ALIBABA CLOUD

阿里云

弹性容器实例

网络

文档版本：20220713

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.连接公网

如果您的ECI实例有连接公网的需求，则需要配置NAT网关或者弹性公网IP，并支付相应的网络费用。本文介绍如何为ECI实例绑定EIP，或者为ECI实例所属VPC绑定NAT网关，以实现ECI实例与公网互通。

背景信息

为ECI实例配置公网服务时，支持以下两种方式：

方式	说明	费用
绑定EIP	EIP是独立购买的可单独持有的公网IP地址，可以为绑定的ECI实例提供公网服务。	EIP支持包年包月和按量付费，按固定带宽或者使用流量计费。EIP绑定至ECI实例时，免除配置费用，但可能收取绑定费用。更多信息，请参见EIP计费说明。
绑定NAT网关	NAT网关是可独立购买的网关产品，绑定EIP后，可以为关联VPC下的所有ECI实例提供公网服务。	NAT网关支持包年包月和按量付费。NAT网关需绑定EIP后才能具备公网能力，即除NAT网关费用外，您还需支付EIP费用。更多信息，请参见NAT网关计费说明。

您可以根据业务需要，选择合适的方式来配置公网服务：

- 示例场景一：单个ECI实例配置Nginx外网访问

  如果您有一个ECI实例用于部署Nginx服务，在创建实例时，您需要为该实例绑定EIP。当Nginx启动时，将自动暴露80端口到EIP。您可以通过EIP地址加端口的方式访问Nginx服务。

- 示例场景二：多个ECI实例拉取Docker Hub镜像

  ECI默认不提供外部公网链路进行公网镜像的拉取。如果您有多个ECI实例需要从Docker Hub拉取镜像，您需要为ECI实例所属的VPC绑定NAT网关来实现公网访问，否则镜像将拉取失败。

> **说明**
>
> 为ECI实例配置公网服务时，请确保ECI实例所属的安全组已放行相关地址和端口。更多信息，请参见添加安全组规则。

方式一：为ECI实例绑定EIP

创建ECI实例时，您可以直接为ECI实例绑定EIP。方式如下：

> **说明**
>
> EIP只支持为所绑定的ECI实例提供公网服务，一个EIP只能绑定一个ECI实例。如果您有多个ECI实例需要连接公网，您需要分别为其绑定EIP，或者为所属VPC绑定NAT网关。

Kubernetes方式

您可以在Pod metadata中添加Annotation来绑定已有的EIP，或者自动创建并绑定一个EIP。相关配置项如下：

配置项	说明
k8s.aliyun.com/eci-eip-instanceid	绑定已有的EIP。
k8s.aliyun.com/eci-with-eip	是否自动创建并绑定EIP。
k8s.aliyun.com/eip-bandwidth	设置EIP带宽。默认为5 Mbps。
k8s.aliyun.com/eip-common-bandwidth-package-id	绑定已有的共享带宽包。
k8s.aliyun.com/eip-isp	设置EIP的线路类型。取值范围： • BPG：BGP（多线）线路 • BGP_PRO：BGP（多线）精品线路
k8s.aliyun.com/eip-internet-charge-type	设置EIP的计量方式。取值范围： • PayByBandwidth：按带宽计费 • PayByTraffic：按流量计费

- 示例一：指定已有EIP

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
  annotations:
    k8s.aliyun.com/eci-eip-instanceid: "eip-bp1q5n8cq4p7f6dzu****"     #指定已有的EIP进行绑定
spec:
  containers:
  - image: registry-vpc.cn-hangzhou.aliyuncs.com/jovi/nginx:alpine
    imagePullPolicy: Always
    name: nginx
    ports:
    - containerPort: 80
      name: http
      protocol: TCP
  restartPolicy: OnFailure
```

- 示例二：自动创建EIP，并设置EIP带宽

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
  annotations:
    k8s.aliyun.com/eci-with-eip: "true"   #自动创建并绑定EIP
    k8s.aliyun.com/eip-bandwidth: "10"   #设置EIP带宽
spec:
  containers:
  - image: registry-vpc.cn-hangzhou.aliyuncs.com/jovi/nginx:alpine
    imagePullPolicy: Always
    name: nginx
    ports:
    - containerPort: 80
      name: http
      protocol: TCP
  restartPolicy: OnFailure
```

- 示例三：自动创建EIP，并绑定共享带宽包

```
apiVersion: v1
kind: Pod
metadata:
  name: nginx
  annotations:
    k8s.aliyun.com/eci-with-eip: "true"   #自动创建并绑定EIP
    k8s.aliyun.com/eip-common-bandwith-package-id: "cbwp-2zeukbj916scmj51m****"  #绑定共享带宽包
spec:
  containers:
  - image: registry-vpc.cn-hangzhou.aliyuncs.com/jovi/nginx:alpine
    imagePullPolicy: Always
    name: nginx
    ports:
    - containerPort: 80
      name: http
      protocol: TCP
  restartPolicy: OnFailure
```

