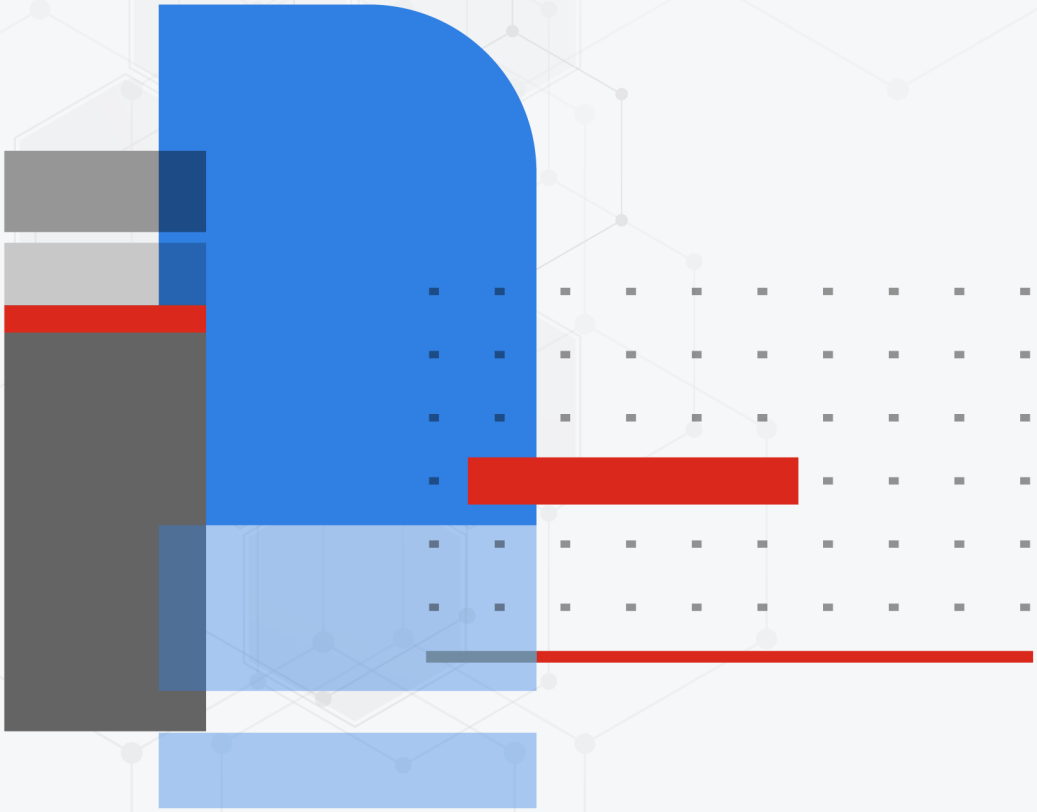
Alibaba Cloud Deployment Guide

FortiADC 7.4.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
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 7.4.0 Alibaba Cloud Deployment Guide
01-544-677187-20220425

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-04-21	Initial release.
2023-07-07	Added Active-Active-VRRP HA 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

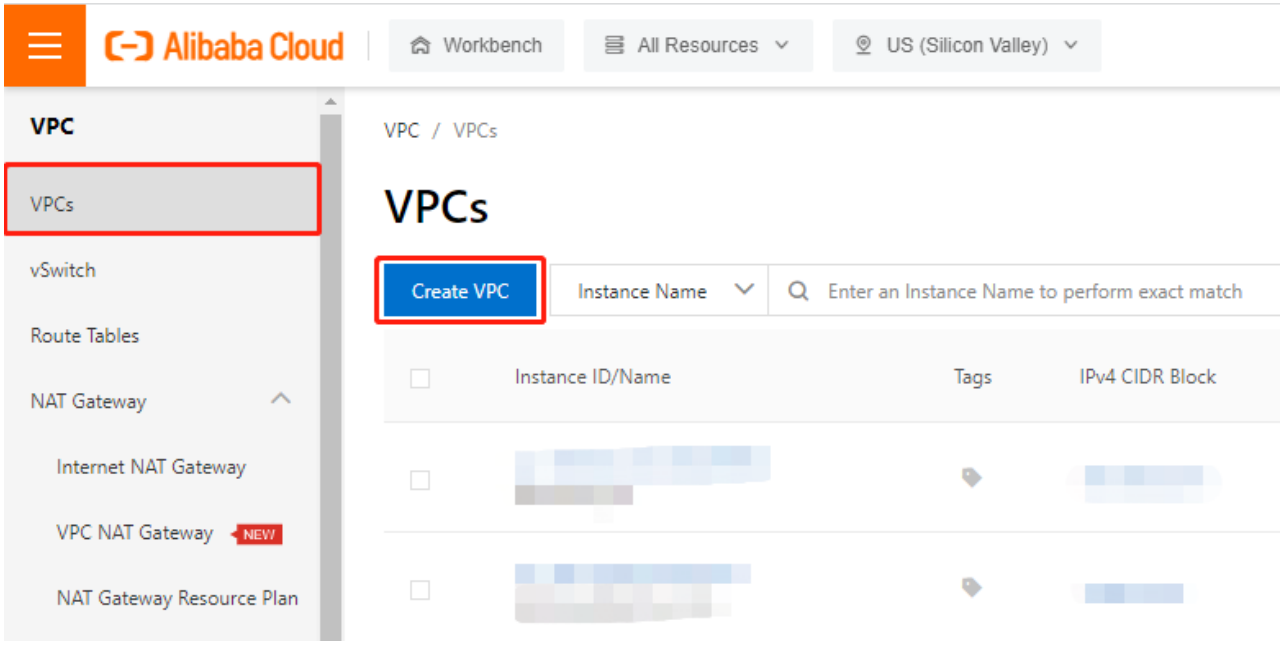
Follow the workflow below to deploy the FortiADC-VM instance on Alibaba Cloud.

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.

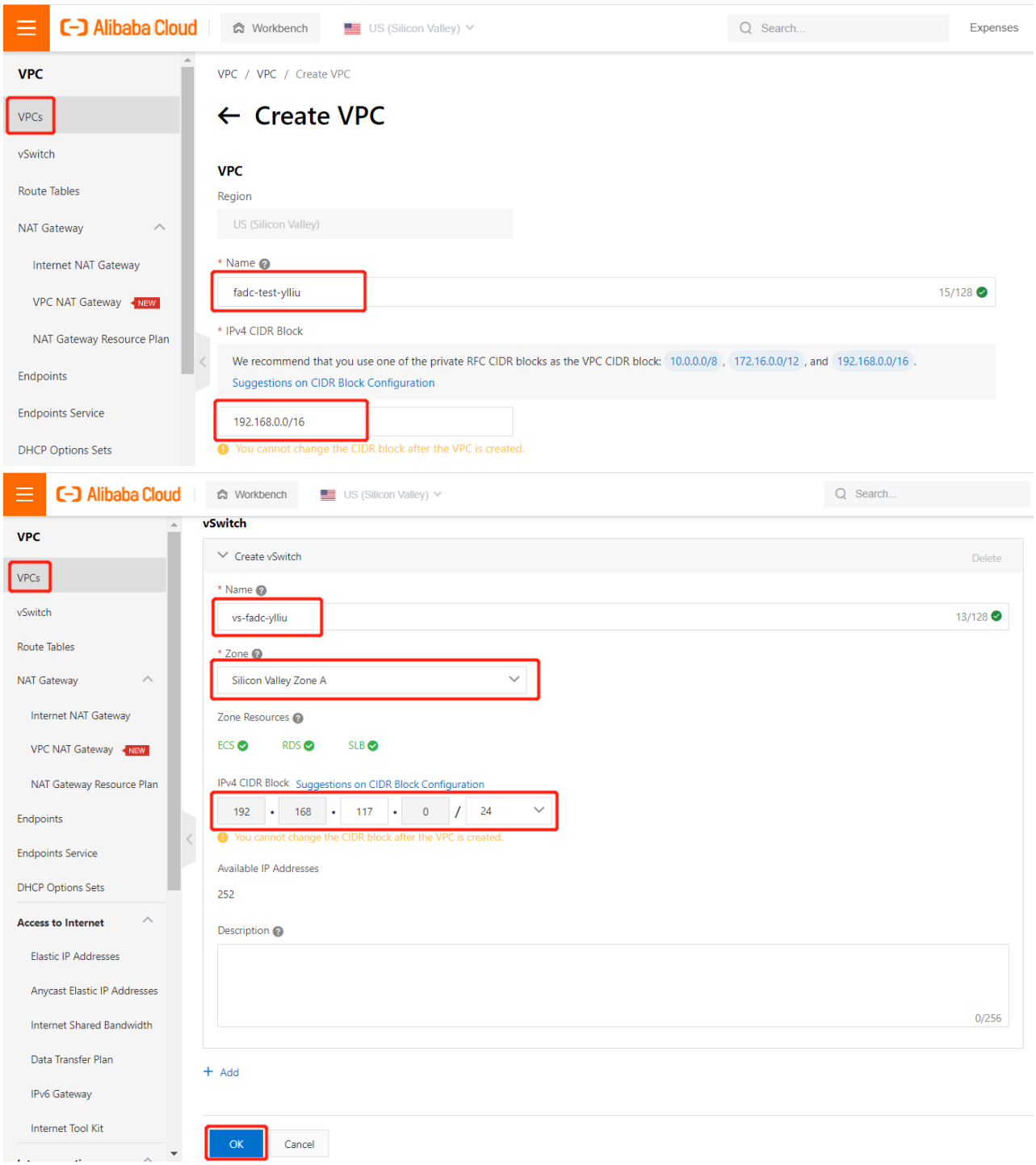
1. Log in to your Alibaba Cloud Account and log on to the VPC console.
2. In the top navigation bar, select the region where you want to deploy the VPC.
   Note: The VPC and the cloud resources that you want to deploy in the VPC must belong to the same region.
3. On the **VPCs** page, click **Create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



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

Parameter	Description
VPC	
Region	Displays the region where you want to create the VPC.

Parameter	Description
Name	Enter a name for the VPC. 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.



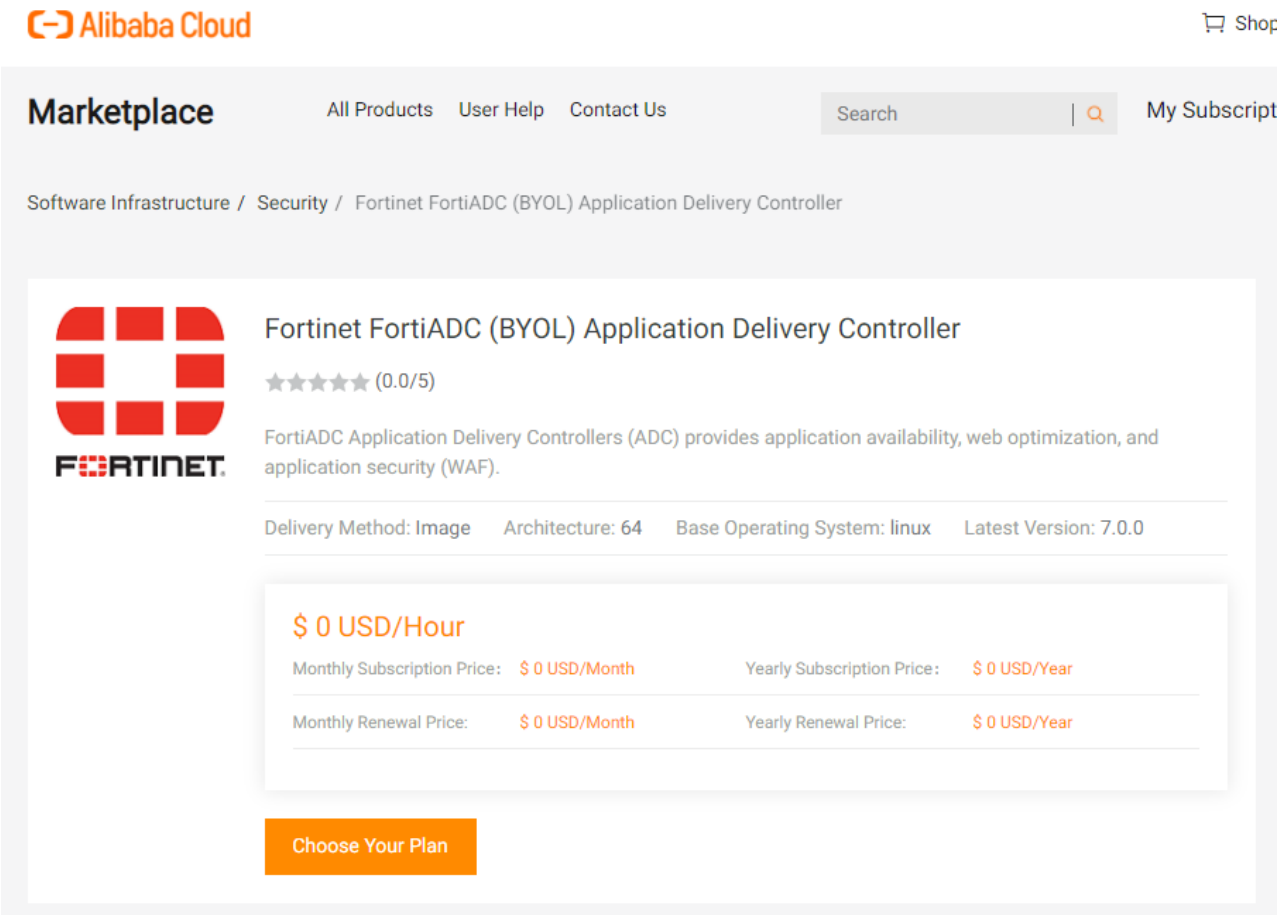
Next Step:

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.

