

安全容器服务 常见问题

产品版本: v6.2.1

发布日期: 2024-06-05

目录

1 常见问题	1
1.1 如何理解安全容器网络方案	1
1.2 容器状态为未知错误，如何排查解决	7
1.3 容器状态为失败，如何排查解决	8

1 常见问题

1.1 如何理解安全容器网络方案

问题描述

安全容器使用的CNI插件是什么？有什么重要特性？用户侧如何使用VPC、Subnet、FIP等各种网络资源？

解决方案

安全容器6.1.1版本CNI是基于易捷行云软SDN网络服务作为后端，以kube-ovn（v1.9.0版本）作为API接口，为不同算力(容器、云原生云主机、裸金属)提供统一网络方案；为实现这个设计目标，对kube-ovn 作为容器CNI 做了一些改动和限制；和社区版本的主要区别体现在：

- 1、当前版本跨节点通信 不支持 underlay 模式，只支持geneve 隧道模式
- 2、VPC 功能增强 1) 容器网络使用的VPC 依赖于软SDN的 router，所以默认VPC的更新配置，及 自定义VPC的创建 需要结合软SDN router页面操作完成，具体步骤见操作手册。
2) 容器网络的VPC 网关出外网配置由软SDN router 自动完成，对应社区kube-ovn文档中 VPC 网关配置相关的操作，这部分无需用户再做配置。同时VPC只支持集中式网关(对应 VPC spec中 gatewaytype 字段)。
3) 支持自定义VPC，且自定义VPC内容器网络也支持 nodeport、探针等功能(当前版本限制：不同vpc间 subnet cidr 不能有 overlap)，同时支持自定义VPC的网关节点的配置。
4) 容器VPC与其他算力的互联需要在 软SDN router页面完成配置。
- 3、新增Floating IP（简称fip）功能 1) fip 作为软SDN管理的统一资源，可以同时被 不同算力(vm、pod、裸金属)使用；fip 在pods中的具体使用方式请参照用户手册。
2) 产品中使用内部CRD fips.neutron.io 管理记录当前容器可用的fip 资源池，用户可以k8s API通过查看对应的 fip CR查看可用的 fip address 使用，fip的记录与回收会自动处理。
- 4、subnet功能增强 支持subnet 中定义projectIDs，表示该subnet只能被哪些projects使用；如果不配置表示该subnet为share subnet，所有用户可用。

如何启用kube-ovn 组件

通过安全容器服务页面创建的命名空间，默认所有负载都是使用kube-ovn作为CNI。

API方式，需要对命名空间打上标签 `managed.es.io/resource=namespace` ；例如：

```
apiVersion: v1
kind: Namespace
metadata:
  name: easystack
  managed.es.io/resource: namespace
```

如何自定义VPC网络

在创建工作负载时，其网络不仅支持使用系统默认生成的ovn-cluster和子网，还支持使用自定义的VPC网络或子网。用户可根据实际业务场景，酌情选择对应方案。

1. 配置外部网络。

1. （可选）创建外部网络。

本操作用于预创建外部网络，以便在自定义VPC网络时能够为其建立外部连接。如使用已有外部网络时，可跳过本步骤。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。

2. 单击 `创建网络` ，进入“创建网络”页面。

3. “网络类型”请选择“外部网络”，并配置其他参数后，单击 `创建网络` ，完成操作。其中，其他参数的具体参数说明，请参考“SDN网络服务”帮助中“网络”的相关内容。

2. 查看外部网络的ID。

在“网络”页面中，单击待操作网络名称，进入其详情页面。在该页面中，查看并记录该网络的ID（即UUID参数的值）。

2. 配置路由器。

1. （可选）创建路由器。

本操作用于预创建路由器，以便在自定义VPC网络时能够为其建立外部连接。如使用已有路由器时，可跳过本步骤。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，即可进入“路由器”页面。
2. 单击 `创建路由器` ，弹出“创建路由器”对话框。
3. 配置参数后，单击 `创建` ，完成操作。

2. （可选）设置路由器网关。

本操作用于预设置路由器网关，以便在自定义VPC网络时能够为其建立外部连接。如路由器已设置网关时，可跳过本步骤。

1. 在“路由器”页面中，勾选待操作路由器后，单击 `更多` - `设置网关` ，弹出“设置路由器网关”对话框。
2. “分配外部IP”选择“手动选择”，“子网”选择上述外部网络子网，并配置其他参数后，单击 `设置` ，完成操作。其中，其他参数的具体参数说明，请参考“SDN网络服务”帮助中“路由器”的相关内容。

3. 查看路由器ID和外部网络IP地址。

在“路由器”页面中，单击上述路由器名称，进入其详情页面。在该页面中，查看并记录该路由器的ID（即UUID参数的值）和外部网络IP地址（即外部IP参数的值）。

3. 导入VPC资源。

1. 在云平台顶部导航栏中，依次选择[产品与服务]-[容器服务]-[安全容器服务]，进入“安全容器服务”页面。
2. 在左侧导航栏选择[管理视图]-[自定义资源管理]，或在左侧导航栏选择[业务视图]，并选择目标命名空间后，选择[自定义资源管理]，进入“自定义资源管理”页面。
3. 单击页面右下角的“Yaml”图标，进入“导入Yaml”页面。
4. 依据实际业务情况，输入Yaml文件内容，或直接单击编辑区域右上角的“导入”图标，导入预先配置的Yaml文件。Yaml文件格式如下（其中，name为自定义输入的VPC名称，externalGatewayIp为外部网络的IP地址，externalNetworkID为外部网络的ID，neutronRouter为路由器的ID）：

```
apiVersion: kubeovn.io/v1
kind: Vpc
metadata:
  name: test-vpc2
```

```
spec:  
  externalGatewayIp: 172.110.0.160  
  externalNetworkID: c9a831a0-6298-44c6-a664-2f362e60e419  
  neutronRouter: c761887f-40bd-4df0-9b43-7c6bb009aab7
```

