端口镜像 使用教程

产品版本：ZStack 3.10.0

文档版本：V3.10.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴科技商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受云轴科技公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，云轴科技公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 介绍

端口镜像：将云主机网卡的网络流量复制一份到远端，对端口上的业务报文进行分析，方便对网络数据进行监控管理。在企业中使用端口镜像功能，可以很好地对企业内部的网络数据进行监控管理，在网络故障时可以快速定位故障。

注: 端口镜像使用流量网络作为专用网络，用于将网卡的网络流量镜像到远端，不能作为其他网络使用，不能用于创建云主机。

2 前提

在此教程中，假定已安装最新版本ZStack，并完成基本的初始化，包括区域、集群、物理机、镜像服务器、主存储等基本硬件资源的添加，以及计算规格的创建。具体方式请参考《用户手册》安装部署章节和Wizard引导设置章节。

本教程将详细介绍端口镜像的基本部署以及典型应用场景。

3 基本部署

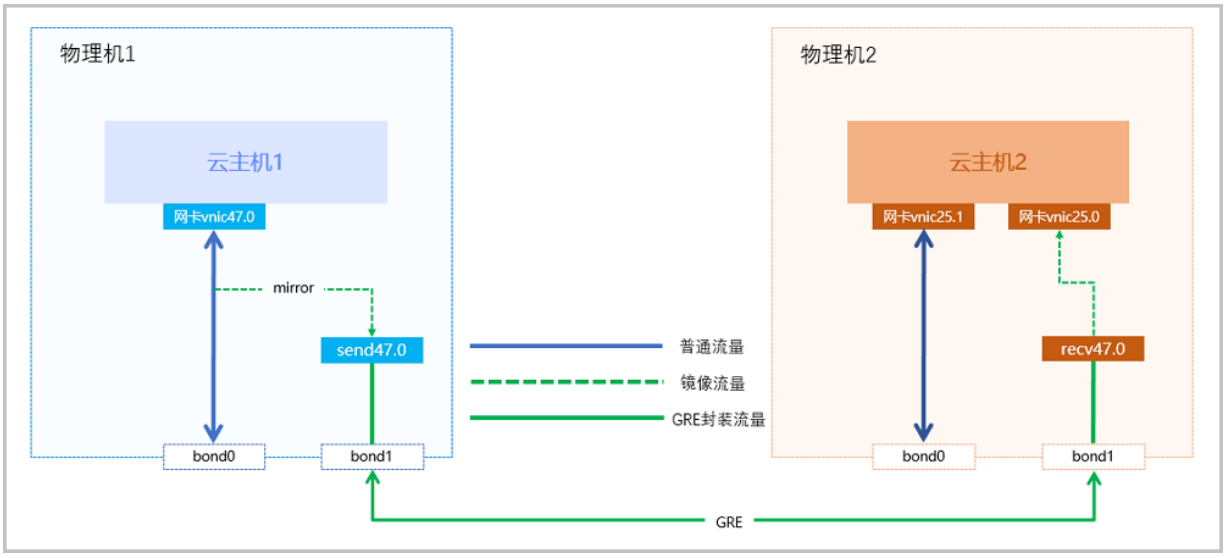
背景信息

端口镜像的基本部署流程如下：

1. 创建流量网络对应的二层网络，并加载此二层网络到相应集群。
2. 创建流量网络，输入相应的IP范围、子网掩码、网关、DNS等信息。
3. 创建端口镜像。
4. 添加会话，指定需要监测的云主机网卡为源端口，指定接收云主机网卡为目的端口。

端口镜像拓扑图如图 *1:* 端口镜像所示：

图 1: 端口镜像



以下介绍部署端口镜像的实践步骤。

操作步骤

1. 在ZStack私有云界面创建二层网络。

   在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考示例输入以下内容：

   - **名称**：设置L2-流量网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：选择网卡

- **集群**：选择集群，如Cluster1

如图 2: 创建*L2*-流量网络所示，点击**确定**，创建L2-公有网络。

图 2: 创建L2-流量网络

2. 在ZStack私有云界面创建流量网络。

   在ZStack私有云主菜单，点击**网络服务** > **流量网络**，进入**流量网络**界面，点击**创建流量网络**，在弹出的**创建流量网络**界面，参考示例输入以下内容：

   - **名称**：设置流量网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-流量网络
   - **添加网络段**：选择IP范围

- **起始IP**：*192.168.29.10*
- **结束IP**：*192.168.29.20*
- **子网掩码**：*255.255.255.0*
- **网关**：*192.168.29.1*

