

Pulse Connect Secure Virtual Appliance on Alibaba Cloud

Deployment Guide

Published Date

Pulse Secure, LLC 2700 Zanker Road, Suite 200 San Jose CA 95134

https://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Connect Secure Virtual Appliance on Alibaba Cloud - Deployment Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.pulsesecure.net/product-service-policies/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

Revision and Date	Added/Updated/Removed	Remarks
1.0, January 2020	NA	Initial publication for 9.1R4 release

Table of Contents

Revision History	3
Overview	5
About This Guide	5
Assumptions	5
Pulse Connect Secure on Alibaba Cloud	5
Prerequisites and System Requirements on Alibaba Cloud	5
Deploying Pulse Connect Secure on Alibaba Cloud	5
Supported Platform Systems	6
Deploying Alibaba Cloud PCS using Alibaba Cloud Portal	6
Steps to Deploy Pulse Connect Secure on Alibaba Cloud	6
Creating Alibaba Cloud PCS Image	6
Creating Virtual Private Cloud	11
Creating VSwitches	13
Creating Security Groups	14
Creating PCS-VA Instance	16
Deploying Alibaba Cloud PCS using Terraform Template	20
Installing Terraform Template	20
Configuring Base Setup	20
Deploying PCS with 2 NICs	21
Deploying PCS with 3 NICs	21
Pulse Connect Secure Provisioning Parameters	21
Limitations	23
Appendix A: Security Group (SG)	24
Appendix B: Pulse Connect Secure Terraform Template	27
Base Setup	27
PCS with 2 NICs	34
PCS with 3 NICs	37
Variables	40
User Data	41
References	42
Requesting Technical Support	42

Overview

About This Guide

This guide helps in deploying the Pulse Connect Secure Virtual Appliance on Alibaba Cloud (Aliyun). In this release a Pulse Connect Secure administrator can manually upload the Pulse Connect Secure Virtual Appliance image (KVM) into Alibaba Cloud storage account. Once the package is available in the storage account, the Pulse Connect Secure administrator can deploy Pulse Connect Secure on Alibaba Cloud.

Assumptions

The basic understanding of deployment models of Pulse Connect Secure on a data center and basic experience in using Alibaba Cloud is needed for the better understanding of this guide.

Pulse Connect Secure on Alibaba Cloud

Prerequisites and System Requirements on Alibaba Cloud

To deploy the Pulse Connect Secure Virtual Appliance on Alibaba Cloud, you need the following:

- An Alibaba Cloud account
- Access to the Alibaba Cloud portal (https://account.alibabacloud.com/login/login.htm)*
- Pulse Connect Secure Virtual Appliance Image (file)
- Alibaba Cloud Terraform template
- Pulse Connect Secure (PSA-V) licenses
- Site-to-Site VPN between Alibaba Cloud and the corporate network (optional)
 Note: This is needed only if the Pulse Connect Secure users need to access corporate resources
- Pulse Connect Secure configuration in XML format (optional)

Deploying Pulse Connect Secure on Alibaba Cloud

As depicted in the below diagram, a remote user can use Pulse Connect Secure to securely access cloud resources as well as corporate resources. To access corporate resources, the Pulse Connect Secure administrator needs to ensure that site-to-site VPN is already established between Alibaba Cloud and the corporate network.



Figure 1: Pulse Connect Secure on Alibaba Cloud

Supported Platform Systems

This section helps you in choosing the instance types that should be deployed with Pulse Connect Secure for Alibaba Cloud.

• PSA7000v is equivalent to ecs.g6.2xlarge in Beijing region.

Model	Region	vCPU	Memory (GB)
ecs.g6.2xlarge	Beijing	8	32

Deploying Alibaba Cloud PCS using Alibaba Cloud Portal

This section describes Alibaba Cloud PCS deployment with two NIC cards.

Steps to Deploy Pulse Connect Secure on Alibaba Cloud

- Creating Alibaba Cloud PCS Image
- Creating Virtual Private Cloud
- Creating Security Groups
- Creating PCS-VA Instance

Creating Alibaba Cloud PCS Image

To create Alibaba Cloud PCS image, do the following:

- 1. Download Alibaba Cloud PCS image, which is in the zip format, from the Pulse Secure Support site.
- 2. Unzip the file.
- 3. Log in to Alibaba Cloud with your account and credentials.

Figure 2: Alibaba Cloud Account Login Page

C-3 Alibaba Cloud CCC	🕄 Inti - English 🗸 Homepage Sign Up
Try Over 40 Products for Free Up to 12 Months Usage for Elastic Compute Service Try Us Free	Account: ali.pulse@pulsesecure.net Password: Forgot Password? ••••••• Sign In

4. In the ECS Console displayed, select **Object Storage Service**. The Object Storage Service page allows OSS bucket management such as store and retrieve a variety of unstructured data files, including text files, images, audio files, and video files, over the network at any time.

Figure 3: Object	Storage	Service	Option
------------------	---------	---------	--------

=	C-) Alibaba Cloud						٥	Billing Management	More	Alibaba Cloud	2	Ċ	Engl
	Products	>	ry					⑦ Operation reference	•				
=	Bastic Compute Service			Inst	ances		Snapshots						
			stal	Running	Expiring	Expired	Snapshot Size	Total		Common Setting	s		
*	ApsaraDB for RDS		5	10	0	0	140 16 GiB	26					
	Virtual Private Cloud		-				110.10 08	20		Renewal	Cust	om Sett	ings
	Officet Storage Service		ources							Pending Events	_		
-	object statoge some					Create Instance	Export Data of All Regions -	Show All Regions		Privileges & Que	otas		
×	Alibaba Cloud CDN						Specify a search condition	Saarch		Matifications			
4	Server Load Balancer							Juiten		NOUNCAUONS			
A	D		Mumbai))	China (Beijing))					
	Domains									No notifica	tions no	ed to fo	low
3	Marketplace		ic Compu	te Service	🕞 Runn	ing 7	Elastic Compute Service 🕟	Running 1		no notine			
					Receipt	ntly Created 5	Ð	Recently Created 1					
e	Diplus Overview				(7) Expin	ing 0	0	Expiring 0					

5. Sign up for OSS and create one or more OSS buckets. For details, refer to Alibaba Cloud Documentation.

E C-C Alibaba Cloud	🛞 Global	Q	Billing Management	More	Alibaba Cloud	۵_	Ţ.
Object Storage Service	Bucket Manage	ment					
Overview	4 buckets available Create Bucket	Export CSV	Obtain AccessKey				
 bucket Name bucket-beijing-darumuga bucket-california 	Alert Rules 0 Alert Rules, 0 Trig Manage	gered, 0 Warn	ings, 0 Disabled 😰				

Figure 4: Bucket Management

- 6. From the buckets list, click on the name of the created bucket.
- 7. In the window displayed, select the **Files** tab and then click **Create Folder** to create a folder for the Alibaba Cloud PCS-VA image.

Figure 5: Create Folder

😑 🕞 Alibaba Cloud	Q Search		Biling Ticket ICP Enterprise Support Alibaba Cloud 🔄	🖞 EN	0
Object Storage Service	Object Storage Service / bucket-beijing	Create Fol	der		×
Overview Buckets + O JF Bucket Name auto-bucket-california bucket-beijing-damaga	b Access Control List (ACL) Prin Overview Files Basic Settings Domain Name Log Overview Basic Statistics	Folder Name	pcs-va image 1 Folder naming conventions: 1. 1. The name can contain only UTF-8 characters. The name cannot contai emojis. 2. 2. Folders are separated with forward slashes (1/1). Folders in this path cautomatically created. The name cannot start with a forward slash (1/1) backslash (1/1). The name cannot contain consecutive forward slashes	L2/254 in an be) or (/).	

- 8. After creating the folder, change to the newly created folder and then click Upload.
- 9. In the Upload section, drag and drop one or more Alibaba Cloud PCS-VA images.

Figure 6: Upload Alibaba Cloud PCS VA Image

😑 🕞 Alibaba Cloud			Billing Ticket ICP Enterprise Support Alibaba Cloud 🔄 🗳 E	м 📀
Object Storage Service	Object Storage Service / bucket-beijing	Upload		×
Overview Buckets + 이 내 II Bucket Name Q	b Access Control List (ACL) Print Overview Files Basic Settings Domain Name	Upload To	Current Specified oss://bucket-beijing-darumuga/pcs-va image/	
 auto-bucket-california bucket-beijing-darumuga bucket-california 	Log Overview Basic Statistics File ACL		Inherited from Bucket Private Public Read Public Read/Write Inherited from Bucket: The ACLs of each file are the same as those of the bucket. Inherited from Bucket: The ACLs of each file are the same as those of the bucket.	E
 bucket-mumbai bucket-shanghai File/Object Name L pcs-va image/ 		Upload	Drag and drop one or more files in a folder here, or click <mark>Upload.</mark> A maximum of 100 files can be uploaded at a time.	