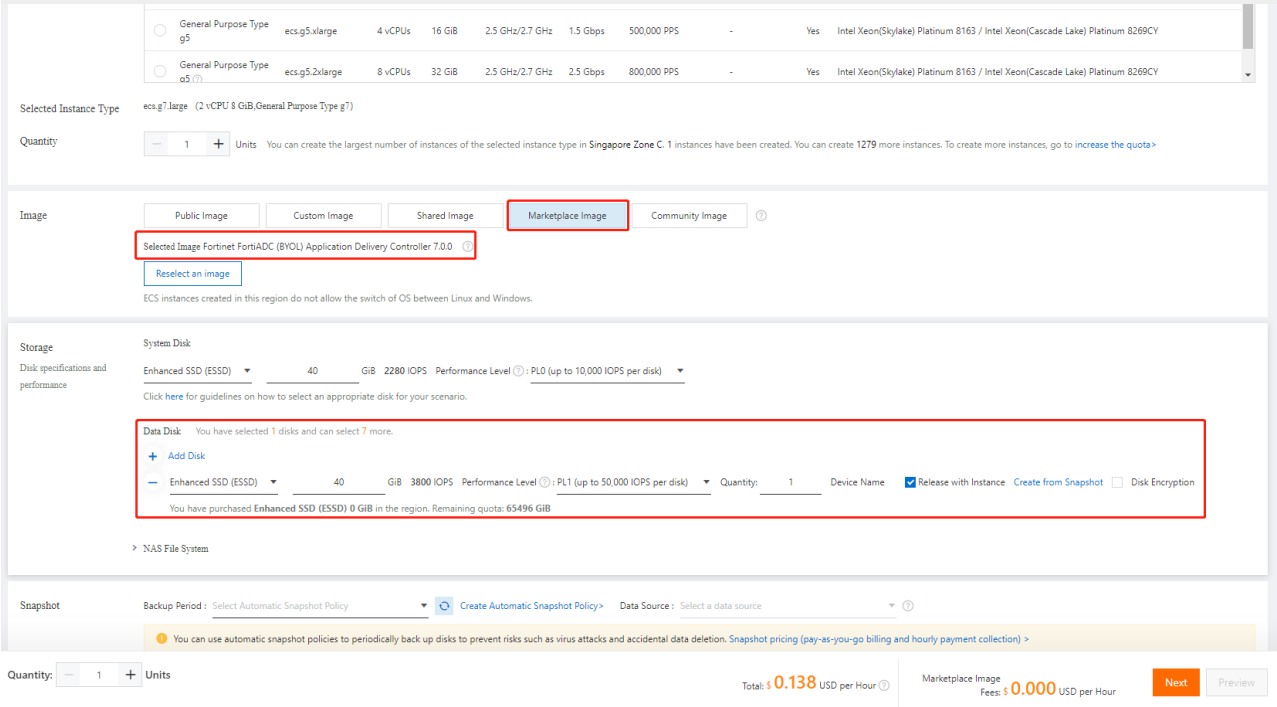
1. Go to **Alibaba Cloud > Marketplace**, and search for **FortiADC**.
   The search will return the **Fortinet FortiADC (BYOL) Application Delivery Controller**.



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.

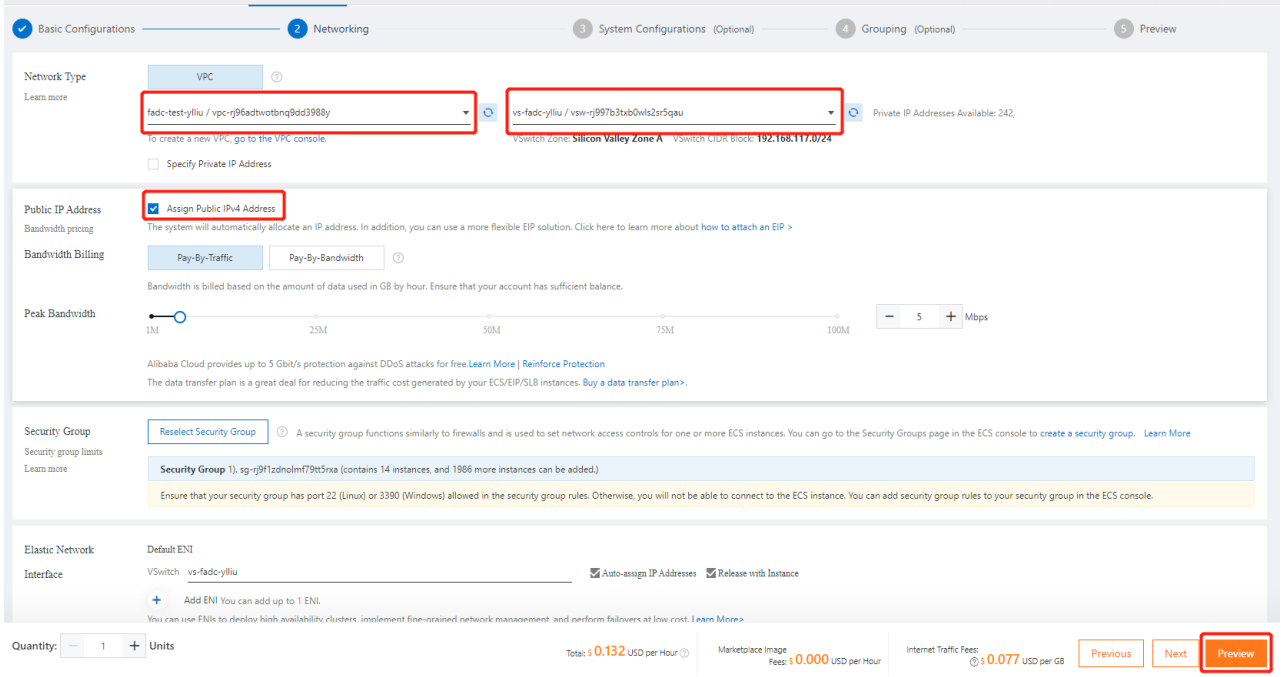
Setting	Description
	• Preemptive Instance — Use resources first and pay for them afterward. You place a bid for available instance resources to create preemptible instances at a discount compared with pay-as-you-go instance pricing. Preemptible instances may be automatically released due to fluctuations in market price or insufficient resources of instance types.
Region and 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 **Marketplace Image**.
Storage	Add a **Data Disk** for the FortiADC log Disk. We suggest to select a disk with a minimum of 30 GB.



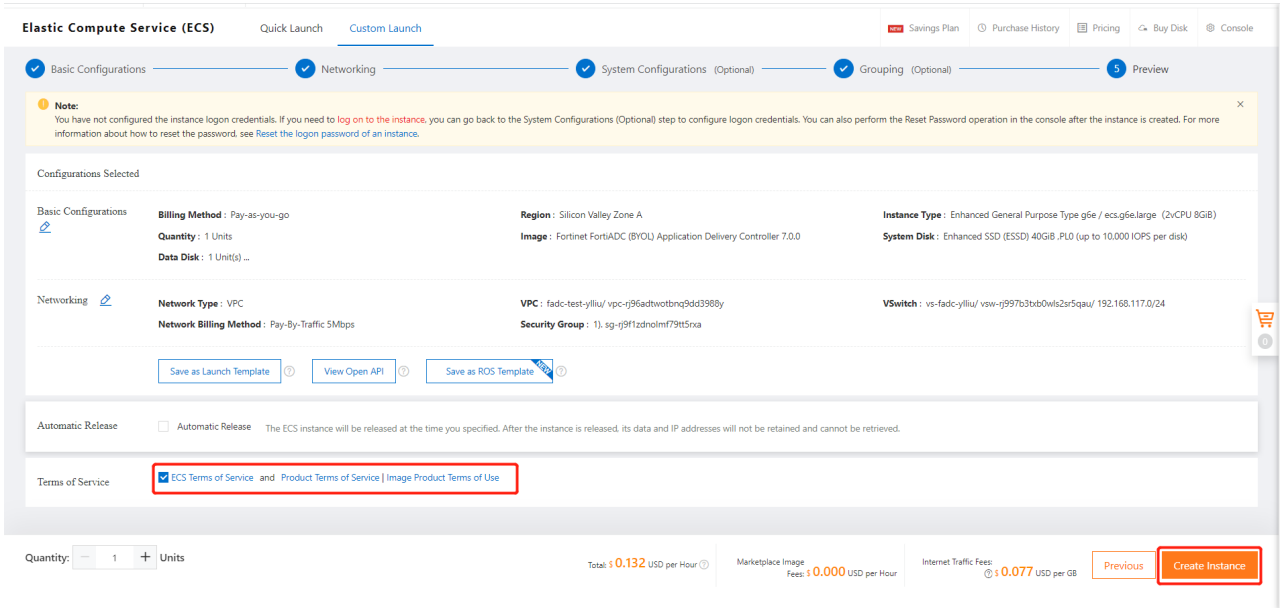
6. Click **Next** to move forward to **Networking** and configure the following settings:

Setting	Description
Network Type	Select the VPC and vSwitch that was previously configured in the VPC you created.
Public IP Address	Select **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.



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

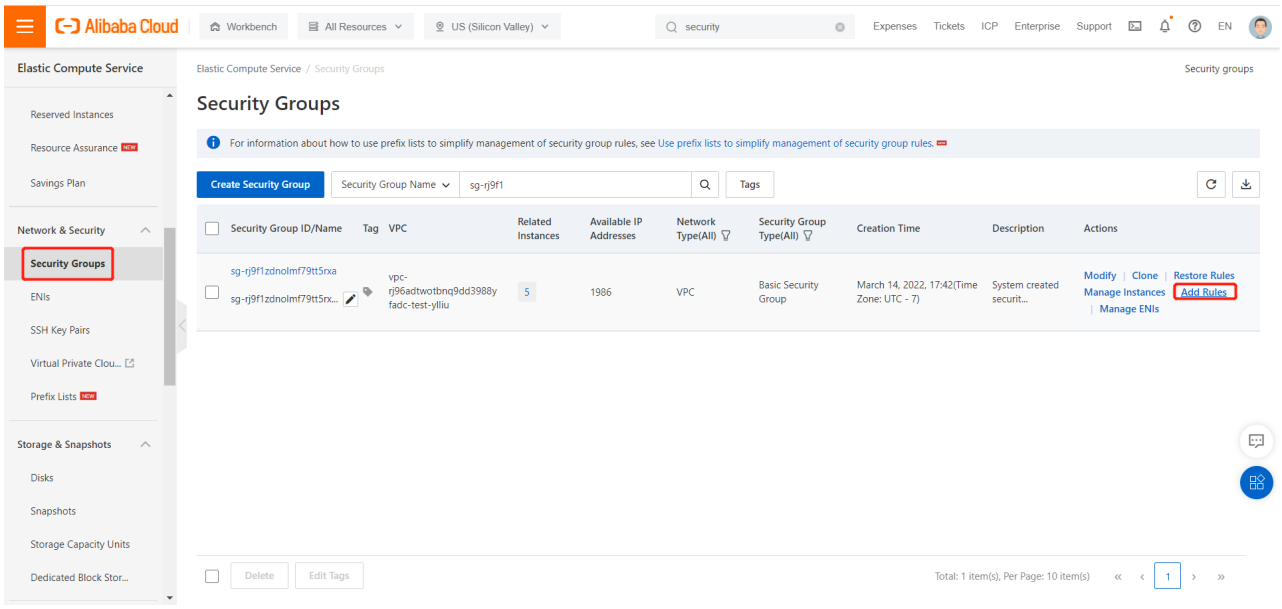
Configuring the Security Group Rules on page 12

Configuring the Security Group Rules

A security group is a set of firewall rules that control the traffic for your VM instances. When you create a VPC, a default Security Group protects instances in it. It is recommended to add inbound rules so that the traffic will be allowed to flow on the specified ports.

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.



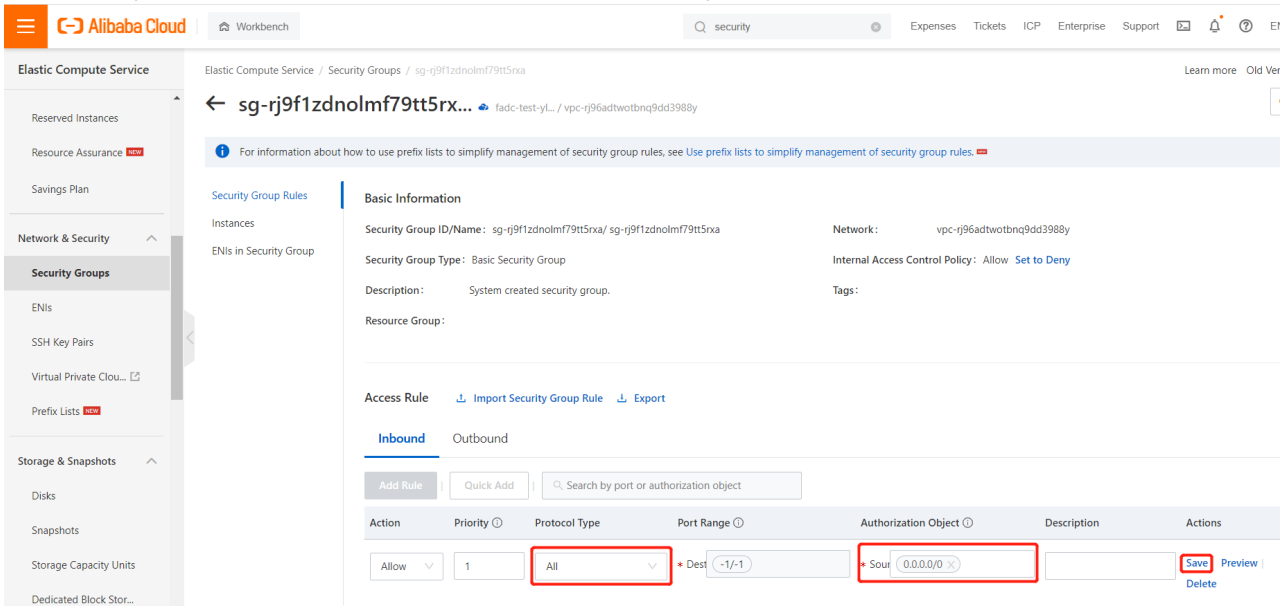
4. Configure the following Access Rules settings:

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)

Parameter	Description
	• 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 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 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.
	  • 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 **Account Management > Basic Information** to view your account ID.
	• 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.



