



FortiADC - Alibaba Cloud Deployment Guide

Version 7.0.0



FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE https://video.fortinet.com

FORTINET BLOG https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

NSE INSTITUTE https://training.fortinet.com

FORTIGUARD CENTER https://www.fortiguard.com

END USER LICENSE AGREEMENT https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK Email: techdoc@fortinet.com



April 25, 2022 FortiADC 7.0.0 Alibaba Cloud Deployment Guide 01-544-677187-20220425

TABLE OF CONTENTS

Change Log	
Introduction	5
Deploying the FortiADC-VM in Alibaba Cloud	6
Creating a VPC (Virtual Private Cloud)	6
Creating the FortiADC-VM instance	
Configuring the Security Group Rules	
Accessing the FortiADC GUI and CLI	14
Important notes	

Change Log

Date	Change Description
April 21, 2020	Initial release.
March 29, 2022	Second release with Marketplace support.

Introduction

Alibaba Cloud Elastic Compute Service (ECS) provides fast memory and the latest Intel CPUs to help you power your cloud applications and achieve faster results with low latency.

This guide describes how to create an ECS instance of FortiADC-VM on Alibaba Cloud Infrastructure, including image upload to Cloud, instance creation, and console access.

Deploying the FortiADC-VM in Alibaba Cloud

Follow the workflow below to deploy the FortiADC-VM instance on Alibaba Cloud.

- 1. Creating a VPC (Virtual Private Cloud) on page 6
- 2. Creating the FortiADC-VM instance on page 9
- 3. Configuring the Security Group Rules on page 12
- 4. Accessing the FortiADC GUI and CLI on page 14

Creating a VPC (Virtual Private Cloud)

Create a virtual private cloud (VPC) to deploy your Alibaba Cloud resources. In the following steps you will be specifying the CIDR block and vSwitch required to deploy the FortiADC-VM.

- 1. Log in to your Alibaba Cloud Account and log on to the VPC console.
- In the top navigation bar, select the region where you want to deploy the VPC.
 Note: The VPC and the cloud resources that you want to deploy in the VPC must belong to the same region.
- 3. On the VPCs page, click Create VPC.

≡	C-) Alibaba Cloud	合 Workb	ench 🗧 All Resources 🗸	✓ ● US (Silicon Valley)	~
VPC	<u>^</u>	VPC / VPCs			
VPCs		VPCs			
vSwitc	h	Create VP	C Instance Name 🗸	Q Enter an Instance Name to	perform exact match
Route	Tables				
NAT G	ateway ^		Instance ID/Name	Tags	IPv4 CIDR Block
Inte	rnet NAT Gateway		-	¢	
VPC	CNAT Gateway				
NA	F Gateway Resource Plan			•	

4. On the Create VPC page, set the following parameters and click OK.

Parameter	Description
VPC	
Region	Displays the region where you want to create the VPC.
Name	Enter a name for the VPC.

Parameter	Description
	The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (–). It must start with a letter.
IPv4 CIDR Block	Enter an IPv4 CIDR block for the VPC. You can specify one of the following CIDR blocks or their subsets as the primary IPv4 CIDR block of the VPC: 192.168.0.0/16, 172.16.0.0/12 and 10.0.0.0/8. These CIDR blocks are standard private CIDR blocks as defined by Request for Comments (RFC) documents. The subnet mask must be 8 to 28 bits in length. For example, enter 192.168.0.0/24. Note : After you create a VPC, you cannot change its primary IPv4 CIDR block.
vSwitch	
Name	Enter a name for the vSwitch. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). The name must start with a letter.
Zone	Select a zone for the vSwitch. In the same VPC, vSwitches in different zones can communicate with each other.
Zone Resources	Displays the cloud resources that can be created in the specified zone.
IPv4 CIDR Block	 Specify the IPv4 CIDR block of the vSwitch. When you specify an IPv4 CIDR block for the vSwitch, take note of the following limits: The CIDR block of a vSwitch must be a subset of the CIDR block of the VPC to which the vSwitch belongs. For example, if the CIDR block of a VPC is 192.168.0.0/16, the CIDR block of a vSwitch in the VPC must be a subset of 192.168.0.0/16. In this example, the CIDR block of the vSwitch can range from 192.168.0.0/17 to 192.168.0.0/29.
	 The first IP address and last three IP addresses of a vSwitch CIDR block are reserved. For example, if a vSwitch CIDR block is 192.168.1.0/24, the IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.
	 If a vSwitch is required to communicate with vSwitches in other VPCs or with data centers, make sure that the CIDR block of the vSwitch does not overlap with the destination CIDR blocks. Note: After you create a vSwitch, you cannot change its CIDR block

