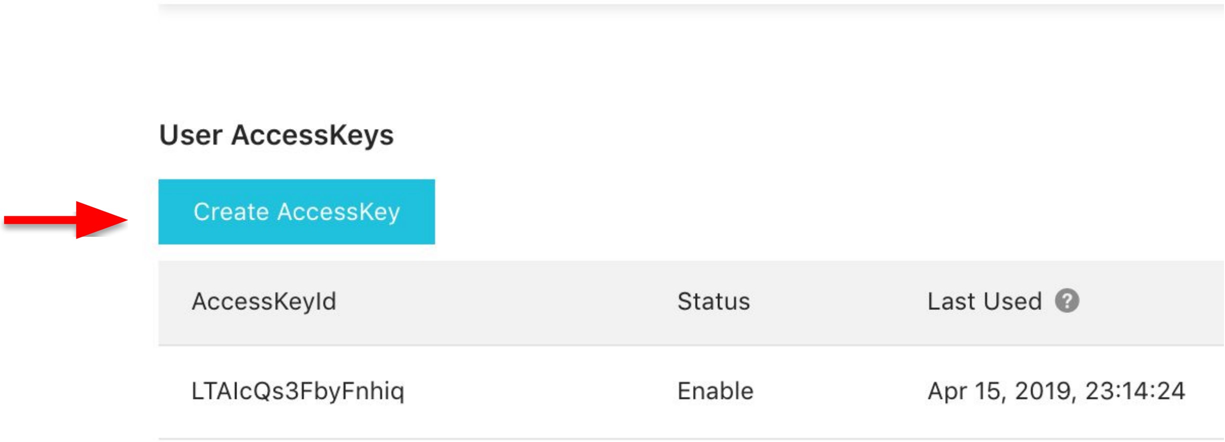
Principal: kambizadmin@5713154914831867.onaliyun.com

Select Policy

Policy Name	Note
AdministratorAccess	Provides full access to Alibaba Cloud services and resources.

Building Outbound flow architecture with HA

- Lastly, create an Access Key for this user and download the CSV file. You’ll need the to set up your aliyun on the monitor-vm

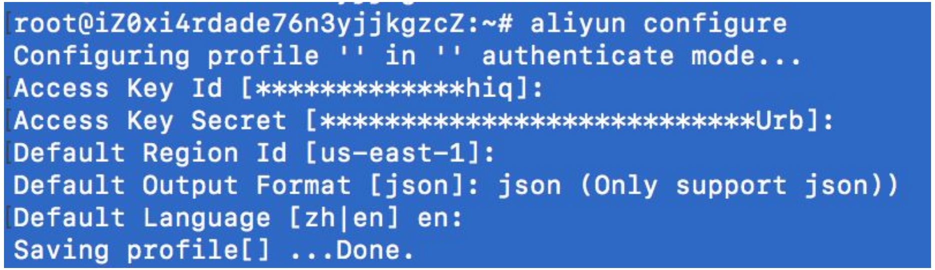


User AccessKeys

AccessKeyId	Status	Last Used ?
LTAIcQs3FbyFnhiq	Enable	Apr 15, 2019, 23:14:24

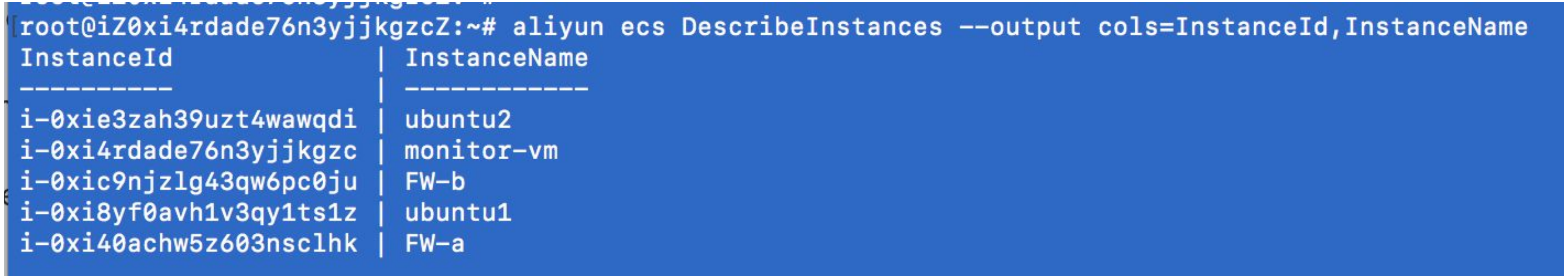
Building Outbound flow architecture with HA

- On the monitor-vm, set up your aliyun configuration.



```
root@iZ0xi4rdade76n3yjjkgzcZ:~# aliyun configure
Configuring profile '' in '' authenticate mode...
Access Key Id [*************hiq]:
Access Key Secret [***************************Urb]:
Default Region Id [us-east-1]:
Default Output Format [json]: json (Only support json))
Default Language [zh|en] en:
Saving profile[] ...Done.
```

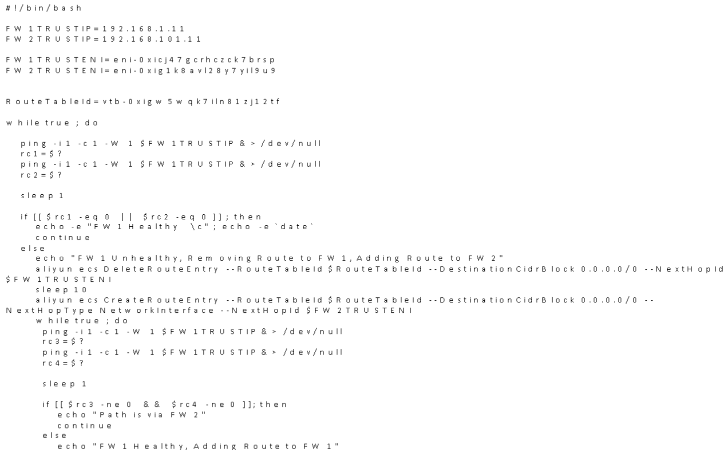
- Issue a command to make sure the monitor-vm can access Alibaba Cloud and make API calls.



```
root@iZ0xi4rdade76n3yjjkgzcZ:~# aliyun ecs DescribeInstances --output cols=InstanceId,InstanceName
InstanceId             | InstanceName
----------             | ------------
i-0xie3zah39uzt4wawqdi | ubuntu2
i-0xi4rdade76n3yjjkgzc | monitor-vm
i-0xic9njzlg43qw6pc0ju | FW-b
i-0xi8yf0avh1v3qy1ts1z | ubuntu1
i-0xi40achw5z603nsclhk | FW-a
```

Building Outbound flow architecture with HA

- ha-script can be found here(double click to open)



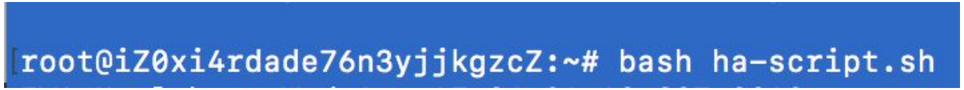
```
#!/bin/bash

FW1TRUSTIP=192.168.1.11
FW2TRUSTIP=192.168.101.11

FW1TRUSTENI=eni-0xicj47gcrhczck7brsp
FW2TRUSTENI=eni-0xig1k8avl28y7yil9u9


RouteTableId=vtb-0xigw5wqk7iln81zj12tf

while true ; do

  ping -i1 -c1 -W 1 $FW1TRUSTIP &> /dev/null
  rc1=$?
  ping -i1 -c1 -W 1 $FW1TRUSTIP &> /dev/null
  rc2=$?

  sleep 1

  if [[ $rc1 -eq 0 || $rc2 -eq 0 ]]; then
    echo -e "FW1 Healthy \c"; echo -e `date`
    continue
  else
    echo "FW1 Unhealthy, Removing Route to FW1, Adding Route to FW2"
    aliyun ecs DeleteRouteEntry --RouteTableId $RouteTableId --DestinationCidrBlock 0.0.0.0/0 --NextHopId
$FW1TRUSTENI
    sleep 10
    aliyun ecs CreateRouteEntry --RouteTableId $RouteTableId --DestinationCidrBlock 0.0.0.0/0 --
NextHopType NetworkInterface --NextHopId $FW2TRUSTENI
    while true ; do
     ping -i1 -c1 -W 1 $FW1TRUSTIP &> /dev/null
     rc3=$?
     ping -i1 -c1 -W 1 $FW1TRUSTIP &> /dev/null
     rc4=$?

     sleep 1

     if [[ $rc3 -ne 0 && $rc4 -ne 0 ]]; then
       echo "Path is via FW2"
       continue
     else
       echo "FW1 Healthy, Adding Route to FW1"
```

- In the ha-script provided, adjust your variables such as FW-a/FW-b ENIs, the web RouteTableId and FW-a/FW-b trust interface IP and then run the script.