Next Step:

Accessing the FortiADC GUI and CLI on page 14

Accessing the FortiADC GUI and CLI

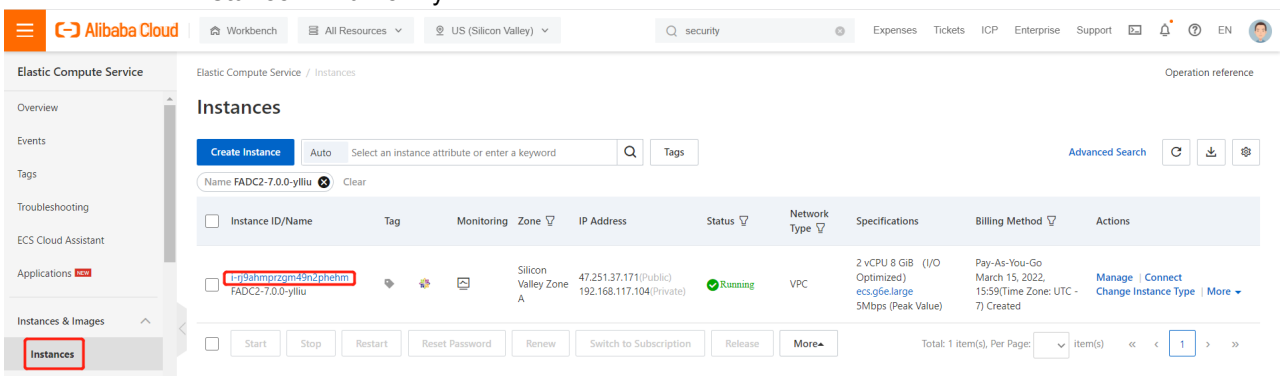
After deploying the FortiADC-VM instance in Alibaba Cloud, you will need to access FortiADC to configure the instance.

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:

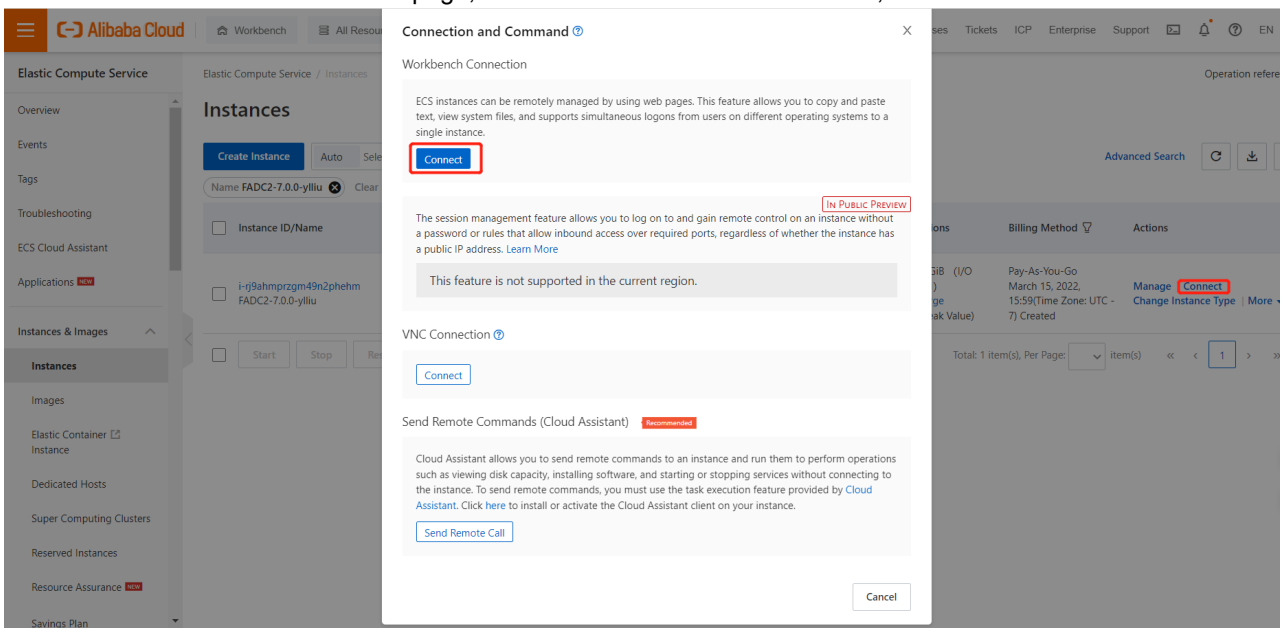
1. Navigate to **Elastic Compute Service > Instances**.
2. Take note of the **Instance ID/Name** of your instance.



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**.

High Availability for FortiADC on Alibaba Cloud

You can deploy FortiADC-VM HA (High Availability) on Alibaba Cloud (AliCloud) in Active-Active-VRRP mode.

In an Active-Active-VRRP cluster, one of the nodes is selected as the primary node of a traffic group, and all other nodes in the traffic group are member nodes. Traffic from upstream can be load-balanced to up to two member nodes. When failover occurs in an Active-Active-VRRP cluster, the traffic group active on the primary node will fail over to one of the backup nodes which will send gratuitous ARP to adjacent devices to redirect traffic for its own MAC address to all network interfaces within the traffic group.

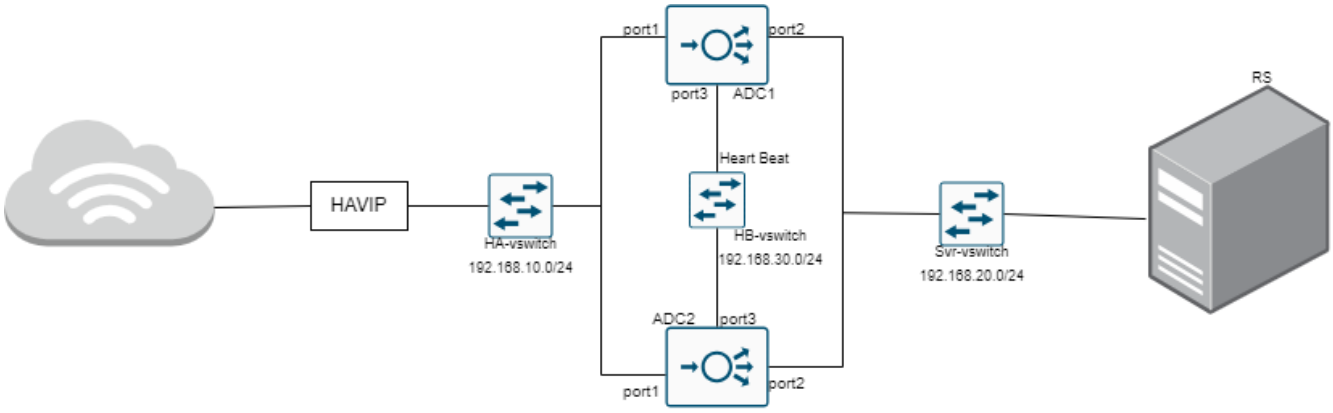
For more information about HA modes, see the FortiADC Handbook topic on High Availability Deployments.

Currently, FortiADC HA on AliCloud is supported only for Active-Active-VRRP mode with Layer 7 virtual servers and Layer 4 virtual servers in Full NAT mode. For AliCloud Active-Active-VRRP mode with Layer 4 virtual servers in Full NAT mode, only one IP is supported.

Deploying Active-Active-VRRP mode with L7 VS

For Layer 7 virtual servers, the following resources will be created in the Active-Active-VRRP deployment process:

- A VPC including three VSwitches respectively for:
  - External traffic forwarded from the HAVIP.
  - The heartbeat traffic between HA members.
  - The connection between FortiADC and the back-end server.
- Two FortiADC-VM instances.
- An HAVIP with an EIP. The HAVIP's public IP address will be the IP address that clients use to access your application.



Follow the workflow below to deploy HA in Active-Active-VRRP mode with Layer 7 virtual server on Alibaba Cloud.

1. Setting up the VPC for L7 VS HA on page 17
2. Creating the FortiADC-VM instance and binding to Elastic Network Interfaces (ENIs) on page 18
3. Setting up the HAVIP for L7 VS on page 19
4. Configuring FortiADC-VM Active-Active-VRRP HA with L7 VS on page 21

Setting up the VPC for L7 VS HA

Assuming this is a new environment, the first step is to create the VPC and define the three vSwitches required for the L7 VS HA deployment.

As part of the VPC setup, you will need to create at least three vSwitches:

- One for the external traffic forwarded from the HAVIP.
- One for the heartbeat traffic between HA members.
- One for the connection between FortiADC and the back-end server.

For detailed steps on how to create and configure a VPC, see Creating a VPC (Virtual Private Cloud) on page 6.

After you have set up your VPC and created the required vSwitches, configure the security group rules. For detailed steps, see Configuring the Security Group Rules on page 12.

Creating the FortiADC-VM instance and binding to Elastic Network Interfaces (ENIs)

After you have set up your VPC and required vSwitches for deploying HA with L7 VS, you need to create a FortiADC-VM instance and bind it to three Elastic Network Interfaces (ENIs). The three ENIs will be associated with each of the three vSwitches previously created when setting up the VPC.

During the instance creation process, you will bind one primary ENI and one secondary ENI to the instance. Then, for the third remaining ENI (the second secondary ENI), you will create it and bind it to the FortiADC-VM after the installation is complete.

1. Create the FortiADC-VM instance and configure the primary and secondary ENIs as part of the Networking settings. Associate the primary and secondary ENIs with the vSwitches previously created in the VPC setup. For details, see Setting up the VPC for L7 VS HA on page 17.
   For detailed steps on how to create the FortiADC-VM instance, see Creating the FortiADC-VM instance on page 9.
2. After creating the FortiADC instance and binding the primary ENI and first secondary ENI, create the second secondary ENI.
   a. Navigate to **Network & Security > ENIs**. Click **Create ENI** to display the configuration editor.
   b. Configure the following **ENI** settings:

Setting	Description
ENI Name	Enter a name for the ENI. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-), and it must start with a letter.
VPC	Select the VPC you have previously created. To bind the created ENI to an instance, select the PVC in which the instance resides. After the ENI is created, you cannot change the VPC in which the ENI belongs to. **Note**: An ENI can only be bound to an instance that is in the same VPC as the ENI.
vSwitch	Select the vSwitch you want to associate with. This should be the remaining vSwitch that has not been associated with the primary and secondary ENIs during the instance installation.
Primary Private IP	Optionally, enter an IPv4 address as the primary private IP address of the ENI. The IPv4 address must be an idle IP address within the CIDR block of the selected vSwitch. If you do not specify an IPv4 address, an idle private IPv4 address is automatically assigned to the ENI after the ENI is created.
Secondary Private IP Addresses	Optionally, specify secondary private IPv4 addresses for the ENI. • Not set — No secondary private IPv4 addresses are assigned to the ENI. • Auto — The system automatically assigns the specified number of idle IPv4 addresses from within the CIDR block of the selected vSwitch to the ENI. Range is 1 to 9. • Manual — Manually assign secondary private IPv4 addresses to the ENI. Range is 1 to 9.

Setting	Description
Security Group	Select security groups in the selected VPC. This should be the Security Group you have previously created. You can specify up to five security groups. **Note**: Basic security groups and advanced security groups cannot be selected at the same time.
Description	Optionally, enter a description to help you manage the ENI.
Resource Group	Select the Resource Group. It should be in the same resource group as that of the FortiADC-VM instance.
Tag	Optionally, select one or more tags to add to the ENI for easy search and management.

   c. Click **Create**.
   When the ENI is created, the **Status** column of the ENI will display as **Available** on the **Network Interfaces** page.
   You can then bind the ENI to an instance.

3. Bind the remaining secondary ENI to the FortiADC-VM instance.
   a. Navigate to **Instances & Images > Instances**.
   b. On the Instances page, select the FortiADC-VM instance you want to bind the secondary ENI to.
   c. On the FortiADC-VM instance details page, go to the **ENIs** tab and click **Bind Secondary ENI** to display the configuration editor.
   d. Select the secondary ENI you want to bind to the FortiADC-VM and click **OK**.
   After you bind the ENI to the FortiADC-VM instance, you can go to the Instance Details page and view the state of the ENI on the **ENIs** tab. If the ENI is bound to the instance, **InUse** is displayed in the Status/Creation Time column corresponding to the ENI.

Setting up the HAVIP for L7 VS

To deploy HA with L7 VS, you will need to create an HAVIP (high-availability virtual IP address) and associate it with an EIP (elastic IP address). An HAVIP is a private IP address that can be created and released as an independent resource. After an HAVIP is associated with an EIP, the HAVIP can use the EIP to provide services over the Internet.

Before you begin:

- You must already have an EIP. If you do not have an EIP, you can create an EIP in **VPC > Access to Internet > Elastic IP Address**.

