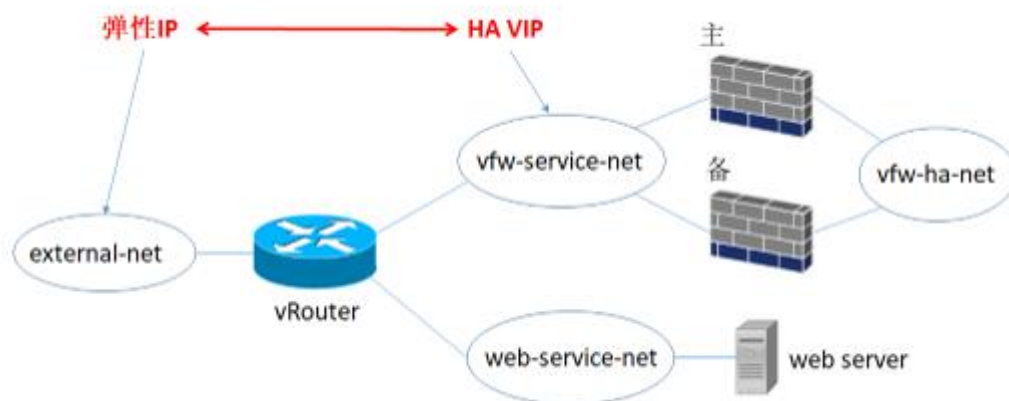


阿里云平台山石云·界 HA 实践方案配置

1. 场景描述及拓扑

该云·界 HA 方案在阿里云平台上实践，配合阿里云平台的高可用虚拟 IP（HA VIP），通过在阿里云环境中部署虚拟防火墙保护服务器的同时提供高可靠的 HA 方案，以保证用户业务长期安全稳定运行。

拓扑如下所示：



2. 云平台 VPC 以及实例创建

按照拓扑要求，需在云平台同一个 VPC 下创建 2 台云界实例（一主一备）以及一台 Web_Server 实例（可用 ubuntu 代替），并且至少需要有 3 个子网（交换机）。其中 2 个分别为云界实例使用的 vfw_server_net 与 vfw_ha_net，因此创建云界实例的时候需额外添加一张网卡来做 HA。另外一个子网就是 Web_Server 实例的 web_service_net。

拓扑中的弹性 IP 以及 HA VIP 需在阿里云平台进行创建，HA VIP 应选择与云界实例的 vfw_service_net 同一个子网。创建完成之后可将弹性 IP 绑定给 HA VIP，再将两台云界实例按照主备顺序绑定在 HA VIP 上。

1) 创建 VPC

The screenshot shows the Alibaba Cloud console interface for creating a VPC. At the top, there are tabs for different regions: 华北 1, 华北 2, 华北 3, 华东 1, 华东 2, 华南 1, 香港, 亚太东北 1 (东京), 亚太东南 1 (新加坡), 亚太东南 2 (悉尼), 美国东部 1 (弗吉尼亚), 美国西部 1 (硅谷), 中东东部 1 (迪拜), and 欧洲中部 1 (法兰克福). A '刷新' (Refresh) button and a '创建专有网络' (Create VPC) button are visible. Below the tabs is a table listing existing VPCs.

VPC ID/名称	网段	状态	描述	创建时间	默认专有网络	操作
vpc-zg33hnlgr huadong1-vpc	172.16.0.0/16	可用	System created defau...	2016-07-15 17:35:41	是	管理 编辑 删除

共有 1 条，每页显示：10 条

2) 创建实例需要用到的 3 个交换机（3 个交换机需在同一个可用区域）

交换机 ID/名称	ECS实例数	网段	状态	可用区	可用私有IP数	创建时间	默认交换机	描述	操作
vsw-bp1mlu3dxvp914gkryb16 ecs-f	0	172.16.9.0/24	可用	华东 1 可用区 F	252	2017-07-31 15:55:45	否		编辑 删除 创建实例
vsw-bp187ed4mt7h4fv1n9s4t hillstone-f	0	172.16.8.0/24	可用	华东 1 可用区 F	252	2017-07-31 15:55:06	否		编辑 删除 创建实例
vsw-bp18optq20ss07ejysidj Hillstone-e-...	0	172.16.7.0/24	可用	华东 1 可用区 E	252	2017-07-21 16:00:20	否		编辑 删除 创建实例
vsw-bp15syw4k13u00zk3sjxv hillstone-e	0	172.16.6.0/24	可用	华东 1 可用区 E	251	2017-02-06 11:05:25	否		编辑 删除 创建实例
vsw-bp1y5a8d65bjauu716igv ecs-e	0	172.16.5.0/24	可用	华东 1 可用区 E	252	2017-02-06 11:05:07	否		编辑 删除 创建实例