Building Outbound flow architecture with HA

- ha-script can be found here(double click to open)

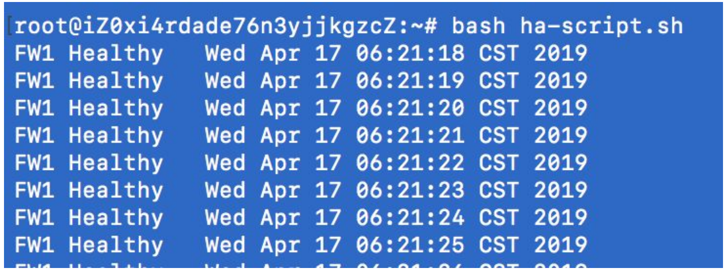
- In the ha-script provided, adjust your variables such as FW-a/FW-b ENIs, the web RouteTableId and FW-a/FW-b trust interface IP and then run the script (on the monitor-vm)



```
[root@iZ0xi4rdade76n3yjjkgzcZ:~# bash ha-script.sh
```

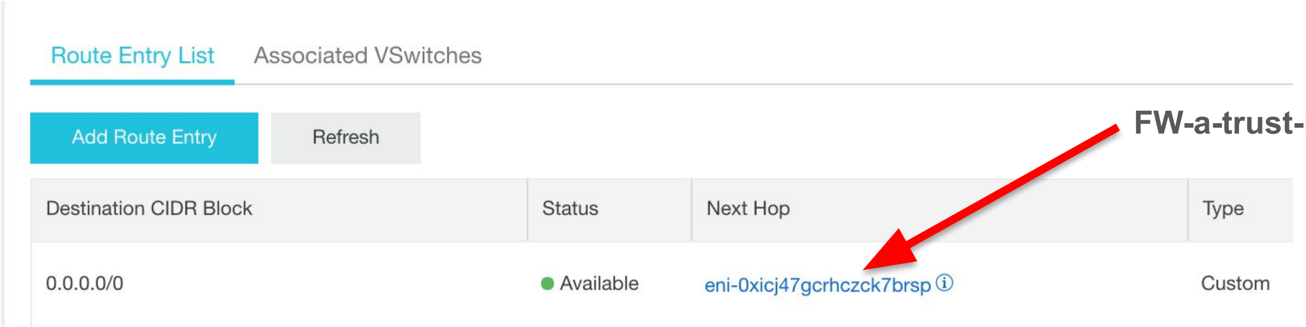
Building Outbound flow architecture with HA

- Below is the output of script when FW-a is healthy.



```
root@iZ0xi4rdade76n3yjjkgzcZ:~# bash ha-script.sh
FW1 Healthy   Wed Apr 17 06:21:18 CST 2019
FW1 Healthy   Wed Apr 17 06:21:19 CST 2019
FW1 Healthy   Wed Apr 17 06:21:20 CST 2019
FW1 Healthy   Wed Apr 17 06:21:21 CST 2019
FW1 Healthy   Wed Apr 17 06:21:22 CST 2019
FW1 Healthy   Wed Apr 17 06:21:23 CST 2019
FW1 Healthy   Wed Apr 17 06:21:24 CST 2019
FW1 Healthy   Wed Apr 17 06:21:25 CST 2019
```

- And the RT of web1 subnet points to FW-a-trust-ENI

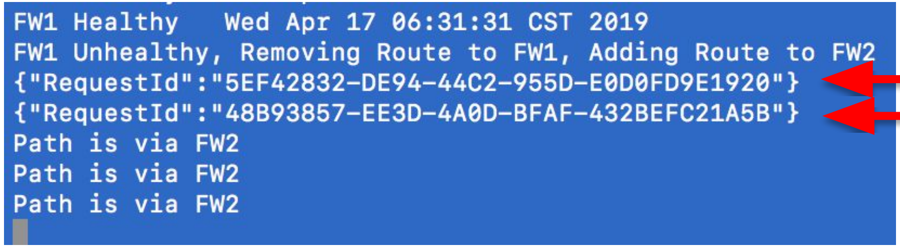


Destination CIDR Block	Status	Next Hop	Type
0.0.0.0/0	● Available	eni-0xicj47gcrhczck7brsp ⓘ	Custom

FW-a-trust-ENI

Building Outbound flow architecture with HA

- If FW-a is rebooted or crashes, the script will remove the route in web1 subnet to FW-a-trust-ENI and add the route to FW-b-trust-ENI

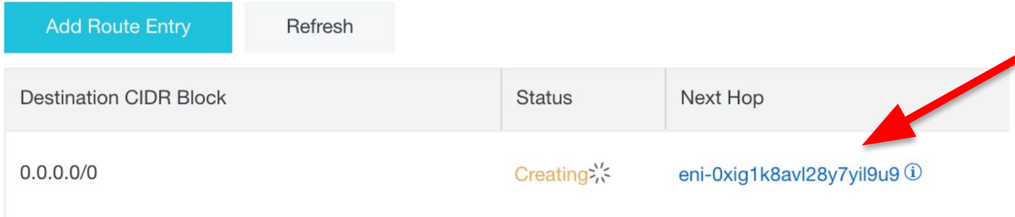


```
FW1 Healthy   Wed Apr 17 06:31:31 CST 2019
FW1 Unhealthy, Removing Route to FW1, Adding Route to FW2
{"RequestId":"5EF42832-DE94-44C2-955D-E0D0FD9E1920"}
{"RequestId":"48B93857-EE3D-4A0D-BFAF-432BEFC21A5B"}
Path is via FW2
Path is via FW2
Path is via FW2
```

Remove the route to **FW-a-trust-ENI**
Add the route to **FW-b-trust-ENI**

- Packet loss happens for around 20 seconds.