😑 🕞 Alibaba Cloud	✿ Workbench ■ US (Silicon Valley) ∨	Search	Expenses
VPC	VPC / VPC / Create VPC		
VPCs	← Create VPC		
vSwitch			
Route Tables	VPC Region		
NAT Gateway	US (Silicon Valley)		
Internet NAT Gateway	* Name 📀		
VPC NAT Gateway	fadc-test-ylliu		15/128 🥥
NAT Gateway Resource Plan	* IPv4 CIDR Block		
Endpoints	We recommend that you use one of the private RFC CIDR blocks as the VPC CIDR block: 10.0.0.0/8 , 172.16 Suggestions on CIDR Block Configuration	5.0.0/12 , and 192.168.0.0/16 .	
Endpoints Service			
DHCP Options Sets	 You cannot change the CIDR block after the VPC is created. 		
= (-) Alibaba Cloud	Workbench IS (Silicon Valley)	Q Search	
	vSwitch		
VPC	✓ Create vSwitch		Delete
VPCs	* Name 🕢		
vSwitch	vs-fadc-ylliu		13/128 🥑
Route Tables	* Zone 🕢		
NAT Gateway	Silicon Valley Zone A 🗸		
Internet NAT Gateway	Zone Resources 🕢		
VPC NAT Gateway	ECS 🔗 RDS 🛇 SLB 🥥		
NAT Gateway Resource Plan	IPv4 CIDR Block Suggestions on CIDR Block Configuration		
Endpoints	192 • 168 • 117 • 0 / 24 ·		
Endpoints Service	Available IP Addresses		
DHCP Options Sets	252		
Access to Internet	Description 🕜		
Elastic IP Addresses			
Anycast Elastic IP Addresses			
Internet Shared Bandwidth			0/256
Data Transfer Plan	+ Add		
IPv6 Gateway			
Internet Tool Kit	OK Cancel		
· · · · · · · · · · · · · · · · · · ·			

Next Step:

Creating the FortiADC-VM instance on page 9

Creating the FortiADC-VM instance

Create the FortiADC-VM instance from the Marketplace to automatically deploy the latest FortiADC version. To use earlier FortiADC versions, you can manually downgrade to the specified version in the FortiADC GUI after deploying the VM.

1. Go to Alibaba Cloud > Marketplace, and search for FortiADC. The search will return the Fortinet FortiADC (BYOL) Application Delivery Controller.

C-) Alibaba Cloud					몃 Shop
Marketplace	All Products User Help C	Contact Us	Search	Q	My Subscript
Software Infrastructure /	Security / Fortinet FortiADC (BYOL)	Application Delivery Control	ler		
	Fortinet FortiADC (BYOL)	Application Deliver	y Controller		
FORTIDET	FortiADC Application Delivery Contro application security (WAF).	ollers (ADC) provides applica	ation availability,	web optimization, a	nd
	Delivery Method: Image Architect	ture: 64 Base Operating S	System: linux	Latest Version: 7.0.	0
	\$ 0 USD/Hour Monthly Subscription Price: \$ 0 USD	/Month Yearly Sut	oscription Price :	\$ 0 USD/Year	
	Monthly Renewal Price: \$ 0 USD	/Month Yearly Rer	newal Price:	\$ 0 USD/Year	
	Choose Your Plan				

2. Click Choose Your Plan.

This creates a FortiADC instance using a default image of the latest version.

- 3. Navigate to Elastic Compute Service > Instances. Click Create Instance.
- 4. Go to the Custom Launch tab.
- 5. Complete the following Basic Configuration settings.

Setting	Description
Billing method	 Select a billing method: Subscription — Pay for resources before you use them. Pay-As-You-Go — Use resources first and pay for them afterward. The billing cycles of pay-as-you-go instances are accurate to the second. You can purchase and release instances on demand.

