



# 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](mailto:techdoc@fortinet.com)



April 25, 2022

FortiADC 7.0.0 Alibaba Cloud Deployment Guide

01-544-677187-20220425

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Deploying the FortiADC-VM in Alibaba Cloud</b> .....	<b>6</b>
Creating a VPC (Virtual Private Cloud) .....	6
Creating the FortiADC-VM instance .....	9
Configuring the Security Group Rules .....	12
Accessing the FortiADC GUI and CLI .....	14
<b>Important notes</b> .....	<b>16</b>

# 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

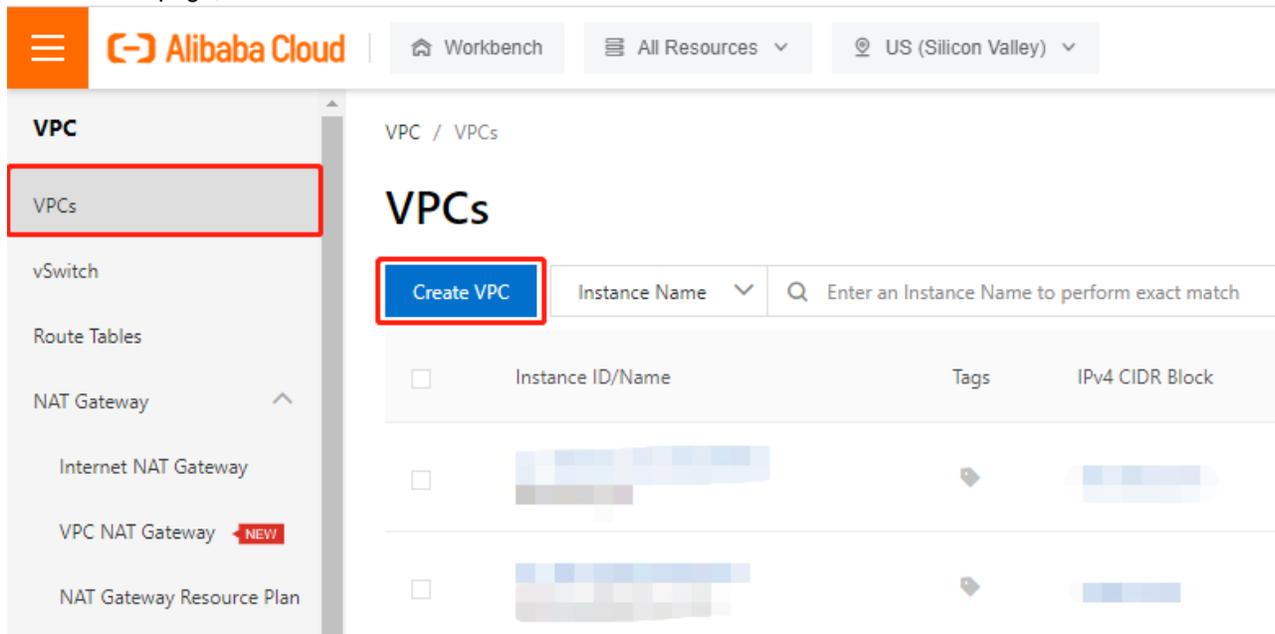
Follow the workflow below to deploy the FortiADC-VM instance on Alibaba Cloud.

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.