OpenAPI方式

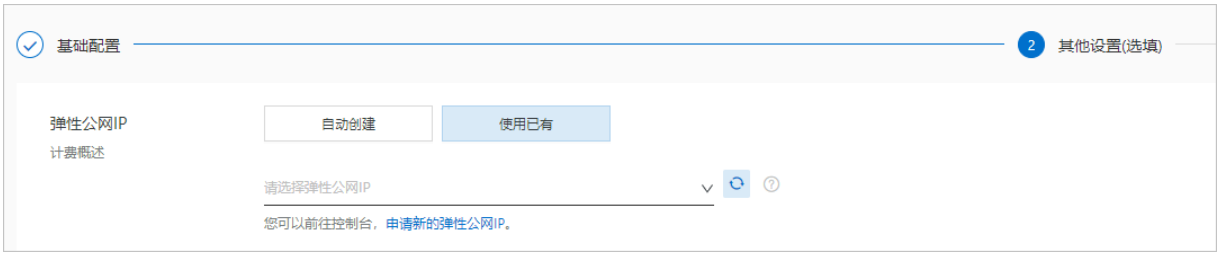
调用CreateContainerGroup接口创建ECI实例时，您可以通过EipInstanceId参数来绑定已有的EIP，或者通过AutoCreateEip和EipBandwidth参数来创建并绑定一个EIP。相关参数说明如下表所示。更多信息，请参见CreateContainerGroup。

名称	类型	示例值	描述
EipInstanceId	String	eip-uf66jeqopgqa9hdn****	指定EIP，将其绑定到ECI实例上。

名称	类型	示例值	描述
AutoCreateEip	Boolean	true	是否自动创建一个EIP，并绑定到ECI实例上。
EipBandwidth	Integer	5	EIP的带宽，默认为5 Mbps。当AutoCreateEip取值为true时，可以设置该参数。

控制台方式

创建ECI实例时，完成基础配置后，在**其他设置**处，您可以直接为ECI实例绑定EIP。支持使用已有EIP或者自动创建EIP，如下图所示。



方式二：为VPC绑定NAT网关

您可以在专有网络控制台为VPC绑定NAT网关，并为NAT网关绑定EIP，使其能够提供NAT代理（SNAT和DNAT）功能：

- SNAT功能：可以为VPC中没有公网IP的ECI实例提供访问公网的代理服务。
- DNAT功能：可以将NAT网关绑定的EIP映射给VPC中的ECI实例使用，使其能够面向公网提供服务。

操作步骤如下：

1. 登录专有网络控制台。
2. 在顶部菜单栏左上角处，选择地域。
3. 在**NAT网关**页面，创建NAT网关。
   i. 单击**创建NAT网关**。
   ii. 完成购买NAT网关相关的参数配置。

   配置时，请选择ECI实例所属的地域和可用区，以及对应的VPC和交换机。更多信息，请参见购买NAT网关。
   iii. 确认配置信息和费用，单击**立即购买**。
4. 在**弹性公网IP**页面，创建EIP。
   i. 单击**创建弹性公网IP**。
   ii. 完成购买EIP相关的参数配置。

   配置时，请选择ECI实例所属的地域。更多信息，请参见申请新EIP。
   iii. 确认配置信息和费用，单击**立即购买**。
5. 绑定EIP与NAT网关。
   i. 在**NAT网关**页面，找到目标NAT网关，单击对应的**立即绑定**。

ii. 在弹出的对话框中选择要绑定的EIP，然后单击**确定**。

6. 如果您的ECI实例需要访问公网，您需要创建SNAT条目。

i. 在**NAT网关**页面，找到目标NAT网关，单击对应的**设置SNAT**。

ii. 单击**创建SNAT条目**。

iii. 配置SNAT相关条目的参数。

配置时，需要关注的参数如下表所示。更多信息，请参见创建SNAT实现访问公网服务。

参数	描述
SNAT条目粒度	选择**交换机粒度**。
选择交换机	选择用于创建ECI实例的交换机，支持配置多个。配置后，交换机下所有ECI实例均可以通过SNAT功能访问公网。
选择公网IP地址	选择**使用单IP**，然后选择NAT网关绑定的EIP，用于访问公网。

iv. 单击**确定**。

> **说明**
>
> 如果ECI实例已经绑定了EIP，则优先使用ECI实例绑定的EIP来访问公网，而不会使用NAT网关的SNAT功能访问公网。

7. 如果您的ECI实例需要面向公网提供服务，您需要创建DNAT条目。

i. 在**NAT网关**页面，找到目标NAT网关，单击对应的**设置DNAT**。

ii. 单击**创建DNAT条目**。

iii. 配置DNAT相关条目的参数。

配置时，需要关注的参数如下表所示。更多信息，请参见创建DNAT提供公网访问服务。

参数	描述
选择公网IP地址	选择NAT网关绑定的EIP，用于公网访问。
选择私网IP地址	选择要通过DNAT规则进行公网通信的ECI实例，支持指定ECI实例对应的弹性网卡，或者手动输入ECI实例的私网IP。
端口设置	选择DNAT映射的方式： ■ 任意端口：该方式输入IP映射。任何访问NAT所绑定EIP的请求都将转发到目标ECI实例。 ■ 具体端口：该方式输入端口映射。NAT网关会将以指定协议和端口访问NAT所绑定EIP的请求转发到目标ECI实例的指定端口上。

iv. 单击**确定**。

2.将ECI实例挂载到SLB

负载均衡SLB是一种对流量进行按需分发的服务，可以将流量分发到不同的后端服务来扩展应用系统的服务吞吐能力，并且可以消除系统中的单点故障，提升应用系统的可用性。本文介绍如何将ECI实例添加到SLB实例的后端服务器中，并配置监听，实现通过SLB将流量分发到ECI实例。