- You can verify that web1 subnet route has changed to FW-b-trust ENI

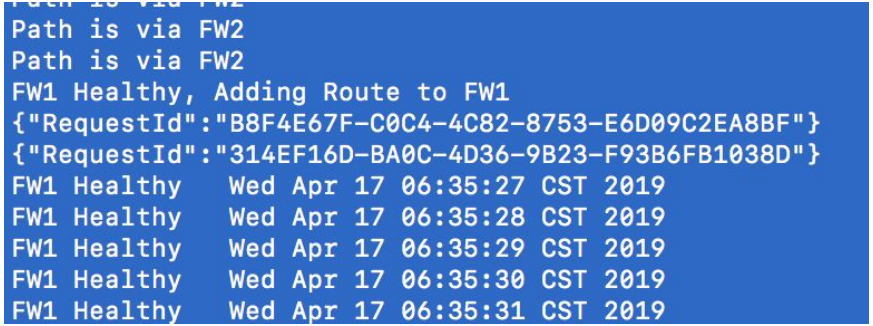


Destination CIDR Block	Status	Next Hop
0.0.0.0/0	Creating	eni-0xig1k8avl28y7yil9u9 ⓘ

FW-b-trust-ENI

Building Outbound flow architecture with HA

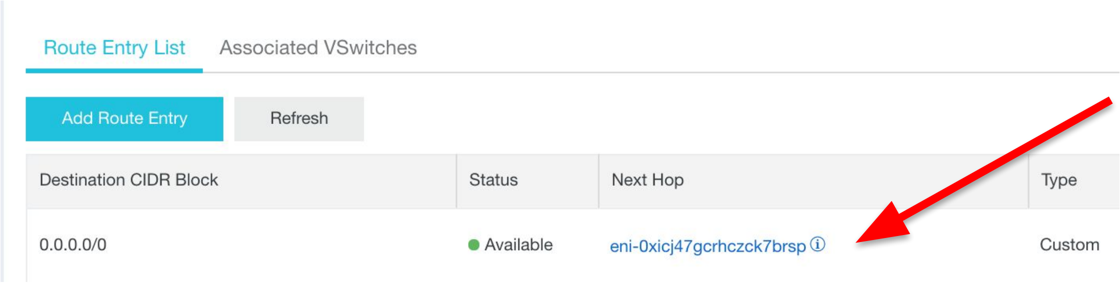
- When FW-a becomes available again, ha-script moves the route back to FW-a



```
Path is via FW2
Path is via FW2
FW1 Healthy, Adding Route to FW1
{"RequestId":"B8F4E67F-C0C4-4C82-8753-E6D09C2EA8BF"}
{"RequestId":"314EF16D-BA0C-4D36-9B23-F93B6FB1038D"}
FW1 Healthy   Wed Apr 17 06:35:27 CST 2019
FW1 Healthy   Wed Apr 17 06:35:28 CST 2019
FW1 Healthy   Wed Apr 17 06:35:29 CST 2019
FW1 Healthy   Wed Apr 17 06:35:30 CST 2019
FW1 Healthy   Wed Apr 17 06:35:31 CST 2019
```

Remove the route to **FW-b-trust-ENI**
Add the route to **FW-a-trust-ENI**

- Verify that route has changed back to FW-a-trust-ENI



Destination CIDR Block	Status	Next Hop	Type
0.0.0.0/0	● Available	eni-0xicj47gcrhczck7brsp ⓘ	Custom

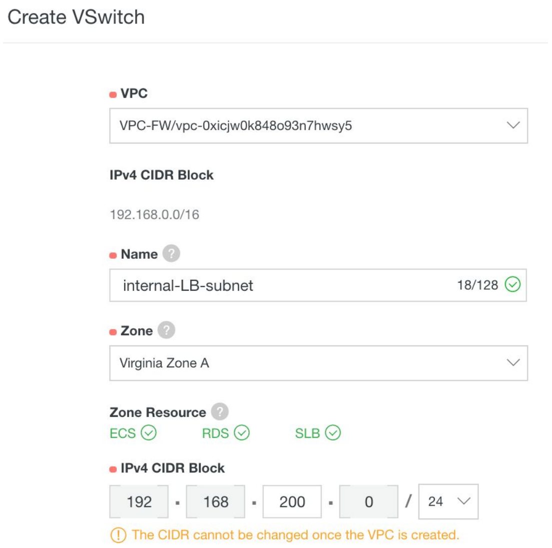
FW-a-trust-ENI

Building Outbound flow architecture with HA

- This concludes the use case for outbound use case in a single VPC.
- Next we turn our focus to building the Inbound use case in a single VPC.

Building Inbound flow architecture – LB Sandwich

- For Inbound use case, we use our traditional LB-Sandwich design. We will create a Public-LB that has the Firewalls in the backend and an internal-LB that has ubuntu1/ubuntu2 in the backend.
- The internal-LB need its own subnet (vSwitch), so let's create it first. This interna-LB-subnet=192.168.200.0/24 can sit in either of Zones. Here we create it in Zone-A



Create VSwitch

VPC
VPC-FW/vpc-0xicjw0k848o93n7hwsy5

IPv4 CIDR Block
192.168.0.0/16

Name
internal-LB-subnet 18/128

Zone
Virginia Zone A

Zone Resource
ECS ✓ RDS ✓ SLB ✓

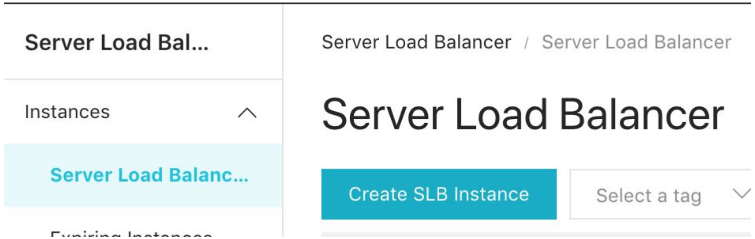
IPv4 CIDR Block
192 . 168 . 200 . 0 / 24

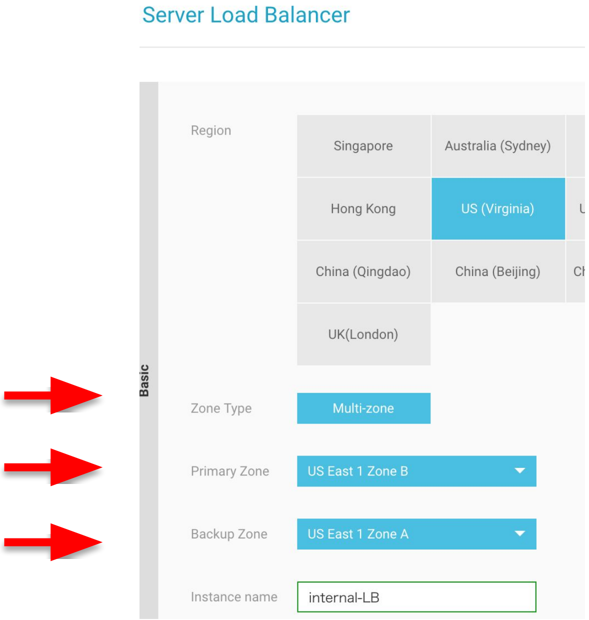
ⓘ The CIDR cannot be changed once the VPC is created.

Building Inbound flow architecture – LB Sandwich

- Now navigate to SLB and create an internal-LB in your Region (all LBs in Alibaba Cloud are Regional) that will have ubuntu1 and ubuntu2 in its backend

- Choose multi-zone and select Zone-A and Zone-B




Server Load Balancer

Basic

Region: US (Virginia)

Zone Type: Multi-zone

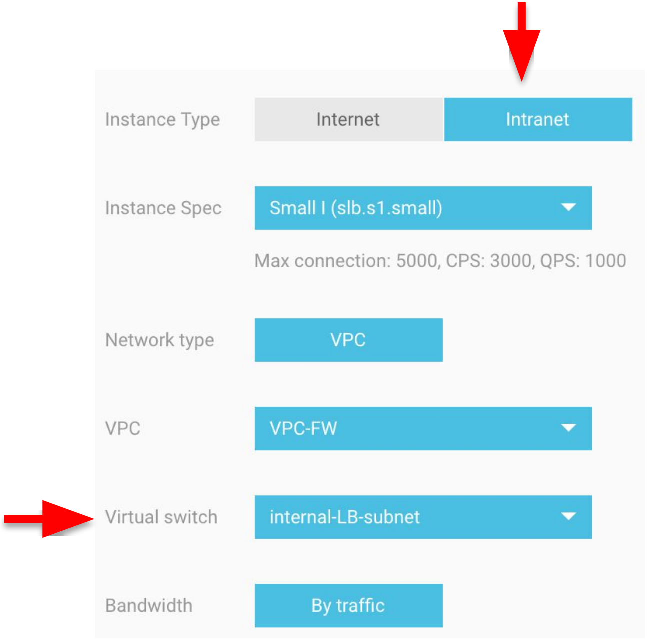
Primary Zone: US East 1 Zone B

Backup Zone: US East 1 Zone A

Instance name: internal-LB

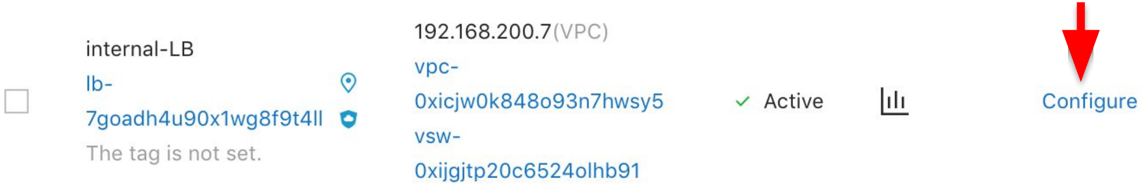
Building Inbound flow architecture – LB Sandwich

- Choose Type=Intranet (internal LB)
- Choose the internal-LB-subnet that we just created.