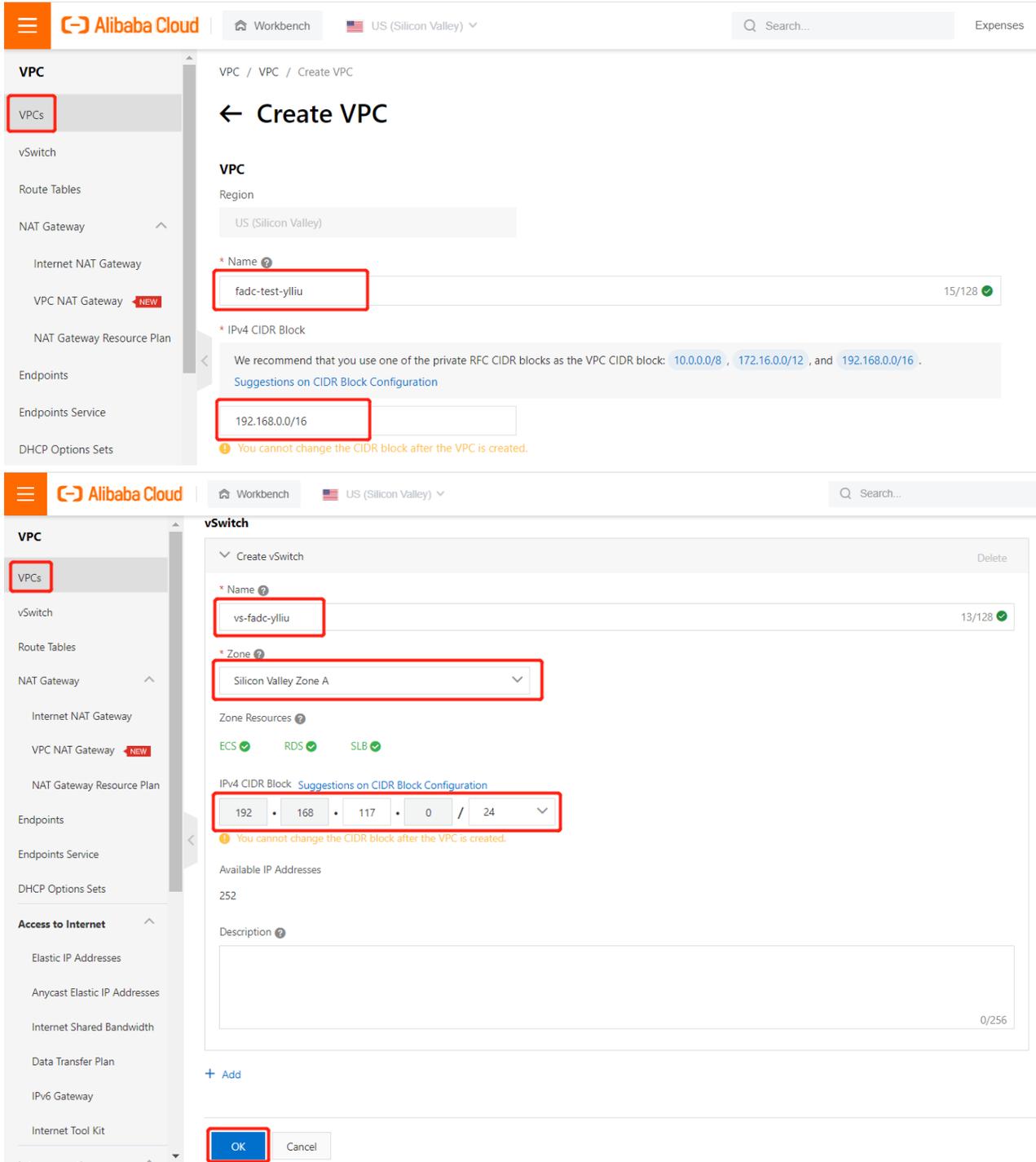
1. Log in to your Alibaba Cloud Account and log on to the VPC console.
2. In the top navigation bar, select the region where you want to deploy the VPC.  
**Note:** The VPC and the cloud resources that you want to deploy in the VPC must belong to the same region.
3. On the **VPCs** page, click **Create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



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

Parameter	Description
<b>VPC</b>	
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	<p>Enter an IPv4 CIDR block for the VPC.</p> <p>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.</p> <p><b>Note:</b> After you create a VPC, you cannot change its primary IPv4 CIDR block.</p>
<b>vSwitch</b>	
Name	<p>Enter a name for the vSwitch.</p> <p>The name must be 2 to 128 characters in length and can contain digits, underscores ( _ ), and hyphens ( - ). The name must start with a letter.</p>
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	<p>Specify the IPv4 CIDR block of the vSwitch. When you specify an IPv4 CIDR block for the vSwitch, take note of the following limits:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ul> <p><b>Note:</b> After you create a vSwitch, you cannot change its CIDR block.</p>



**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**.

The screenshot shows the Alibaba Cloud Marketplace interface. At the top, there's a navigation bar with 'Marketplace', 'All Products', 'User Help', and 'Contact Us'. A search bar contains 'FortiADC' and a 'My Subscript' link. Below the navigation, the breadcrumb path is 'Software Infrastructure / Security / Fortinet FortiADC (BYOL) Application Delivery Controller'. The main content area features the Fortinet logo, the product name 'Fortinet FortiADC (BYOL) Application Delivery Controller', a 0.0/5 star rating, and a description: 'FortiADC Application Delivery Controllers (ADC) provides application availability, web optimization, and application security (WAF)'. Technical details include 'Delivery Method: Image', 'Architecture: 64', 'Base Operating System: linux', and 'Latest Version: 7.0.0'. A pricing box shows '\$ 0 USD/Hour', 'Monthly Subscription Price: \$ 0 USD/Month', 'Yearly Subscription Price: \$ 0 USD/Year', 'Monthly Renewal Price: \$ 0 USD/Month', and 'Yearly Renewal Price: \$ 0 USD/Year'. A 'Choose Your Plan' button is located at the bottom of the pricing box.