10. Wait for the upload to complete.

Figure 7: Upload Tasks

Upload Tasks			>
Removed Cancel All			
Do not reload or close the page when upload cleared.	is not complete. Otherwise, the upload	d queue will be interrupted a	and
File	Upload To	Status	Actions
pcs_9.1R4_alibaba.img 761.68 MB	oss://bucket-beijing-theory /pcs-va image/	Uploaded	Remove

11. Click on the View Details link corresponding to the uploaded file.

Figure 8: View Details

Ov	Overview Files Basic Settings Domain Names Image Processing (IMG) Event Notification Function Compute Log Overview Basic Statistics Ranking Statistics API Statistics Object Access Statistics						
Uploa	ad	Create Folder Parts Aut	horize Batch Operation	∨ Refresh	Selected: 1 / 1	Enter	a file name prefix Q
~		File/Object Name		Size	Storage Class	Updated At	Actions
	ن	/ pcs-va image/					
~		pcs_9.1R4_alibaba.img		761.68MB	IA	January 22, 2020, 12:48	View Details

12. Make note of the URL of the image. You need to enter this URL when importing the image.

Figure 9: Image URL

View Details		\odot Image Processing $ imes$		
ETag	74B730AAF5227DBAC825C265BE3010D3			
Validity Period (Seconds)	300			
HTTPS				
URL	https://bucket-beijing-darumuga.oss-cn-beijing.aliyuncs.com/pcs-va% 20image/pcs_9.1R4_alibaba.img?Expires=1579680063&OSSAccessKeyI d=TMP.hib1f4KTHsfM2HrCoejRqfQJvKXAVZTq1sLTLZL6ZUSAkaCnh257 MbfESSE4azRy8BxvbK2dxg4RTAFzCWJVYMA6AFtt78MKqvMjPiPnf3v14 bYgNbHNzi7gFFLFBn.tmp&Signature=GEw%2BZ9OQqabhC%2FszqI7C yWeB28M%3D			
	Download Open File URL Copy File URL	Copy File Path		
Туре	application/octet-stream	Set HTTP Header		
File ACL	Inherited from Bucket	Set ACL		
Storage Class	IA			
Server-side Encryption	None			

13. In the ECS Console, select Elastic Compute Service > Instances & Images > Images.

😑 🕞 Alibaba Clou	Jd		Q Billing Manag	gement More Alib	aba Cloud 🗈 🖞
Elastic Compute Serv	Summary			⑦ Operation reference	
Overview	Inst	ances	Snapshots		
Tags	Total Running	Expiring Expired	Snapshot Size	Total	Common Settings
Instances & Images 🔨 🔨	9 6	2 0	92.94 Gib	19	Custom Settings
Instances	My Perources				Pending Events
Elastic Container In 🖸	My Resources	Create Instance Export	Data of All Regions -	Show All Regions	Privileges & Quotas
Dedicated Hosts	-		Specify a search condition	on Search	Notifications
Super Computing Clus					Nouncations
Reserved Instances	> India (Mumbai)	广	China (Beijing)) Ē	
Images					No notifications need
Deployment & Elastic 🔤 🗸 🗸	Elastic Compute Service	8	Elastic Compute Service 1		
Storage & Snapshots 🛛 🗸					

Figure 10: Images Option

- 14. In the Images page displayed, select the region from the drop-down list located at the top-left corner of the page.
- 15. Click the Import Image button located at the top-right corner of the page and select Manual Import.

Figur	igure 11: Images Page – Manual Import Image												
Cł	iina (Beijing) 🔻						QE	Billing Management	More	Alibaba Cloud	⊡ <u>¢</u>	English	6
Im	ages							(?) Create c	custom imag	ge from snapshot	C Imp	ort Image 👻	
Cus	stom Images	Public Image	s	Share	d Images						Manual imp	ort	
As o base	of August 21, 203 ad on snapshots	.9, the ECS snaps , we recommend	shot se d that	ervice l you d	has been for elete the cus	mally launch stom images	hed on Al	ibaba Cloud Internat e no longer needed	tional site (a to avoid ur	libabacloud.com). B inecessary fees.	ecause custom	images are	
Ima	ge Name 💌	Search by ima	ge nar	me		s	earch	€тад				2 0	ł
	ID/Name		Tag		Туре	Platform	Bit Size of OS	Created At	Status	Progress		Actions	5
	m-2ze2haltmo beijing_pcs_91	dxjh5x2p3ya r3_3534	۲	ø	Custom Image	CentOS	64bit	18 November 2019, 13:32	Available	100%	Create Dele Modify Related Copy Imag	e Instance ete Image Description Instances e More v	

16. In the Import Image page displayed, enter the following details and click **OK**.

Figure 12: Import Image Page

Import Image (?) Import custo	am image X
Perform the following steps b 1. Perform the following 2. Upload the image file 3. Make sure that you ha	sefore importing or exporting an image: ;:Activate OSS to a bucket in the region where the image is to be imported. we authorized ECS to access your OSS resources. Verify
4. Check if the image me	eets the requirements specified in Notes
* Region of Image:	China (Beijing)
* OSS Object Address:	e=6v%29BQ64Z0KU4%29B0YEcwpq10Wow9Q%3D Learn how to obtain OSS file addresses.
* Image Name:	pcs_9.1R4_alibabacloud_image
* Operating System:	Linux
* System Disk Size (GB):	The system disk cannot be smaller than the image file in size. 40 to 500 GB for Windows and 40 to 500 GB for Linux.
* System Architecture:	x86_64
* Platform:	CentOS
Image Format:	QCOW2
License Type	Auto
Image Description:	
	Add Data Disk Image

• OSS Object Address: Type the URL of the Alibaba Cloud PCS image that was uploaded to OSS bucket.

- Image Name: Type a unique name for the image.
- Operating System: Linux
- System Disk Size (GB): 40
- System Architecture: Select an appropriate value from the drop-down list.
- Platform: CentOS
- Image Format: QCOW2

The imported image is listed in the Images page.

Figure 13: Images List

mages									@G	eate custom image from snapshot 2 Import Image -
Cus	tom Images Public Images	Share	ad Ima	ges						
As of the o	FAugust 21, 2019, the ECS snapshot s custom images which are no longer r	ervice reeded	has be I to av	en formally launc oid unnecessary f	hed on Alib ees.	aba Cloud Intern	ational site (alibabacloud.co	om). Because	e custom in	mages are based on snapshots, we recommend that you delete
Imag	e Name 💌 Search by image na	me			Search	€Tag				<u>a</u> o
	ID/Name	Tag		Туре	Platform	Bit Size of OS	Created At	Status	Progress	Actions
	m-a2d9x6zdjxafje9pj3ru 🕖 Pradeep-3996-SS-image	۲	*	Custom Image	CentOS	64bit	9 December 2019, 16:31	Available	100%	Create Instance Delete Image Modify Description Related Instances Copy Image More-
	m-a2d4ls002xqvg24rmze6 🕖 PCS_91R4_3996_SS_image	۲	*	Custom Image	CentOS	64bit	2 December 2019, 10:39	Available	100%	Create Instance Delete Image Modify Description Related Instances Copy Image More+
	m-a2d1ecc8lysabo7f6omd 🕖 PCS_91R4_3996_kvm	۲	*	Custom Image	CentOS	64bit	28 November 2019, 19:12	Available	100%	Create Instance Delete Image Modify Description Related Instances Copy Image More+
	m-a2d7475xbl6kyvt5wvlz () pcs_2_nics_91r4_snapsh	۲	*	Custom Image	CentOS	64bit	19 November 2019, 16:27	Available	100%	Create Instance Delete Image Modify Description Related Instances Copy Image More+
	m-a2da5zt52o3qjdjOwhrs () pcs_91r4_3708	۲	*	Custom Image	CentOS	64bit	5 November 2019, 21:04	Available	100%	Create Instance Delete Image Modify Description Related Instances Copy Image More+
	Delete Image Edit Tags								1	iotal: 6 item(s), Per Page: 50 item(s) 1

Creating Virtual Private Cloud

To create Virtual Private Cloud (VPC), do the following:

1. Select Elastic Compute Service > Network & Security > VPC.

Figure 14: VPC Option

😑 🕞 Alibaba C	loud				Q Billing Manage	ement More Alib
Elastic Compute Service		Summary			G	Operation reference
Overview		Inst	ances		Snapshots	
Tags		Total Running	Expiring	Expired	Snapshot Size	Total
Instances & Images 🛛 🗸		16 11	0	0	141.08 Gib	28
Deployment & Elasticity 🗸 🗸		My Resources				
Storage & Snapshots 🛛 🗸	=	c	reate Instance	Export D	lata of All Regions 🗸 🖸	Show All Regions
Network & Security					Specify a search condition	Search
Security Groups		India (Mumbai)		æ	China (Beijing))面
ENI						
SSH Key Pair		Elastic Compute Service	12		Elastic Compute Service 2	
EIP 🖸		D Purping 0			Pumping 1	

2. In the VPCs page, select the required region from the drop-down list located at the top-left corner of the page and click **Create VPC**.

😑 🕞 Alibaba C	Oud China (Beijing) 🗸		Q Billing	Management	More Alibaba C	loud Ъ	🖨 English	0
VPC	VPCs							
VPCs	Create VPC Refresh	Custom		1	nstance Name 🗸	Enter an ID		Q
VSwitches	Instance ID/Name	IPv4 CIDR Block	Status	Default VPC	Route Table	VSwitch	Actions	
Internet Shared Ba	vpo-2zerbyseo3f77t402bivp 🖫 amar-vpo-beijing	10.40.0.0/16	 Available Not Bound to CEN 	No	1	3	Manage Delete	Ð
■ Elastic IP Addresses	vpo-2zeqowo24gmga49ggmxyf 🖽 vpo_beijing	192.168.5.0/24	Available Bound to CEN	No	1	8	Manage Delete	8

Figure 15: VPCs Page

3. In the Create VPC page displayed, enter the VPC and VSwitch (Internal Port) details and click OK.

Create VP	с		×
VPC			
	Region China (Beijing)		
	• Name 💿		
	vpc-beijing 17/128	0	
	IPv4 CIDR Block		
	Default CIDR Block		
	Custom CIDR Block	_	
	192.168.0.0/16	\sim	
	() The CIDR cannot be changed once the VPC is created.		
	Description 💿		
	VPC-Beljing		
	17/2	256	
VSwitch			
	• Name 💿		
	vsw-zoneb-pcs-int-port-subnet 29/128	0	
	• Zone 💿		
	Beljing Zone B	\sim	
	Zone Resource 💿		
	ECS 🕗 RDS 🕗 SLB ⊗		
	IPv4 CIDR Block		
	192 . 168 . 0 . 0 / 24 🗸		
	ок		Cancel

4. In the Create VPC - Details page, verify **Status** and click **Complete**. The created VPC is listed in the VPCs page.

