

安全容器服务

部署指南

产品版本: v7.0.2

发布日期: 2026-10-09

目录

1 部署指南	1
1.1 Kube-OVN部署指南	1

1 部署指南

1.1 Kube-OVN部署指南

前言

安全容器云产品使用kube-ovn作为cni，底层调用的ovn，和proton底层的实现是一致的，并且一部分功能复用了proton。所以使用kube-ovn的pod可以类比为虚拟机，通过网络隔离加强了安全。

使用kube-ovn的pod以下场景是预期的：1.pod内只通网络节点和安全容器节点的ovn0地址（br-roller，br-mgmt等地址是不通的）。2.网络节点和安全容器节点可以访问所有的kube-ovn地址，非网络节点和安全容器节点角色，一般是不通pod的，要看云平台的网络规划。3.不同vpc之间的pod默认是互相隔离的，包括service。4.所有的kube-ovn网络的pod内都可以访问coredns服务和kubernetes服务（kubernetes.default.svc.cluster.local）。

另外，使用上有些限制需要注意：1.所有subnet的网段不能重叠，即使跨vpc。2.创建ns(namespace)时，如果没有设置全局默认subnet，namespace不会自动绑定subnet，如果没有手动给ns设置subnet，且此ns下的pod也不设置subnet，创建pod不会成功。3.创建np(networkpolicy)时，如果np所在ns没有设置subnet，np的规则如果涉及到跨子网则会有问题。4.已创建的subnet不能修改其vpc。5.lic中指定的cluster-router参数指定的neutron router如果已存在，external-network参数则不会起作用。

云产品安装

使用场景的不同，云产品的一些参数需要灵活配置，可以通过license传入，目前kube-ovn相关的license是下面的参数：值为"代表是有值的，只是值是空字符串，所以想用默认值，参数不需要写在license里。

```
cloud-product:
- eks-managed: {
  ttl: '-1',
  values: {
    cluster-router: 'test-router', //默认vpc名字，填写手动创建的neutron
    router name,如果不设置或者传的router不存在，会默认创建名字为ovn-cluster的router。邮储
    应设置为手动创建的neutron router name
    disable-init-subnet: True, //是否创建默认的全局subnet ovn-default，不设置
    的话默认为False会创建。邮储应设置为True
```

```

        external-network: '', //默认vpc外部网关绑定的公网名字, 如果传的为空字符串的话, 代表kube-ovn默认创建的默认vpc不绑定外部网关, 如果未设置此参数, 默认值为public-net。邮箱应设置为'', 即不绑定默认网关。需要注意的是如果cluster-router指定的router为提前手动创建好的, 此参数不起作用。
        node-switch-cidr: '100.64.0.0/16', //默认创建的join subnet的网段, 不设置默认为100.64.0.0/16。邮箱应根据规定填入此值
        default-cidr: '10.16.0.0/16', //默认subnet ovn-default的网段。如果设置了disable-init-subnet为true, 此值不生效。可以不设置, 默认值为10.16.0.0/16
        default-gateway: '10.16.0.1', //默认subnet ovn-default的网关地址, 与default-cidr类似, 默认值为10.16.0.1
        default-exclude-ips: '10.16.0.1,10.16.0.2', //默认subnet ovn-default的不可分配地址, 与default-cidr, 默认值为网关地址
        node-switch-gateway: '100.64.0.1', //join子网默认网关, 一般不用设置, 不设置默认为node-switch-cidr的第一个ip
        service-cluster-ip-range: '10.222.0.0/16', //k8s集群svc网段, 不设置默认值为10.222.0.0/16
        flannel-pod-ip-range: '10.232.0.0/14', //flannel 网段, 不设置默认值为10.232.0.0/14
        network-type: 'geneve', //网络模式, 不设置默认geneve
        enable_lb: True, //是否开启ovn lb, 不设置默认为True
        enable_np: True, //是否开启networkpolicy, 不设置默认为True
        keep_vm_ip: True, //是否开启kubevirt vmip保持, 不设置默认为False, 不保持, 一般建议设置为True
        shared_services: '', //所有的vpc的lb上负载的svc, 默认为空, 格式为namespace/svc-name, 用, 分割
        gateway_node_labels: 'node-role.kubernetes.io/master=true' //kube-ovn pod访问coredns和k8s服务经过的容器网关节点label, 不写此值, 默认值为node-role.kubernetes.io/master=true; 要么就必须设置此值, 不能写空字符串
    }
}
    
```