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: <ul style="list-style-type: none"> <li>• Subscription — Pay for resources before you use them.</li> <li>• 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.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>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.</li> </ul>
Region and 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 type	Select the instance type. We suggest to select an instance type that has a minimum of 4 GB of memory.
Image	Select the <b>Marketplace Image</b> .
Storage	Add a <b>Data Disk</b> for the FortiADC log Disk. We suggest to select a disk with a minimum of 30 GB.

The screenshot shows the configuration interface for an Alibaba Cloud instance. In the 'Image' section, 'Marketplace Image' is selected, and the specific image 'Fortinet FortiADC (BYOL) Application Delivery Controller 7.0.0' is chosen. In the 'Storage' section, a 'Data Disk' is added with a size of 40 GIB and performance level PL1. The total cost is shown as 0.138 USD per hour.

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 <a href="#">Creating the FortiADC-VM instance on page 9</a> .
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** System Configurations (Optional) Grouping (Optional) Preview

Network Type: VPC

Public IP Address:  Assign Public IPv4 Address

Bandwidth Billing: Pay-By-Traffic

Peak Bandwidth: 5 Mbps

Security Group: Reselect Security Group

Elastic Network: Default ENI

Interface: vs-fadc-ylliu

Quantity: 1 Units

Total: \$ 0.132 USD per Hour

Marketplace Image Fees: \$ 0.000 USD per Hour

Internet Traffic Fees: \$ 0.077 USD per GB

Buttons: Previous, Next, Preview

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

Elastic Compute Service (ECS) Quick Launch Custom Launch Savings Plan Purchase History Pricing Buy Disk Console

Basic Configurations **3 System Configurations (Optional)** Grouping (Optional) **5 Preview**

**Note:** You have not configured the instance logon credentials. If you need to log on to the instance, you can go back to the System Configurations (Optional) step to configure logon credentials. You can also perform the Reset Password operation in the console after the instance is created. For more information about how to reset the password, see Reset the logon password of an instance.

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 Delivery Controller 7.0.0	Instance Type: Enhanced General Purpose Type g6e / ecs.g6e.large (2vCPU 8GB) System Disk: Enhanced SSD (ESSD) 40GiB, PL0 (up to 10,000 IOPS per disk)
Networking	Network Type: VPC Network Billing Method: Pay-By-Traffic 5Mbps	VPC: fadc-test-ylliu / vpc-rj96adtwtbng9dd3988y Security Group: 1). sg-rj9f1zdnolm79tt5xa	VSwitch: vs-fadc-ylliu / vsw-rj997b3tb0wls2sr5qau / 192.168.117.0/24

Buttons: Save as Launch Template, View Open API, Save as ROS Template

Automatic Release:  Automatic Release

Terms of Service:  ECS Terms of Service and Product Terms of Service | Image Product Terms of Use

Quantity: 1 Units

Total: \$ 0.132 USD per Hour

Marketplace Image Fees: \$ 0.000 USD per Hour

Internet Traffic Fees: \$ 0.077 USD per GB

Buttons: Previous, Create 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.

The screenshot shows the Alibaba Cloud console interface. The left sidebar contains a navigation menu with 'Security Groups' highlighted. The main area displays the 'Security Groups' page with a table of existing groups. One group is selected, and the 'Add Rules' button in its 'Actions' column is highlighted.