如图 *3:* 创建流量网络所示，点击**确定**，创建流量网络。

图 3: 创建流量网络

3. 在ZStack私有云界面创建端口镜像。

   在ZStack私有云主菜单，点击**网络服务** > **端口镜像**，进入**端口镜像**界面，点击**创建端口镜像**，在弹出的**创建端口镜像**界面，可参考以下示例输入相应内容：

- **名称**：设置端口镜像名称
- **简介**：可选项，可留空不填
- **流量网络**：选择端口镜像使用的流量网络

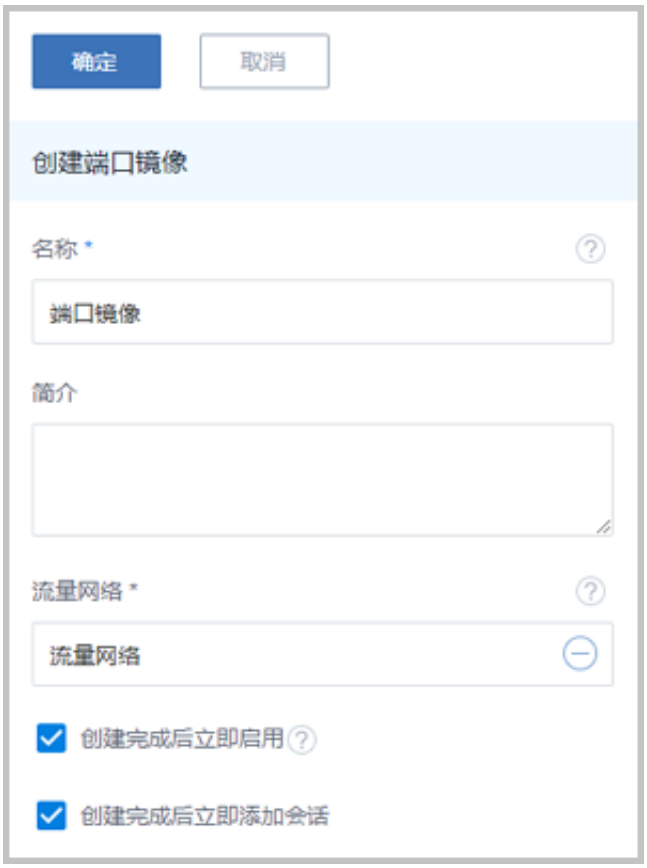
注:

- 流量网络是端口镜像的专用网络，用于将网卡的网络流量镜像到远端；
- 流量网络仅用于端口镜像，不能作为其他网络使用；
- 一个端口镜像占用一条流量网络；
- 需确保端口镜像监测的云主机在流量网络加载的集群内。

- **创建完成后立即启用**：立即启用端口镜像，启用后可能占用物理网络带宽，若勾选请确保业务能够正常运行。
- **创建完成后立即添加会话**：会话用于创建云主机网卡流量的端口镜像，可勾选是否立即添加，一个端口镜像可添加多个会话。

如图 *4:* 创建端口镜像所示：

图 4: 创建端口镜像



4. 创建会话

会话用于创建云主机网卡流量的端口镜像，创建后会将源端口的流量复制并发送至目的端口。创建端口镜像时勾选**创建完成后立即添加会话**，可以直接添加会话，或在已创建的端口镜像中进行添加，可参考以下示例输入相应内容：

- **名称**：设置会话名称
- **类型**：选择端口镜像复制的网络流量方向，支持入方向、出方向或双向
  - 入方向：将源端口接收的报文复制到目的端口上；
  - 出方向：将源端口发送的报文复制到目的端口上；
  - 双向：将源端口接收和发送的报文都复制到目的端口上。
- 源端口**云主机**和**网卡**：选择需要监测的云主机和网卡，源端口收发的报文将被复制一份到目的端口
- 目的端口**云主机**和**网卡**：选择用于接收端口镜像的云主机和网卡，目的端口用于将源端口复制过来的报文发送给监控设备

注:

- 目的端口的云主机网卡不能为默认网卡；
- 为保证端口镜像正常运行，请不要对源端口和目的端口网卡设置QoS。

如图 *5:* 会话所示：

图 5: 会话

端口镜像详细部署教程请参考《端口镜像 使用教程》。

后续操作

至此，端口镜像的基本部署已介绍完毕。

4 典型场景实践

背景信息

端口镜像的典型场景：

- 用户的核心业务运作于云主机VM-2上，需要监测VM-2的网络出入流量信息，以便分析业务报文，但直接在VM-2上进行监测将会影响业务，为确保业务稳定运行，在ZStack私有云环境中对VM-2创建端口镜像，将VM-2网卡出入方向的流量报文镜像一份发送至VM-1接收端用于分析，即可达成需求。