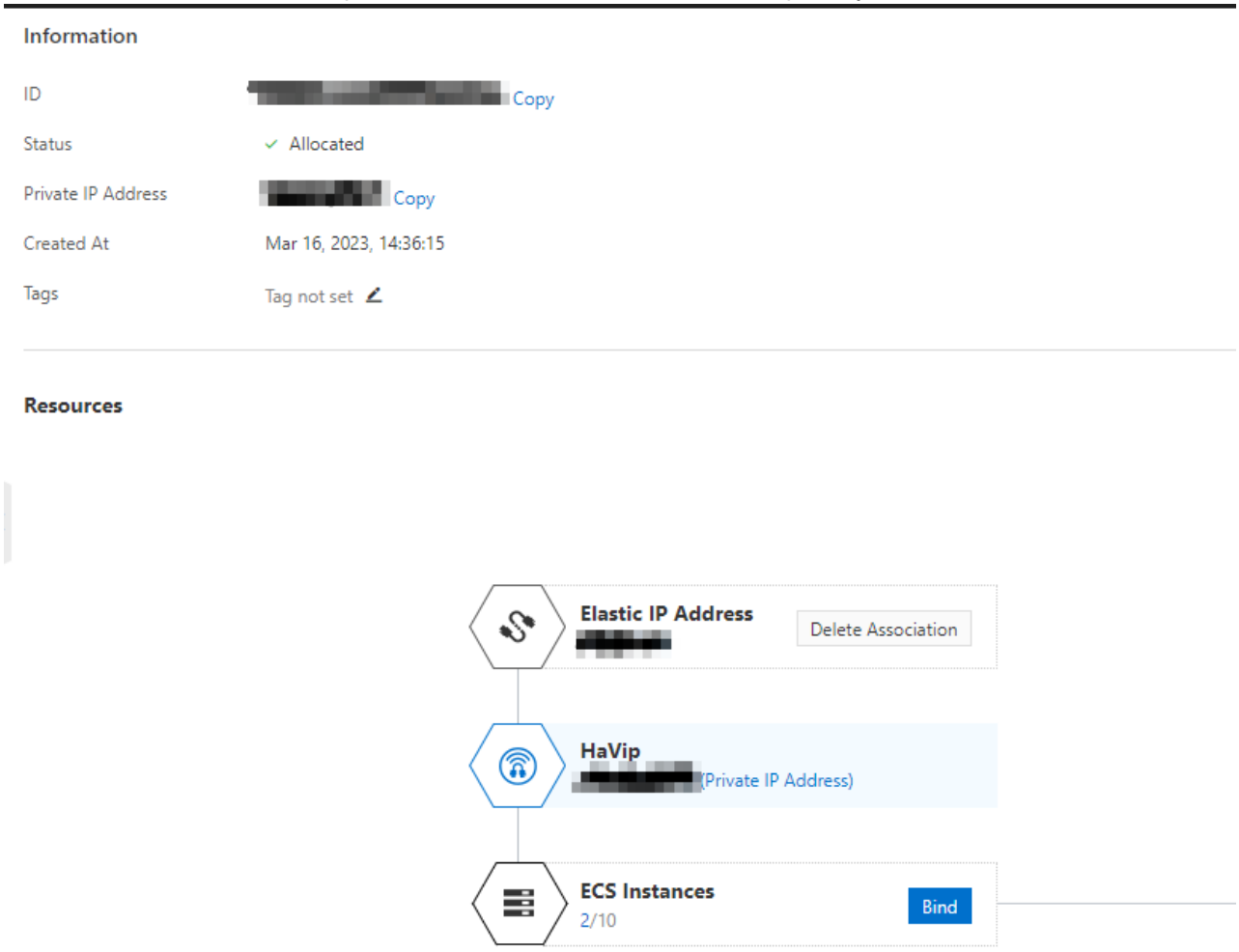
To create the HAVIP and bind it to an EIP:

1. Navigate to the **VPC** page and click **HaVIp**.
2. On the HaVIp page, click **Create HaVIp** to display the configuration editor.
3. Configure the following HAVIP settings:

Setting	Description
Resource Group	Select the Resource Group you have created.

Setting	Description
Name	Enter a name for the HAVIP.
VPC	Select the VPC you have created previously.
vSwitch	Select the vSwitch you have created previously for the Internet Access.
vSwitch CIDR Block	Displays the CIDR block of the vSwitch.
Whether to automatically assign private IP addresses	Select whether to automatically allocate a private IP address. • Yes — The system automatically allocates an idle private IP address from the vSwitch CIDR block. • No — Manually enter an idle private IP address from the vSwitch CIDR block.

4. Click **OK**.
   Once the HAVIP is created, take note of the **Internal IP address**. The Internal IP address will be the virtual server IP of your L7 VS configuration.
5. Select the newly created HAVIP and click **Bind EIP Address**.
6. Click the name of the HAVIP and click **Bind** to bind the FortiADC-VM instances you have created with this HAVIP.
   Traffic destined for the HAVIP's public IP address will be forwarded to the primary FortiADC-VM.



After you have set up your FortiADC-VM instance and the required HAVIP, the next step is to log into FortiADC through GUI or CLI to configure the HA cluster. For detailed steps, see Accessing the FortiADC GUI and CLI on page 14.

Configuring FortiADC-VM Active-Active-VRRP HA with L7 VS

After setting up the FortiADC-VM instances in AliCloud, log in to the FortiADC-VMs to set up your HA and L7 VS configurations. In the L7 VS configuration of the primary FortiADC-VM, you will need to set the virtual IP as the Internal IP of the HAVIP.

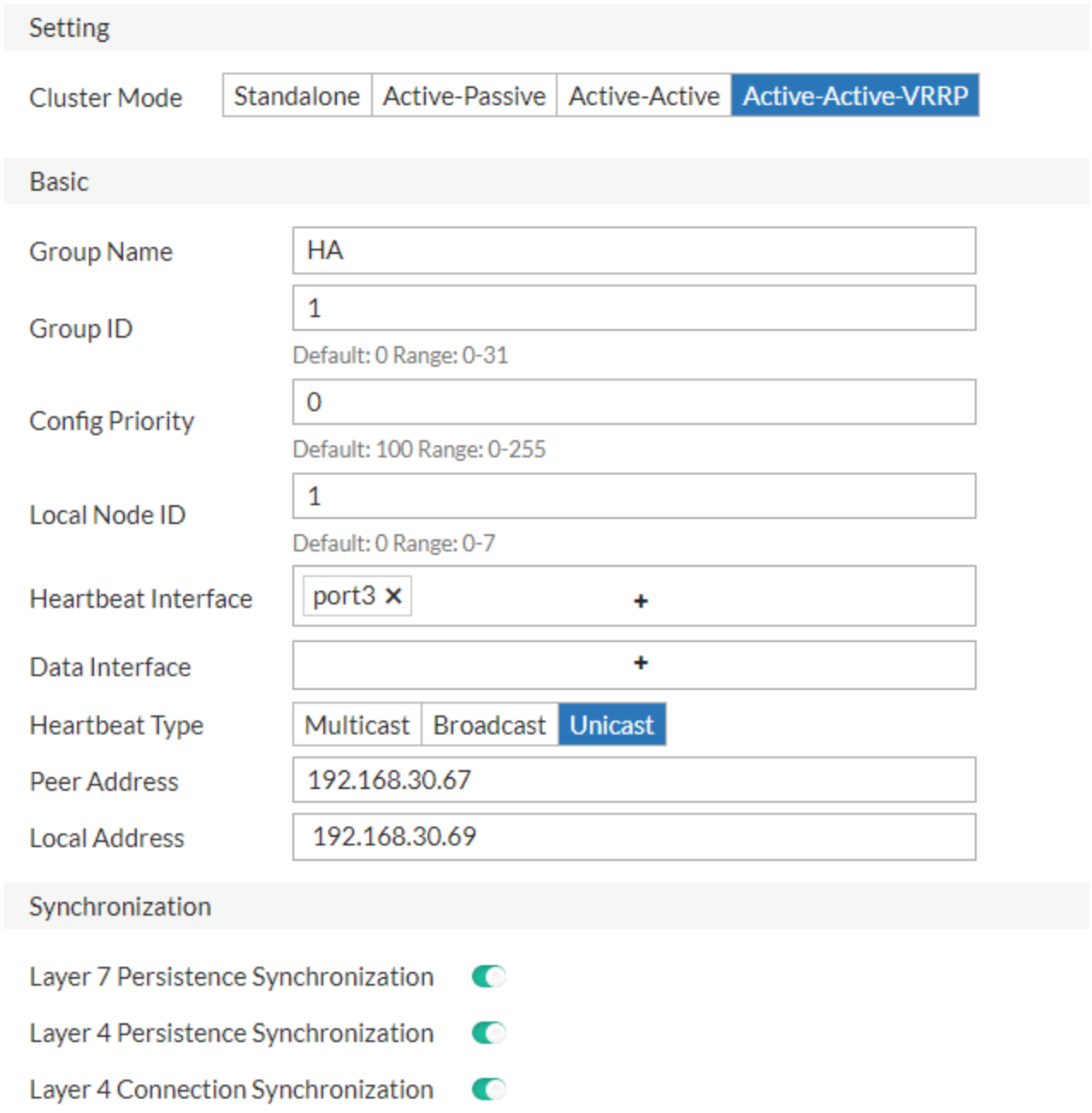
Example: Configuring the HA primary and secondary FortiADC-VMs

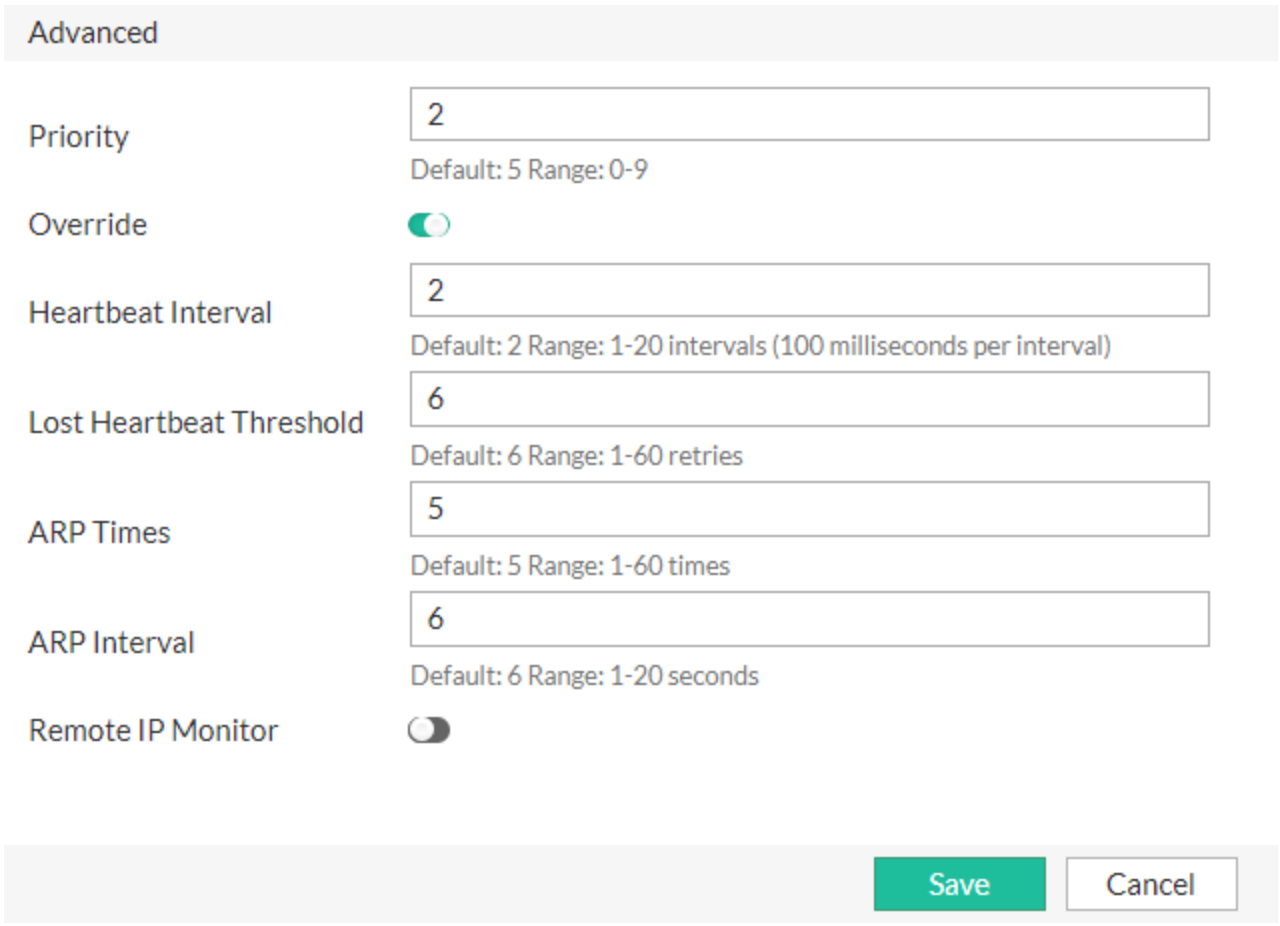
The following example describes how to configure your HA primary and secondary FortiADC-VMs.

Configure the primary HA configuration:

1. Log in to the primary FortiADC-VM.
2. Go to **System > High Availability > Settings**.
3. Configure the following relevant HA settings for the example primary FortiADC-VM:

Settings	Guidelines
Cluster Mode	Select the **Active-Active-VRRP** cluster mode.
Basic	
Group Name	Enter the Group Name as **HA**.
Group ID	Specify the Group ID as **1**.
Local Node ID	Specify the Local Node ID as **1**.
Heartbeat Interface	Select **port3** as the Heartbeat Interface.
Heartbeat Type	Select **Unicast** as the Heartbeat Type,
Peer Address	Enter the Peer Address as **192.168.30.67**.
Local Address	Enter the Local Address as **192.168.30.69**.
Synchronization	
Layer 7 Persistence Synchronization	Enable Layer 7 Persistence Synchronization.
Layer 4 Persistence Synchronization	Enable Layer 4 Persistence Synchronization.
Layer 4 Connection Synchronization	Enable Layer 4 Connection Synchronization.
Advanced	
Priority	Set the HA priority as **2**.
Override	Enable the override on resurge.