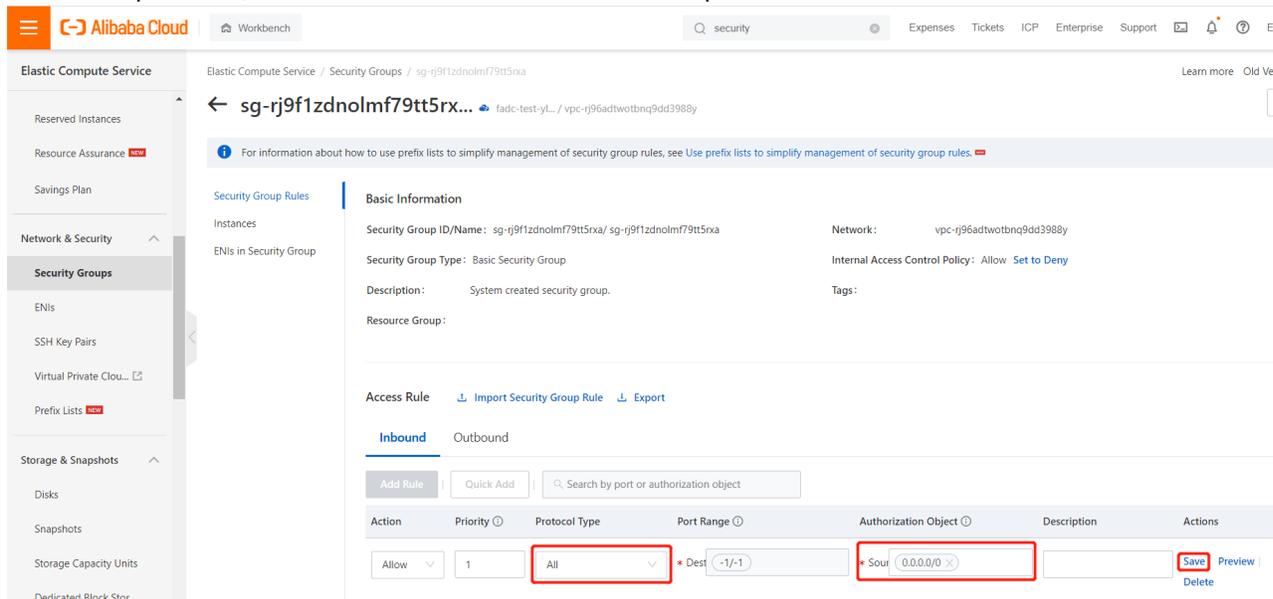
Security Group ID/Name	Tag	VPC	Related Instances	Available IP Addresses	Network Type(All)	Security Group Type(All)	Creation Time	Description	Actions
sg-rj9f1zdnoimf79tt5rxa		vpc-rj96adtwtobnq9dd3988y	5	1986	VPC	Basic Security Group	March 14, 2022, 17:42(Time Zone: UTC - 7)	System created securit...	Modify   Clone   Restore Rules   Manage Instances   <b>Add Rules</b>   Manage ENIs

4. Configure the following Access Rules settings:

Parameter	Description
Action	<p>Select the access action:</p> <ul style="list-style-type: none"> <li>• Allow — allows access requests on a specific port.</li> <li>• Forbid — drops packets without returning messages.</li> </ul> <p>If two security group rules differ only in their actions, the <b>Forbid</b> rule is used but the <b>Allow</b> rule is ignored.</p>
Priority	A smaller value indicates a higher priority. Valid values: 1 to 100.
Protocol Type	<p>Select the protocol type of the security group rule:</p> <ul style="list-style-type: none"> <li>• All</li> <li>• Custom TCP</li> <li>• Customized UDP</li> <li>• All ICMP (IPv4)</li> <li>• All ICMP (IPv6)</li> <li>• All GRE</li> </ul>
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	<p>You can specify an authorization object of the following types:</p> <ul style="list-style-type: none"> <li>• IP addresses — You can enter individual IP addresses. For example, 192.168.0.100 or 2408:4321:180:1701:94c7:bc38:3bfa:.</li> <li>• CIDR blocks — You can enter a CIDR block. For example: 192.168.0.0/24 or 2408:4321:180:1701:94c7:bc38:3bfa:*/128.</li> <li>• 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. <ul style="list-style-type: none"> <li>• Grant permissions to a security group within the current account: Enter the ID of the security group to which you want to grant permissions within the current account. If the current security group is of the VPC type, the security group to which you want to grant permissions must reside within the same VPC as the current security group.</li> <li>• 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 in the ID of the Alibaba Cloud account/ID of the security group format. You can choose <b>Account Management &gt; Basic Information</b> to view your account ID.</li> </ul> </li> <li>• 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.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• You can enter up to 10 authorization objects at a time. Separate multiple objects with commas ( , ).</li> <li>• 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.</li> <li>• 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.</li> </ul>

- Under the **Actions** column, click **Save**.  
In the example below, the inbound access rule is set to allow all ports for all IP addresses.