Instance Type	Internet / **Intranet**
Instance Spec	Small I (slb.s1.small) Max connection: 5000, CPS: 3000, QPS: 1000
Network type	VPC
VPC	VPC-FW
Virtual switch	internal-LB-subnet
Bandwidth	By traffic

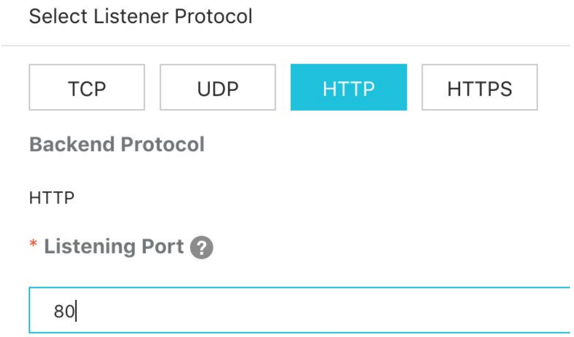
- internal-LB gets created. Click on Configure to set up the LB



□	internal-LB lb-7goadh4u90x1wg8f9t4ll The tag is not set.	192.168.200.7(VPC) vpc-0xicjw0k848o93n7hwsy5 vsw-0xijgjtp20c6524olhb91	✓ Active		Configure

Building Inbound flow architecture – LB Sandwich

- Listener = HTTP-80
- Note: If you're hosting web apps, choose HTTP listeners for both internal-LB and Public-LB. I had issues with TCP Loadbalancers on port 80



Select Listener Protocol

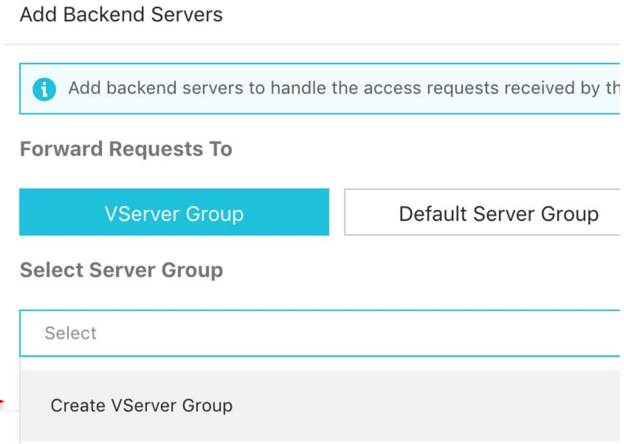
TCP | UDP | **HTTP** | HTTPS

Backend Protocol

HTTP

* Listening Port ?

80



Add Backend Servers

Add backend servers to handle the access requests received by th

Forward Requests To

VServer Group | Default Server Group

Select Server Group

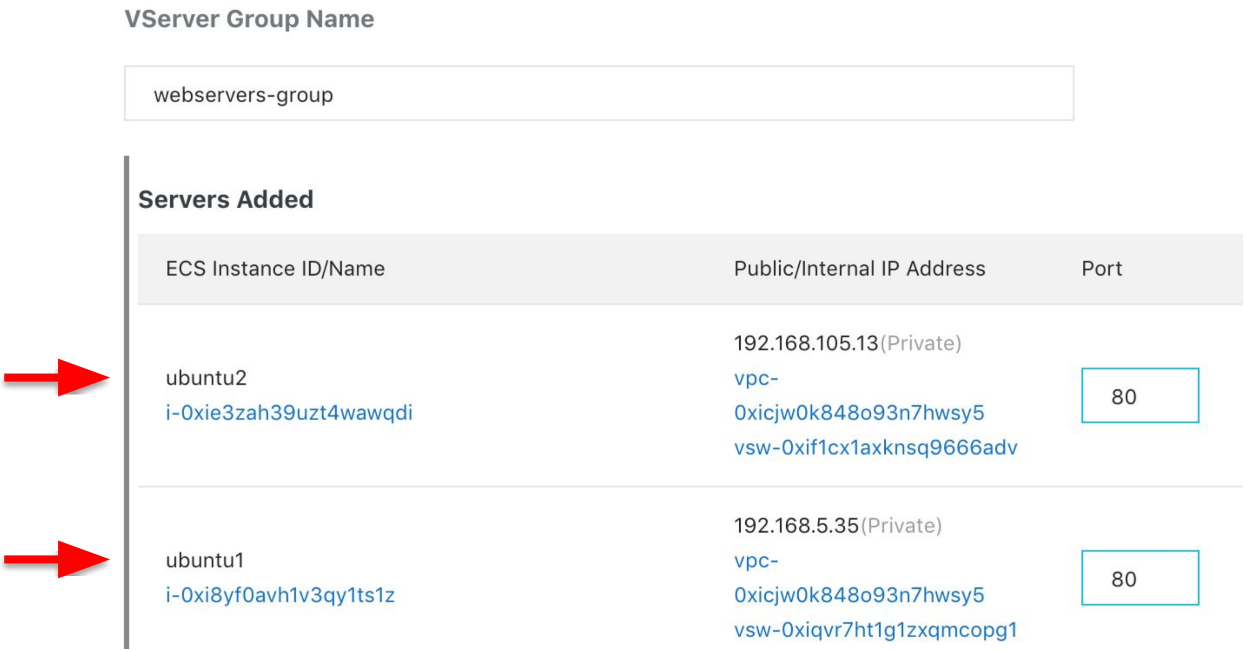
Select

Create VServer Group

- For backend, choose to create a 'VServer Group'

Building Inbound flow architecture – LB Sandwich

- Add ubuntu1 and ubuntu2 to the VServer Group. Choose TCP-80 (This is the ports web servers expect the traffic on)



VServer Group Name

webservers-group

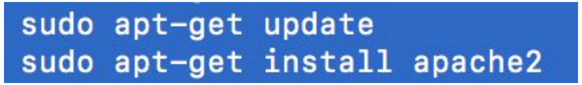
Servers Added

ECS Instance ID/Name	Public/Internal IP Address	Port
ubuntu2 i-0xie3zah39uzt4wawqdi	192.168.105.13(Private) vpc- 0xicjw0k848o93n7hwsy5 vsw-0xif1cx1axknsq9666adv	80
ubuntu1 i-0xi8yf0avh1v3qy1ts1z	192.168.5.35(Private) vpc- 0xicjw0k848o93n7hwsy5 vsw-0xiqvr7ht1g1zxqmcopg1	80

Building Inbound flow architecture – LB Sandwich

- Finish creating the internal-LB.