背景信息

负载均衡SLB（Server Load Balancer）由SLB实例、后端服务器和监听三部分组成，配置ECI实例挂载到SLB的操作流程如下：

1. 创建ECI实例

   搭建负载均衡服务前，您需要根据业务需求规划地域和网络，然后在此基础上创建ECI实例，完成相关应用部署。

2. 创建SLB实例

   使用负载均衡服务时，您需要创建一个SLB实例，每个SLB实例代表一个负载均衡服务实体，用于接收流量并将其分发给后端服务器。

   SLB分为应用型负载均衡ALB和传统型负载均衡CLB，您可以根据业务需求进行选择。两者的功能差异，请参见负载均衡SLB产品家族介绍。

3. 将ECI实例添加到SLB实例的后端服务器中

   后端服务器是一组接收前端请求的服务器。将ECI实例添加到后端服务器后，可以接收SLB实例转发的客户端请求。对于ALB实例，您需要先创建一个服务器组，然后再添加ECI实例；对于CLB实例，您可以直接将ECI实例添加到默认服务器组。

4. 配置监听

   监听用于检查客户端请求，并将请求转发给后端服务器。您需要为SLB实例配置监听，包括协议、端口和调度算法等。

下文以CLB为例介绍具体的操作步骤，ALB的操作类似。更多信息，请参见ALB快速入门。

准备工作

1. 创建多个ECI实例。

   此处以创建两个运行Nginx服务的ECI实例为例，创建时请开启日志收集。具体操作，请参见使用Nginx镜像创建实例。

2. 创建CLB实例。

   创建一个具备公网能力的CLB实例。具体操作，请参见创建CLB实例。

操作步骤

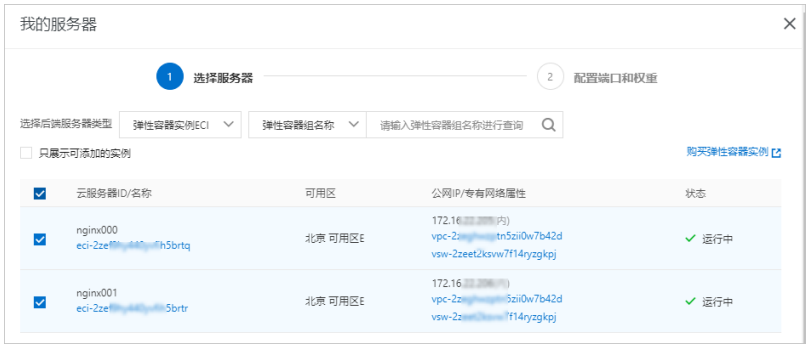
将ECI实例添加到CLB实例的后端服务器中并配置监听，可以实现将监听请求转发到ECI实例。

> **说明**
>
> 不支持挂载状态为最终状态（如：Succeeded、Failed）的ECI实例。

控制台方式

您可以在CLB控制台直接挂载ECI实例并配置监听。操作步骤如下：

1. 登录传统型负载均衡CLB控制台。
2. 在**实例管理**页面，找到目标CLB实例，在对应操作列中单击**添加后端服务器**。
3. 在**我的服务器**面板，完成服务器添加。
   i. 选择后端服务器类型为**弹性容器实例ECI**，然后选中多个ECI实例，单击**下一步**。



   ii. 根据需要配置权重，单击**添加**。

   权重默认为100，权重越大，转发的请求越多。

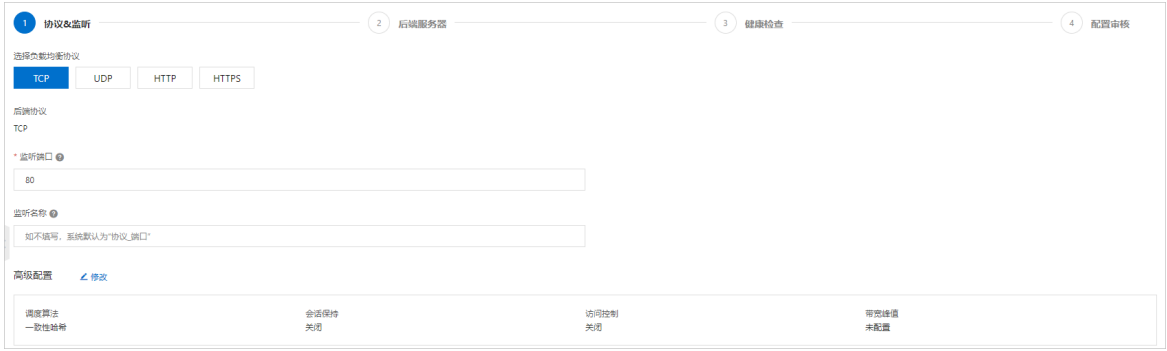
   iii. 单击**确定**，然后在弹出的对话框中单击**确认**。

   在实例的**默认服务器组**页签下，您可以看到新添加的ECI实例。

4. 在**实例管理**页面，找到目标CLB实例，在对应操作列中单击**监听配置向导**。
5. 在**协议&监听**配置向导页，完成监听配置，然后单击**下一步**。