Setting
Cluster Mode
Standalone
Active-Passive
Active-Active
Active-Active-VRRP
Basic
Group Name
HA
Group ID
1
Default: 0 Range: 0-31
Config Priority
0
Default: 100 Range: 0-255
Local Node ID
1
Default: 0 Range: 0-7
Heartbeat Interface
port3
Data Interface
Heartbeat Type
Multicast
Broadcast
Unicast
Peer Address
192.168.30.67
Local Address
192.168.30.69
Synchronization
Layer 7 Persistence Synchronization
Layer 4 Persistence Synchronization
Layer 4 Connection Synchronization

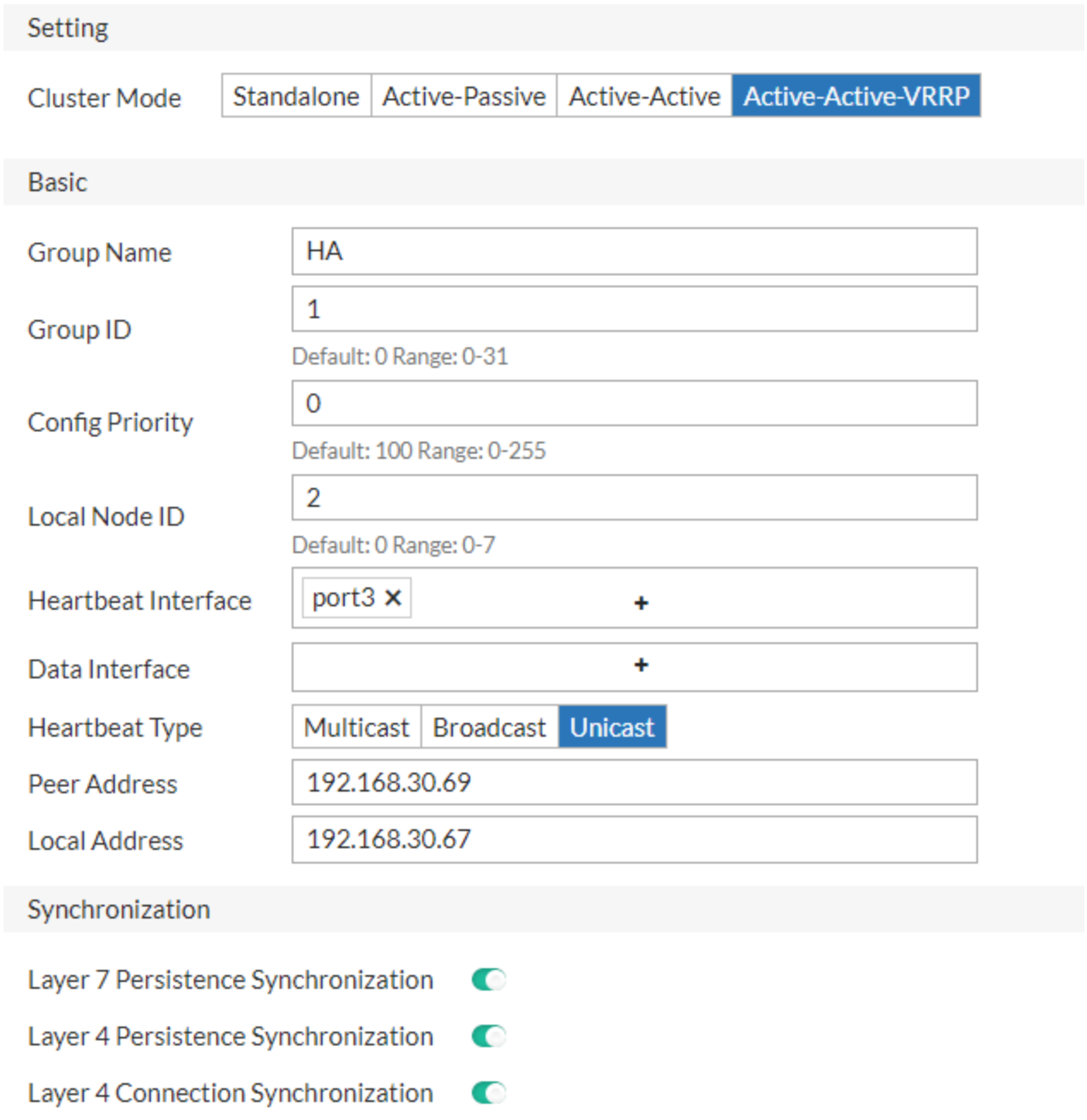


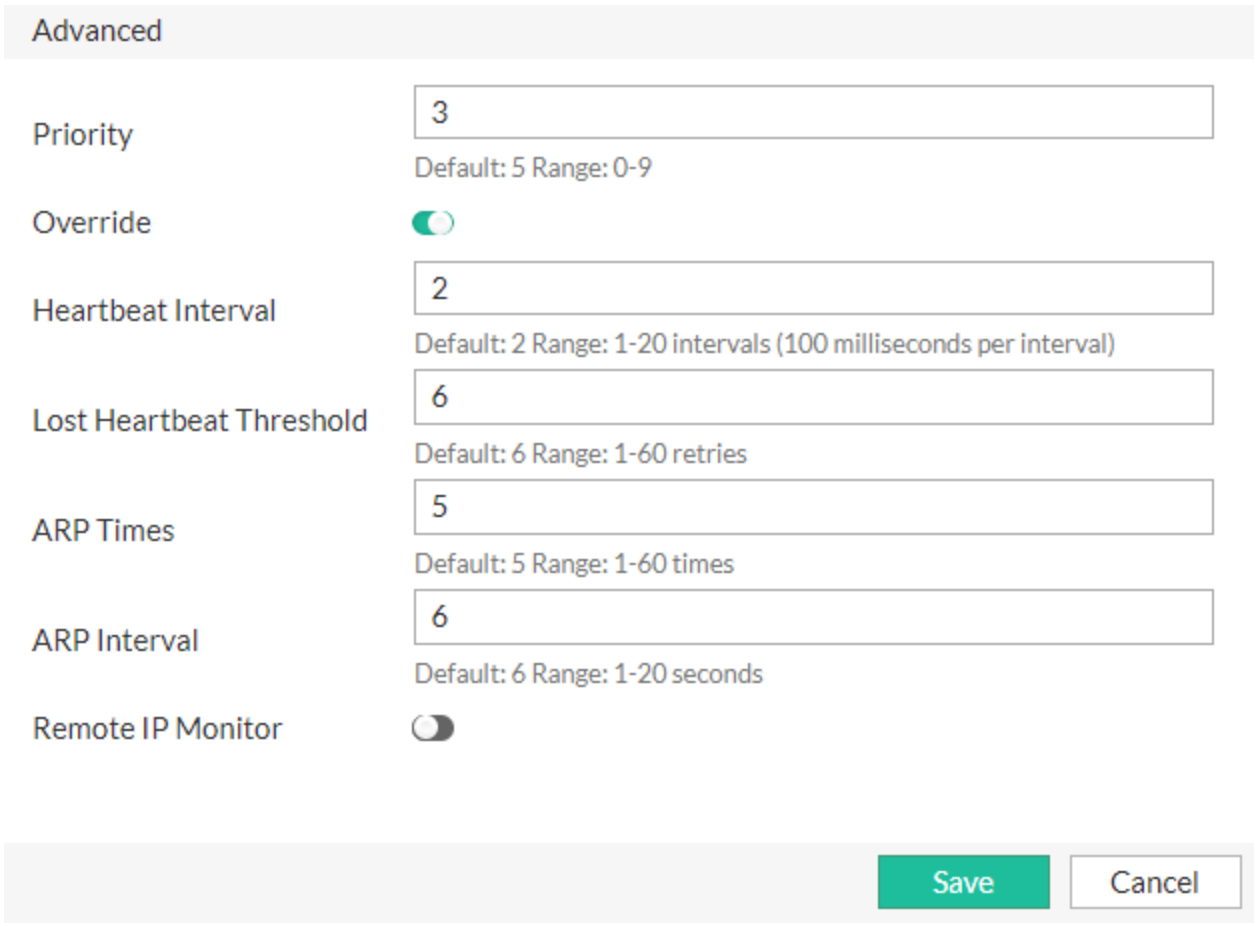
Configure the secondary HA configuration:

1. Log in to the secondary FortiADC-VM.
2. Go to **System > High Availability > Settings**.
3. Configure the following relevant HA settings for the example secondary FortiADC-VM:

Settings	Guidelines
Cluster Mode	Select the **Active-Active-VRRP** cluster mode.
Basic	
Group Name	Enter the Group Name as **HA**.
Group ID	Specify the Group ID as **1**.
Local Node ID	Specify the Local Node ID as **2**.
Heartbeat Interface	Select **port3** as the Heartbeat Interface.
Heartbeat Type	Select **Unicast** as the Heartbeat Type,
Peer Address	Enter the Peer Address as **192.168.30.69**.

Settings	Guidelines
Local Address	Enter the Local Address as **192.168.30.67**.
Synchronization	
Layer 7 Persistence Synchronization	Enable Layer 7 Persistence Synchronization.
Layer 4 Persistence Synchronization	Enable Layer 4 Persistence Synchronization.
Layer 4 Connection Synchronization	Enable Layer 4 Connection Synchronization.
Advanced	
Priority	Set the HA priority as **3**.
Override	Enable the override on resurge.


Setting
Cluster Mode
Standalone
Active-Passive
Active-Active
Active-Active-VRRP
Basic
Group Name
HA
Group ID
1
Default: 0 Range: 0-31
Config Priority
0
Default: 100 Range: 0-255
Local Node ID
2
Default: 0 Range: 0-7
Heartbeat Interface
port3
Data Interface
Heartbeat Type
Multicast
Broadcast
Unicast
Peer Address
192.168.30.69
Local Address
192.168.30.67
Synchronization
Layer 7 Persistence Synchronization
Layer 4 Persistence Synchronization
Layer 4 Connection Synchronization


Advanced
Priority
3
Default: 5 Range: 0-9
Override
Heartbeat Interval
2
Default: 2 Range: 1-20 intervals (100 milliseconds per interval)
Lost Heartbeat Threshold
6
Default: 6 Range: 1-60 retries
ARP Times
5
Default: 5 Range: 1-60 times
ARP Interval
6
Default: 6 Range: 1-20 seconds
Remote IP Monitor
Save
Cancel

Alternatively, you can configure the HA settings through CLI.

Sample ADC1 configuration:

```
config system ha
   set mode active-active-vrrp
   set hbdev port3
   set group-id 1
   set local-node-id 1
   set group-name HA
   set priority 2
   set override enable
   set l7-persistence-pickup enable
   set l4-persistence-pickup enable
   set l4-session-pickup enable
   set hb-type unicast
   set local-address 192.168.30.69
   set peer-address 192.168.30.67
end
```

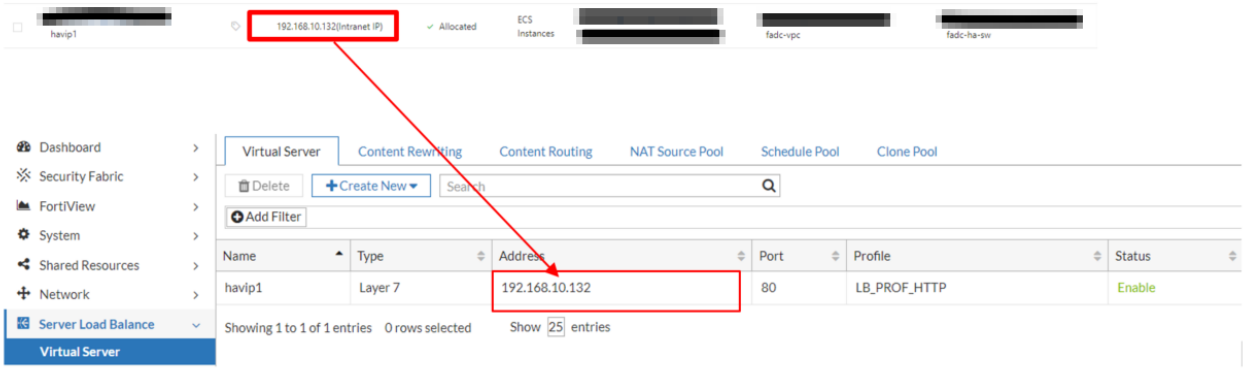
Sample ADC2 configuration:

```
config system ha
   set mode active-active-vrrp
   set hbdev port3
   set group-id 1
   set local-node-id 2
   set group-name HA
   set priority 3
   set override enable
   set l7-persistence-pickup enable
   set l4-persistence-pickup enable
   set l4-session-pickup enable
   set hb-type unicast
   set local-address 192.168.30.67
   set peer-address 192.168.30.69
end
```

Example: Setting the L7 VS virtual IP as the HAVIP Internal IP

1. Log in to the primary FortiADC-VM.
2. Go to **Server Load Balance > Virtual Server**.
3. Edit an existing Layer 7 virtual server configuration or create new.
4. In your Layer 7 virtual server configuration editor, go to the **General** tab.

5. On the General page, under Configuration, specify the Address as the Internal IP of the HAVIP.



Alternatively, you can configure the L7 VS settings through CLI.

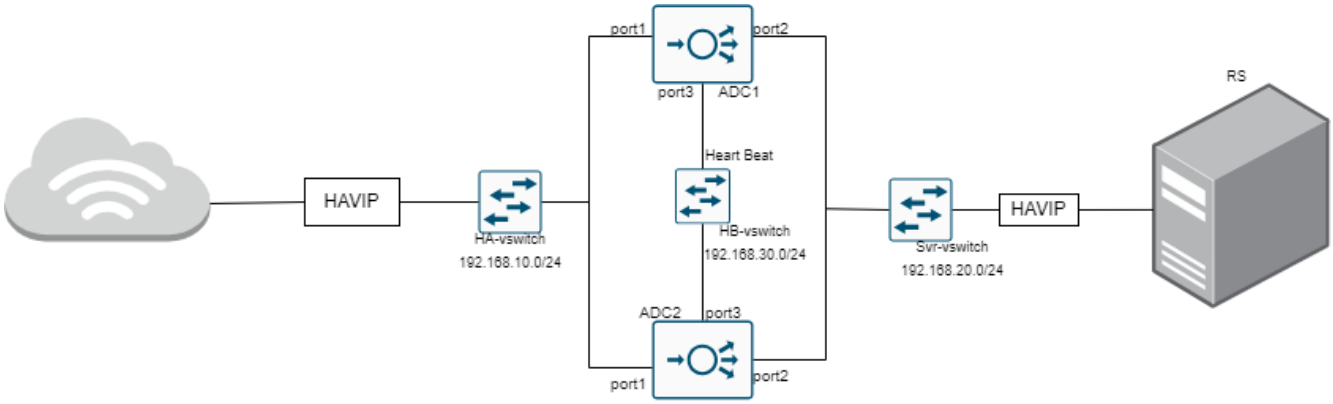
Sample configuration:

```
config load-balance virtual-server
   edit "havip1"
      set type l7-load-balance
      set interface port1
      set ip 192.168.10.132
      set load-balance-profile LB_PROF_HTTP
      set load-balance-persistence app_havip1_20230412205027
      set load-balance-method app_havip1_20230412205027
      set load-balance-pool server1
      set comments "TCP APP_havip1_20230412205027"
      set traffic-group default
   next
end
config load-balance profile
   edit "app_havip1_20230412205027"
   next
end
config load-balance real-server
   edit "server1"
      set ip 192.168.20.244
   next
end
```

Deploying Active-Active-VRRP mode with L4 VS

For Layer 4 virtual servers, the following resources will be created in the Active-Active-VRRP deployment process:

- A VPC including three VSwitches respectively for:
  - External/internal traffic forwarded from the HAVIP.
  - The heartbeat traffic between HA members.
  - The connection between FortiADC and the back-end server.
- Two FortiADC-VM instances.
- An HAVIP with an EIP. The HAVIP's public IP address will be the IP address that clients use to access your application.
- An HAVIP without an EIP. This HAVIP will be the IP address that backend servers use to access FortiADC.