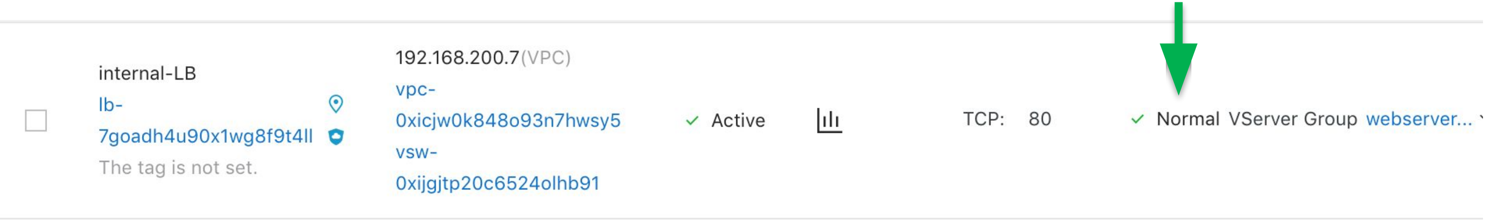
- Now, through your monitor-vm or through one of the firewalls (as a jumpbox), SSH into ubuntu1 and ubuntu2 and bring up apache2 (repeat these steps on both ubuntu servers).



```
sudo apt-get update
sudo apt-get install apache2
```

- Before you continue, make sure from your monitor-vm you can ‘curl’ into ubuntu1 and ubuntu2

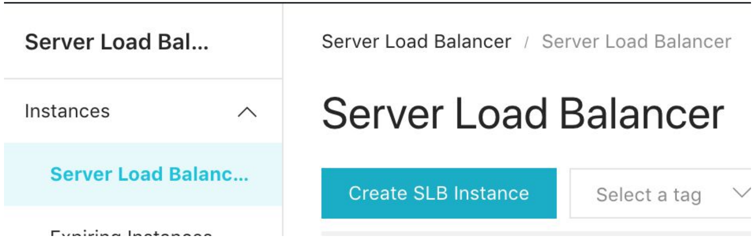
- After 30 seconds or so, the backend for internal-LB should show healthy (normal)



□	internal-LB lb-7goadh4u90x1wg8f9t4ll The tag is not set.	192.168.200.7(VPC) vpc-0xicjw0k848o93n7hwsy5 vsw-0xijgjtp20c6524olhb91	✓ Active		TCP: 80	✓ Normal VServer Group webserver...

Building Inbound flow architecture – LB Sandwich

- Now, navigate to SLB again and create a Public-LB in your Region (all LBs in Alibaba Cloud are Regional)
- Choose multi-zone and select Zone-A and Zone-B



Server Load Bal...

Instances

Server Load Balanc...

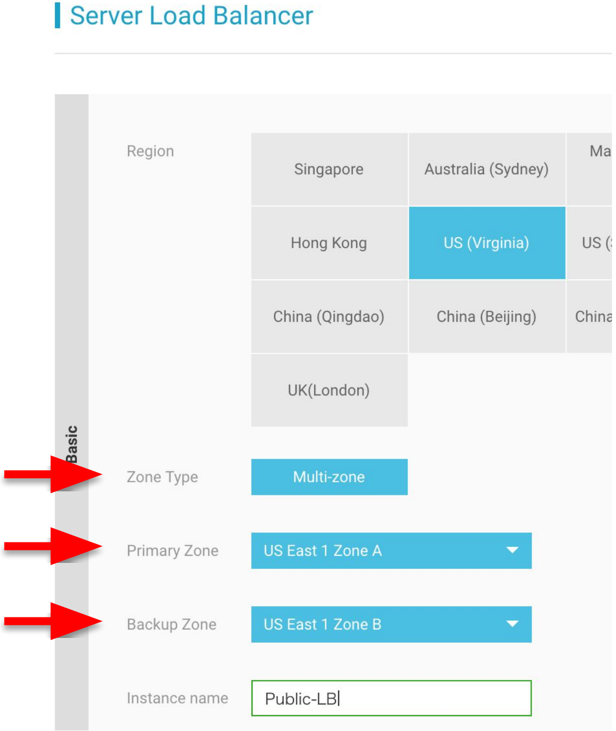
Expiring Instances

Server Load Balancer / Server Load Balancer

Server Load Balancer

Create SLB Instance

Select a tag



Server Load Balancer

Basic

Region: Singapore | Australia (Sydney) | Ma | Hong Kong | US (Virginia) | US (| China (Qingdao) | China (Beijing) | China | UK(London)

Zone Type: Multi-zone

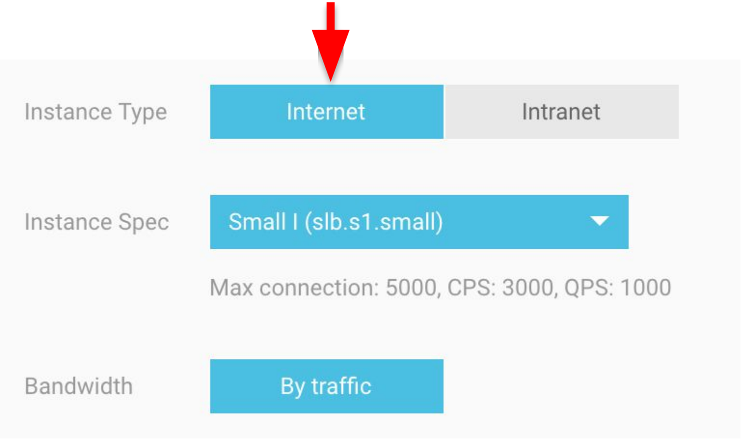
Primary Zone: US East 1 Zone A

Backup Zone: US East 1 Zone B

Instance name: Public-LB

Building Inbound flow architecture – LB Sandwich

- Choose Type=Internet (public LB)



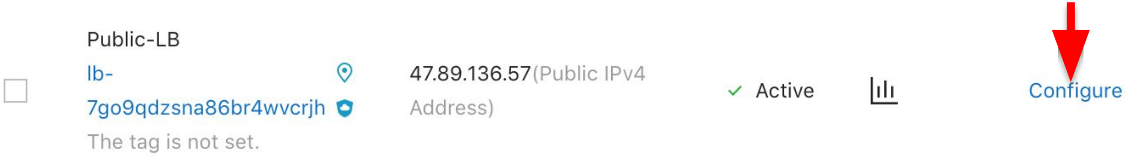
Instance Type [✓ Internet] Intranet

Instance Spec Small I (slb.s1.small)

Max connection: 5000, CPS: 3000, QPS: 1000

Bandwidth By traffic

- Public-LB gets created. Click on Configure to set up the LB



□ Public-LB
lb-7go9qdzsna86br4wvcrjh
The tag is not set.

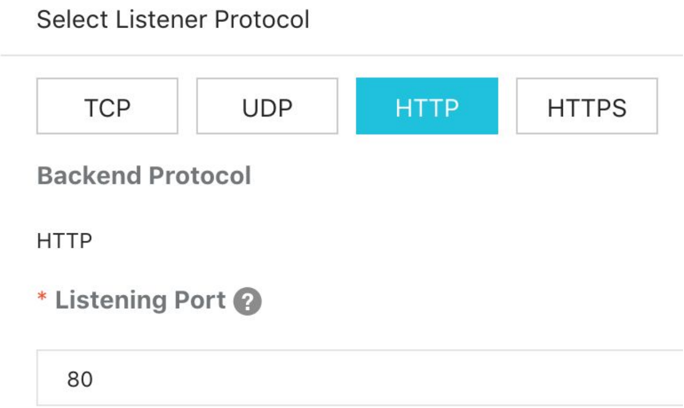
47.89.136.57(Public IPv4 Address)

✓ Active

Configure

Building Inbound flow architecture – LB Sandwich

- Listener = HTTP-80



Select Listener Protocol

TCP | UDP | HTTP | HTTPS

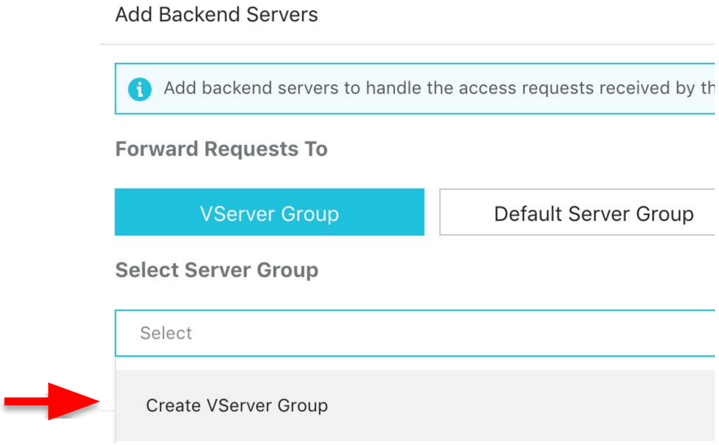
Backend Protocol

HTTP

* Listening Port ?