Figure 17: Create VPC – Details Page

Create VPC	×
Details	
VPC Name	vpc-beljing
VPC ID	vpc-2zelfnl0/kmhpucsp4waf
Status	Success Create NAT Gateway
V\$witch name	vsw-zoneb-pcs-Int-port-subnet
V\$witch ID	vsw-2zeollymgla8xuoyw0eb1
Status	Success Purchase 🗸
	Complete

Creating VSwitches

While creating VPC, you created VSwitch for Internal Port. You need to create VSwitches for External and Management ports.

To create VSwitches, do the following:

- 1. Select Elastic Compute Service > Network & Security > VPC > VSwitches.
- 2. In the VSwitches page displayed, select the required region from the drop-down list located at the top-left corner of the page and click **Create VSwitch**.

😑 🕞 Alibaba Cloud	Chins (Beijing) 👻	Q. Search	Bi	illing Ticket	ICP Enter;	rise Support	Alibaba Cloud 🛛 🖻	1 Q' EN 🌀
VPC	VSwitches							
VPCs Route Tables	Create VSwitch Refresh	Customize Columns				Instance Name \checkmark	Search by Instance	name Q
VSwitches	Instance ID/Name	VPC	Status	IPv4 CIDR Block	Number of Available Private IPs	Default VSwitch	Zone $\boldsymbol{\tau}$	Actions
Internet Shared Bandwl Data Transfer Plan	vsw-2zevggz671pko9aaeoadi 🗟 vsw-on-beijing-a	vpo-2zeeev40r1109x6x23xb4 @ vpo-beljing-darumuga	Available	192.168.5.16/28	12	No	Beijing Zone A	Manage Delete Purchase V
✓ Elastic IP Addresses Elastic IP Addresses	vsw-2ze6vah48hvz0qwatact8 🔄 vsw-cn-beljing-a	vpo-2zeesv40r1109x6x23xb4 🕞 vpo-beljing-darumuga	Available	192.168.5.48/28	12	No	Beijing Zone A	Manage Delete Purchase V
NAT Gateways Global Acceleration	vsw-2zegrsekeuu9r31sq5725 🗟 vsw-cn-beljing-b	vpo-2zeesv40r1109x6x23xb4 🕞 vpo-beljing-darumuga	Available	192.168.5.80/28	12	No	Beijing Zone B	Manage Delete Purchase V
✓ VPN VPN Gateways	vsw-2ze04):nenur5gb6cy1he 🖻 vsw-cn-beijing-b	vpo-2zeesv40r1109x6x23xb4 🕞 vpo-beljing-darumuga	Available	192.168.5.64/28	12	No	Beijing Zone B	Manage Delete Purchase V
Customer Gateways	vsw-2ze1re7n7jtxogdjjaa9o 🕞 vsw-cn-beljing-b	vpo-2zeesv40r1109x6x23xb4 🕞 vpo-beljing-darumuga	Available	192.168.5.96/28	12	No	Beijing Zone B	Manage Delete Purchase V
SSL Servers	vsw-2zev64rx5ukgitb6shpbf 🕞 vsw-on-beijing-a	vpo-2zeesv40r1109x6x23xb4 🕞 vpo-beljing-darumuga	Available	192.168.5.32/28	12	No	Beijing Zone A	Manage Delete Purchase V
SSL Cilents Flow Log	vsw-2zehw70e7510ajeo4nq94 📄 amar-vpn-pool-bel	vpc-2ze848pb8nc6bt8uste3u @ amar-vpc-beijing	Available	10.13.0.0/16	65532	No	Beijing Zone H	Manage Delete
Ousta Management								

Figure 18: VSwitches Page

- 3. In the Create VSwitch window displayed, do the following:
 - a. Select VPC from the drop-down list.
 - b. Enter a unique name for VSwitch for External port.
 - c. Select **Zone** from the drop-down list.
 - d. Click OK. The created VSwitch is listed in the VSwitches page.

Figure 19: Create VSwitch Window

Create VSwitch	×
• VPC vpc-beijing-zoneb/vpc-2zeifni0/tm/pvcsp4waf V	
CIDR 192.168.0.016	
Name vsw-cn-beijing-ext-port 23/128	
• Zone 🔘 Beijing Zone B	
Zone Resources 💿 ECS 📀 RDS 📀 SLB ⊗	
IPV4 CIDR Block 192 . 168 . 0 . 0 / 24 192 . 168 to clark the VPC is created.	
Number of Available Private IPs 252	
ОК	Cance

4. Repeat the procedure to create VSwitch for Management Port.

Creating Security Groups

Security groups are groups of VPC instances that are located within the same region and share the same security requirements.

To create a security group, do the following:

- 1. Select Elastic Compute Service > Network & Security > Security Groups.
- 2. In the Security Groups page, select the region from the drop-down list located at the top-right corner of the page and click **Create Security Group**.

<u> </u>	1 0							
😑 🕞 Alibaba Clou	China (Beijing) 🕶	c	Q Billing	Manageme	nt Mo	re Alibaba	Cloud [🖬 🖞 English
Elastic Compute Service	Security Groups				2 🕥	ecurity group	5 C	Create Security Group
Overview Tags	Security Group Name	Search	€тад					2
Instances & Images V	Security Group ID/Name Tags VPC	Related Instances	Available IP Addresses	Network Type(All) *	Security Group Type	Created At	Description	Actions
Storage & Snapshots V	sg-2zeiw2bqogm7fahkb58z				Basic	5 December		Modify Clone Restore Rules
Network & Security	amar-sg-beijing-mgmt 🔊 amar-vpc-beijing-manual	0	2000	VPC	Group	2019, 11:01	-	Manage Instances Add Rules Manage ENIs
ENI SSH Key Pair	sg-2zeap6bro517jwpf2bna vpc-2zerbyseo3f77t402bivp				Basic	5 December		Modify Clone Restore Rules
VPC 🖸	Delete Edit Tags			Tota	- ···	Per Page: 10	item(s) «	< 1 > >>

Figure 20: Security Groups Page

- 3. In the Create Security Group window, select a template from the drop-down list.
- 4. Enter a name for the Security Group.
- 5. Select Security Group Type from the drop-down list.
- 6. Select Network Type as VPC.
- 7. Select **VPC** from the drop-down list.
- 8. Click OK.

Figure 21: Create Security Group Window

Create Security Group 곗 Cr	eating security group	×
Template:	Customize	
* Security Group Name:	sg-int-port	
	The name must be 2 to 128 characters in length and can contain peri (_), hyphens (-), and colons (:). It cannot start with a special character	ods (.), underscores or digit.
Description:	\$Q-i01-ROI3	
	It must be 2 to 256 characters in length and cannot start with "http://	" or "https://".
Security Group Type:	Basic Security Group	
Network Type:	VPC 💌	
*VPC:	vpc-2zeifhi0ykmhpvcsp4waf	
Tag:	Select a tag key.	ew one 🔻
Inbound Outbound		
Authorization Object	Protocol Type Port Range	Action

9. In the Notes dialog that is displayed, click **Create Rules Now**.

Notes		×
0	After creating a security group, we recommend that you immediately create security group rules. Otherwise, you may not be able to access the internal network or Internet.	
	Create Rules Now Clos	æ

10. In the page that is displayed, click Add Security Group Rule to create the Inbound rules.

≡	C-J Alibaba Clou	i		Q Billing Management	More	Alibaba Cloud	Þ Á	English
	<	sg-int-port 💩 vpc-beijing / v	pc-2zeifhi0ykmhpvcsp4waf	Tutorial C Back	Add S	ecurity Group Rule	Quick R	ule Creation
Securi	ty Group Rules	Jabaurad Outbourad				.↑. Import Rule	s .¥. Ex	port Rules 👻
Instand	tes in Securit							
ENIS IN	Security Gro	The security group does not have any cus to allow access to the relevant instance po	tom rules for access permissions. In this case, rts.	you cannot access any instanc	es in the si	ecurity group. To re	solve this issue	e, add rules
		Action Protocol Type Por	: Range Authorization Type(All) 👻	Authorization Object	Descriptio	on Priority	Created At	Actions

For details about Inbound rules, see Appendix A: Security Group (SG). This completes creation of Security Group.

Creating PCS-VA Instance

To create PCS-VA instance, do the following:

- 1. Select Elastic Compute Service > Instances and Images > Instances.
- 2. In the Instances page, select the region from the drop-down list located at the top-left corner of the page and click **Create Instance**.

Figure 22: Instances Page – Create Instance Option

Ш	C-) Alibaba Clo	oud	China (Beijing)			Q Billing Managem	ent More	e Alib	baba Cloud	2_	Ċ.	Englis	sh
Elasti	c Compute Service		Instances				0	Operatio	on reference	С	Create 1	Instan	nce
Overvi Tags	iew		 Select an instance attribution 	ute or enter a keyword	ł		C	۲	Tags Adv	anced S	earch	2	٥
Instan	ces & Images 🔨 🔨		Instance ID/Name	Tag Monitoring	Zone *	IP Address	Status 👻	Network Type 👻	c Specificatio	ns	Billing Method		
Instan Elastic	Container Instance 🖸		i-2ze3c9v5ig6rqcrqakyc		Beijing				2 vCPU 4 G	iB (I/O	Pay-As- You-Go 3		
Dedica	ated Hosts		pcs_91r4_3996_2	≫ ‡ ⊵	Zone 101.200.89.5(Internet A 192.168.5.19(Private)) 🕞 Running VPC		C Optimized) ecs.hfc5.large		Decembe 2019,	er Ch	ange
Super	Computing Cluster									,	23:20 Create		

- 3. In the Basic Configurations page, select the **Custom Launch** tab.
- 4. Select the Billing Method as Pay-As-You-Go.
- 5. Select the appropriate zone in **Region**.
- 6. In Instance Type, type ecs.ic5.large.

The Selected Instance Type displays the details of the instance type.

7. In the Image section, select the **Custom Image** tab.

8. From the drop-down list, select the required Alibaba Cloud PCS image that you want to deploy. For details about Alibaba Cloud PCS image, see "Creating Alibaba Cloud PCS Image".