Follow the workflow below to deploy HA in Active-Active-VRRP mode with Layer 4 virtual server on Alibaba Cloud.

1. Setting up the VPC for L4 VS HA on page 29
2. Creating the FortiADC-VM instance and binding to Elastic Network Interfaces (ENIs) on page 30
3. Setting up the HAVIPs for L4 VS on page 31
4. Configuring FortiADC-VM Active-Active-VRRP HA with L4 VS on page 35

Setting up the VPC for L4 VS HA

Assuming this is a new environment, the first step is to create the VPC and define the three vSwitches required for the L4 VS HA deployment.

As part of the VPC setup, you will need to create at least three vSwitches:

- One for the external/internal traffic forwarded from the HAVIP.
- One for the heartbeat traffic between HA members.
- One for the connection between FortiADC and the back-end server.

For detailed steps on how to create and configure a VPC, see Creating a VPC (Virtual Private Cloud) on page 6.

After you have set up your VPC and created the required vSwitches, configure the security group rules. For detailed steps, see Configuring the Security Group Rules on page 12.

Creating the FortiADC-VM instance and binding to Elastic Network Interfaces (ENIs)

After you have set up your VPC and required vSwitches for deploying HA with L4 VS, you need to create a FortiADC-VM instance and bind it to three Elastic Network Interfaces (ENIs). The three ENIs will be associated with each of the three vSwitches previously created when setting up the VPC.

During the instance creation process, you will bind one primary ENI and one secondary ENI to the instance. Then, for the third remaining ENI (the second secondary ENI), you will create it and bind it to the FortiADC-VM after the installation is complete.

1. Create the FortiADC-VM instance and configure the primary and secondary ENIs as part of the Networking settings. Associate the primary and secondary ENIs with the vSwitches previously created in the VPC setup. For details, see Setting up the VPC for L4 VS HA on page 29.
   For detailed steps on how to create the FortiADC-VM instance, see Creating the FortiADC-VM instance on page 9.
2. After creating the FortiADC instance and binding the primary ENI and first secondary ENI, create the second secondary ENI.
   a. Navigate to **Network & Security > ENIs**. Click **Create ENI** to display the configuration editor.
   b. Configure the following **ENI** settings:

Setting	Description
ENI Name	Enter a name for the ENI. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-), and it must start with a letter.
VPC	Select the VPC you have previously created. To bind the created ENI to an instance, select the PVC in which the instance resides. After the ENI is created, you cannot change the VPC in which the ENI belongs to. **Note**: An ENI can only be bound to an instance that is in the same VPC as the ENI.
vSwitch	Select the vSwitch you want to associate with. This should be the remaining vSwitch that has not been associated with the primary and secondary ENIs during the instance installation.
Primary Private IP	Optionally, enter an IPv4 address as the primary private IP address of the ENI. The IPv4 address must be an idle IP address within the CIDR block of the selected vSwitch. If you do not specify an IPv4 address, an idle private IPv4 address is automatically assigned to the ENI after the ENI is created.
Secondary Private IP Addresses	Optionally, specify secondary private IPv4 addresses for the ENI. • Not set — No secondary private IPv4 addresses are assigned to the ENI. • Auto — The system automatically assigns the specified number of idle IPv4 addresses from within the CIDR block of the selected vSwitch to the ENI. Range is 1 to 9. • Manual — Manually assign secondary private IPv4 addresses to the ENI. Range is 1 to 9.

Setting	Description
Security Group	Select security groups in the selected VPC. This should be the Security Group you have previously created. You can specify up to five security groups. **Note**: Basic security groups and advanced security groups cannot be selected at the same time.
Description	Optionally, enter a description to help you manage the ENI.
Resource Group	Select the Resource Group. It should be in the same resource group as that of the FortiADC-VM instance.
Tag	Optionally, select one or more tags to add to the ENI for easy search and management.

   c. Click **Create**.
   When the ENI is created, the **Status** column of the ENI will display as **Available** on the **Network Interfaces** page.
   You can then bind the ENI to an instance.

3. Bind the remaining secondary ENI to the FortiADC-VM instance.
   a. Navigate to **Instances & Images > Instances**.
   b. On the Instances page, select the FortiADC-VM instance you want to bind the secondary ENI to.
   c. On the FortiADC-VM instance details page, go to the **ENIs** tab and click **Bind Secondary ENI** to display the configuration editor.
   d. Select the secondary ENI you want to bind to the FortiADC-VM and click **OK**.
   After you bind the ENI to the FortiADC-VM instance, you can go to the Instance Details page and view the state of the ENI on the **ENIs** tab. If the ENI is bound to the instance, **InUse** is displayed in the Status/Creation Time column corresponding to the ENI.

Setting up the HAVIPs for L4 VS

To deploy HA with L4 VS, you will need to create two HAVIPs (high-availability virtual IP address) and associate one of the HAVIPs with an EIP (elastic IP address). An HAVIP is a private IP address that can be created and released as an independent resource. After an HAVIP is associated with an EIP, the HAVIP can use the EIP to provide services over the Internet.

You will need to create two HAVIPs:

- An HAVIP with an EIP. The HAVIP's public IP address will be the IP address that clients use to access your application.
- An HAVIP without an EIP. This HAVIP will be the IP address that backend servers use to access FortiADC.

Before you begin:

- You must already have an EIP. If you do not have an EIP, you can create an EIP in **VPC > Access to Internet > Elastic IP Address**.

To create the first HAVIP and bind it to an EIP:

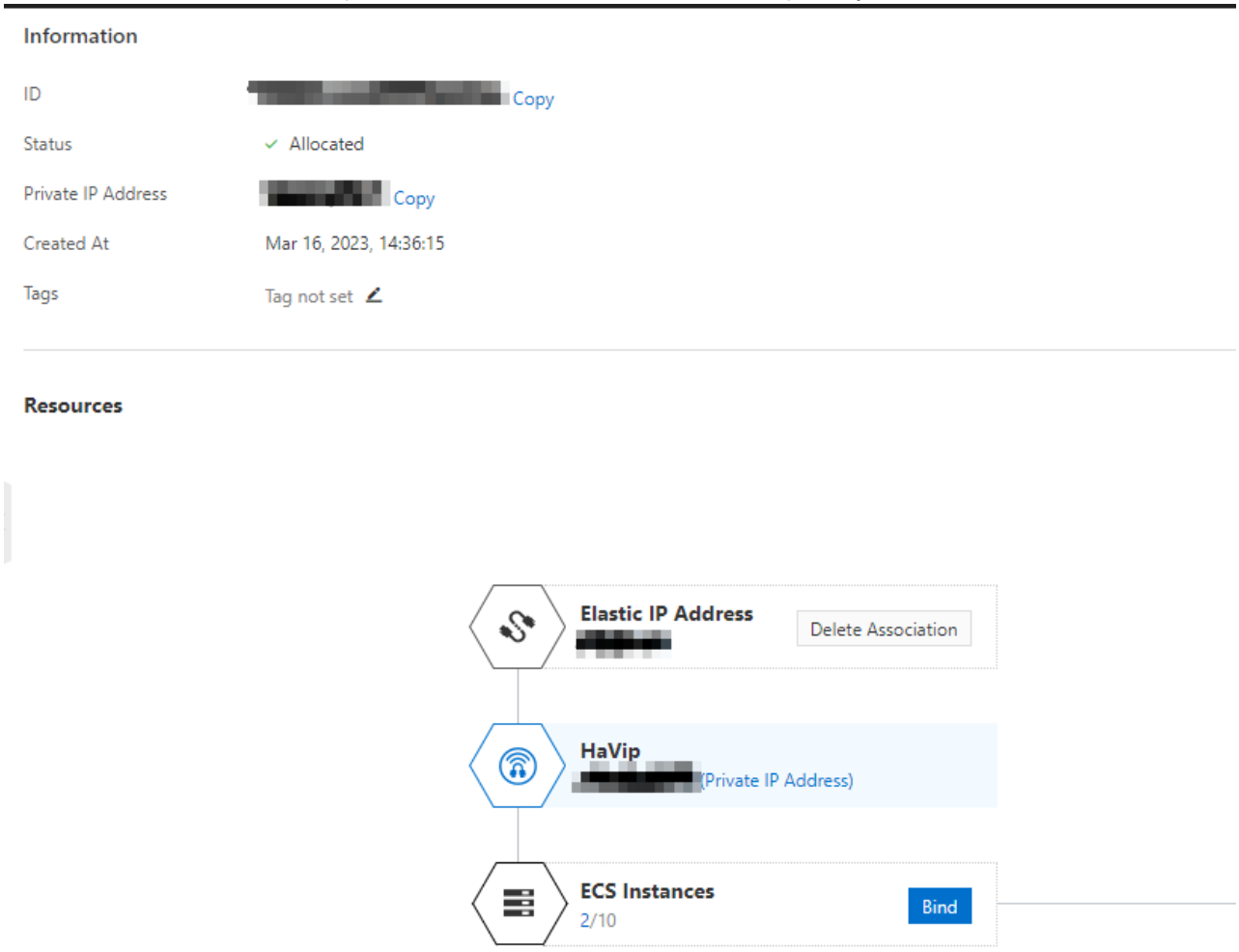
1. Navigate to the **VPC** page and click **HaVIp**.
2. On the HaVIp page, click **Create HaVIp** to display the configuration editor.

3. Configure the following HAVIP settings:

Setting	Description
Resource Group	Select the Resource Group you have created.
Name	Enter a name for the HAVIP.
VPC	Select the VPC you have created previously.
vSwitch	Select the vSwitch you have created previously for the Internet Access.
vSwitch CIDR Block	Displays the CIDR block of the vSwitch.
Whether to automatically assign private IP addresses	Select whether to automatically allocate a private IP address. • Yes — The system automatically allocates an idle private IP address from the vSwitch CIDR block. • No — Manually enter an idle private IP address from the vSwitch CIDR block.

4. Click **OK**.
   Once the HAVIP is created, take note of the **Internal IP address**. The Internal IP address will be the virtual server IP of your L4 VS configuration.
5. Select the newly created HAVIP and click **Bind EIP Address**.

6. Click the name of the HAVIP and click **Bind** to bind the FortiADC-VM instances you have created with this HAVIP. Traffic destined for the HAVIP's public IP address will be forwarded to the primary FortiADC-VM.



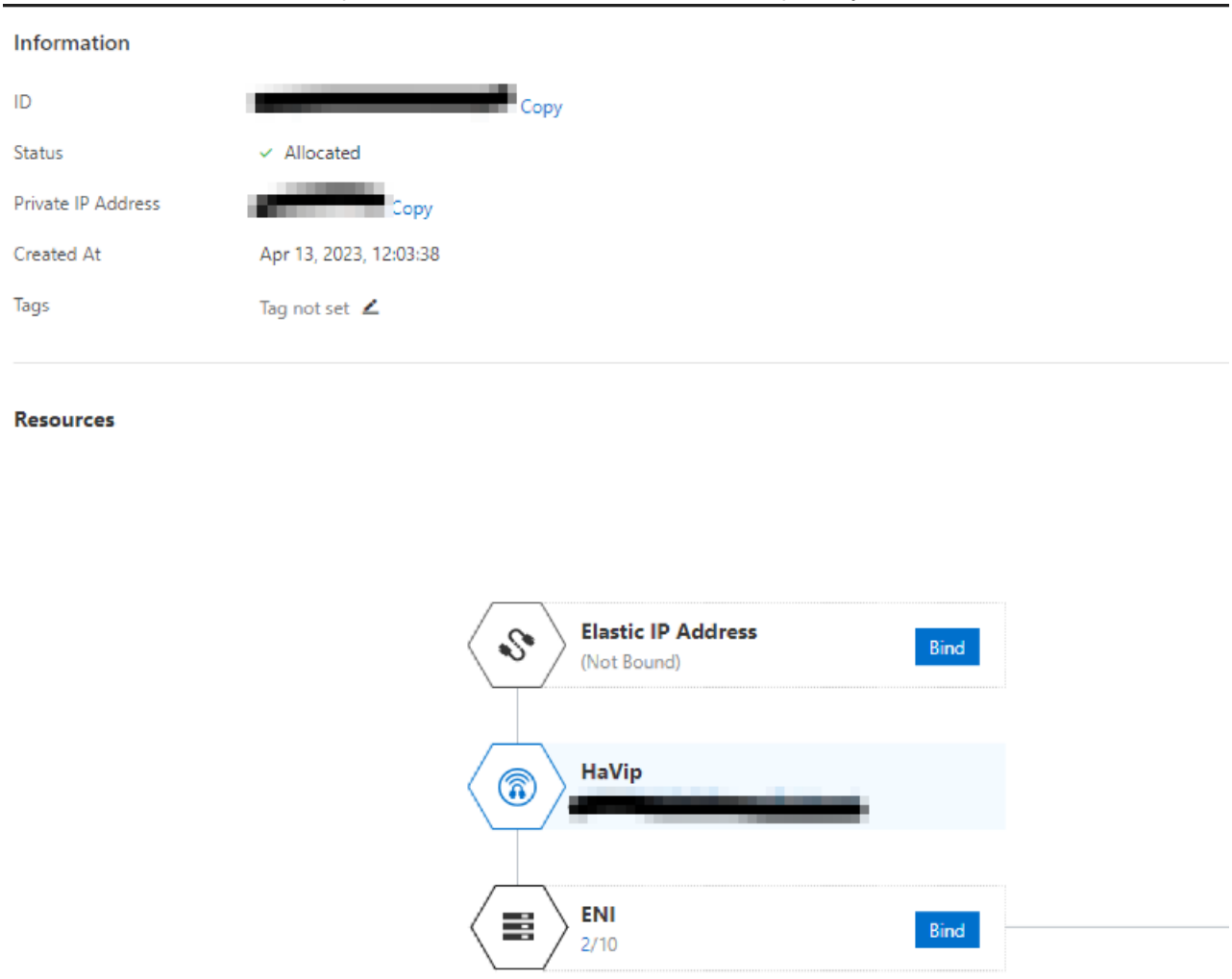
Create the second HAVIP:

1. Navigate to the **VPC** page and click **HaVIp**.
2. On the HaVIp page, click **Create HaVIp** to display the configuration editor.
3. Configure the following HAVIP settings:

Setting	Description
Resource Group	Select the Resource Group you have created.
Name	Enter a name for the HAVIP.
VPC	Select the VPC you have created previously.
vSwitch	Select the vSwitch you have created previously for the connection between FortiADC and the back-end server.
vSwitch CIDR Block	Displays the CIDR block of the vSwitch.