80

- For backend, choose to create a ‘VServer Group’



Add Backend Servers

Add backend servers to handle the access requests received by th

Forward Requests To

VServer Group | Default Server Group

Select Server Group

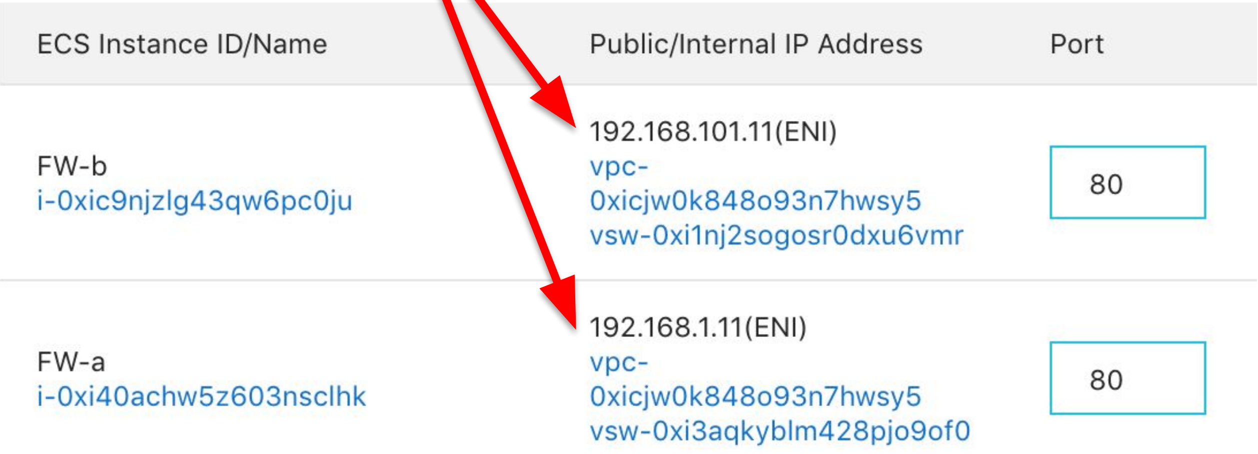
Select

Create VServer Group

Building Inbound flow architecture – LB Sandwich

- Add FW-a and FW-b to the VServer Group and choose port=80 (This is the port Firewalls expect to receive the traffic on)

Make sure you choose the correct ENIs (untrust)



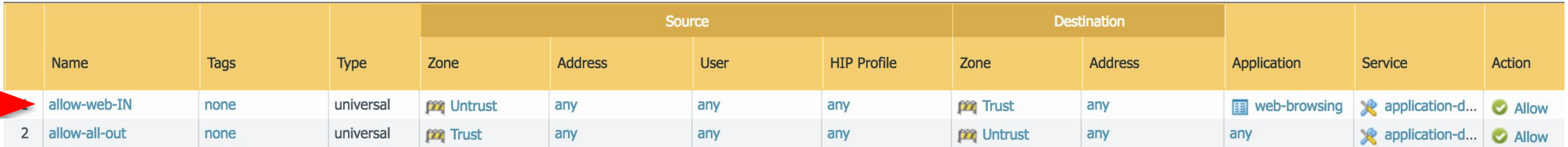
ECS Instance ID/Name	Public/Internal IP Address	Port
FW-b i-0xic9njzlg43qw6pc0ju	192.168.101.11(ENI) vpc-0xicjw0k848o93n7hwsy5 vsw-0xi1nj2sogosr0dxu6vmr	80
FW-a i-0xi40achw5z603nsclhk	192.168.1.11(ENI) vpc-0xicjw0k848o93n7hwsy5 vsw-0xi3aqkyblm428pjo9of0	80

Building Inbound flow architecture – LB Sandwich

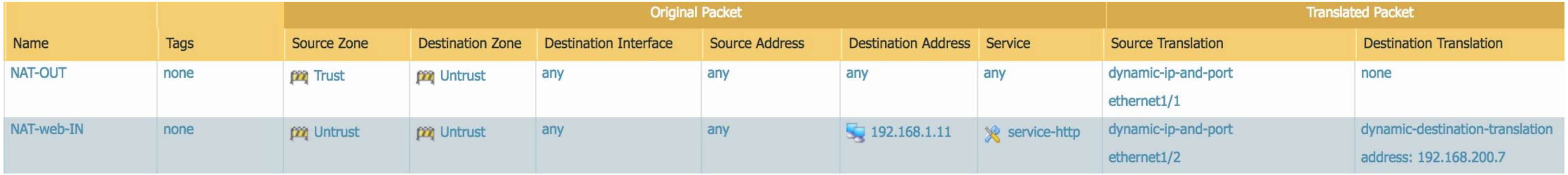
- At this point, we have to configure FW-a and FW-b to SNAT and DNAT incoming traffic from Public-LB.
  - SNAT will be to FW-trust interface. DNAT will be to the internal-LB frontend address (192.168.200.7)

- We also have to allow web traffic from Untrust to Trust

- Configuration for FW-a



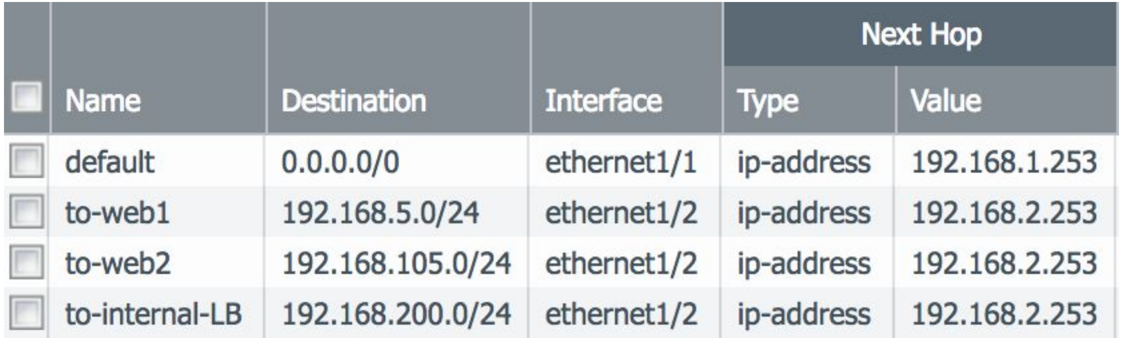
				Source				Destination				
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	allow-web-IN	none	universal	Untrust	any	any	any	Trust	any	web-browsing	application-d...	Allow
2	allow-all-out	none	universal	Trust	any	any	any	Untrust	any	any	application-d...	Allow



		Original Packet						Translated Packet	
Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
NAT-OUT	none	Trust	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none
NAT-web-IN	none	Untrust	Untrust	any	any	192.168.1.11	service-http	dynamic-ip-and-port ethernet1/2	dynamic-destination-translation address: 192.168.200.7