Basic Configurations	2 Netwo	orking	3 System Configurations	(Optional) 4 Groupi	ng (Optional)		5 Preview	
illing Method	Subscription	Pay-As-You-Go 🕜						
egion earn more	China (Beijing) Instances in different regions of	Random Zone H (7) annot communicate with each of	Zone G (2) Zone F	Zone C Zone E at the region nearest to your c	Zone D ustomers to reduce th	Zone A	Zone B	
nstance Type	Current Generation All	Generations Purchase History	,					
lect a configuration stance types available f each region equest higher specificati is for pay-as-you-go in	Filter Select a type Architecture x86-Architect Category General Purpor	Select a type Search by instructure Heterogeneous Comp Se Compute Optimized	tance type name, such Q I/O Op uting ECS Bare Metal Instance Memory Optimized Big Da	ndicates whet	n Clock Speed	Entry-Level (Sh	ared)	
inces	🔁 Family I	nstance Type VCPUs 🍦	Memory Physical Processor		Clock Speed	Internal Netw ork Bandwidt h 👙	Packet Forwardi ng Rate 🌲	IPv6-su pporte d
	 General Purpose Type g6 ⊘ 	ecs.g6.large 2 vCPL	Js 8 GiB Intel Xeon(Cascade La	ke) Platinum 8269CY	2.5 GHz/3.2 GHz	1 Gbps	300,000 PPS	Yes
	General Purpose Type g6	ecs.g6.2xlarge 8 vCPl	Js 32 GiB Intel Xeon(Cascade La	ske) Platinum 8269CY	2.5 GHz/3.2 GHz	2.5 Gbps	800,000 PPS	Yes
	General Purpose Type g6	ecs.g6.3xlarge 12 vCPU	Js 48 GiB Intel Xeon(Cascade La	ake) Platinum 8269CY	2.5 GHz/3.2 GHz	4 Gbps	900,000 PPS	Yes
	General Purpose Type g5	ecs.g5.large 2 vCPU	Js 8 GiB Intel Xeon(Skylake) Pl Xeon(Cascade Lake) F	atinum 8163 / Intel Platinum 8269CY	2.5 GHz/2.7 GHz	1 Gbps	300,000 PPS	Yes
elected Instance	ecs.g6.large (2 vCPU 8 GiB, Gene	ecs.g5.xlarge 4 vCPl aral Purpose Type g6)	Js 16 GiB Intel Xeon(Skylake) Pl	atinum 8163 / Intel	2.5 GHz/2.7 GHz	15 Gbps	500,000 PPS	Yes
rpe urchased Instances	- 1 + Units 5	2 vCPUs have been enabled, and	-42 more vCPUs can be enabled. The	selected instance type occupi	es 2 vCPUs . You can c	reate a maximui	m of 0 more ECS i	nstances.
nage	Public Image	Custom Image	Shared Image Marketplace	e Image				
torage Visk specifications and p	PCS_91R4_4763_ALICLOUD System Disk Standard SSD	40 GiB 3000 IC	DPS 🔽 Release with Instance					
			_					

Figure 23: Basic Configurations Page

- 9. Click **Next Networking** to proceed to networking configuration.
- 10. In the Networking page, go to the Network Type section and select the required **VPC** and **VSwitch** from the drop-down lists. For details about creating VPC and VSwitch, see "Creating Virtual Private Cloud".
- 11. In the Public IP Address section, select the **Assign Public IP Address** check box to select an IP address for the Internal Port.

Figure 24: Ne	tworking Page			
Basic Configurations	2 Networking	3 System Configurations (Optional)	4 Grouping (Optional)	5 Preview
Network Type Learn more				
	To create a new VPC, go to the VPC console.	VSwitch Zone: Beijing Zone B VSwitch CIDR Block: 172.16.5	.64/28	ses Available: 11.
Public IP Address Bandwidth pricing	Assign Public IP Address If you do not select Assign Public IP Address, the instance will not be auto upgrade the bandwidth for the instance to be automatically assigned a pu	matically assigned a public IP address and cannot access the public netwo blic IP address.	rk. To enable the instance to access the p	oublic network, bind an Elastic IP Address (EIP) to it, or
Security Group Security group limits Learn more	Select Security Group ③ A security group functions similarly to fir Learn more.	ewalls and is used to set network access controls for one or more ECS insta	nces. You can go to the Security Groups	page in the ECS console to create a security group.
Elastic Network Interf	Instance family ecs.nl.tiny does not support ENI. For the ECS instance fam	ilies that support ENIs, see Documentation>.		
ald				
		Total: \$ 0.036 USD per Hou	Prev: Basic Configuration	ns Next: System Configurations Preview

12. In the Security Group section, click **Select Security Group**. In the Select Secure Group window displayed, select the security group assigned to the Internal Port and click **Save**. For details about creating Security Group, see "Creating Security Groups".

Figure 25: Select Security Group Window

Select	t Security Group					×	
Securit Securit	Security Group Name Enter a security group name Security Group: sg_pcs_int_port / sg-a2ddgla4c5jod6mf6no5 × Selected 1						
	Security Group ID	Security Group Name	Creation Time	Elastic Network Interface	VPC ID	Rule	
\circ	sg-a2ddgla4c5jod6mf6no6	sg_pcs_ext_port	22 Nov 2019, 20:23:07 IST	10	vpc-a2dfo4egldzvkobu77otw	See Rules>	
\bigcirc	sg-a2datwbf205ycwq5esbx	sg_backend_svr	22 Nov 2019, 20:23:06 IST	1	vpc-a2dfo4egldzvkobu77otw	See Rules>	
۲	sg-a2ddgla4c5jod6mf6no5	sg_pcs_int_port	22 Nov 2019, 20:23:03 IST	5	vpc-a2dfo4egldzvkobu77otw	See Rules>	
0	sg-a2datwbf205ycwq5esbw	sg_pcs_mgmt_port	22 Nov 2019, 20:23:02 IST	l	vpc-a2dfo4egldzvkobu77otw	See Rules>	
						1	
					Select	Cancel	

13. In the Elastic Network Interface section, click Add ENI and select the External Port.

Figure 26: Elastic Network Interface Section

❀ Elastic Network Interface	Default ENI			
	VSwitch: vsw-zone-b-pcs-int-port-subnet Auto-assign IP Addresses Release with Instance			
	New ENI			
	VSwitch: vsw-zone-b-pcs-ext-port-subnet VSwitch:			
	You can only attach 1 ENIs when creating an ECS instance. Click here to learn more about ENIs			

- 14. Click Next System Configuration to proceed to system configuration.
- 15. In the System Configurations page, for Logon Credentials, select Set Later.
- 16. For Instance Name, enter the name of the virtual appliance.
- 17. In the User Data section, provide <u>Provisioning Parameters</u> in the XML format.

Figure 27: System Configurations Page

Basic Configurations	Networking	- 3 System Configurations (Opti 4) Grouping (Optional) 5) Preview				
Logon Credentials :	Key Pair Inherit Password From Image	Password 💽 Set Later	Ä			
Instance Name :	launch-advisor-20191216	How to customize ordered instance names ③	0			
The name must be 2 to 128	characters in length and can contain letters, Chinese charac	ters, digits, and the following special characters: - \bigcirc The name must start with a letter or Chinese character.				
Description :	Description	The description must be 2 to 256 characters in length. It cannot start with "http://" or "https://".				
Host: ⊘	.il Enter a hostname	How to customize ordered hostnames ⑦				
For Linux systems and other operating systems: The name must be 2 to 64 characters in length. It can contain several segments delimited by periods (.). Each segment can contain letters, digits, and hyphens (-), but consecutive periods (.) or hyphens (-) are not allowed. The name cannot start or end with a period (.) or hyphen (-).						
Bandwidth: 5Mbps Pay-By-Trai	ffic Total: \$ 0.077 USD per Hour +	Internet Traffic Fees: (0\$ 0.090 USD per GB Prev: Networking Next: Grouping Prev	iew			

18. Click Preview. In the Summary page, accept Terms of Service and click Create Instance.

Figure 28: Terms of Service

	System Configurations I Logon Credentials : Set Later. To connect to the ECS Instance Name : launch-advisor-20191216 instance remotely, go back to step 3 to configure the logon credentials.	
	Save as Launch Template ② View Open API ③	Ä
🛲 Automatic Release	Automatic Release The ECS instance will be released at the time you specified. After the instance is released, its data and IP addresses will not be retained and cannot be retrieved.	0
R Terms of Service	ECS Terms of Service and Product Terms of Service	
Bandwidth: 5Mbps Pay-By-Traffic	Total: \$ 0.077 USD per Hour + Internet Traffic Fees: (0) \$ 0.090 USD per GB Prev: Grouping Create Insta	ince

The instance will be created. × (~) Created The ECS instance(s) you purchased are being created. The creation process may take 1 to 5 minutes to complete. Click Back to purchase more instances or click Console to manage instances. Back Alibaba Cloud provide you with more preferential and flexible cloud services, including the following functions: Auto Scaling Service> No fees for stopped instances(VPC-Connected)> Switch from pay-as-you-go to subscription> Change configurations of pay-as-you-go instances> Change EIP Internet bandwidth>

Deploying Alibaba Cloud PCS using Terraform Template

This section describes how to install terraform template, deploy PCS with 2 NICs and 3 NICs.

Installing Terraform Template

- 1. Go to the <u>Terraform website</u> and install Terraform on a Linux VM of your choice.
- 2. Download the following directories and files in it:

Directory	Files
base_setup	base_setup.tfvariables.tf
pcs_2_nics	 pcs_2_nics.tf user_data.txt variables.tf
pcs_3_nics	 pcs_3_nics.tf user_data.txt variables.tf

Configuring Base Setup

- 1. Customize and set the variables in variables.tf file.
- 2. Copy user_data.txt and variables.tf file to each of the directories (base_setup, pcs_2_nics, pcs_3_nics). Alternatively, create a softlink to these files.
- Change directory to base_setup directory, and run the following commands: linux# terraform init linux# terraform apply

Deploying PCS with 2 NICs

- 1. Change directory to pcs_2_nics.
- 2. Customize the user_data.txt file. This file contains the PCS initial configuration data.
- 3. Run the following commands:

linux# terraform init linux# terraform apply

Deploying PCS with 3 NICs

- 1. Change directory to **pcs_3_nics**.
- 2. Customize the user_data.txt file. This file contains the PCS initial configuration data.
- 3. Run the following commands:

linux# terraform init linux# terraform apply

Pulse Connect Secure Provisioning Parameters

Provisioning parameters are those parameters which are required during the deployment of a virtual appliance. Pulse Connect Secure accepts the following parameters as provisioning parameters in the XML format.