安装完成后, 根据disable-init-subnet参数, 创建的默认资源会不同, 如果disable-init-subnet为False, 代表创建默认全局subnet ovn-default。

```

[root@node-3 ~]# kubectl get vpc
NAME          STANDBY   SUBNETS                                NAMESPACES
ovn-cluster   true      ["join","ovn-default"]
[root@node-3 ~]# kubectl get subnet
NAME          PROVIDER   VPC          PROTOCOL   CIDR
PRIVATE      NAT       DEFAULT      GATEWAYTYPE V4USED    V4AVAILABLE V6USED
V6AVAILABLE  EXCLUDEIPS
    
```

```

join      ovn      ovn-cluster  IPv4      100.64.0.0/16  false
false    false    distributed  11        65522         0          0
["100.64.0.1"]
ovn-default ovn      ovn-cluster  IPv4      10.16.0.0/16   false
true     true     distributed  4         65527         0          0
["10.16.0.1"]
  
```

disable-init-subnet为True，不创建默认全局subnet ovn-default。

```

[root@node-3 ~]# kubectl get vpc
NAME          STANDBY  SUBNETS          NAMESPACES
ovn-cluster   true     ["join"]
[root@node-3 ~]# kubectl get subnet
NAME          PROVIDER  VPC          PROTOCOL  CIDR
PRIVATE  NAT      DEFAULT  GATEWAYTYPE  V4USED  V4AVAILABLE  V6USED
V6AVAILABLE  EXCLUDEIPS
join      ovn      ovn-cluster  IPv4      100.64.0.0/16  false
false    false    distributed  11        65522         0          0
["100.64.0.1"]
  
```

另外还会创建ip资源，所有的网络和安全容器节点都会占用一个join网络的地址。

```

[root@node-3 ~]# kubectl get ip
NAME          V4IP          V6IP  MAC
NODE          SUBNET
node-node-1   100.64.0.3    00:00:00:74:BF:BB
node-1        join
node-node-2   100.64.0.4    00:00:00:66:A6:AE
node-2        join
node-node-25  100.64.0.2    00:00:00:E3:DF:5A
node-25       join
node-node-3   100.64.0.5    00:00:00:10:AD:31
node-3        join
node-node-39  100.64.0.9    00:00:00:4C:22:A5
node-39       join
  
```

创建VPC和Subnet

如果不使用默认创建的vpc，可以创建自定义vpc和subnet，两种方式: 1.通过网络页面创建容器路由器，选择容器路由器，如果不设置网关，vpc下资源不能出外网，选择连接子网，代表是否给vpc绑定subnet。这里也可以选择不连接子网，等容器路由器创建好后，在网络页面创建容器网络并连接到此路由器。

路由器类型 普通路由器 容器路由器

* 名称

* 可用区 default-az x

* VPC 名称 ?

设置路由器网关

是否设置路由器网关 ☒ 是

① 您设置的网关将占用公网 IP 资源

* 外部网络 public_net v

* 分配外部 IP ☒ 自动分配 ☐ 手动选择

QoS ☒ 禁用 ☐ 激活

带宽 1 Mbps ~ 10000 Mbps 1 Mbps

开启 SNAT ☒

连接子网

是否连接子网 ☒ 是

① 连接容器子网会先创建一个容器子网并连接。

容器子网列表

*名称	*CIDR ?
test-subnet	100.10.0.1/16

[+ 添加容器子网](#)

new-test-ovn-router 路由器 / 详情				刷新 更多操作	
基本信息				标签	
名称	new-test-ovn-router	VPC 名称	new-vpc	暂无数据	
UUID	86c090d5-a2e8-461f-9107-6d230ac5b276	带宽	无限制		
可用区	default-az	部门	Default		
外部网络	public_net	项目	admin		
外部IP	172.41.0.82	SNAT	开启		
网关防火墙	-	创建时间	2024-04-25 15:22:15		