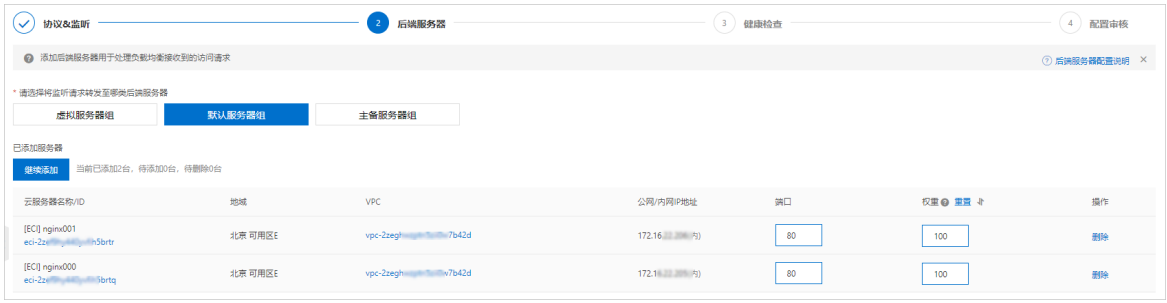
   配置时，请根据需要选择协议并设置监听端口，此处配置示例如下：

   - 协议选择TCP
   - 监听端口设置为80
   - 其它配置保持默认配置



6. 在**后端服务器配置**向导页，完成服务器配置，然后单击**下一步**。

配置时，选择**默认服务器组**，您可以看到步骤3添加的ECI实例已经显示在列表中，请根据需要设置各服务器的监听端口，此处示例设置端口为80。



7. 在**健康检查**向导页，保持默认配置，单击**下一步**。
8. 在**配置审核**向导页，确认配置，单击**提交**。

openAPI方式

您可以通过CLB的openAPI挂载ECI实例对应的弹性网卡ENI，并配置监听。操作步骤如下：

1. 调用ECI的DescribeContainerGroups接口查询ECI实例相关信息。

   在返回参数中获取并记录ECI实例相关信息：

   - 弹性网卡ID，对应参数为EniInstanceId。
   - ECI实例内网IP，对应参数为IntranetIp。

2. 调用CLB的AddBackendServers接口添加后端服务器。

   主要参数说明如下表所示。更多信息，请参见AddBackendServers。

名称	类型	示例值	描述
LoadBalancerId	String	lb-2ze7o5h52g02kkzz******	CLB实例ID。
BackendServers	String	[{ "ServerId": "eni-6wejdtelaz2bv526****", "Weight": "100", "Type": "eni", "ServerIp": "172.16.12.**", "Port":"80","Description":"test" },{ "ServerId": "eni-6wejdtelaz2bv321****", "Weight": "100", "Type": "eni", "ServerIp": "172.16.12.**", "Port":"80","Description":"test" }]	要添加的后端服务器列表。包含以下参数： - ServerId：后端服务器实例ID。此处填入ECI实例的弹性网卡ID。 - Weight：后端服务器权重。取值为0~100，默认值为100。如果值为0，则不会将请求转发给该后端服务器。 - Description：后端服务器描述，长度为1~80个字符。 - Type：后端服务器类型。此处配置为eni。 - ServerIp：实例IP地址。此处填入ECI实例内网IP。

3. 调用CLB的监听相关API接口创建监听。

- 创建TCP监听：CreateLoadBalancerTCPListener
- 创建UDP监听：CreateLoadBalancerUDPListener
- 创建HTTP监听：CreateLoadBalancerHTTPListener
- 创建HTTPS监听：CreateLoadBalancerHTTPSListener

此处以创建TCP监听为例，主要参数说明如下表所示。更多信息，请参见CreateLoadBalancerTCPListener。

名称	类型	示例值	描述
Bandwidth	Integer	-1	监听的带宽峰值。取值范围： - -1：对于按流量计费的公网CLB实例，可以将带宽峰值设置为-1，即不限制带宽峰值。 - 1~5120：对于按带宽计费的公网CLB实例，可以设置每个监听的带宽峰值，但所有监听的带宽峰值之和不能超过实例的带宽峰值。单位为Mbps。
BackendServers	Integer	80	CLB实例后端使用的端口。 取值范围：1~65535。
LoadBalancerId	String	lb-2ze7o5h52g02kkzz******	CLB实例ID。
ListenerPort	Integer	80	CLB实例前端使用的端口。 取值范围：1~65535。

4. 调用CLB的StartLoadBalancerListener接口启动监听。

结果验证

1. 在本地重复以下命令，多次curl CLB实例的公网IP。

```
curl 39.106.**.** 80
```

2. 查看ECI实例的日志，可以看到请求已通过CLB实例分发到不同的ECI实例上。

3.Serverless集群基于云解析PrivateZone的服务发现

阿里云Serverless Kubernetes已经支持服务发现功能，目前支持Intranet service、Headless service、ClusterIP service。

前提条件

- 需要先开通云解析PrivateZone，在云解析DNS控制台中开通。
- 创建Serverless Kubernetes集群。
- 您已成功连接到Kubernetes集群，参见通过kubectl连接Kubernetes集群。

背景信息

云解析PrivateZone，是基于阿里云专有网络VPC（Virtual Private Cloud）环境的私有域名解析和管理服务。您能够在自定义的一个或多个专有网络中将私有域名映射到IP资源地址，同时在其他网络环境无法访问您的私有域名。