3) 按照下图所示配置创建两台云界实例（实例规格需选择 4 核 8G，默认网卡选择同一 VPC 下同一个交换机，另外两个实例还需添加一张网卡选择与默认网卡不同的交换机来做云界的 HA）

产品名称	付费方式	购买周期	数量
服务商: 阿里云计算有限公司			
云服务器 ECS			
地域: 华东 1			
可用区: 华东 1 可用区 E			
安全组 ID: sg-2383zb68t			
I/O 优化实例: I/O 优化实例			
1.	实例规格: 4核8GB	按量付费	1 台
网络类型: 专有网络			
交换机 ID: vsw-bp15syw4k13u00zk3sjxv			
公网带宽: 0Mbps (按使用流量)			
镜像: CloudEdge-r0927			
系统盘: 40GB SSD 云盘			
密码: 已设置			
实例名称: Hillstone_vfw_M			
<input type="checkbox"/> 设置自动释放服务时间			

4) 创建 Web_Server 实例（可用 ubuntu 代替，注意这边 Web_Server 网卡所选交换机与云界实例的两个网卡都不一样）

产品名称	付费方式	购买周期	数量
服务商: 阿里云计算有限公司			
云服务器 ECS			
地域: 华东 1			
可用区: 华东 1 可用区 E			
安全组 ID: sg-2383zb68t			
I/O 优化实例: I/O 优化实例			
1. 实例规格: 2核4GB	按量付费	-	1台
网络类型: 专有网络			
交换机 ID: vsw-bp18optq20ss07eyjsidj			
公网带宽: 0Mbps (按使用流量)			
镜像: ubuntu			
系统盘: 40GB SSD 云盘			
密码: 已设置			
实例名称: Web_Server			
<input type="checkbox"/> 设置自动释放服务时间			

5) 创建 HA VIP (选择与云界实例默认网卡相同的交换机)

创建高可用虚拟IP
✕

地域: 华东 1

专有网络: vpc-zg33hnlgr

*交换机: vsw-bp15syw4k13u00zk3sjxv

交换机网段: 172.16.6.0/24

私网IP地址: 172.16.6.128

指定的私网IP必须为交换机网段中的未被占用的私网IP, 如果不指定将自动为高可用虚拟IP分配一个交换机中空闲的私网IP

确定
取消

6) HA VIP 绑定弹性 IP 以及两个云界实例



3. Loopback 口 https 映射 HA VIP 做网管使用

- 1) 在作为主的云界实例上创建 Loopback 口，配置 IP 地址并开启 https

```

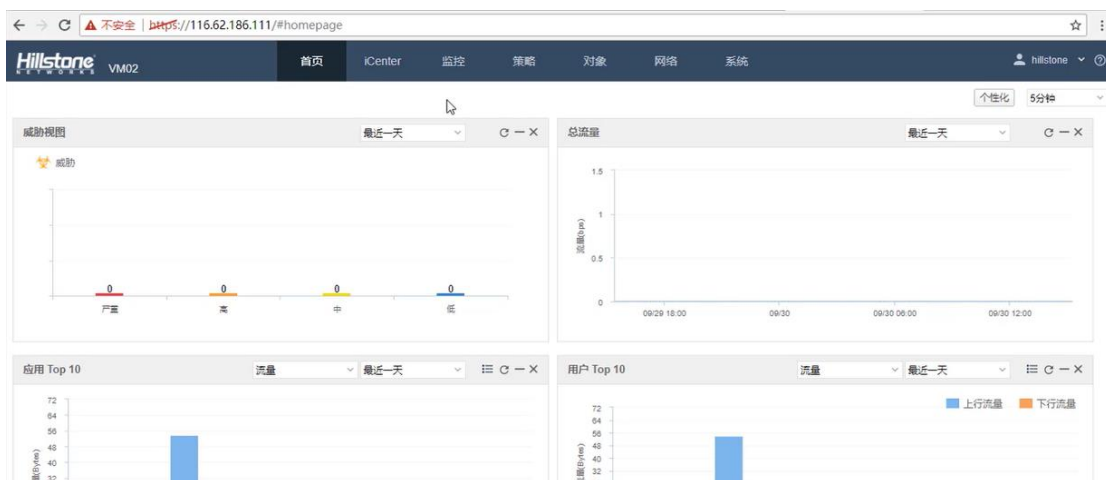
SG-6000# configure
SG-6000(config)# interface loopback1
SG-6000(config-if-loo1)# zone untrust
SG-6000(config-if-loo1)# ip address 11.11.11.1/24 (该地址可任选一个不常用的私网地址)
SG-6000(config-if-loo1)# manage https
  