<pulse-config>

<wins-server><value></wins-server>
<dns-domain><value></dns-domain>
<admin-username><value></admin-username>
<admin-password><value></admin-password>
<cert-common-name><value></cert-common-name>
<cert-random-text><value></cert-organisation>
<cert-organisation><value></cert-organisation>
<config-download-url><value></config-download-url>
<config-data><value></config-data>
<auth-code-license></auth-code-license>
<enable-license-server><value></auth-code-license-server>
<accept-license-agreement><value></accept-license-agreement>
</pulse-config>

#	Parameter Name	Туре	Description
1	wins-server	IP address	Wins server for Pulse Connect Secure
2	dns-domain	string	DNS domain of Pulse Connect Secure
3	admin-username	string	admin UI username
4	admin-password	string	admin UI password.
5	cert-common-name	string	Common name for the self-signed certificate
6	cert-random-text	string	generation. This certificate is used as the device
7	cert-organization	string	Random text for the self-certificate generation Organization name for the self-signed certificate generation
8	config-download-url	String URL	Http based URL where XML based Pulse Connect Secure configuration can be found. During provisioning, Pulse Connect Secure fetches this file and comes up with preloaded configuration. XML based configuration can be present in another VM in Alibaba Cloud or at corporate network which is accessible for Pulse Connect Secure through site to site VPN between Alibaba Cloud and corporate data center.
9	config-data	string	base64 encoded XML based Pulse Connect Secure configuration
10	auth-code-license	string	Authentication code that needs to be obtained from Pulse Secure
11	enable-license- server	string	If set to 'y , PCS will be deployed as a License server. If set to 'n' , PCS will be deployed as a normal server.
12	accept-license- agreement	string	This value is passed to the instance for configuration at the boot time. By default, this value is set to "n". This value must be set to "y" .
13	enable-rest	string	If set to $\mathbf{\dot{y}}$, REST API access for the administrator user is enabled.

The below table depicts the details of the xml file.

Note:

A

- In the above list of parameters, **dns domain, admin username, admin password, cert-random name, cert-random text, cert-organization** and **accept-license-agreement** are mandatory parameters. The other parameters are optional parameters.
- From 9.1R3 release, Pulse Connect Secure supports zero touch provisioning. This feature can detect and assign DHCP networking settings automatically at the Pulse Connect Secure boot up. The Pulse Connect Secure parameters should be set to null in order to fetch the networking configuration automatically from the DHCP server.

Limitations

The following list of Pulse Connect Secure features are not supported in this release:

- Default VLAN on Internal, External and Management Ports
- VLAN functionality
- AP Cluster
- Layer 3 Tunnel IP pool assignment via DHCP
- Virtual Ports

Appendix A: Security Group (SG)

Alibaba Cloud has a limitation where virtual machine with multiple network interfaces cannot connect to different Virtual Private Cloud (VPCs). For example, a VM with two NICs, NIC1 and NIC2, will not be able to connect to VPC1 and VPC2 respectively.

Figure 29: Virtual Machine with two NICs Connecting to VPC1 and VPC2



Alibaba Cloud supports a virtual machine with multiple NICs to connect to different Subnets under a same Virtual Private Cloud. For example, a VM with two NICs, NIC1 and NIC2, can connect to 'Subnet1' and 'Subnet2' where these subnets exist under a same Virtual Private Cloud respectively.





Alibaba Cloud provides isolation between different VPCs. But it does not provide the same kind of isolation when it comes to subnets in the same VPC. For example, consider a VPC has two subnets, Subnet1 and Subnet2. And consider two VMs, VM-1 and VM-2, which are connected to Subnet1 and Subnet2 respectively. In this scenario VM-1 can access the resources from VM-2 and vice versa.



Figure 31: Virtual Machine VM-1 can Access Resources in VM-2 and Vice Versa

Application isolation is an important concern in enterprise environments, as enterprise customers seek to protect various environments from unauthorized or unwanted access. To achieve the traffic isolation between subnets, go for an option of filtering traffic using "Security Group" provided by Alibaba Cloud.



Figure 32: Traffic Filtering by Alibaba Cloud Support Group

Pulse Connect Secure, when provisioned through the Terraform template provided by Pulse Secure, creates three subnets under a virtual private cloud named "PCSVirtualNetwork". The three Subnets are:

- 1. vsw-zone-a-pcs-int-port-subnet
- 2. vsw-zone-a-pcs-ext-port-subnet
- 3. vsw-zone-a-pcs-mgmt-port-subnet

Along with above mentioned subnets, create the following three Security Groups (SG) policies:

- 1. sg_pcs_int_port
- 2. sg_pcs_ext_port
- 3. sg_pcs_mgmt_port

Figure 33: SG External, Internal and Management Subnets



In Security Group (SG) we need to create policies for Inbound traffic.

- 1. Select Elastic Compute Service > Network & Security > Security Groups.
- 2. The list of SG Inbound rules created "sg_pcs_ext_port" are:

Figure 34: sg_pcs_ext_port - Inbound Rules

sg_pcs_ext_port 💩 vpc_beijing / vpc-2zellq7kn9ou27c8xz1ie						Learn more. 🙄
Inbound		Outbound				
	Action	Protocol Type	Port Range	Authorization Type(All) 👻	Authorization Object	Description
	Allow	Custom TCP	80/80	IPv4 CIDR Block	0.0.0.0/0	HTTP port 80
	Allow	Custom TCP	443/443	IPv4 CIDR Block	0.0.0.0/0	HTTPS port 443
	Allow	Customized UDP	4500/4500	IPv4 CIDR Block	0.0.0/0	UDP Ports for Pulse L3
	Allow	All ICMP (IPv4)	-1/-1	IPv4 CIDR Block	0.0.0/0	Allow All ICMP

3. The list of SG Inbound rules created "sg_pcs_int_port" are:

Figure 35: sg_pcs_int_port - Inbound Rules

sg_	pcs_	int_port 💩	vpc_beijing	/ vpc-2zellq7kn9ou27c8xz1	ie	Learn more. 🙄	
Inbound		Outbound					
	Action	Protocol Type	Port Range	Authorization Type(All) 👻	Authorization Object	Description	
	Allow	All ICMP (IPv4)	-1/-1	IPv4 CIDR Block	0.0.0.0/0	Allow All ICMP	
	Allow	Custom TCP	4808/4809	IPv4 CIDR Block	0.0.0.0/0	TCP Ports 4808 and 480	
	Allow	Custom TCP	4900/4910	IPv4 CIDR Block	0.0.0.0/0	TCP Ports 4900 - 4910	
	Allow	Custom TCP	4804/4804	IPv4 CIDR Block	0.0.0.0/0	UDP Ports for Cluster	
	Allow	Custom TCP	11000/11099	IPv4 CIDR Block	0.0.0/0	TCP Ports for Cluster	
	Allow	Customized UDP	4500/4500	IPv4 CIDR Block	0.0.0.0/0	UDP Ports for Pulse L3	
	Allow	Custom TCP	830/830	IPv4 CIDR Block	0.0.0.0/0	DMI Netconf port	
	Allow	Custom TCP	4803/4803	IPv4 CIDR Block	0.0.0.0/0	UDP Ports for Cluster	
	Allow	Custom TCP	443/443	IPv4 CIDR Block	0.0.0.0/0	HTTPS port 443	

4. The list of SG Inbound rules created "sg_pcs_mgmt_port" are:

Figure 36: sg_pcs_mgmt_port - Inbound Rules

sg_pcs_mgmt_port vpc_beijing / vpc-2zellq7kn9ou27c8xz1ie						Learn more.
Int	ound	Outbound				
	Action	Protocol Type	Port Range	Authorization Type(All) 👻	Authorization Object	Description
	Allow	All ICMP (IPv4)	-1/-1	IPv4 CIDR Block	0.0.0.0/0	Allow All ICMP
	Allow	Custom TCP	443/443	IPv4 CIDR Block	0.0.0.0/0	HTTPS port 443
	Allow	Custom TCP	830/830	IPv4 CIDR Block	0.0.0.0/0	DMI Netconf port 830
	Allow	Custom TCP	80/80	IPv4 CIDR Block	0.0.0.0/0	HTTP port 80

Appendix B: Pulse Connect Secure Terraform Template

Terraform is an open source tool to easily define, preview, and deploy cloud infrastructure on Alibaba Cloud. Pulse Secure provides sample Terraform template files for 2 NICs and 3 NICs to deploy the Pulse Connect Secure Virtual Appliance on Alibaba Cloud. Users can modify this to make it suitable for their need. Visit <u>https://www.pulsesecure.net</u> and download the template file.