> **说明** PrivateZone的收费规则参见收费标准。

操作步骤

1. 部署Deployment和创建Service。

   样例模板如下所示，在YAML文件中复制如下YAML代码，然后执行 `kubectl create -f nginx-service.yaml` 命令进行创建。

```
apiVersion: v1
kind: Service
metadata:
  name: nginx-headless-service
spec:
  ports:
  - port: 80
    protocol: TCP
  selector:
    app: nginx
  clusterIP: None
---
apiVersion: v1
kind: Service
metadata:
  name: nginx-clusterip-service
spec:
  ports:
  - port: 80
    protocol: TCP
  selector:
    app: nginx
  type: ClusterIP
---
```

```
apiVersion: v1
kind: Service
metadata:
  name: nginx-intranet-service
  annotations:
    service.beta.kubernetes.io/alicloud-loadbalancer-address-type: intranet
spec:
  ports:
  - port: 80
    protocol: TCP
  selector:
    app: nginx
  type: LoadBalancer
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image:  nginx:alpine
        ports:
        - containerPort: 80
```

2. 执行以下命令，查看应用的运行状况。

```
kubectl get svc,pod,deployment
```

3. 登录云解析DNS控制台。
4. 在控制台左侧导航栏中，单击**PrivateZone**，选择**权威Zone**页签。
5. 选中目标Zone，单击目标Zone右侧**操作**列下的**解析设置**。

> **说明** Zone里面的Record格式为 `$svc.$ns` ，对应相应的IP解析。解析规则如下：
>
> - LoadBalancer service：PrivateZone中只对应一条解析Record，为SLB IP。
> - ClusterIP service：PrivateZone中只对应一条解析Record，为Cluster IP。
> - Headless service：PrivateZone中对应多条解析Record，分别为后端Pod的IP。

您可在该VPC网络环境中通过私有域名访问Service。

- 长域名访问： `$svc.$ns.svc.cluster.local.$clusterId` ，通过这种方式也可以访问其他集群中同

步到PrivateZone的Service。

- 短域名访问：您可以通过 `$svc` 访问本Namespace下的Service，通过 `$svc.$ns` 访问其他Namespace中的Service。

更多信息，请参见serverless-k8s-examples。

4.部署Ingress应用

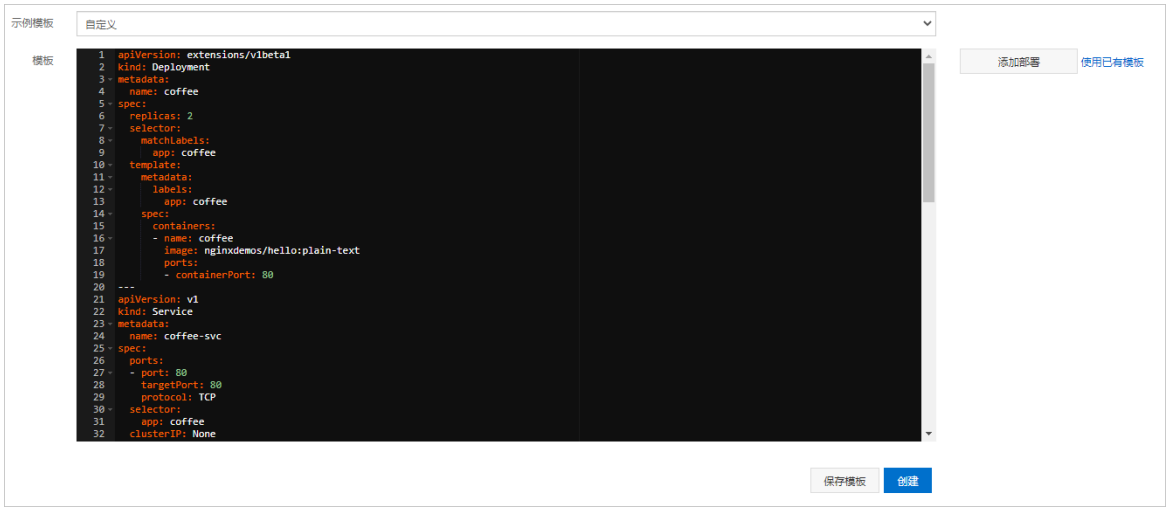
本文主要介绍在虚拟节点上部署Ingress应用，使得集群无需创建新节点即可为该应用扩充无限容量，满足业务高峰低谷的弹性需求。

前提条件

- 您已经部署了一个虚拟节点。具体操作，请参见通过部署ACK虚拟节点组件创建ECI Pod。
- 您已经给命名空间**vk**打上*virtual-node-affinity-injection: enabled*标签。具体操作，请参见通过配置namespace标签的方式创建Pod。

操作步骤

1. 登录容器服务管理控制台。
2. 在控制台左侧导航栏中，单击**集群**。
3. 在**集群列表**页面中，单击目标集群名称或者目标集群右侧**操作**列下的**详情**。
4. 在集群管理页左侧导航栏中，选择**工作负载 > 无状态**。
5. 单击右上角的**使用YAML创建资源**。
6. 选择样例模板或自定义，然后单击**创建**。



您可以使用如下YAML示例模板创建Ingress。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: coffee
spec:
  replicas: 2
  selector:
    matchLabels:
      app: coffee
  template:
    metadata:
      labels:
        app: coffee
    spec:
      containers:
```

```
      containers:
      - name: coffee
        image: nginxdemos/hello:plain-text
        ports:
        - containerPort: 80
---
apiVersion: v1
kind: Service
metadata:
  name: coffee-svc
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  selector:
    app: coffee
  clusterIP: None
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: tea
spec:
  replicas: 3
  selector:
    matchLabels:
      app: tea
  template:
    metadata:
      labels:
        app: tea
    spec:
      containers:
      - name: tea
        image: nginxdemos/hello:plain-text
        ports:
        - containerPort: 80
---
apiVersion: v1
kind: Service
metadata:
  name: tea-svc
  labels:
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  selector:
    app: tea
  clusterIP: None
---
apiVersion: networking.k8s.io/v1
kind: Ingress
```