```

- 2) 配置 DNAT 将 Loopback 口 https 服务映射到 HA VIP

```

SG-6000(config-vrouter)# dnatrul from any to 172.16.6.128/32 service https trans-to 11.11.11.1/32 port 443 (172.16.6.128 为 HA VIP)
  
```

- 2) 通过如上配置, 可通过访问绑定在 HA VIP 上的弹性 IP 用 web 来管理云界 (116.62.186.111 为绑定在 HA VIP 上的弹性 IP)



4. 云界实例 HA 配置

两个云界实例 e0/0 接口地址都由 DHCP 自动获取，无需手动配置，e/1 地址在实例控制台无法查看，需在阿里云平台实例详情里查看，e0/1 接口用于两台云界实例 HA 协商，之后的 HA 配置需要用到，因此需要知道。

由于两台云界是一主一备的 HA 模式，因此大部分配置只需在做主的云界实例上配置即可，备云界实例只需做相关 HA 配置能与主云界实例相互协商即可。

主设备 HA 配置：

```

SG-6000#configure
SG-6000(config)# track track1 （创建检测对象，名字为 track1）
SG-6000(config-trackip)# interface ethernet0/0 weight 255 （配置检测 e0/0 接口）
SG-6000(config)# ha link interface ethernet0/1 （e0/1 接口用于 HA）
SG-6000(config)# ha link ip x.x.x.x/x （用于 HA 协商的地址，根据阿里云平台分配的地址配置）
SG-6000(config)# ha link mac 1st-interface-mac
SG-6000(config)# ha peer ip x.x.x.x mac x.x.x （配置备云界实例用于 HA 的 e0/1 接口的地址，mac 地址可在控制台 show interface 查看）
SG-6000(config)# ha group 0 （加入组 0）
SG-6000(config-ha-group)# priority 50 （设置优先级，值越小优先级越高，优先级高的为主设备）
SG-6000(config-ha-group)# preempt 3 （设置抢占时间为 3 秒）
SG-6000(config-ha-group)# monitor track track1 （添加检测对象）
SG-6000(config)# ha cluster 1 （加入簇 1）

```

备设备 HA 配置：

```

SG-6000#configure
SG-6000(config)# ha link interface ethernet0/1
SG-6000(config)# ha link ip x.x.x.x/x

```

```

SG-6000(config)# ha link mac 1st-interface-mac
SG-6000(config)# ha peer ip x.x.x.x mac x.x.x
SG-6000(config)# ha group 0
SG-6000(config-ha-group)# priority 100
SG-6000(config)# ha cluster 1

```

通过以上两台云界实例的 HA 配置，优先级高的会自动协商为主设备，优先级低的为备设备，在控制台可以看到主设备会用 M 来标识，而备设备是 B。

设备状态如下图所示：

由于两台设备已经协商成功，因此之后的配置只需在主设备上配置即可，配置完后会自动同步到备设备上。

5. 地址映射配置

- 1) 源地址为 web 服务器网段地址的流量转发出去的时候将源地址改为 HA VIP，172.16.7.0/24 是 web_server 的地址段。172.16.6.128/32 是 HA VIP

对应 CLI 配置命令如下：

```

SG-6000(M)(config-vrouter)# snatrule from 172.16.7.0/24 to any service any eif ethernet0/0
trans-to 172.16.6.128/32 mode dynamicport