Building Inbound flow architecture – LB Sandwich

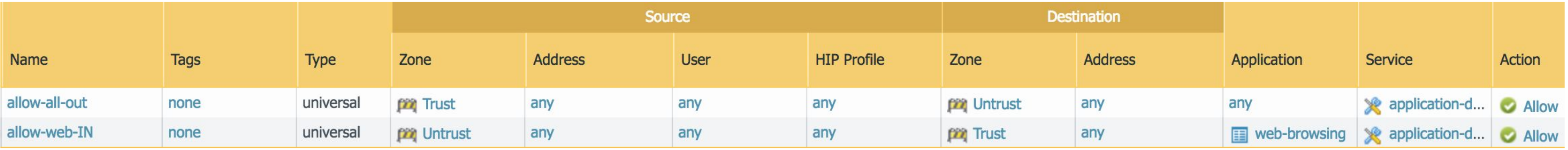
- Add a route on FW-a to the internal-LB-subnet



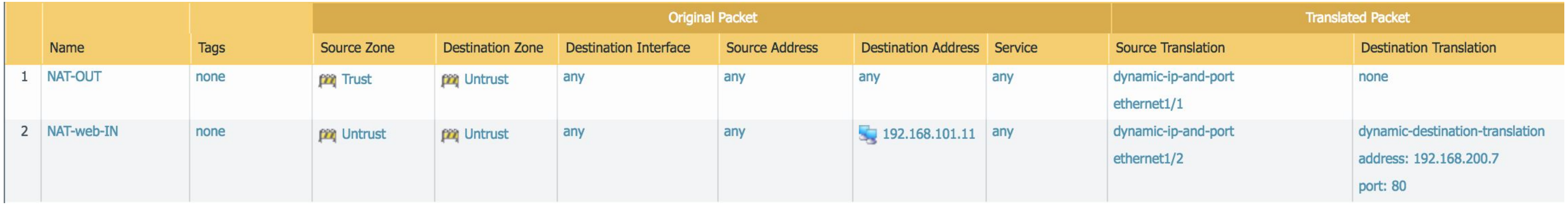
				Next Hop	
□	Name	Destination	Interface	Type	Value
□	default	0.0.0.0/0	ethernet1/1	ip-address	192.168.1.253
□	to-web1	192.168.5.0/24	ethernet1/2	ip-address	192.168.2.253
□	to-web2	192.168.105.0/24	ethernet1/2	ip-address	192.168.2.253
□	to-internal-LB	192.168.200.0/24	ethernet1/2	ip-address	192.168.2.253

Building Inbound flow architecture – LB Sandwich

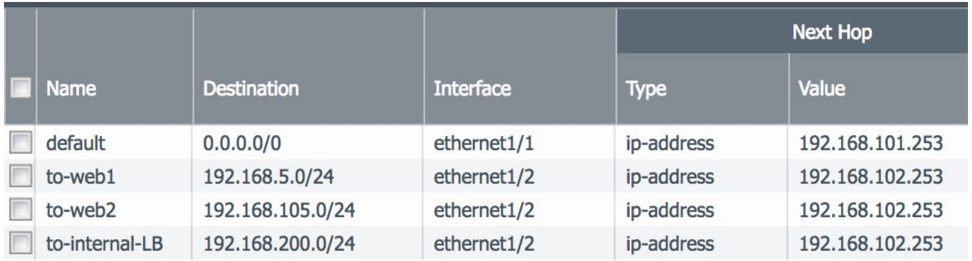
- Repeat (with slight changes) this config on FW-b



			Source				Destination				
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
allow-all-out	none	universal	Trust	any	any	any	Untrust	any	any	application-d...	Allow
allow-web-IN	none	universal	Untrust	any	any	any	Trust	any	web-browsing	application-d...	Allow



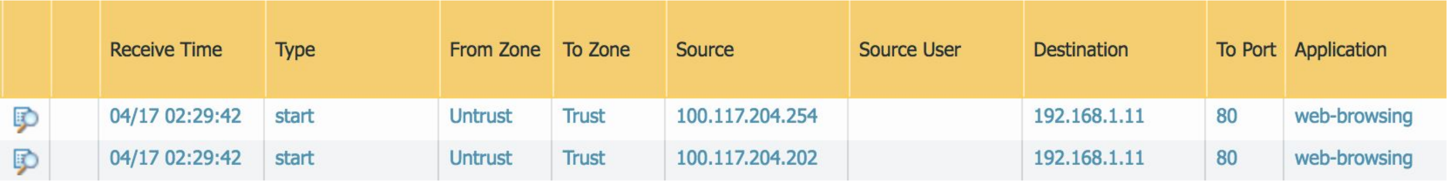
			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	NAT-OUT	none	Trust	Untrust	any	any	any	any	dynamic-ip-and-port ethernet1/1	none
2	NAT-web-IN	none	Untrust	Untrust	any	any	192.168.101.11	any	dynamic-ip-and-port ethernet1/2	dynamic-destination-translation address: 192.168.200.7 port: 80



				Next Hop	
☐	Name	Destination	Interface	Type	Value
☐	default	0.0.0.0/0	ethernet1/1	ip-address	192.168.101.253
☐	to-web1	192.168.5.0/24	ethernet1/2	ip-address	192.168.102.253
☐	to-web2	192.168.105.0/24	ethernet1/2	ip-address	192.168.102.253
☐	to-internal-LB	192.168.200.0/24	ethernet1/2	ip-address	192.168.102.253

Building Inbound flow architecture – LB Sandwich

- You should see the probes coming into FW-a and FW-b and detected as web-browsing



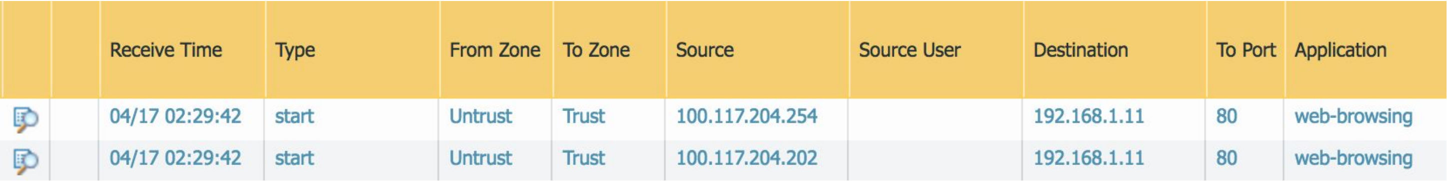
		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
		04/17 02:29:42	start	Untrust	Trust	100.117.204.254		192.168.1.11	80	web-browsing
		04/17 02:29:42	start	Untrust	Trust	100.117.204.202		192.168.1.11	80	web-browsing

- Public-LB should show also healthy backends now.

- From your laptop, browse to the Public-LB IP address. You should see the web page for backend ubuntu servers.