- Base Setup
- PCS with 2 NICs
- PCS with 3 NICs
- <u>Variables</u>
- <u>User Data</u>

Base Setup

#Terraform version terraform { required_version = ">= 0.12.18" } #Access Keys provider "alicloud" { access_key = var.access_key secret_key = var.secret_key #region is important region = var.region }

```
#Bucket Creation
```

```
terraform {
   backend "oss" {
    bucket = "bucket-beijing-darumuga"
    prefix = "terraform_state/base_setup_beijing"
    key = "terraform.tfstate"
    region = "cn-beijing"
    tablestore_endpoint = "https://oss-cn-beijing.aliyuncs.com"
   }
  }
#VPCs, VSwitches, Security Groups and Alibaba Cloud PCS VA Images
  #VPCs
  data "alicloud_vpcs" "vpcs_ds" {
        #No args required
  }
  #vSwitches
  data "alicloud_vswitches" "vswitches_ds" {
            = "${local.vpc id}"
   vpc_id
  }
  #available security groups
  data "alicloud_security_groups" "sec_groups_ds" {
   vpc_id
             = "${local.vpc_id}"
  }
  #available images loaded by the user
  data "alicloud_images" "self_images_ds" {
   owners
             = "self" #system | marketplace | others | self
```

```
#Local variables
```

}

```
locals {
    vpcs list
                = "${data.alicloud vpcs.vpcs ds.vpcs}"
            = join ( "", [ for vpc in local.vpcs_list : vpc.id if vpc.vpc_name == "${var.vpc}" ] )
    vpc id
    vsws_list_in_vpc = "${data.alicloud_vswitches.vswitches ds.vswitches}"
    sec groups list = "${data.alicloud security groups.sec groups ds.groups}"
    images list = {
      "self" = "${data.alicloud images.self images ds.images}",
    }
    instance_type = var.instance_type
        region = var.region
        zone
                    = var.zone
        vswitch names map = {
       "${var.zone a}" = {
         "pcs int port" = "vsw-zone-a-pcs-int-port-subnet",
         "pcs ext port" = "vsw-zone-a-pcs-ext-port-subnet",
         "pcs mgmt port" = "vsw-zone-a-pcs-mgmt-port-subnet",
      },
       "${var.zone_b}" = {
         "pcs int port" = "vsw-zone-b-pcs-int-port-subnet",
         "pcs_ext_port" = "vsw-zone-b-pcs-ext-port-subnet",
         "pcs_mgmt_port" = "vsw-zone-b-pcs-mgmt-port-subnet",
      },
    }
    security_group_names_map = {
        "pcs_int_port" = "sg_pcs_int_port",
        "pcs_ext_port" = "sg_pcs_ext_port",
        "pcs_mgmt_port" = "sg_pcs_mgmt_port",
   }
  }
#Create a VPC
  resource "alicloud vpc" "vpc" {
   name
           = "vpc_beijing_darumuga"
   cidr block = "172.16.5.0/24"
  }
#Create vSwitch for zone-a
  #for pcs internal port
  resource "alicloud vswitch" "vsw-zone-a-pcs-int-port-subnet" {
    vpc_id = alicloud_vpc.vpc.id
                 = local.vswitch_names_map[var.zone_a]["pcs_int_port"]
    name
    cidr block = "172.16.5.16/28"
    availability_zone = var.zone_a
  }
  #for pcs external port
  resource "alicloud_vswitch" "vsw-zone-a-pcs-ext-port-subnet" {
    vpc id
            = alicloud vpc.vpc.id
    name
                 = local.vswitch_names_map[var.zone_a]["pcs_ext_port"]
    cidr_block = "172.16.5.32/28"
    availability_zone = var.zone_a
  }
  #for pcs management port
  resource "alicloud vswitch" "vsw-zone-a-pcs-mgmt-port-subnet" {
    vpc_id
                 = alicloud_vpc.vpc.id
    name
                 = local.vswitch_names_map[var.zone_a]["pcs_mgmt_port"]
```

```
cidr block
                  = "172.16.5.48/28"
    availability zone = var.zone a
  }
#Create vSwitch for zone-b
  #for pcs internal port
  resource "alicloud vswitch" "vsw-zone-b-pcs-int-port-subnet" {
              = alicloud vpc.vpc.id
   vpc id
              = local.vswitch_names_map[var.zone_b]["pcs_int_port"]
   name
   cidr block = "172.16.5.64/28"
   availability zone = var.zone b
  }
  #for pcs external port
  resource "alicloud_vswitch" "vsw-zone-b-pcs-ext-port-subnet" {
   vpc id
           = alicloud vpc.vpc.id
              = local.vswitch names map[var.zone b]["pcs ext port"]
   name
   cidr block = "172.16.5.80/28"
   availability zone = var.zone b
  }
  #for pcs management port
  resource "alicloud_vswitch" "vsw-zone-b-pcs-mgmt-port-subnet" {
   vpc id
           = alicloud vpc.vpc.id
              = local.vswitch_names_map[var.zone_b]["pcs_mgmt_port"]
   name
   cidr block = "172.16.5.96/28"
   availability_zone = var.zone_b
  }
#Create Security Groups
  #create security group for pcs internal port
  resource "alicloud_security_group" "sg_pcs_int_port" {
    name
              = local.security_group_names_map["pcs_int_port"]
    description = "Security Group for PCS internal port"
    vpc_id = alicloud_vpc.vpc.id
  }
  #create security group for pcs external port
  resource "alicloud_security_group" "sg_pcs_ext_port" {
              = local.security_group_names_map["pcs_ext_port"]
    name
    description = "Security Group for PCS external port"
    vpc_id = alicloud_vpc.vpc.id
  }
  #create security group for pcs management port
  resource "alicloud_security_group" "sg_pcs_mgmt_port" {
    name
              = local.security_group_names_map["pcs_mgmt_port"]
    description = "Security Group for PCS management port"
    vpc id
            = alicloud_vpc.vpc.id
  }
  #create security group for backend servers
  resource "alicloud_security_group" "sg_backend_svr" {
              = "sg backend svr"
    name
    description = "Security Group for backend servers in protected network"
    vpc_id = alicloud_vpc.vpc.id
  }
#Create Security Group Rules for PCS Internal Port and Assign to Security Group
  #HTTP port 80
  resource "alicloud_security_group_rule" "int_port_allow_tcp_80" {
    description
                 = "HTTP port 80"
    type
                = "ingress"
```

```
ip protocol = "tcp"
  nic_type = "intranet"
  policy = "accept"
  port_range = "80/80"
  priority = 1
  security_group_id = alicloud_security_group.sg pcs int port.id
             = "0.0.0.0/0"
  cidr ip
}
#HTTPS port 443
resource "alicloud security group rule" "int port allow tcp 443" {
  description = "HTTPS port 443"
        = "ingress"
  tvpe
  ip protocol = "tcp"
  nic_type = "intranet"
         = "accept"
  policy
  port_range = "443/443"
  priority = 1
  security group id = alicloud security group.sg pcs int port.id
  cidr_ip = "0.0.0.0/0"
}
#DMI Netconf port
resource "alicloud_security_group_rule" "int_port_allow_tcp_dmi_830" {
  description = "DMI Netconf port"
  type
        = "ingress"
  ip_protocol = "tcp"
  nic_type = "intranet"
         = "accept"
  policy
  port_range = "830/830"
  priority = 1
  security_group_id = alicloud_security_group.sg_pcs_int_port.id
  cidr_ip = "0.0.0.0/0"
}
#Allow All ICMP
resource "alicloud_security_group_rule" "int_port_allow_all_icmp" {
  description = "Allow All ICMP"
  type = "ingress"
  ip_protocol = "icmp"
  nic_type = "intranet"
  policy
         = "accept"
  port_range = "-1/-1"
           = 1
  priority
  security_group_id = alicloud_security_group.sg_pcs_int_port.id
  cidr_ip = "0.0.0.0/0"
}
#TCP Ports for Cluster Communication
resource "alicloud_security_group_rule" "int_port_allow_tcp_cluster_comms" {
  description = "TCP Ports for Cluster Communication"
          = "ingress"
  type
  ip_protocol = "tcp"
  nic_type = "intranet"
  policy
           = "accept"
  port_range = "11000/11099"
             = 1
  priority
  security_group_id = alicloud_security_group.sg_pcs_int_port.id
             = "0.0.0.0/0"
  cidr_ip
}
#TCP Ports 4808 and 4809 for Cluster Communication
```

```
resource "alicloud security group rule" "int port allow tcp cluster comms 4808 4809" {
  description
               = "TCP Ports 4808 and 4809 for Cluster Communication"
  type
           = "ingress"
  ip_protocol = "tcp"
  nic_type
              = "intranet"
  policy
         = "accept"
  port_range = "4808/4809"
  priority = 1
  security_group_id = alicloud_security_group.sg pcs int port.id
          = "0.0.0.0/0"
  cidr ip
}
#TCP Ports 4900 - 4910 for Cluster Key Exchange and State Sync
resource "alicloud_security_group_rule" "int_port_allow_tcp cluster key exchange and svnc" {
  description = "TCP Ports 4900 - 4910 for Cluster Key Exchange and State Sync"
          = "ingress"
  tvpe
  ip_protocol = "tcp"
  nic_type = "intranet"
  policy
             = "accept"
  port_range = "4900/4910"
  priority
             = 1
  security group id = alicloud security group.sg pcs int port.id
          = "0.0.0.0/0"
  cidr_ip
}
#UDP Ports for Cluster Communication
resource "alicloud_security_group_rule" "int_port_allow_udp_cluster_comms" {
  description = "UDP Ports for Cluster Communication"
          = "ingress"
  type
  ip_protocol = "tcp"
  nic_type = "intranet"
  policy
             = "accept"
  port_range = "4803/4803"
             = 1
  priority
  security_group_id = alicloud_security_group.sg_pcs_int_port.id
          = "0.0.0.0/0"
  cidr_ip
}
#UDP Ports for Cluster HeartBeat
resource "alicloud_security_group_rule" "int_port_allow_udp_cluster_hearbeat" {
  description = "UDP Ports for Cluster HeartBeat"
  type
          = "ingress"
  ip_protocol = "tcp"
           = "intranet"
  nic_type
  policy
              = "accept"
  port_range = "4804/4804"
  priority = 1
  security_group_id = alicloud_security_group.sg_pcs_int_port.id
             = "0.0.0.0/0"
  cidr_ip
}
#UDP Ports for Pulse L3 Connection
resource "alicloud_security_group_rule" "int_port_allow_udp_pulse_client" {
  description = "UDP Ports for Pulse L3 Connection"
  type
            = "ingress"
  ip_protocol = "udp"
  nic_type = "intranet"
             = "accept"
  policy
  port_range = "4500/4500"
  priority
              = 1
  security_group_id = alicloud_security_group.sg_pcs_int_port.id
```

```
cidr ip
                = "0.0.0/0"
  }
#Create Security Group Rules for PCS External Port and Assign to Security Group
  #HTTP port 80
  resource "alicloud_security_group_rule" "ext_port_allow_tcp 80" {
        description
                                  = "HTTP port 80"
        type
                   = "ingress"
        ip_protocol = "tcp"
                 = "intranet"
        nic type
                 = "accept"
        policy
        port_range = "80/80"
        priority = 1
        security_group_id = alicloud_security_group.sg_pcs_ext_port.id
                  = "0.0.0.0/0"
        cidr ip
  }
  #HTTPS port 443
  resource "alicloud_security_group_rule" "ext_port_allow_tcp_443" {
        description
                                  = "HTTPS port 443"
                 = "ingress"
        type
        ip_protocol = "tcp"
                   = "intranet"
        nic type
               = "accept"
        policy
        port_range = "443/443"
                 = 1
        priority
        security_group_id = alicloud_security_group.sg_pcs_ext_port.id
                = "0.0.0.0/0"
        cidr_ip
  }
  #Allow All ICMP
  resource "alicloud_security_group_rule" "ext_port_allow_all icmp" {
                                  = "Allow All ICMP"
        description
              = "ingress"
        type
        ip_protocol = "icmp"
        nic_type = "intranet"
                  = "accept"
        policy
        port_range = "-1/-1"
        priority
                 = 1
        security_group_id = alicloud_security_group.sg_pcs_ext_port.id
        cidr ip
                   = "0.0.0.0/0"
  }
  #UDP Ports for Pulse L3 Connection
  resource "alicloud_security_group_rule" "ext_port_allow_udp_pulse_client" {
        description
                                  = "UDP Ports for Pulse L3 Connection"
              = "ingress"
        type
        ip_protocol = "udp"
        nic_type = "intranet"
        policy
               = "accept"
        port_range = "4500/4500"
                 = 1
        priority
        security_group_id = alicloud_security_group.sg_pcs_ext_port.id
                   = "0.0.0.0/0"
        cidr ip
  }
#Create Security Group Rules for PCS Management Port and Assign to Security Group
  #HTTP port 80
  resource "alicloud_security_group_rule" "mgmt_port_allow_tcp_80" {
        description
                                  = "HTTP port 80"
        type
                   = "ingress"
```

```
ip protocol = "tcp"
        nic type = "intranet"
                 = "accept"
        policy
        port_range = "80/80"
        priority = 1
        security group id = alicloud security group.sg pcs mgmt port.id
                   = "0.0.0.0/0"
        cidr ip
  }
  #HTTPS port 443
  resource "alicloud_security_group_rule" "mgmt_port_allow_tcp_443" {
                                = "HTTPS port 443"
        description
              = "ingress"
        type
        ip protocol = "tcp"
        nic_type = "intranet"
               = "accept"
        policy
        port_range = "443/443"
        priority = 1
        security group id = alicloud security group.sg pcs mgmt port.id
                = "0.0.0.0/0"
        cidr ip
  }
  #DMI Netconf port 830
  resource "alicloud_security_group_rule" "mgmt_port_allow_tcp_dmi_830" {
        description
                                 = "DMI Netconf port 830"
        type
                  = "ingress"
        ip_protocol = "tcp"
        nic_type = "intranet"
               = "accept"
        policy
        port_range = "830/830"
        priority = 1
        security_group_id = alicloud_security_group.sg_pcs_mgmt_port.id
        cidr_ip = "0.0.0.0/0"
  }
  #Allow All ICMP
  resource "alicloud_security_group_rule" "mgmt_port_allow_all_icmp" {
        description
                                 = "Allow All ICMP"
              = "ingress"
        type
        ip_protocol = "icmp"
        nic_type = "intranet"
        policy
               = "accept"
        port_range = "-1/-1"
                 = 1
        priority
        security_group_id = alicloud_security_group.sg_pcs_mgmt_port.id
        cidr_ip
                = "0.0.0.0/0"
  }
#Create Security Group Rules for Backend Servers and Assign to Security Group
  #HTTP port 80
  resource "alicloud_security_group_rule" "backend_svr_allow_tcp_80" {
                                 = "HTTP port 80"
        description
                = "ingress"
        type
        ip_protocol = "tcp"
        nic_type
                  = "intranet"
                   = "accept"
        policy
        port_range = "80/80"
        priority = 1
        security_group_id = alicloud_security_group.sg_backend_svr.id
                   = "0.0.0/0"
        cidr_ip
```

```
#HTTPS port 443
resource "alicloud_security_group_rule" "backend_svr_allow_tcp_443" {
                               = "HTTPS port 443"
      description
      type
              = "ingress"
      ip_protocol = "tcp"
               = "intranet"
      nic_type
              = "accept"
      policy
      port_range = "443/443"
      priority = 1
      security_group_id = alicloud_security_group.sg_backend_svr.id
      cidr_ip = "0.0.0.0/0"
}
#SSH port 22
resource "alicloud_security_group_rule" "backend_svr_allow_tcp_ssh_22" {
                               = "SSH port 22"
      description
      type
                = "ingress"
      ip_protocol = "tcp"
      nic_type = "intranet"
      policy
             = "accept"
      port range = "22/22"
      priority = 1
      security_group_id = alicloud_security_group.sg_backend_svr.id
      cidr_ip = "0.0.0.0/0"
}
#Allow All ICMP
resource "alicloud_security_group_rule" "backend_svr_allow_all_icmp" {
                               = "Allow All ICMP"
      description
      type
              = "ingress"
      ip_protocol = "icmp"
      nic_type = "intranet"
              = "accept"
      policy
      port_range = "-1/-1"
      priority
               = 1
      security_group_id = alicloud_security_group.sg_backend_svr.id
              = "0.0.0.0/0"
      cidr_ip
}
```