路由器连接 静态路由 公网 IP						
🔄 连接子网 ➡️ 断开连接 ➡️ 连接容器子网 点击选择过滤条件 🔍 ⚙️						
☐ 网络名称	子网名称	网络地址	网关IP	子网IP	网络 ACL	操作
☐ new-ovn-subnet	容器子网 new-ovn-subnet	172.16.100.0/24	172.16.100.1	172.16.100.1	-	断开连接
共 1 条数据, 最近更新 2024-04-29 16:57:04						

并会在后台创建vpc和subnet资源。

```
[root@node-9 ~]# kubectl get vpc new-vpc
NAME          STANDBY   SUBNETS          NAMESPACES
new-vpc       true      ["new-ovn-subnet"]
[root@node-9 ~]# kubectl get subnet new-ovn-subnet
NAME          PROVIDER   VPC          PROTOCOL   CIDR          PRIVATE
NAT          DEFAULT   GATEWAYTYPE  V4USED     V4AVAILABLE   V6USED     V6AVAILABLE
EXCLUDEIPS
new-ovn-subnet  ovn        new-vpc      IPv4        172.16.100.0/24  false
false false    distributed   2           251           0           0
["172.16.100.1"]
```

2.yaml创建 先创建vpc:

- externalGatewayIp: 外部网关地址, 选填,该ip为vpc下pod 访问外网默认 snat ip, 允许pod访问外网有两种方式: vpc yaml中定义该字段 或者 网络页面设置路由网关开启snat。
- externalNetworkID: 外部网络ID,如果vpc需要访问外部网络并要使用EIP和SNAT功能, 此值为必填, 如果不需要上述功能, 此值不要设置。
- externalNetworkName: 外部网络名字, 选填。
- neutronRouter: proton router id, 必填。
- gatewayNode: 选填, kube-ovn pod访问节点的出入口节点, 默认为网络节点。
- namespaces: 选填, 指定哪些namespace可以使用此vpc, 不可与其他vpc下的namespace重叠。

```
apiVersion: kubeovn.io/v1
kind: Vpc
metadata:
  name: ovn-cluster
spec:
  externalGatewayIp: 172.110.0.207
```

```
externalNetworkID: c9a831a0-6298-44c6-a664-2f362e60e419
externalNetworkName: public_net
neutronRouter: c58a843a-b007-4fcf-949f-02836b71b7f3
gatewayNode: node-1,node-2,node-3
namespaces:
- test1
- test2
```

一般就设置neutronRouter和externalNetworkID即可。

```
apiVersion: kubeovn.io/v1
kind: Vpc
metadata:
  name: ovn-cluster
spec:
  externalNetworkID: c9a831a0-6298-44c6-a664-2f362e60e419
  neutronRouter: c58a843a-b007-4fcf-949f-02836b71b7f3 //proton router id, 必填
```

创建subnet:

- cidrBlock: subnet cidr, 必填。
- default: true/false, 默认为false, vpc下哪个subnet为默认subnet, 要避免一个vpc下多个subnet设置为true。如果一个vpc下多个subnet设置为true, 其中一个subnet会被认为是默认subnet, 不保证时间顺序, 选填。
- excludeIps: 不能被分配的地址, 默认为网关地址, 选填。
- gateway: 网关地址, 默认为子网的第一个地址, 选填。
- namespaces: 能使用此subnet的namespace, 必须是关联vpc的namespaces子集, 选填。
- private: 默认为false, 如果设置成true, 则该子网将和其他子网以及外部网络隔离, 只能进行子网内部的通信。如需开白名单, 可以通过 allowSubnets 进行设置。allowSubnets 内的网段和该子网可以双向互访, 选填。
- allowSubnets: private设置为true后, 允许访问的网段, 单独设置无意义, 选填。
- projectIDs: 配置该subnet只能被哪些projects使用, 如果不配置表示 该subnet为share subnet 所用用户可用, 目前页面上创建的容器网络不带有project id, 后期可能会加上此选项, 选填。
- vpc: 属于哪个vpc, 必填。

```
apiVersion: kubeovn.io/v1
kind: Subnet
metadata:
  name: custom-subnet
spec:
  cidrBlock: 192.168.233.0/24
  default: false
  excludeIps:
    - 192.168.233.1
  gateway: 192.168.233.1
  namespaces:
    - net2
    - test
  private: false
  allowSubnets:
    - 100.64.0.1/16
  projectIDs:
    - 3a4a2f23238d4851a64f79b4411bbee3
  vpc: custom-vpc
```