```
metadata:
  name: cafe-ingress
spec:
  rules:
  - host: cafe.example.com
    http:
      paths:
      - path: /tea
        backend:
          serviceName: tea-svc
          servicePort: 80
      - path: /coffee
        backend:
          serviceName: coffee-svc
          servicePort: 80
```

预期结果

- 在集群管理页左侧导航栏中，选择**工作负载 > 无状态**，可以看到刚刚创建的coffee和tea。
- 在集群管理页左侧导航栏中，选择**工作负载 > 容器组**，可以看到Pod都运行在Virtual-Kubelet节点上。
- 在集群管理页左侧导航栏中，选择**网络 > 路由**，可以看到刚刚创建的路由。
- 您可以执行如下命令，确保可以访问Ingress应用。

```
kubectl  get ing
```

预期输出：

```
NAME           HOSTS              ADDRESS          PORTS   AGE
cafe-ingress   cafe.example.com   114.55.252.185   80      6m18s
```

执行以下命令，验证访问Ingress应用的 `"Host:cafe.example.com" <EXTERNAL_IP>/tea` 地址。

```
curl -H "Host:cafe.example.com" <EXTERNAL_IP>/tea
```

预期输出：

```
Server address: 192.168.xx.xx:80
Server name: tea-658d56f6cc-cxxxx
Date: 25/Sep/2020:12:36:50 +0000
URI: /tea
Request ID: b01d5bab9ae07abb8bc385377193xxxx
```

执行以下命令，验证访问Ingress应用的 `"Host:cafe.example.com" <EXTERNAL_IP>/coffee` 地址。

```
curl -H "Host:cafe.example.com" <EXTERNAL_IP>/coffee
```

预期输出：

```
Server address: 192.168.xx.xx:80
Server name: coffee-8c8ff9b4f-hxxxx
Date: 25/Sep/2020:12:36:47 +0000
URI: /coffee
Request ID: 722fe41a65a7fb552613c56e0a9axxxx
```

5.配置IPv6地址

ECI实例同时支持IPv4和IPv6地址，相比IPv4，IPv6大大扩展了地址的可用空间。本文介绍如何为ECI实例配置IPv6地址。

背景信息

IPv4的应用范围虽广，但网络地址资源有限，制约了互联网的发展。IPv6不仅可以解决网络地址资源有限的问题，还可以解决多种接入设备连入互联网障碍的问题。更多信息，请参见Pv6网关介绍。

ECI实例配置IPv6地址的相关限制如下：

- 每台ECI实例最多只能绑定一个IPv6地址。
- 通过指定vCPU和内存方式创建的ECI实例均支持配置IPv6地址，通过指定ECS规格创建的ECI实例仅部分ECS规格支持配置IPv6地址。支持的规格如下：
  - 通用型：g6e、g6、g5、sn2ne
  - 计算型：c6e、c6a、c6、c5、sn1ne
  - 内存型：r6e、r6、r5、se1ne
  - 高主频：hfc6、hfg6
  - GPU计算型：gn6i、gn6v、gn5i
  - 大数据网络增强型：d1ne
  - 本地SSD型：i2
  - 突发性能型：t6、t5
  - 共享型：s6

  更多信息，请参见ECS实例规格族。

准备工作

使用IPv6前，请完成以下准备工作：

1. 为ECI实例所属的VPC和交换机开通IPv6网段。具体操作，请参见VPC开启IPv6和交换机开启IPv6。
2. （可选）创建IPv6网关。具体操作，请参见创建和管理IPv6网关。

   IPv6网关提供不同的规格（免费版、企业版和企业增强版），不同规格网关提供的能力不同。VPC开通IPv6网段后，系统会为VPC自动创建一个免费版的IPv6网关。您可以根据需要创建不同规格的IPv6网关。
3. 如果想要通过IPv6地址进行公网通信，需要为IPv6网关开通IPv6公网带宽。具体操作，请参见开通和管理IPv6公网带宽。

配置说明

Kubernetes场景下，您可以在Pod metadata中添加Annotation来为Pod绑定一个IPv6地址，开通并设置IPv6地址的公网带宽。相关配置项如下：

配置项	说明
k8s.aliyun.com/eci-enable-ipv6	配置为true表示为Pod绑定一个IPv6地址。
k8s.aliyun.com/eci-ipv6-bandwidth-enable	配置为true表示开通ECI的IPv6公网通信能力。

k8s.aliyun.com/eci-ipv6-bandwidth	配置IPv6地址的公网带宽峰值。取值如下：
	• 当IPv6网关的公网带宽计费方式为按固定带宽计费时，IPv6地址的公网带宽范围为1~2000 Mbps。
	• 当IPv6网关的公网带宽计费方式为按使用流量计费时，IPv6地址的公网带宽范围受网关规格约束。
	  ○ 网关为免费版，IPv6地址的公网带宽范围为1~200 Mbps。
	  ○ 网关为企业版，IPv6地址的公网带宽范围为1~500 Mbps。
	  ○ 网关为企业增强版，IPv6地址的公网带宽范围为1~1000 Mbps。

说明

如果配置了 `k8s.aliyun.com/eci-enable-ipv6: "true"` 和 `k8s.aliyun.com/eci-ipv6-bandwidth-enable: "true"` ，没有配置k8s.aliyun.com/eci-ipv6-bandwidth，则Pod所绑定的IPv6地址的公网带宽默认为网关支持的公网带宽最大值，例如网关为免费版，公网带宽计费方式为按使用流量计费，则Pod所绑定的IPv6地址的公网带宽默认为200 Mbps。

配置示例如下：

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx
  labels:
    alibabacloud.com/eci: "true"
spec:
  replicas: 2
  selector:
    matchLabels:
      alibabacloud.com/eci: "true"
  template:
    metadata:
      labels:
        alibabacloud.com/eci: "true"
      annotations:
        k8s.aliyun.com/eci-enable-ipv6: "true"     #为Pod绑定一个IPv6地址
        k8s.aliyun.com/eci-ipv6-bandwidth-enable: "true"      #开通ECI的IPv6公网通信能力
        k8s.aliyun.com/eci-ipv6-bandwidth: 100M     #设置IPv6地址的公网带宽峰值
    spec:
      containers:
      - name: nginx
        image: nginx:1.7.9
        ports:
        - containerPort: 80
```