Setting		Description
		 Preemptive Instance — Use resources first and pay for them afterward. You place a bid for available instance resources to create preemptible instances at a discount compared with pay-as-you-go instance pricing. Preemptible instances may be automatically released due to fluctuations in market price or insufficient resources of instance types.
Region and	d zone	Select a region that is close to your geographical location to reduce latency. After an instance is created, the region and the zone of the instance cannot be changed.
Instance ty	vpe	Select the instance type. We suggest to select an instance type that has a minimum of 4 GB of memory.
Image		Select the Marketplace Image.
Storage		Add a Data Disk for the FortiADC log Disk.
		We suggest to select a disk with a minimum of 30 GB.
Selected Instance Type	General Purpose Type ecs.g5.xlarge 4 g5 General Purpose Type ecs.g5.xlarge 4 g5 ecs.g5.xlarge 4 g6 monos ecs.g5.xlarge 4 g6 ecs.g5.xlarge 4 4 g6 ecs.g5.xlarge 4 4 g6 ecs.g5.xlarge 4 4	VCPUs 16 Gi8 2.5 GHz/2.7 GHz 1.5 Gbps 500,000 PPS - Yes Intel Xeon(Skylake) Platinum 8163 / Intel Xeon(Cascade Lake) Platinum 8269CY vCPUs 32 Gi8 2.5 GHz/2.7 GHz 2.5 Gbps 800,000 PPS - Yes Intel Xeon(Skylake) Platinum 8163 / Intel Xeon(Cascade Lake) Platinum 8269CY •
Quantity	- 1 + Units You can create the largest n	umber of instances of the selected instance type in Singapore Zone C. 1 instances have been created. You can create 1279 more instances. To create more instances, go to increase the quota>
Image	Public Image Custom Image Selected Image FortiADC (BYOL) Application Delive Reselect an image Reselect an image ECS instances created in this region do not allow the switch	Shared Image Marketplace Image Community Image (7) y Controller 7.0.0 (7) h of OS between Linux and Windows.
Storage Disk specifications and performance	System Disk Enhanced SSD (ESSD) ¥ 40 GiB Click here for guidelines on how to select an appropriate of	2280 ICPS Performance Level 💮 : PL0 (up to 10.000 ICPS per disk) 🔹
	Data Daik You have selected 1 disks and can select 7 md + Add Disk - Enhanced SSD (ESSD) You have purchased Enhanced SSD (ESSD) 0 GiB in > NAS File System	GiB 3800 IOPS Performance Level (): PL1 (up to 50,000 IOPS per disk) 💌 Quantity: 1 Device Name 🔽 Release with Instance Create from Snapshot 🗌 Disk Encryption the region. Remaining quota: 65496 GiB
Snapshot	Backup Period : Select Automatic Snapshot Policy	Create Automatic Snapshot Policy> Data Source : Select a data source * ①
	9 You can use automatic snapshot policies to periodi	cally back up disks to prevent risks such as virus attacks and accidental data deletion. Snapshot pricing (pay-as-you-go billing and hourly payment collection) >
Quantity: - 1 +	- Units	Total: \$ 0.138 USD per Hour (*) Marketplace Image Fees: \$ 0.000 USD per Hour Preview

6. Click Next to move forward to Networking and configure the following settings:

Setting	Description
Network Type	Select the VPC and vSwitch that was previously configured in Creating the FortiADC-VM instance on page 9.
Public IP Address	Select the Assign Public IPv4 Address if you want to have the internet access the FortiADC.
Security Group	Select HTTP and HTTPS.

Setting	Description						
	Take note of the Security Group ID/Name. It will be used in later steps.						
Basic Configurations	2 Networking 3 System Configurations (Optional) 4 Grouping (Optional) 5 Preview						
Network Type	VPC ()						
Learn more	fado:test:ylliu / vpc-rj96adtwotbrag8dd3988y 📀 vs-fadocylliu / vsw-rj997b3bb0wls2xr5qau 💿 Private IP Addresses Available: 242,						
	To create a new VPC, go to the VPC console. VSwitch Zone: Silicon Valley Zone A VSwitch CIDR Block: 192.168.117.0/24						
Public IP Address Bandwidth pricing	Assign Public IPv4 Address The system will automatically allocate an IP address. In addition, you can use a more flexible EIP solution. Click here to learn more about how to attach an EIP >						
Bandwidth Billing	Pay-8y-Traffic Pay-8y-Bandwidth 0						
Peak Bandwidth	рани и страна и стр						
	Alibaba Cloud provides up to 5 Gbit/s protection against DDoS attacks for free.Learn More Reinforce Protection The data transfer plan is a great deal for reducing the traffic cost generated by your ECS/EIP/SLB instances. Buy a data transfer plan>.						
Security Group Security group limits	Reselect Security Group 🕥 A security group functions similarly to firewalls and is used to set network access controls for one or more ECS instances. You can go to the Security Groups page in the ECS console to create a security group. Learn More						
Learn more	Security Group 1). sg-tyPlzdnolmf/9ttSrna (contains 14 instances, and 1906 more instances can be added.)						
	Ensure that your security group has port 22 (Linux) or 3390 (Windows) allowed in the security group rules. Unnewise, you will not be able to connect to the CS instance. You can add security group rules to your security group in the CS console.						
Elastic Network	Default ENI						
Interface	VSwitch vs-fade-ylliu State-assign IP Addresses Release with Instance						
	T Row Give Top Can app up to 1 cm.						
Quantity: - 1 +	Units Total: \$ 0.132 USD per Hour (*) Marketprace Image Fees: \$ 0.000 USD per Hour						