Setting	Description
Whether to automatically assign private IP addresses	Select whether to automatically allocate a private IP address. • Yes — The system automatically allocates an idle private IP address from the vSwitch CIDR block. • No — Manually enter an idle private IP address from the vSwitch CIDR block.

4. Click **OK**.
   Once the HAVIP is created, take note of the **Internal IP address**. The Internal IP address will be the Full NAT IP pool of your L4 VS configuration.
5. Click the name of the HAVIP and click **Bind** to bind the FortiADC-VM instances you have created with this HAVIP. Traffic destined for the HAVIP's public IP address will be forwarded to the primary FortiADC-VM.



After you have set up your FortiADC-VM instance and the required HAVIPs, the next step is to log into FortiADC through GUI or CLI to configure the HA cluster. For detailed steps, see Accessing the FortiADC GUI and CLI on page 14.

Configuring FortiADC-VM Active-Active-VRRP HA with L4 VS

After setting up the FortiADC-VM instances in AliCloud, log in to the FortiADC-VMs to set up your HA and L4 VS configurations. In the L4 VS configuration of the primary FortiADC-VM, you will need to set the virtual IP as the Internal IP of the HAVIP bound to an EIP, and the source IP Pool as the Internal IP of the HAVIP not bound to an EIP.

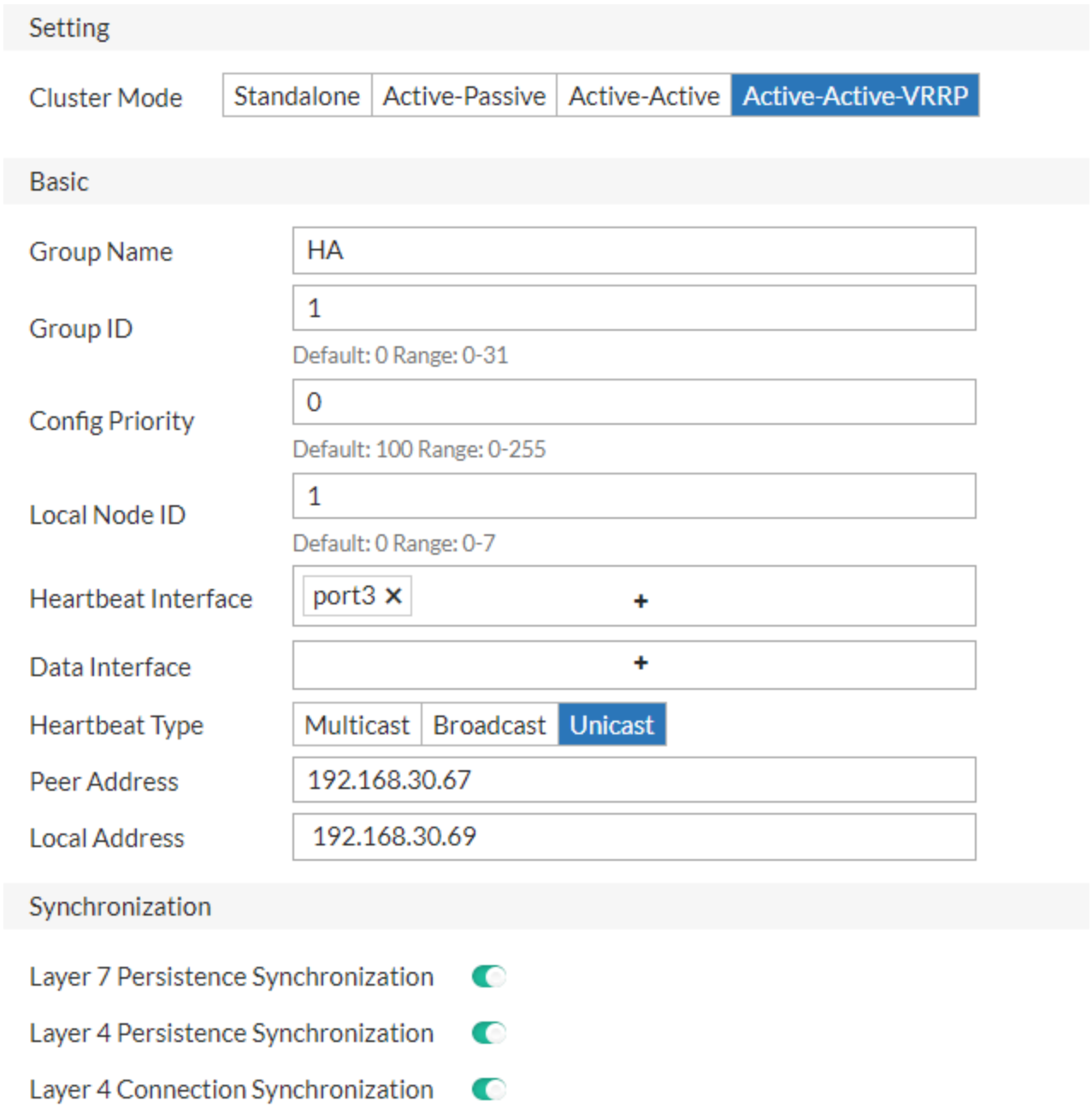
Example: Configuring the HA primary and secondary FortiADC-VMs

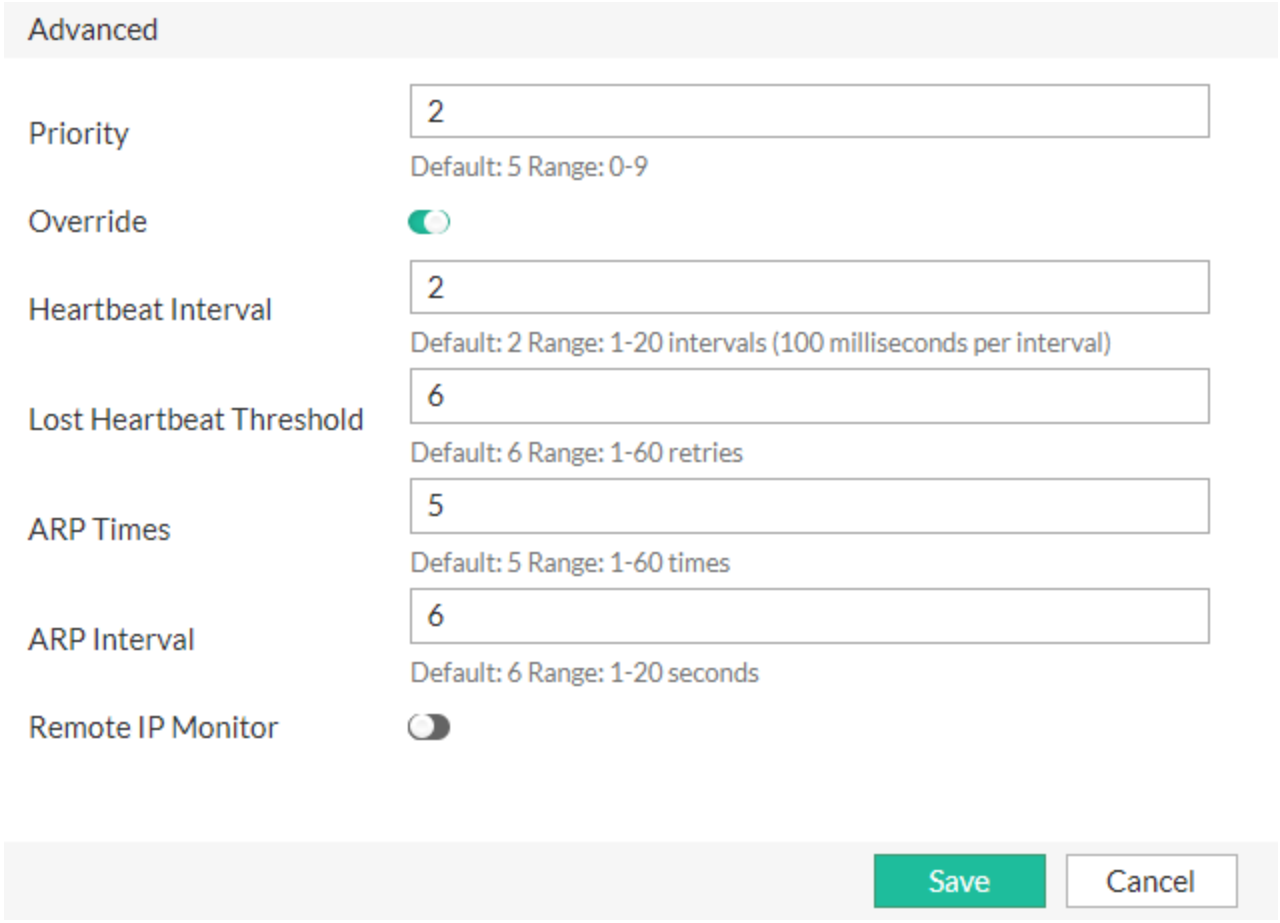
The following example describes how to configure your HA primary and secondary FortiADC-VMs.

Configure the primary HA configuration:

1. Log in to the primary FortiADC-VM.
2. Go to **System > High Availability > Settings**.
3. Configure the following relevant HA settings for the example primary FortiADC-VM:

Settings	Guidelines
Cluster Mode	Select the **Active-Active-VRRP** cluster mode.
Basic	
Group Name	Enter the Group Name as **HA**.
Group ID	Specify the Group ID as **1**.
Local Node ID	Specify the Local Node ID as **1**.
Heartbeat Interface	Select **port3** as the Heartbeat Interface.
Heartbeat Type	Select **Unicast** as the Heartbeat Type,
Peer Address	Enter the Peer Address as **192.168.30.67**.
Local Address	Enter the Local Address as **192.168.30.69**.
Synchronization	
Layer 7 Persistence Synchronization	Enable Layer 7 Persistence Synchronization.
Layer 4 Persistence Synchronization	Enable Layer 4 Persistence Synchronization.
Layer 4 Connection Synchronization	Enable Layer 4 Connection Synchronization.
Advanced	
Priority	Set the HA priority as **2**.
Override	Enable the override on resurge.


Setting
Cluster Mode
Standalone
Active-Passive
Active-Active
Active-Active-VRRP
Basic
Group Name
HA
Group ID
1
Default: 0 Range: 0-31
Config Priority
0
Default: 100 Range: 0-255
Local Node ID
1
Default: 0 Range: 0-7
Heartbeat Interface
port3
Data Interface
Heartbeat Type
Multicast
Broadcast
Unicast
Peer Address
192.168.30.67
Local Address
192.168.30.69
Synchronization
Layer 7 Persistence Synchronization
Layer 4 Persistence Synchronization
Layer 4 Connection Synchronization