PCS with 2 NICs

}

```
#Terraform version
    terraform {
        required_version = ">= 0.12.18"
    }
#Access Keys
    provider "alicloud" {
        access_key = var.access_key
        secret_key = var.access_key
        secret_key = var.secret_key
        #region is important
        region = var.region
    }
#VPCs , VSwitches, Security Groups and Alibaba Cloud PCS VA Images
    #VPCs
```

```
data "alicloud vpcs" "vpcs ds" {
        #No args required
  }
  #vSwitches
  data "alicloud vswitches" "vswitches_ds" {
            = "${local.vpc_id}"
   vpc id
  }
  #available security groups
  data "alicloud_security_groups" "sec_groups ds" {
             = "${local.vpc_id}"
   vpc id
  }
  #available images loaded by the user
  data "alicloud images" "self images ds" {
   owners = "self" #system | marketplace | others | self
  }
#Local variables
  locals {
    vpcs_list
                 = "${data.alicloud vpcs.vpcs ds.vpcs}"
    vpc id = join ("", [ for vpc in local.vpcs list : vpc.id if vpc.vpc name == "${var.vpc}"])
    vsws_list_in_vpc = "${data.alicloud_vswitches.vswitches_ds.vswitches}"
     sec_groups_list = "${data.alicloud_security_groups.sec_groups_ds.groups}"
     images_list = {
       "self" = "${data.alicloud_images.self_images_ds.images}",
    }
     instance_type = var.instance_type
        region = var.region
        zone
                     = var.zone
        security_group_id_map = {
                 "pcs_int_port" = join ("", [ for sec_group in local.sec_groups_list : sec_group.id if
  sec_group.name == "sg_pcs_int_port" ]),
                 "pcs_ext_port" = join ("", [ for sec_group in local.sec_groups_list : sec_group.id if
  sec_group.name == "sg_pcs_ext_port" ]),
                 "pcs mgmt port" = join ("", [ for sec group in local.sec groups list : sec group.id if
  sec_group.name == "sg_pcs_mgmt_port" ]),
        }
        vswitch_id_map = {
                 "${var.zone_a}" = {
                           "pcs_int_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-a-pcs-int-port-subnet" ]),
                          "pcs_ext_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-a-pcs-ext-port-subnet" ]),
                          "pcs_mgmt_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-a-pcs-mgmt-port-subnet" ])
                 },
                  "${var.zone b}" = {
                          "pcs_int_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-b-pcs-int-port-subnet" ]),
                          "pcs_ext_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-b-pcs-ext-port-subnet" ]),
                          "pcs_mgmt_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-b-pcs-mgmt-port-subnet" ])
                 }
        }
  }
#PCS instance on Alibaba Cloud
  resource "alicloud_instance" "pcs_instance" {
```

```
instance name
                        = var.instance name
    image id = join ("", [ for pcs image in local.images list[var.image from] : pcs image.image id if
  pcs_image.name == var.image_name ])
    availability_zone = var.zone
    #instance_type = var.instance_type #ecs.hfc5.large
    instance type = "ecs.n1.large" #customise according to your needs
    instance charge type = var.instance charge type #PayByBandwidth
    system disk category = "cloud efficiency"
    vswitch id = local.vswitch id map[local.zone]["pcs int port"]
    security groups = [local.security group id map["pcs int port"]]
    #internet max bandwidth out = 1 #in mbps, when this value is set, a public IP(not elastic IP) is assigned
    #internet charge type = "PavBvBandwidth"
    #user-data
    user data = file("user data.txt")
  }
#Create External Port
  resource "alicloud network interface" "pcs ext port" {
    name = "pcs_ext_port"
    vswitch id = local.vswitch id map[local.zone]["pcs ext port"]
    security_groups = [ local.security_group_id_map["pcs_ext_port"] ]
  }
  resource "alicloud_network_interface_attachment" "pcs_ext_port_attachment" {
                = alicloud instance.pcs instance.id
   instance id
   network_interface_id = alicloud_network_interface.pcs_ext_port.id
  }
#Create a new EIP
  # Create a new EIP for Internal Port.
  resource "alicloud_eip" "pcs_int_port_eip" {
   bandwidth = "5"
   internet_charge_type = "PayByTraffic"
  }
  resource "alicloud_eip_association" "pcs_int_port_eip_asso" {
   allocation_id = alicloud_eip.pcs_int_port_eip.id
   instance id = alicloud instance.pcs instance.id
  }
  # Create a new EIP for External Port.
  resource "alicloud_eip" "pcs_ext_port_eip" {
                = "5"
   bandwidth
   internet_charge_type = "PayByTraffic"
  }
  resource "alicloud_eip_association" "pcs_ext_port_eip_asso" {
   allocation_id = alicloud_eip.pcs_ext_port_eip.id
   instance_id = alicloud_network_interface.pcs_ext_port.id #if instance_type is NetworkInterface,
  instance_id should point to the ENI ID(not VM instance ID)
   instance_type = "NetworkInterface" #for assigning EIP to ext port(which is secondary ENI)
   private_ip_address = alicloud_network_interface.pcs_ext_port.private_ip
  }
#Output
  output "pcs_int_port" {
   value = "${alicloud_instance.pcs_instance.private_ip}"
  }
  output "pcs_ext_port" {
    value = "${alicloud_network_interface.pcs_ext_port.private_ip}"
```