**Next Step:**

Accessing the FortiADC GUI and CLI on page 14

## Accessing the FortiADC GUI and CLI

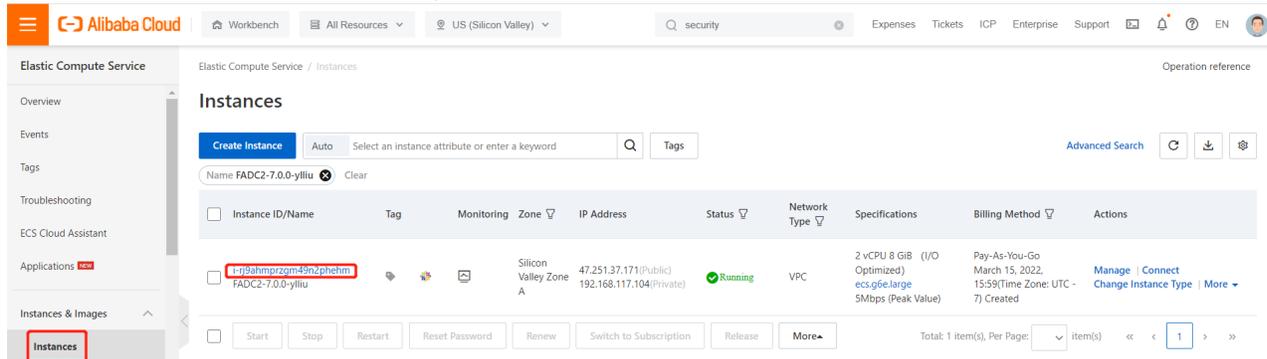
After deploying the FortiADC-VM instance in Alibaba Cloud, you will need to access FortiADC to configure the instance.

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:**

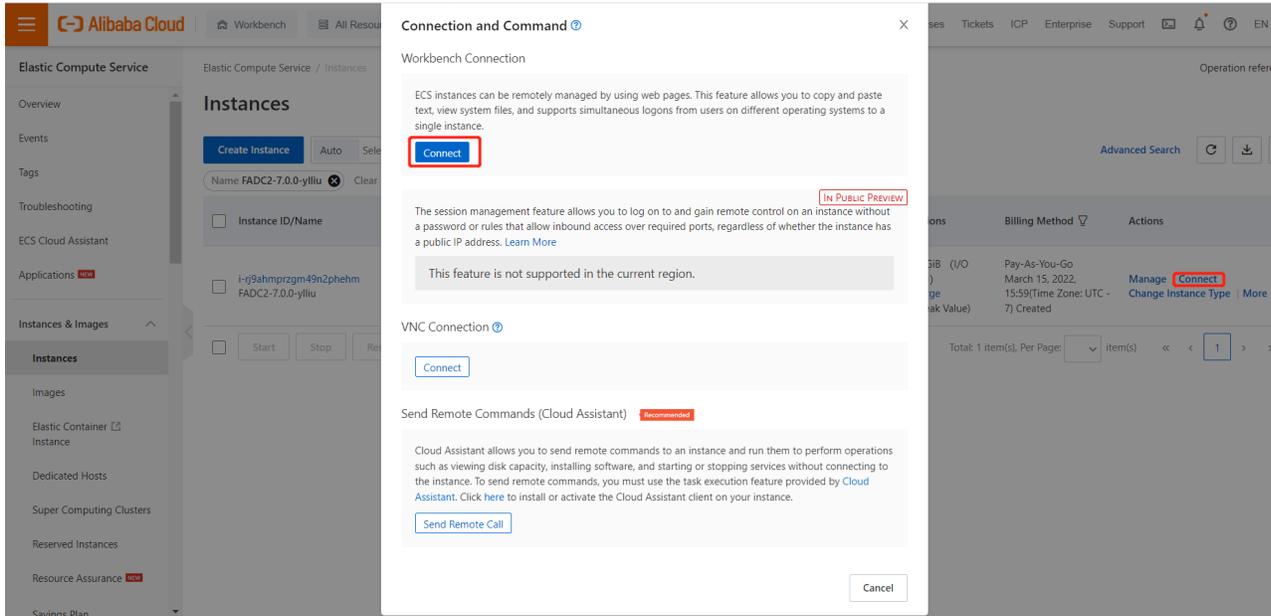
1. Navigate to **Elastic Compute Service > Instances**.
2. Take note of the **Instance ID/Name** of your instance.



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**.



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.



**FORTINET**<sup>®</sup>



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 and, in such event, only the specific 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.