5. 待调试通过后，单击 **导入** ，完成操作。

6. spec关键字段说明：

externalNetworkID：外部网络ID(必填)

externalNetworkName：外部网络名字(选填)

外部网关IP(选填)；注：该ip为vpc下pod访问外网的默认 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

neutronRouter：路由ID(必填)

gatewayNode(选填, ovn pod访问节点的出入口节点，默认为网络节点)

自定义子网

> 警告：

>

> * 在同一VPC内，请确保各子网不发生冲突。

> * 在不同VPC之间，如需配置多个用户路由器之间的云内对等连接，请确保各路由器的子网不发生冲突。

1. 在云平台顶部导航栏中，依次选择[产品与服务]-[容器服务]-[安全容器服务]，进入“安全容器服务”页面。
2. 在左侧导航栏选择[管理视图]-[自定义资源管理]，或在左侧导航栏选择[业务视图]，并选择目标命名空间后，选择[自定义资源管理]，进入“自定义资源管理”页面。
3. 单击页面右下角的“Yaml”图标，进入“导入Yaml”页面。
4. 依据实际业务情况，输入子网内容，或直接单击编辑区域右上角的“导入”图标，导入预先配置的Yaml文件。Yaml文件格式如下（其中，name为自定义输入的子网名称，vpc为该子网所属VPC的名称，cidrBlock为该子网的网段，natOutgoing为是否允许访问外部网络）：

```
kind: Subnet
apiVersion: kubeovn.io/v1
metadata:
  name: net192
spec:
  vpc: test-vpc-2
  cidrBlock: 192.168.100.0/24
  natOutgoing: true
```

5. 待调试通过后，单击 **导入** ，完成操作。

6. spec 关键字段说明

vpc: 属于哪个vpc

cidrBlock: subnet cidr

natOutgoing: 是否可以访问外部网络

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

7. 如果通过页面部署工作负载时不选择Subnet子网，会使用vpc中默认子网进行部署；如果通过yaml定义，spec样例如下：

```
apiVersion: v1
kind: Pod
metadata:
  annotations:
    ovn.kubernetes.io/logical_switch: another-subnet
  namespace: default
  name: another-subnet-pod
```

Floating IP 使用

fip 在容器产品中使用包括两个场景：pods 指定使用 SNAT作为出口IP；允许kubevirt 云原生云主机 使用 EIP。

使用方式有两种：页面操作，用户可在网络高级配置中可以选择正确的fip资源；或者yaml定义。

两种使用场景yaml spec定义样例如下： 1) SNAT出口IP

```
apiVersion: v1
kind: Pod
metadata:
  annotations:
    ovn.kubernetes.io/snat: 172.35.0.18
  name: snat-busybox
```

2) EIP

```
apiVersion: kubevirt.io/v1
kind: VirtualMachine
metadata:
  name: kubevirt-eip
spec:
  template:
    metadata:
      annotations:
        ovn.kubernetes.io/eip: 172.35.0.20
```

1.2 容器状态为未知错误，如何排查解决

问题描述

在云平台中，查看到容器的状态为“未知错误”。具体使用现象可能表现为：

- 在连接容器终端正常使用过程中，断开连接后无法再次建立连接。
- 在云监控服务中，上报微服务管理停止告警。
- 维护此容器时，维护失败。

问题原因

容器发生未知错误。

解决方案

1. 在顶部导航栏选择[产品与服务]-[容器服务]-[安全容器服务]，进入“安全容器服务”页面。
2. 在左侧导航栏选择[业务视图]页签-选择目标命名空间后，选择“容器组”，进入“容器组”页面。
3. 单击目标容器所在容器组的名称链接，进入详情页面。
4. 在[终端]页签中，选择目标容器后，执行以下命令：

```
ctr -n k8s.io t ls | grep UNKNOWN |awk '{print $1}'|xargs -I % ctr -n k8s.io t rm %
```

5. 确认问题已解决。具体命令如下（无返回数据，即表示问题已解决）：

```
ctr -n k8s.io t ls | grep UNKNOWN
```

1.3 容器状态为失败，如何排查解决

问题描述

在云平台中，查看到容器的状态为“失败”。

问题原因

容器命令执行错误。

解决方案

1. 在顶部导航栏选择[产品与服务]-[容器服务]-[安全容器服务]，进入“安全容器服务”页面。
2. 在左侧导航栏选择[业务视图]页签-选择目标命名空间后，选择“容器组”，进入“容器组”页面。
3. 单击目标容器所在容器组的名称链接，进入详情页面。
4. 在[事件]或[终端]页签中，排查具体执行错误的命令并解决。

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1号楼1层107-2号

南京易捷思达软件科技有限公司：

江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

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)