PCS with 3 NICs

}

```
#Terraform version
  terraform {
    required_version = ">= 0.12.18"
  }
#Access Keys
  provider "alicloud" {
    access_key = var.access_key
    secret_key = var.secret_key
    #region is important
    region = var.region
  }
#VPCs, VSwitches, Security Groups and Alibaba Cloud PCS VA Images
  #VPCs
  data "alicloud vpcs" "vpcs ds" {
        #No args required
  }
  #vSwitches
  data "alicloud_vswitches" "vswitches_ds" {
            = "${local.vpc_id}"
   vpc id
  }
  #available security groups
  data "alicloud security groups" "sec groups ds" {
            = "${local.vpc id}"
   vpc id
  }
  #available images loaded by the user
  data "alicloud_images" "self_images_ds" {
   owners = "self" #system | marketplace | others | self
  }
#Local variables
  locals {
    vpcs_list = "${data.alicloud_vpcs.vpcs_ds.vpcs}"
             = join ( "", [ for vpc in local.vpcs_list : vpc.id if vpc.vpc_name == "${var.vpc}" ] )
    vpc_id
    vsws_list_in_vpc = "${data.alicloud_vswitches.vswitches_ds.vswitches}"
    sec_groups_list = "${data.alicloud_security_groups.sec_groups_ds.groups}"
    images_list
                     = {
      "self" = "${data.alicloud_images.self_images_ds.images}",
    }
    instance_type = var.instance_type
        region
                     = var.region
```

```
zone
                     = var.zone
        security group id map = {
                 "pcs int port" = join ("", [ for sec group in local.sec groups list : sec group.id if
  sec group.name == "sg pcs int port" ]),
                 "pcs_ext_port" = join ("", [ for sec_group in local.sec_groups_list : sec_group.id if
  sec group.name == "sg pcs ext port" ]),
                 "pcs mgmt port" = join ("", [ for sec group in local.sec groups list : sec group.id if
  sec group.name == "sg pcs mgmt port" ]),
        }
        vswitch id map = {
                 "${var.zone a}" = {
                          "pcs int port" = join ("", [ for vswitch in local.vsws list in vpc : vswitch.id if
  vswitch.name == "vsw-zone-a-pcs-int-port-subnet" ]).
                          "pcs ext port" = join ("", [ for vswitch in local.vsws list in vpc : vswitch.id if
  vswitch.name == "vsw-zone-a-pcs-ext-port-subnet" ]).
                          "pcs mgmt port" = join ("", [ for vswitch in local.vsws list in vpc : vswitch.id if
  vswitch.name == "vsw-zone-a-pcs-mgmt-port-subnet" ])
                 },
                 "${var.zone b}" = {
                          "pcs_int_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-b-pcs-int-port-subnet" ]),
                          "pcs_ext_port" = join ("", [ for vswitch in local.vsws_list_in_vpc : vswitch.id if
  vswitch.name == "vsw-zone-b-pcs-ext-port-subnet" ]),
                          "pcs mgmt port" = join ("", [ for vswitch in local.vsws list in vpc : vswitch.id if
  vswitch.name == "vsw-zone-b-pcs-mgmt-port-subnet" ])
                 }
        }
  }
#PCS Instance on Alibaba Cloud
  resource "alicloud instance" "pcs instance" {
     instance_name = var.instance_name
                      = join ("", [ for pcs_image in local.images_list[var.image_from] : pcs_image.image_id if
     image_id
  pcs image.name == var.image name ])
     availability_zone = var.zone
     #instance_type = var.instance_type #ecs.hfc5.large
     instance_type = "ecs.n1.xlarge" #customise according to your needs
     instance_charge_type = var.instance_charge_type #PayByBandwidth
     system_disk_category = "cloud_efficiency"
                            = local.vswitch_id_map[local.zone]["pcs_int_port"]
     vswitch_id
     security_groups
                            = [ local.security_group_id_map["pcs_int_port"] ]
     #internet max bandwidth out = 1 #in mbps, when this value is set, a public IP(not elastic IP) is assigned
     #internet_charge_type = "PayByBandwidth"
     #user-data
     user_data = file("user_data.txt")
  }
#Create External Port and Management Port
  #create external port and attach to PCS instance
  resource "alicloud network interface" "pcs ext port" {
                    = "pcs_ext_port"
    name
    vswitch id
                    = local.vswitch_id_map[local.zone]["pcs_ext_port"]
     security_groups = [ local.security_group_id_map["pcs_ext_port"] ]
  }
  resource "alicloud network interface attachment" "pcs ext port attachment" {
                        = alicloud_instance.pcs_instance.id
   instance id
```

```
network interface id = alicloud network interface.pcs ext port.id
  }
  #create management port and attach to PCS instance
  resource "alicloud network interface" "pcs mgmt port" {
    name
            = "pcs ext port"
    vswitch id = local.vswitch id map[local.zone]["pcs mgmt port"]
    security_groups = [ local.security_group_id_map["pcs_mgmt_port"] ]
  }
  resource "alicloud network interface attachment" "pcs mgmt port attachment" {
                   = alicloud instance.pcs instance.id
   instance id
   network interface id = alicloud network interface.pcs mgmt port.id
  }
#Create a new EIP
  # Create a new EIP for External Port.
  resource "alicloud eip" "pcs ext port eip" {
                = "5"
   bandwidth
   internet_charge_type = "PayByTraffic"
  }
  resource "alicloud eip association" "pcs ext port eip asso" {
                      = alicloud_eip.pcs_ext_port_eip.id
   allocation_id
   instance id
                                           = alicloud network interface.pcs ext port.id #if instance type is
  NetworkInterface, instance_id should point to the ENI ID(not VM instance ID)
                                           = "NetworkInterface" #for assigning EIP to ext port(which is secondary
   instance_type
  ENI)
   private_ip_address = alicloud_network_interface.pcs_ext_port.private_ip
  }
  # Create a new EIP for Management Port.
  resource "alicloud_eip" "pcs_mgmt_port_eip" {
                = "5"
   bandwidth
   internet_charge_type = "PayByTraffic"
  }
  resource "alicloud_eip_association" "pcs_mgmt_port_eip_asso" {
        allocation id
                       = alicloud_eip.pcs_mgmt_port_eip.id
        instance_id
                                                   = alicloud_network_interface.pcs_mgmt_port.id
                                           = "NetworkInterface"
        instance type
        private_ip_address = alicloud_network_interface.pcs_mgmt_port.private_ip
  }
#Output
  output "pcs_int_port" {
   value = "${alicloud_instance.pcs_instance.private_ip}"
  }
  output "pcs_ext_port" {
    value = "${alicloud_network_interface.pcs_ext_port.private_ip}"
  }
  output "pcs mgmt port" {
    value = "${alicloud_network_interface.pcs_mgmt_port.private_ip}"
  }
```

Variables

```
variable access_key {
  default = "alicloud-access-key" #replace with the actual alicloud-access key
}
variable secret_key {
  default = "alicloud-secret-key" #replace with the actual alicloud-secret-key
}
variable region {
  default = "cn-beijing"
}
variable zone {
  default = "cn-beijing-a"
}
variable zone_a {
  default = "cn-beijing-a"
}
variable zone_b {
  default = "cn-beijing-b"
}
variable vpc {
  default = "vpc_beijing"
}
variable image_name {
  default = "pcs_91r4_alicloud_image"
}
variable image_from {
  default = "self"
  #default = "marketplace"
}
variable instance_type {
      default = "ecs.n1.large"
}
variable instance_name {
  default = "pcs_91r4_on_alicloud"
}
variable cpu_core_count {
  default = "4"
}
variable memory_size {
  default = "8"
}
variable eni_amount {
  default = "2"
}
variable oss_bucket {
      default = "bucket-beijing-darumuga"
}
variable instance_charge_type {
  default = "PostPaid"
}
```

User Data

<pulse-config><primary-dns>8.8.8.4/primary-dns><secondary-dns>8.8.8.9</secondary-dns><winsserver>1.1.1.1</wins-server><dns-domain>pcsqa.psecure.net</dns-domain><admin-</pre>

username>admindb</admin-username><admin-password>Psecure123\$</admin-password><cert-common-name>alicloud-pcs.psecure.net</cert-common-name><cert-random-text>fdsfpisonvsfnms</cert-random-text><cert-organisation>Psecure Org</cert-organisation><config-download-

url>http://149.129.181.113/pcs_config/pcs_config.xml</config-download-url><config-data></config-data><auth-code-license></auth-code-license><enable-license-server>n</enable-license-server><accept-license-agreement></pulse-config>

References

Alibaba Cloud documentation: <u>https://www.alibabacloud.com/help/</u>

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

• Product warranties—for product warranty information, visit https://www.pulsesecure.net.