6.修改Pod镜像保持IP不变

对于部署在虚拟节点上的Pod应用，在应用迭代过程中，因为解决bug或者增加功能特性而制作新的镜像后，您可能需要修改镜像，同时为了不影响业务，需要保持Pod的IP不变。本文介绍如何通过kubectl命令修改Pod的容器镜像，并保持Pod的IP不变。

前提条件

已安装kubectl，且kubectl可以与您的kubernetes集群进行交互。

操作步骤

下文以部署Nginx的Pod为例，介绍如何通过kubectl命令，将容器镜像从 `nginx:1.7.9` 修改为 `nginx:1.9.6` ，并保持Pod的IP不变。

1. 创建一个Pod。

   ```
   kubectl create -f nginx.yaml
   ```

   nginx.yaml的内容示例如下，使用的容器镜像为 `nginx:1.7.9` 。

   ```
   apiVersion: v1
   kind: Pod
   metadata:
     name: nginx
     namespace: default
   spec:
     nodeName: virtual-kubelet
     containers:
     - image: nginx:1.7.9
       imagePullPolicy: Always
       name: nginx
   ```

2. 查询Pod信息。

   i. 查询Pod的IP。

   ```
   kubectl get pod/nginx -n default -o wide
   ```

   返回示例如下，可以看到Pod的IP为172.16.22.193。

   ```
   NAME    READY   STATUS    RESTARTS   AGE    IP              NODE
   NOMINATED NODE   READINESS GATES
   nginx   1/1     Running   0          5m5s   172.16.22.193   virtual-kubelet-cn-beij
   ing-e   <none>           <none>
   ```

ii. 查询Pod的镜像tag。

```
kubectl get pod/nginx -n default -o=custom-columns='IMAGE:spec.containers[*].image'
```

返回示例如下，可以查看Pod的容器镜像为 `nginx:1.7.9` 。

```
IMAGE
nginx:1.7.9
```

3. 选择以下一种方式修改镜像。
   - kubectl patch

     执行kubectl命令直接修改容器镜像tag。

     ```
     kubectl patch pod nginx -p '{"spec":{"containers":[{"name": "nginx","image": "nginx:1
     .9.6"}]}}'
     ```

   - kubectl edit

     执行kubectl edit命令编辑Pod，直接修改容器镜像tag。

     ```
     kubectl edit pod/nginx -o yaml
     ```

   - kubectl apply

     打开Pod对应的nginx.yaml配置文件，修改容器镜像tag，然后执行kubectl apply命令重新部署Pod。

     ```
     kubectl apply -f nginx.yaml
     ```

4. 查看修改后的Pod信息。

   i. 查询Pod的IP。

   ```
   kubectl get pod/nginx -n default -o wide
   ```

   返回示例如下，可以看到Pod的IP与修改前一致，为172.16.22.193。

   ```
   NAME    READY   STATUS    RESTARTS   AGE   IP              NODE
   NOMINATED NODE   READINESS GATES
   nginx   1/1     Running   1          19m   172.16.22.193   virtual-kubelet-cn-beiji
   ng-e   <none>           <none>
   ```

   ii. 查询Pod的镜像tag。

   ```
   kubectl get pod/nginx -n default -o=custom-columns='IMAGE:spec.containers[*].image'
   ```

   返回示例如下，可以查看Pod的容器镜像已经修改为 `nginx:1.9.6` 。

   ```
   IMAGE
   nginx:1.9.6
   ```

7.配置安全组

安全组是一种虚拟防火墙，具备状态检测和数据包过滤能力，用于在云端划分安全域。通过添加安全组规则，您可以控制安全组内ECI实例的入流量和出流量。

安全组概述

安全组定义

安全组是一个逻辑上的分组，由同一地域内具有相同安全保护需求并相互信任的实例组成。通过添加安全组规则，安全组可以允许或拒绝安全组内ECI实例对公网或者私网的访问，以及管理是否放行来自公网或私网的访问请求。