7. Click Preview. Agree to the ECS Terms of Service then click Create Instance.

Elastic Compute Se	ervice (ECS) Quick Launch	Custom Launch			Savings Plan	③ Purchase History	Pricing	🖙 Buy Disk	Console
Basic Configuration	s V Netv	vorking	System Configurations (Optional) ——— 🕑 Gro	uping (Optional) –		5	Preview	
Note: You have not configur information about hor	ed the instance logon credentials. If you need to k w to reset the password, see Reset the logon passw	og on to the instance, you can go back to the word of an instance.	e System Configurations (Optional) step to configu	re logon credentials. You can also perfo	rm the Reset Password	l operation in the console	after the instar	nce is created. For	× more
Configurations Selected									
Basic Configurations	Billing Method : Pay-as-you-go Quantity : 1 Units Data Disk : 1 Unit(s)		Region : Silicon Valley Zone A Image : Fortinet FortiADC (BYOL) Application Del	very Controller 7.0.0	Instance Type : Enh System Disk : Enha	anced General Purpose T	/pe g6e / ecs.g6 .0 (up to 10.000	6e.large(2vCPU 8) IOPS per disk)	3GiB)
Networking 🖉	Network Type : VPC Network Billing Method : Pay-By-Traffic 5Mi	bps	VPC : fadc-test-ylliu/ vpc-rj96adtwotbnq9dd3988 Security Group : 1). sg-rj9f1zdnolmf79tt5rxa	у	VSwitch : vs-fadc-y	lliu/ vsw-rj997b3txb0wls2:	sr5qau/ 192.168	8.117.0/24) ()
	Save as Launch Template Image: Save as Launch Template Image: Save as ROS Template Image: Save as ROS Template								
Automatic Release	Automatic Release The ECS instance w	ill be released at the time you specified. Afte	r the instance is released, its data and IP addresses	will not be retained and cannot be ret	ieved.				
Terms of Service	ECS Terms of Service and Product Terms	of Service Image Product Terms of Use							
Quantity: 1	+ Units			Marketolace Image	Internet Tra	fic Fees:	Derei		
			Total 3 Of TOL 030 per Hour ()	Fees: \$ 0.000 USD pe	r Hour	⊚ \$ 0.077 USD per	GB Previ	Crea	te instance

The newly created instance will appear on the **Instances** page (it may take between 1 to 5 minutes for the instance to generate). The instance is ready when the status changes from Stopped to Running.

Next Step:

Configuring the Security Group Rules on page 12

Configuring the Security Group Rules

Configure custom security group rules for your FortiADC-VM instance.

- 1. Navigate to Elastic Compute Service > Security Groups.
- 2. On the Security Groups page, search for your security group using the Security Group ID/Name in previous steps (for details, see Creating the FortiADC-VM instance on page 9).
- 3. For the selected security group, under the **Actions** column, click **Add Rules** to configure custom security group rules.



4. Configure the following Access Rules settings:

Parameter	Description
Action	 Select the access action: Allow — allows access requests on a specific port. Forbid — drops packets without returning messages. If two security group rules differ only in their actions, the Forbid rule is used but the Allow rule is ignored.
Priority	A smaller value indicates a higher priority. Valid values: 1 to 100.
Protocol Type	Select the protocol type of the security group rule: All Custom TCP Customized UDP All ICMP (IPv4) All ICMP (IPv6) All GRE
Port Range	You can specify a custom port range when Protocol Type is set to Custom TCP or Customized UDP. Enter one or more port ranges. Separate multiple