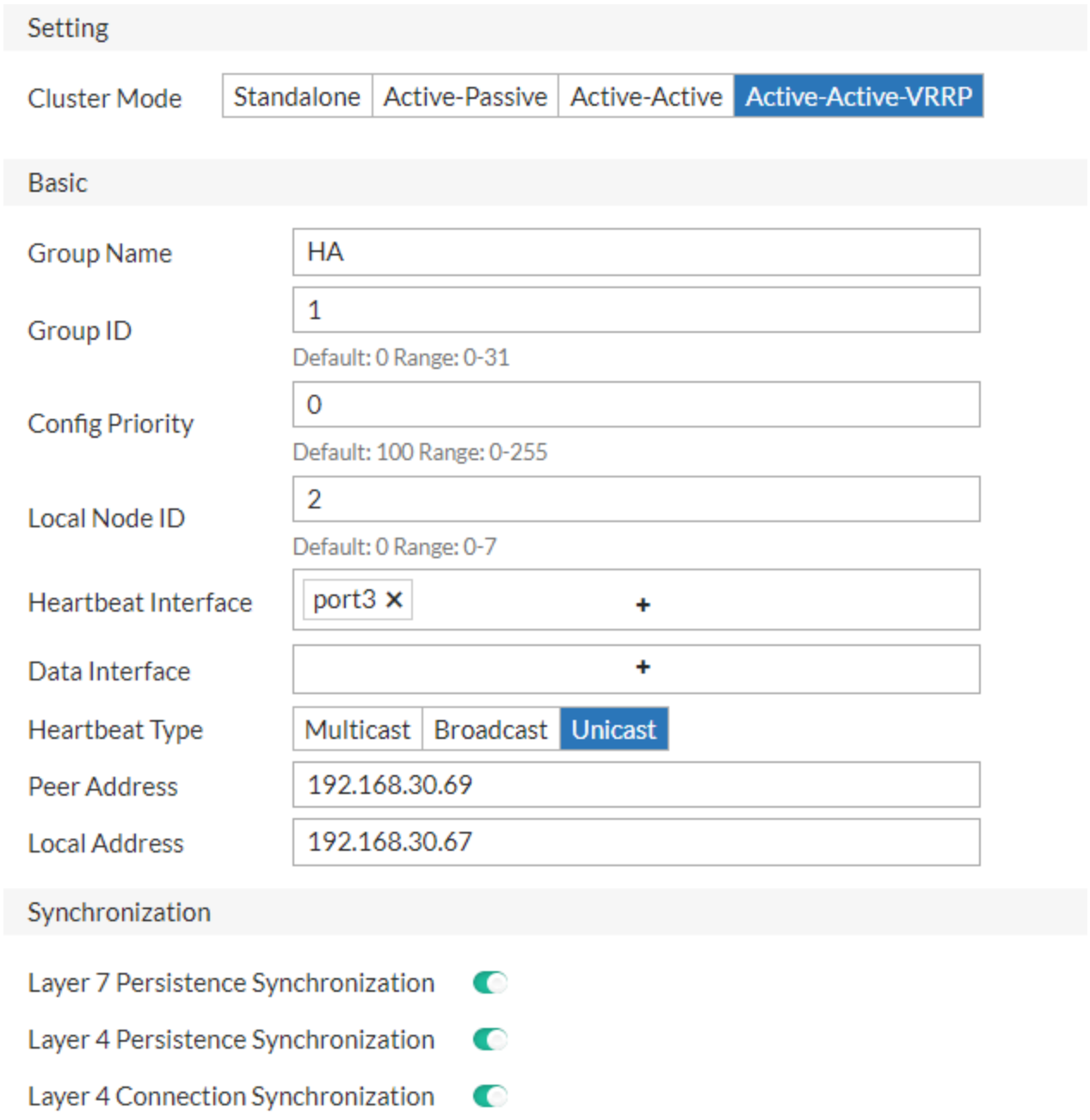


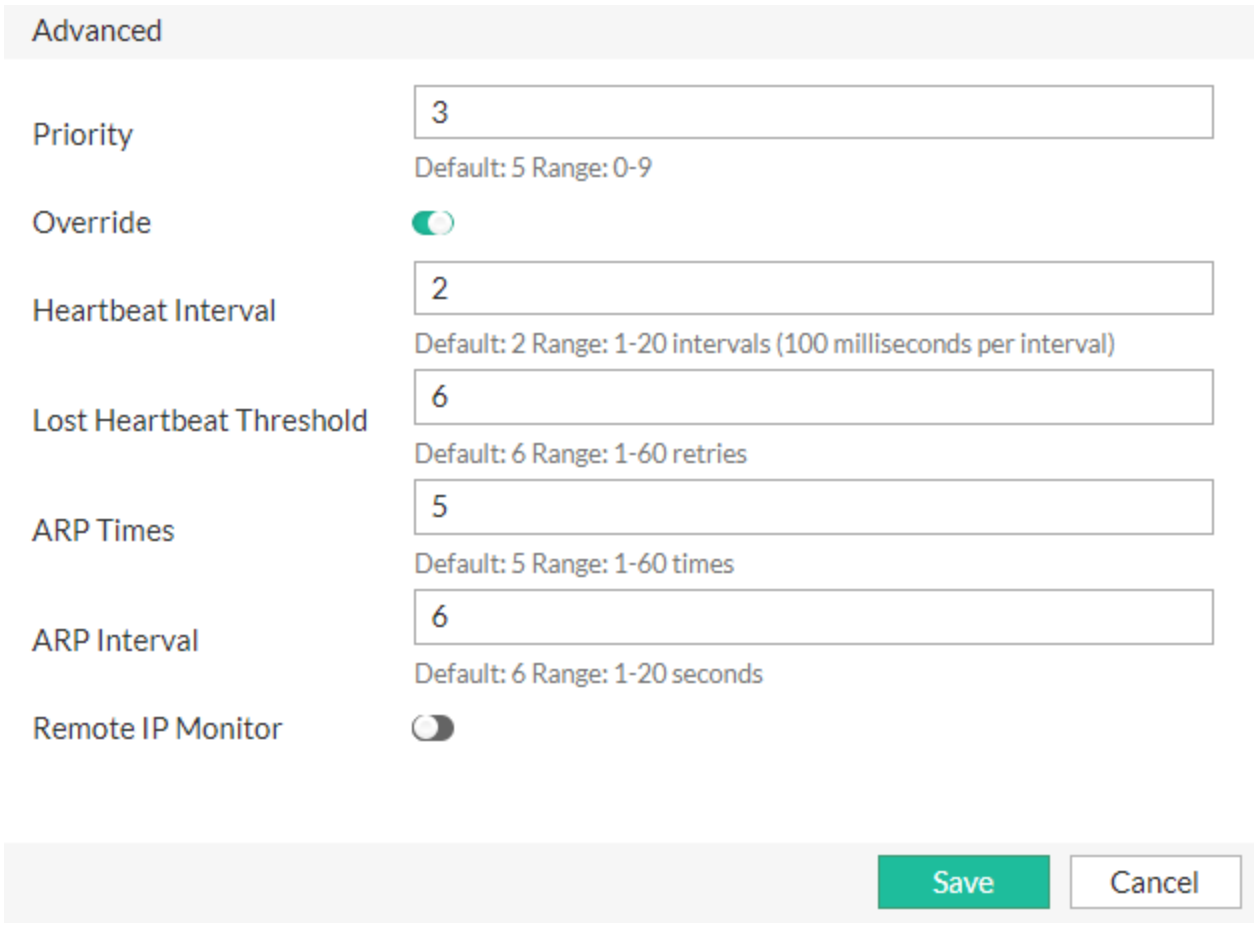
Configure the secondary HA configuration:

1. Log in to the secondary FortiADC-VM.
2. Go to **System > High Availability > Settings**.
3. Configure the following relevant HA settings for the example secondary FortiADC-VM:

Settings	Guidelines
Cluster Mode	Select the **Active-Active-VRRP** cluster mode.
Basic	
Group Name	Enter the Group Name as **HA**.
Group ID	Specify the Group ID as **1**.
Local Node ID	Specify the Local Node ID as **2**.
Heartbeat Interface	Select **port3** as the Heartbeat Interface.
Heartbeat Type	Select **Unicast** as the Heartbeat Type,
Peer Address	Enter the Peer Address as **192.168.30.69**.

Settings	Guidelines
Local Address	Enter the Local Address as **192.168.30.67**.
Synchronization	
Layer 7 Persistence Synchronization	Enable Layer 7 Persistence Synchronization.
Layer 4 Persistence Synchronization	Enable Layer 4 Persistence Synchronization.
Layer 4 Connection Synchronization	Enable Layer 4 Connection Synchronization.
Advanced	
Priority	Set the HA priority as **3**.
Override	Enable the override on resurge.


Setting
Cluster Mode
Standalone
Active-Passive
Active-Active
Active-Active-VRRP
Basic
Group Name
HA
Group ID
1
Default: 0 Range: 0-31
Config Priority
0
Default: 100 Range: 0-255
Local Node ID
2
Default: 0 Range: 0-7
Heartbeat Interface
port3
Data Interface
Heartbeat Type
Multicast
Broadcast
Unicast
Peer Address
192.168.30.69
Local Address
192.168.30.67
Synchronization
Layer 7 Persistence Synchronization
Layer 4 Persistence Synchronization
Layer 4 Connection Synchronization


Advanced
Priority
3
Default: 5 Range: 0-9
Override
Heartbeat Interval
2
Default: 2 Range: 1-20 intervals (100 milliseconds per interval)
Lost Heartbeat Threshold
6
Default: 6 Range: 1-60 retries
ARP Times
5
Default: 5 Range: 1-60 times
ARP Interval
6
Default: 6 Range: 1-20 seconds
Remote IP Monitor
Save
Cancel

Alternatively, you can configure the HA settings through CLI.

Configure HA on ADC1:

```
config system ha
   set mode active-active-vrrp
   set hbdev port3
   set group-id 1
   set local-node-id 1
   set group-name HA
   set priority 2
   set override enable
   set l7-persistence-pickup enable
   set l4-persistence-pickup enable
   set l4-session-pickup enable
   set hb-type unicast
   set local-address 192.168.30.69
   set peer-address 192.168.30.67
end
```

Configure HA on ADC2:

```
config system ha
   set mode active-active-vrrp
   set hbdev port3
   set group-id 1
   set local-node-id 2
   set group-name HA
   set priority 3
   set override enable
   set l7-persistence-pickup enable
   set l4-persistence-pickup enable
   set l4-session-pickup enable
   set hb-type unicast
   set local-address 192.168.30.67
   set peer-address 192.168.30.69
end
```

Example: Setting the L4 VS virtual IP as the Internal IP of the HAVIP with an EIP

1. Log in to the primary FortiADC-VM.
2. Go to **Server Load Balance > Virtual Server**.
3. Edit an existing Layer 4 virtual server configuration or create new.
4. In your Layer 4 virtual server configuration editor, go to the **General** tab.
5. On the General page, under Configuration, specify the Address as the Internal IP of the HAVIP.

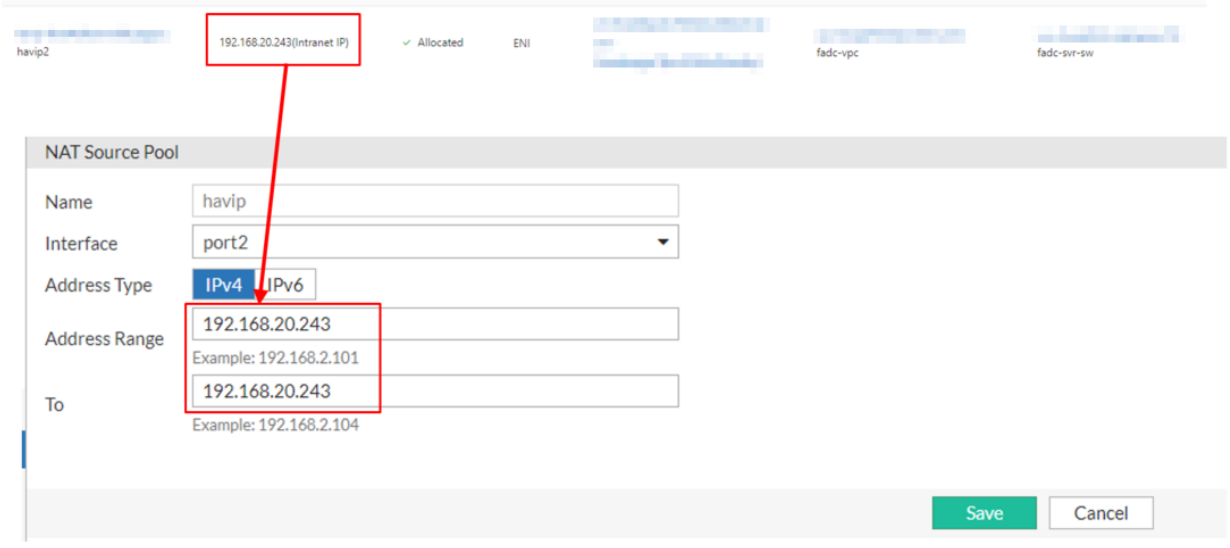
Alternatively, you can configure the L4 VS settings through CLI.

Sample configuration:

```
config load-balance virtual-server
   edit "havip1"
      set type l7-load-balance
      set interface port1
      set ip 192.168.10.132
      set load-balance-profile LB_PROF_HTTP
      set load-balance-persistence app_havip1_20230412205027
      set load-balance-method app_havip1_20230412205027
      set load-balance-pool server1
      set comments "TCP APP_havip1_20230412205027"
      set traffic-group default
   next
end
config load-balance profile
   edit "app_havip1_20230412205027"
   next
end
config load-balance real-server
   edit "server1"
      set ip 192.168.20.244
   next
end
```

Example: Setting the L4 VS source IP Pool as the Internal IP of the HAVIP without an EIP

1. Log in to the primary FortiADC-VM.
2. Go to **Server Load Balance > Virtual Server**.
3. Click the **NAT Source Pool** tab.
4. Edit an existing NAT Source Pool configuration or create new.
5. In your NAT Source Pool configuration editor, specify the Address Range as the Internal IP of the HAVIP without an EIP.



Note: The Full NAT IP should be specified to the HAVIP, IP range is not supported.

Alternatively, you can configure the L4 VS settings through CLI.

Sample configuration:

```
config load-balance ippool
   edit "havip"
      set interface port2
      set ip-min 192.168.20.243
      set ip-max 192.168.20.243
      config node-member
      end
   next
end
```

Sample L4 VS configuration with Full NAT:

```
config load-balance virtual-server
   edit "havip1"
      set packet-forwarding-method FullNAT
      set interface port1
      set ip 192.168.10.132
      set load-balance-profile LB_PROF_TCP
      set load-balance-persistence app_havip1_20230412205027
      set load-balance-method app_havip1_20230412205027
      set load-balance-pool server1
      set ippool-list havip
      set comments "TCP APP_havip1_20230412205027"
      set traffic-group default
   next
end
config load-balance profile
   edit "app_havip1_20230412205027"
   next
end
config load-balance real-server
   edit "server1"
      set ip 192.168.20.244
   next
end
```

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. When HA Active-Active-VRRP mode is enabled, only L7 VS mode and L4 VS Full NAT mode are supported.
3. For L4 VS DNAT, ensure the FortiADC is the gateway of the real server. If the real server is also deployed in the AliCloud, ensure there is no external IP address configured on the real server. Otherwise, the real server will not send back the data to the FortiADC for external traffic, regardless of the routing rules you configure on the real server. This behavior is due to AliCloud prioritizing the routing rules to the public networks which results in all the traffic to Public IP destinations being sent back via its default public route settings instead of the specified gateway.

www.fortinet.com