创建namespace

namespace会和subnet绑定，如果namespace没有绑定subnet，需要pod手动指定subnet。namespace绑定subnet有多种情况：1.假设subnet里namespaces指定了需要绑定subnet的ns，则此namespace会绑定此subnet，即使namespace手动指定了subnet也会被覆盖。2.如果subnet没指定此ns，则会再去vpc的namespaces里找，如果找到了此ns，则会绑定此vpc的默认subnet，如果此vpc没有默认subnet，则会使用全局默认subnet，如果没有全局默认subnet，则此ns不绑定subnet。3.如果没有vpc指定绑定此namespace，则会使用全局默认vpc（ovn-cluster）的默认subnet，如果此vpc没有默认subnet，则会使用全局默认subnet，如果没有全局默认subnet，则此ns不绑定subnet。4.假设上述情况都不满足，则可以手动指定ns需要绑定的subnet，给ns添加注解ovn.kubernetes.io/logical_switch：

```
apiVersion: v1
kind: Namespace
metadata:
  annotations:
    ovn.kubernetes.io/logical_switch: yyx-yyx
  labels:
    managed.es.io/resource: namespace
```

```
name: test123
name: test123
```

namespace绑定subnet的优先级如下:

```
subnet指定ns > vpc指定ns > 全局默认subnet > ns手动指定subnet
```

创建负载

1.负载不手动指定subnet的情况下, 会使用ns绑定的subnet。 2.负载手动指定subnet, 在spec.template.metadata.annotations加上subnet的注解。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: test
  namespace: demo
spec:
  replicas: 1
  selector:
    matchLabels:
      workload.es.io: deployment.demo-2
  type: RollingUpdate
  template:
    metadata:
      annotations:
        ovn.kubernetes.io/logical_switch: ovn-ljj
      labels:
        workload.es.io: deployment.demo-2
    spec:
      containers:
        - image: 'hub.easystack.io/arm64v8/escloud-linux-source-busybox:latest'
          imagePullPolicy: IfNotPresent
          name: container1
```

3.使用eip或snat 使用eip或snat, 使用的subnet关联的vpc必须开启了外部网关。使用eip, deployment, statefulset或daemonset的副本数必须为1。

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: test
  namespace: demo
spec:
  replicas: 1
  selector:
    matchLabels:
      workload.es.io: deployment.demo-2
    type: RollingUpdate
  template:
    metadata:
      annotations:
        ovn.kubernetes.io/logical_switch: ovn-ljj
        ovn.kubernetes.io/eip: 172.35.0.20
      labels:
        workload.es.io: deployment.demo-2
    spec:
      containers:
        - image: 'hub.easystack.io/arm64v8/escloud-linux-source-busybox:latest'
          imagePullPolicy: IfNotPresent
          name: container1
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: test
  namespace: demo
spec:
  replicas: 1
  selector:
    matchLabels:
      workload.es.io: deployment.demo-2
    type: RollingUpdate
  template:
    metadata:
      annotations:
        ovn.kubernetes.io/logical_switch: ovn-ljj
```

```
    ovn.kubernetes.io/snat: 172.35.0.18
  labels:
    workload.es.io: deployment.demo-2
  spec:
    containers:
      - image: 'hub.easystack.io/arm64v8/escloud-linux-source-busybox:latest'
        imagePullPolicy: IfNotPresent
        name: container1
```

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：

北京市海淀区西北旺东路10号院东区23号楼华胜天成科研大楼一层东侧120-123

南京分公司：

江苏省南京市雨花台区软件大道168号润和创智中心B栋一楼西101

上海office：

上海黄浦区西藏中路336号华旭大厦22楼2204

成都分公司：

成都市高新区天府五街168号德必天府五街WE602

邮箱：

contact@easystack.cn (业务咨询)

partners@easystack.cn(合作伙伴咨询)

marketing@easystack.cn (市场合作)

training@easystack.cn (培训咨询)

hr@easystack.cn (招聘咨询)