Parameter	Description
	port ranges with commas (,). For example, 22/23, 443/443.
Authorization Object	 You can specify an authorization object of the following types: IP addresses — You can enter individual IP addresses. For example, 192.168.0.100 or 2408:4321:180:1701:94c7:bc38:3bfa:. CIDR blocks — You can enter a CIDR block. For example: 192.168.0.0/24 or 2408:4321:180:1701:94c7:bc38:3bfa:***/128. Security groups — This authorization type is valid only for the internal network. You can specify a security group within the current account or a different account as the authorization object to allow mutual access between instances in that security group and instances in the current security group over the internal network. Grant permissions to a security group within the current account: Enter the ID of the security group to which you want to grant permissions must reside within the same VPC as the current security group. Grant permissions to a security group within a different account: Enter the ID of the different Alibaba Cloud account and the ID of the security group to which you want to grant permissions us to a security group be within a different account: Enter the ID of the different Alibaba Cloud account and the ID of the security group to which security group to which you want to grant permissions to a security group be which you want to grant permissions to a security group to which you want to grant permissions must reside within the same VPC as the current security group.
	 Prefix lists — A prefix list is a set of network prefixes (CIDR blocks). The prefix list feature is supported only on security groups of the VPC type. After you reference a prefix list in a security group rule, the rule applies to all CIDR blocks in the prefix list. Note: You can enter up to 10 authorization objects at a time. Separate multiple objects with commas (,). If you enter 0.0.0.0/0 or ::/0 as an authorization object, all IP addresses are allowed or denied based on the Action parameter.
	 Evaluate the network risks before you specify 0.0.0.0/0 or ::/0. For security reasons, we recommend that you select a security group for Authorization Object when you add a public inbound rule to a security group of the classic network type. If you want to grant permissions to IP addresses, you must enter individual IP addresses instead of CIDR blocks.

5. Under the Actions column, click Save.

In the example below, the inbound access rule is set to allow all ports for all IP addresses.

😑 🕞 Alibaba Cloud	S Workbench		Q security 💿	Expenses Tickets ICP Enter	prise Support 🔄 🛕 🕜 El	
Elastic Compute Service	Elastic Compute Service / Security Groups / sg-rj9f12dnolm/79tt5rxa					
Reserved Instances	← sg-rj9f1zdn	Jolmf79tt5rx 👁 fadc-test-yl / vpc-rj96adtwotbnq9dd398	88y			
Resource Assurance New	• For information about I	how to use prefix lists to simplify management of security group rules, see	Use prefix lists to simplify management of sec	urity group rules. 🚥		
Savings Plan	Security Group Rules	Basic Information				
Network & Security	Instances	Security Group ID/Name: sg-rj9f1zdnolmf79tt5rxa/ sg-rj9f1zdnolmf	79tt5rxa Network:	vpc-rj96adtwotbnq9dd3988y		
Security Groups	ENIS IN Security Group	Security Group Type: Basic Security Group	Internal Acce	ss Control Policy: Allow Set to Deny		
ENIs		Description: System created security group.	Tags:			
SSH Key Pairs		hesource or oup.				
Virtual Private Clou 🗈						
Prefix Lists		Access Rule I Import Security Group Rule I Export				
Storage & Snapshots		Inbound Outbound				
Disks		Add Rule Quick Add Search by port or authoriz	zation object			
Snapshots		Action Priority ① Protocol Type P	Port Range ① Author	ization Object (i) Descript	ion Actions	
Storage Capacity Units		Allow V 1 All V *	: Dest -1/-1 * Sour	(0.0.0.0/0 ×)	Save Preview Delete	
Dedicated Block Stor						

Next Step:

Accessing the FortiADC GUI and CLI on page 14

Accessing the FortiADC GUI and CLI

After deploying the FortiADC-VM instance in Alibaba Cloud, you will need to access FortiADC to configure the instance. You can access the FortiADC GUI and CLI using either of the following methods:

- Remote access
- Console access

To access the FortiADC GUI and CLI remotely:

- 1. Navigate to Elastic Compute Service > Instances.
- 2. Take note of the Instance ID/Name of your instance.