> **说明**
>
> - 一个安全组可以管理同一个地域内的多台ECI实例。
> - 一台ECI实例必须且仅支持属于一个安全组。

安全组类型

安全组分为普通安全组和企业安全组，创建时默认添加的安全组规则如下：

- 入方向：放行80、443、22、3389及ICMP协议，可修改。
- 出方向：允许所有访问请求。

两种安全组主要的功能差异如下表所示。

功能	普通安全组	企业安全组
未添加任何规则时的访问策略	• 入方向：拒绝所有访问请求 • 出方向：允许所有访问请求	• 入方向：拒绝所有访问请求 • 出方向：拒绝所有访问请求
能容纳的私网IP地址数量	2000	65536
同一个安全组内实例之间的网络连通策略	默认内网互通	默认内网隔离，需要您手动添加安全组规则
授权给其它安全组	支持组组授权	不支持组组授权

> **注意**
>
> 如果您对整体规模和运维效率有较高需求，建议您使用企业安全组。相比普通安全组，企业安全组大幅提升了组内支持容纳的实例数量，简化了规则配置方式。

安全组规则

安全组通过配置规则来控制出入流量。一条安全组规则由规则方向、授权策略、协议类型、端口范围、授权对象等属性确定。关于安全组规则，请注意以下事项：

- 每个安全组的入方向规则与出方向规则的总数不能超过200条。
- 添加规则时遵守最小授权原则。例如：
  - 选择开放具体的端口，如80/80，避免开放端口范围，如1/80。
  - 谨慎授权全网段访问源，即0.0.0.0/0。

更多信息，请参见安全组概述。

指定安全组

创建ECI实例时，必须要指定安全组，将ECI实例加入到安全组中。

> **注意**
>
> ECI实例不支持修改安全组。如果想要变更安全组，需要重新创建ECI实例。

Kubernetes方式

在Kubernetes场景中通过Virtual Kubelet（简称VK）使用ECI时，集群中所有ECI实例将默认加入到VK设置的安全组中。如果有特殊需求，您也可以为某个ECI实例指定其它安全组。

- **集群**

  您可以通过kubectl edit命令修改eci-profile配置文件，在data中修改ECI实例默认使用的安全组ID。

  > **说明**
  >
  > VK版本为v2.0.0.90-15deb126e-aliyun及以上时，支持修改eci-profile实现配置热更新。如果您的VK版本低于该版本，建议您升级VK。

  ```
  kubectl edit configmap eci-profile -n kube-system
  ```

  修改data中的securityGroupId字段，示例如下：

  ```
  data:
    enableClusterIp: "true"
    enableHybridMode: "false"
    enablePrivateZone: "false"
    resourceGroupId: ""
    securityGroupId: sg-2ze0b9o8pjjzts4h**** #指定安全组ID
    selectors: ""
    vSwitchIds: vsw-2zeet2ksvw7f14ryz****,vsw-2ze94pjtfuj9vaymf****
    vpcId: vpc-2zeghwzptn5zii0w7****
  ```

- **ECI实例**

  对于单个ECI实例，您可以在Pod metadata中添加Annotation来指定安全组。配置示例如下：

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: demo
  labels:
    app: nginx
spec:
  replicas: 1
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
        annotations:

            k8s.aliyun.com/eci-security-group: "sg-bp1dktddjsg5nktv****"      #设置安全组

        labels:
            app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:latest
```

OpenAPI方式

调用CreateContainerGroup接口创建ECI实例时，您可以通过SecurityGroupId参数来指定安全组。SecurityGroupId的参数说明如下表所示。更多信息，请参见CreateContainerGroup。

名称	类型	示例值	描述
SecurityGroupId	String	sg-uf66jeqopgqa9hdn****	指定安全组ID。

控制台方式

通过弹性容器实例售卖页创建ECI实例时，您可以指定一个安全组。

添加安全组规则

对于安全组内的ECI实例，您可以添加安全组规则来控制其出入流量。例如：

- 当您的ECI实例需要与所在安全组之外的网络进行通信时，您可以添加允许访问的安全组规则，实现网络互通。
- 当您在运行ECI实例的过程中，发现部分请求来源有恶意攻击行为时，您可以添加拒绝访问的安全组规则，实现网络隔离。

关于如何添加安全组规则，请参见添加安全组规则。

8.ECI实例进行带宽限速

ECI支持配置流入和流出的网络带宽值，本文介绍如何对ECI实例的流入和流出带宽进行限速。

Kubernetes方式

使用Kubernetes方式来创建ECI实例时，您可以在Pod中添加Annotation来指定入方向和出方向带宽值进行限速。相关配置项如下：

- kubernetes.io/ingress-bandwidth：入方向带宽。
- kubernetes.io/egress-bandwidth：出方向带宽。

支持的单位包括：GB、G、MB、M、KB、K、B。如果未填写单位，则默认对应的单位为B，即字节。

```
apiVersion: v1
kind: Pod
metadata:
  name: eci-qos
  annotations:
    kubernetes.io/ingress-bandwidth: 40M    #入方向带宽
    kubernetes.io/egress-bandwidth: 10M    #出方向带宽
spec:
  containers:
  - name: nginx
    image: nginx:latest
    command: ["bash","-c","sleep 100000"]
```

OpenAPI方式

调用CreateContainerGroup接口创建ECI实例时，您可以通过IngressBandwidth和EgressBandwidth参数来指定入方向和出方向的带宽值进行限速，相关参数说明如下表所示。更多信息，请参见CreateContainerGroup。

名称	类型	是否必填	示例值	描述
IngressBandwidth	Long	否	102400	入方向带宽，单位：字节。
EgressBandwidth	Long	否	102400	出方向带宽，单位：字节。