1. 创建流量网络对应的二层网络，并加载此二层网络到相应集群。
2. 创建流量网络，输入相应的IP范围、子网掩码、网关、DNS等信息。
3. 创建VM-1，VM-1需包含至少两张网卡。
4. 创建端口镜像。
5. 添加会话，指定VM-2的网卡为源端口，指定VM-1的网卡为目的端口。
6. 验证端口镜像是否生效。

假定客户环境如下：

表 1: 流量网络配置信息

流量网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.10~192.168.29.20*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

以下介绍具体实践步骤。

操作步骤

1. 参考基本部署章节，创建L2-流量网络。
2. 参考基本部署章节和上述表 *1:* 流量网络配置信息中的IP范围、子网掩码、网关等信息，创建流量网络。
3. 创建目的端口云主机VM-1并加载网卡

创建云主机VM-1，并在云主机详情页，为云主机加载第二张网卡，如图 *6:* 云主机加载网卡所示：

图 6: 云主机加载网卡

4. 参考基本部署章节，创建端口镜像。
5. 添加会话

   在端口镜像中添加会话，指定VM-2为源端口云主机，指定VM-1为目的端口云主机，输入以下内容：

   - **名称**：设置会话名称
   - **类型**：选择双向，即可监测源端口云主机网卡出入方向的网络流量
   - **源端口云主机**：选择VM-2，并选择对应网卡
   - **目的端口云主机**：选择VM-1，并选择非默认的网卡

   如图 *7:* 添加会话所示：

   图 7: 添加会话

6. 验证端口镜像是否生效

   1. 打开源云主机控制台，使用ping dhcp-server-ip命令，使源云主机向DHCP Sever发送ICMP报文，如图 *8:* 源云主机发送*ICMP*报文所示：

      图 8: 源云主机发送ICMP报文

```
[root@10-1-225-37 ~]# ping 10.1.225.124
PING 10.1.225.124 (10.1.225.124) 56(84) bytes of data.
64 bytes from 10.1.225.124: icmp_seq=1 ttl=64 time=1.46 ms
64 bytes from 10.1.225.124: icmp_seq=2 ttl=64 time=0.406 ms
64 bytes from 10.1.225.124: icmp_seq=3 ttl=64 time=0.287 ms
64 bytes from 10.1.225.124: icmp_seq=4 ttl=64 time=0.305 ms
64 bytes from 10.1.225.124: icmp_seq=5 ttl=64 time=0.273 ms
64 bytes from 10.1.225.124: icmp_seq=6 ttl=64 time=0.240 ms
64 bytes from 10.1.225.124: icmp_seq=7 ttl=64 time=0.534 ms
64 bytes from 10.1.225.124: icmp_seq=8 ttl=64 time=0.264 ms
64 bytes from 10.1.225.124: icmp_seq=9 ttl=64 time=0.329 ms
```

2. 打开目的云主机控制台，使用tcpdump -eni vnic17.1 icmp命令，查看是否通过端口镜像复制ICMP报文，如图 *9:* 目的云主机接收*ICMP*报文所示：

图 9: 目的云主机接收ICMP报文

```
13:58:38.393530 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1680, length 64
13:58:39.395244 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1681, length 64
13:58:40.396990 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1682, length 64
13:58:41.399116 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1683, length 64
13:58:42.401077 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1684, length 64
13:58:43.402380 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1685, length 64
13:58:44.403938 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1686, length 64
13:58:45.405754 1e:86:4f:a4:ce:9a > fa:96:cf:63:94:00, ethertype IPv4 (0x0800), length 98: 10.1.225.124 > 10.1.225.37: ICMP echo reply, id 40708, se
q 1687, length 64
```

如上所述，目的云主机已通过端口镜像复制了源云主机的网络报文，端口镜像已正确生效，用户可将VM-1接收到的网络报文用于监控分析。

后续操作

至此，端口镜像的使用方法介绍完毕。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、Shared Mount Point、Shared Block类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。支持ImageStore、Sftp（社区版）、Ceph类型。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一时间点某一磁盘的数据状态文件。包括手动快照和自动快照两种类型。