E C-J Alibaba Cloud	All Resources ∨	⑨ US (Silicon Valley) ∨	Q security	Expenses Tickets	ICP Enterprise Support 🗈 🛕 🕐 EN 🌔
Elastic Compute Service	Elastic Compute Service / Instances				Operation reference
Overview	Instances				
Events	Create Instance Auto Select an instan	nce attribute or enter a keyword Q	Tags		Advanced Search C 👱 🕸
Tags	Name FADC2-7.0.0-ylliu 🚷 Clear				
Troubleshooting	Instance ID/Name Tag	Monitoring Zone $\overleftarrow{\mathcal{V}}$ IP Address	Status $ arrow Vetwork $ Type $ arrow Vetwork $	Specifications	Billing Method 😨 Actions
Applications Inter	FADC2-7.0.0-ylliu	Silicon 47.251.37.171(P Valley Zone 192.168.117.104 A	ublic) 🕜 Running VPC (Private)	2 vCPU 8 GiB (I/O Optimized) ecs.g6e.large 5Mbps (Peak Value)	Pay-As-You-Go March 15, 2022, Manage Connect 15:59(Time Zone: UTC - Change Instance Type More - 7) Created
Instances & Images	Start Stop Restart	Reset Password Renew Switch to Sul	oscription Release More-	Total: 1 ite	m(s), Per Page: vitem(s) « < 1 > »

3. Use the Internet IP to access the FortiADC via GUI/SSH/Telnet. The default login ID is admin and the password is the Instance ID/Name of your instance. After you login for the first time, you may change the password as needed.

To access the FortiADC GUI and CLI through the console:

- 1. Navigate to Elastic Compute Service > Instances.
- 2. For your instance, under the Actions column, click Connect.
- 3. On the Connection and Command page, under the Workbench Connection, click Connect.

E C-) Alibaba Cloud	☆ Workbench	Connection and Command 💿	X s	es Tickets	ICP Enterprise	Support 🗵	ġ (EN EN
Elastic Compute Service	Elastic Compute Service / Instances	Workbench Connection	- 1				Operat	tion refere
Overview	Instances	ECS instances can be remotely managed by using web pages. This feature allows you to copy and paste text, view system files, and supports simultaneous logons from users on different operating systems to a						
Events	Create Instance Auto Sele	single instance.				Advanced Search	C	<u>*</u>
Tags	Name FADC2-7.0.0-yillu 🔇 Clear							
Troubleshooting	Instance ID/Name	IN DURC Pare. The session management feature allows you to log on to and gain remote control on an instance without a password or rules that allow inbound access over required ports, regardless of whether the instance has	IEW t s	ins	Billing Method \square	Actions		
Applications	i-rj9ahmprzgm49n2phehm FADC2-7.0.0-ylliu	a public IP address. Leam More This feature is not supported in the current region.	3) 19	iB (I/O Ie	Pay-As-You-Go March 15, 2022, 15:59(Time Zone: UT	Manage (C - Change In:	Connect stance Type	More ¬
Instances & Images		VNC Connection (2)	58	ik Value)	/) Created			
Instances	Start Stop Res	Connect		Total: 1 item	n(s), Per Page: 🗸 🗸	item(s) «	< 1	> >>
Images			1					
Elastic Container 🖾 Instance		Send Remote Commands (Cloud Assistant)	1					
Dedicated Hosts		Cloud Assistant allows you to send remote commands to an instance and run them to perform operation such as viewing disk capacity, installing software, and starting or stopping services without connecting to the instance. To send remote commands, you must use the task execution feature provided by Cloud	s					
Super Computing Clusters		Assistant. Click here to install or activate the Cloud Assistant client on your instance. Send Remote Call						
Reserved Instances			1					
Resource Assurance		Cance	el					
Caulana Dian								

- 4. In the Instance Login dialog:
 - a. Enter the Username (the default login ID is admin), and select Password-based.
 - b. Enter the Password (which is the Instance ID/Name by default).
 - c. Click OK.

Important notes

- 1. Because Alibaba Cloud does not allow you to configure secondary IP on any interface, features with multiple IP-Addresses on one port may not work on Alibaba Cloud FortiADC-VM, such as the following:
 - NAT related features
 - L4 Full NAT
 - IP floating
- 2. FortiADC does not support High Availability deployment modes (HA-AP, HA-AA, and HA-VRRP) in Alibaba Cloud. HA-VRRP may be supported on other cloud infrastructure (such as AWS, Azure, or GCP).
- 3. For L4 VS DNAT, ensure the FortiADC is the gateway of the RS. If the RS is deployed in the Alibaba Cloud as well, please ensure there is no external IP address configured on the RS. Otherwise, the RS will not send back the data to the FortiADC for external traffic, regardless of the routing rules you configure on the RS. Because Alibaba Cloud always takes the routing rules to public networks as its first priority, all the traffic to Public IP destinations will be sent back via its default public route settings, instead of the gateway you configured.
- 4. Currently, the VNC console login is not working. As a workaround, use the Workbench Connection for console login.





Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.