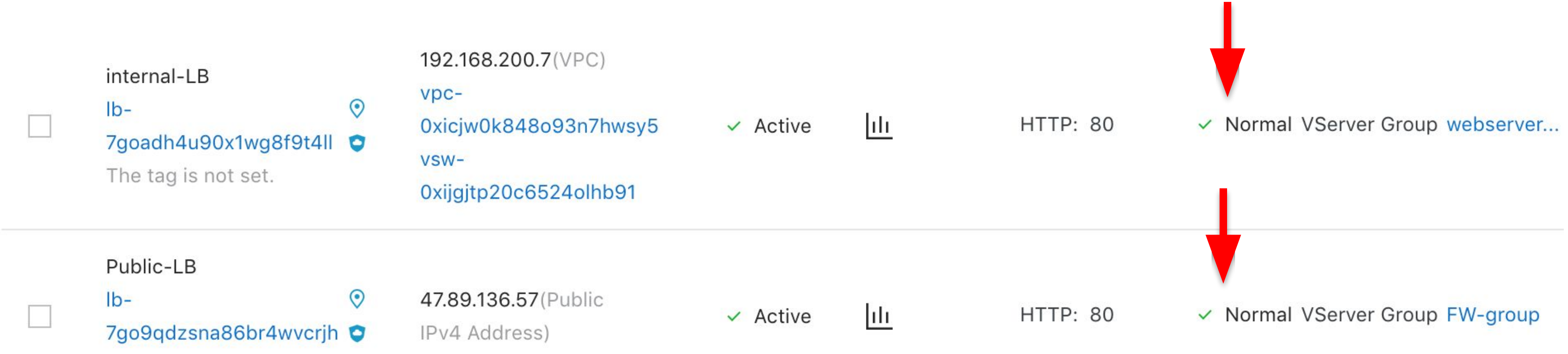
Building Inbound flow architecture – LB Sandwich

- You should see the probes coming into FW-a and FW-b and detected as web-browsing



		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
		04/17 02:29:42	start	Untrust	Trust	100.117.204.254		192.168.1.11	80	web-browsing
		04/17 02:29:42	start	Untrust	Trust	100.117.204.202		192.168.1.11	80	web-browsing

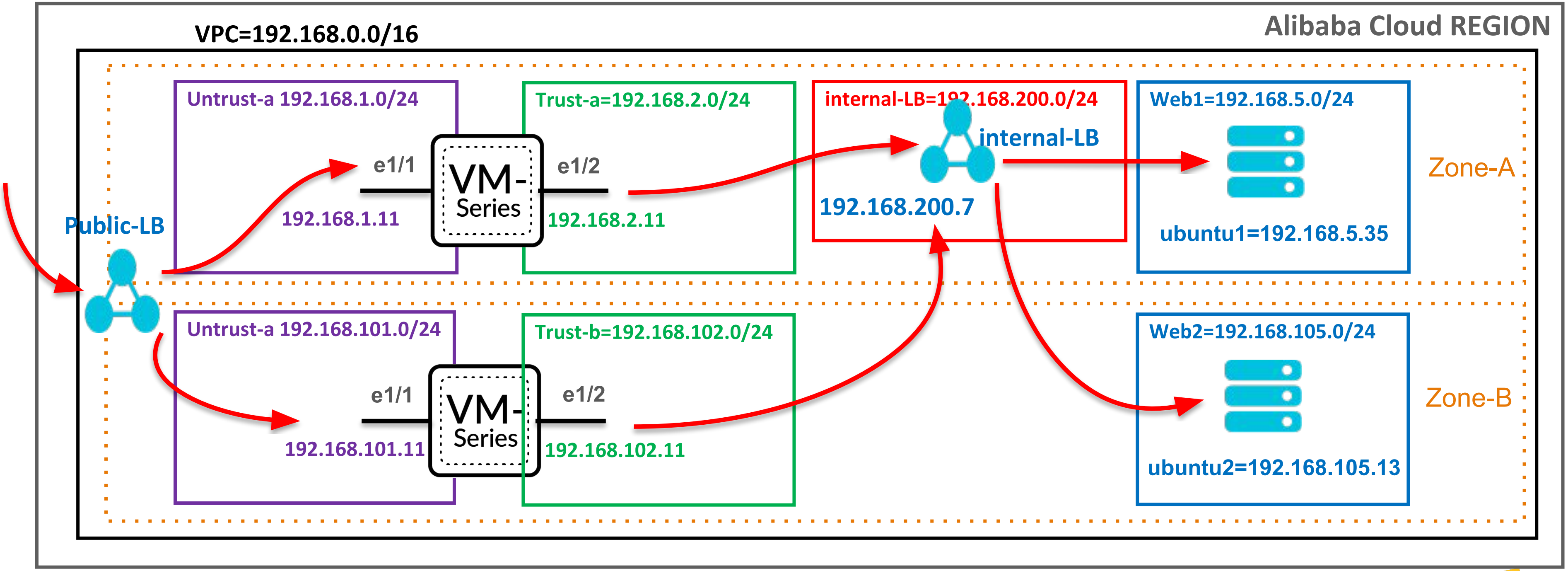
- Public-LB should show also healthy backends now.



□	internal-LB lb-7goadh4u90x1wg8f9t4ll The tag is not set.	192.168.200.7(VPC) vpc-0xicjw0k848o93n7hwsy5 vsw-0xijgjtp20c6524olhb91	✓ Active	HTTP: 80	✓ Normal VServer Group webserver...
□	Public-LB lb-7go9qdzsna86br4wvcrjh	47.89.136.57(Public IPv4 Address)	✓ Active	HTTP: 80	✓ Normal VServer Group FW-group

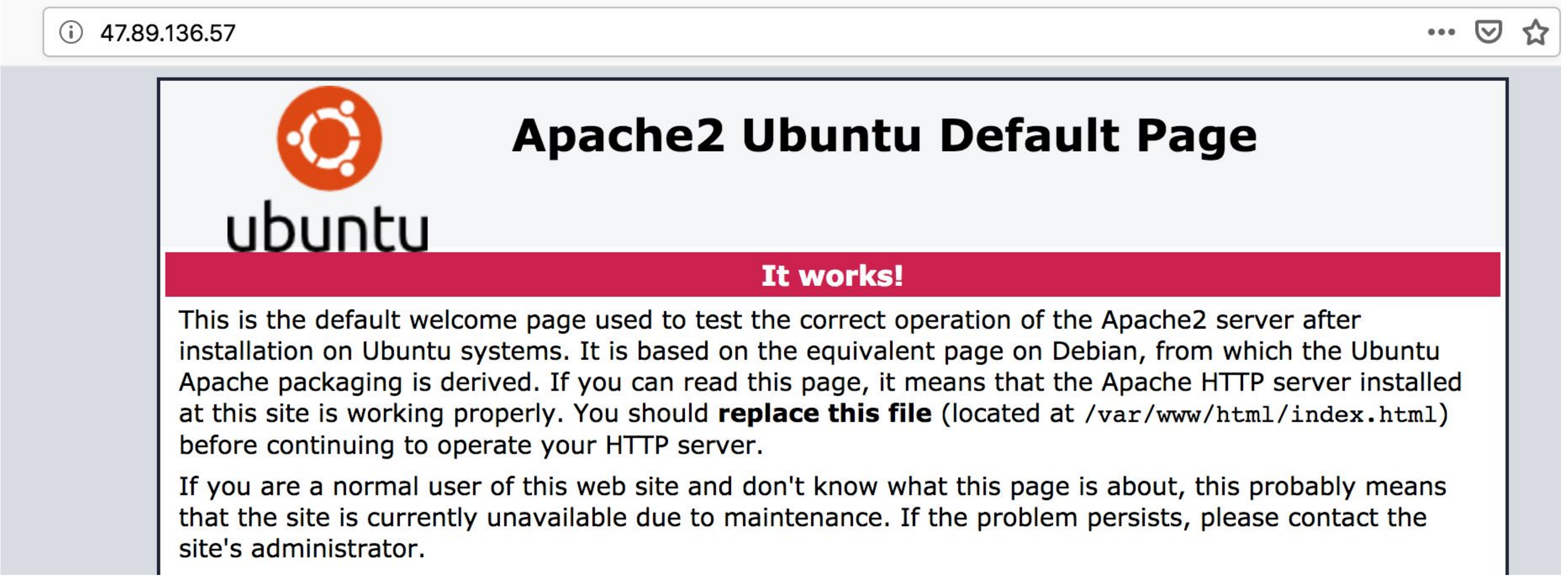
Deploying VM-Series in Alibaba Cloud

- This is what we have built for Inbound Load Balancer Sandwich design



Building Inbound flow architecture – LB Sandwich

- From your laptop, browse to the Public-LB frontend address. You should get the ubuntu web server pages.
- This concludes the Inbound use case.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.