```

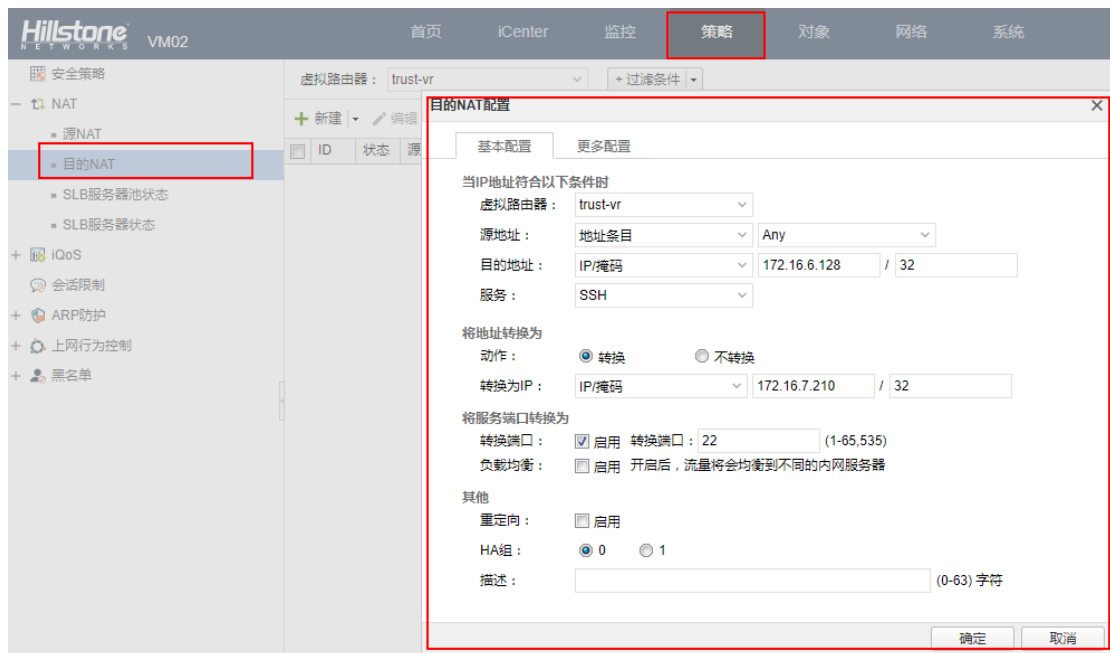
2) 目的地址为 HA VIP 的 SSH 流量不转换



对应的 CLI 配置如下

```
SG-6000(M)(config-vrouter)# snatrule from any to 172.16.6.128/32 service ssh eif ethernet0/0 no-trans
```

3) 目的地址为 HA VIP 的 SSH 流量转发出去的时候映射到 web 服务器的 22 端口上 (172.16.7.210/32 位环境中 web_server 的地址)



对应 CLI 的配置如下:

```
SG-6000(M)(config-vrouter)# dnatrul from any to 172.16.6.128 service ssh trans-to 172.16.7.210/32 port 22
```

4) 最后还需要在阿里云平台上 VPC 的路由器中添加一条目标网段 0.0.0.0/0, 下一跳为 HA VIP 的路由, 将流量都引到 HA VIP 上。

添加路由

*目标网段：

必须是一个合法的CIDR或IP地址，例如：192.168.0.0/24 或 192.168.0.1

下一跳类型：

*高可用虚拟IP：

6. 实践结果

通过以上配置配置，当我们手动去把主云界实例上被监测的接口 e0/0 给 shutdown 之后，原来作为备设备的云界实例就会变为主设备，在这个过程中 SSH 会话并没有中断，而当再把 e0/0 接口给 no shutdown 开启之后，原来的主设备又会重新抢占成为主设备，而且 SSH 会话依旧保持。

随便在一台可以上网的电脑上通过 ssh 弹性 IP 可以连接到环境中的 Web_Server(ubuntu 虚拟机) 上

```
Connecting to 116.62.186.111:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+J'.

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-128-generic x86_64)

 * Documentation: https://help.ubuntu.com/

System information as of Sat Sep 30 15:19:28 UTC 2017

System load: 0.0          Processes:    77
Usage of /:  7.9% of 9.81GB Users logged in: 0
Memory usage: 1%         IP address for eth0: 172.16.7.212
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

Last login: Sat Sep 30 15:19:28 2017
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
```

手动 shutdown 主云界实例上被监测的 e0/0 来让主备进行切换，由下图可见主云界实例的状态由 M 变为 F


```
=====
Interface name      IP address/mask    Zone name          H A L P MAC address
Description
-----
ethernet0/0        172.16.6.136/24   trust              U U U U 0016.3e0c.98ef
-----
ethernet0/1        0.0.0.0/0         HA                 U U U D 0016.3e0f.9ae0
-----
loopback1          11.11.11.1/24    untrust           U U U U -----
-----
vswitchif1        0.0.0.0/0         NULL              D U D D 001c.54ff.0812
-----
=====
SG-6000(M)(config)# inter
SG-6000(M)(config)# interface e0/0
SG-6000(M)(config-if-eth0/0)#
SG-6000(M)(config-if-eth0/0)#
SG-6000(M)(config-if-eth0/0)#
SG-6000(M)(config-if-eth0/0)# shu
SG-6000(M)(config-if-eth0/0)# shutdown
SG-6000(M)(config-if-eth0/0)#
SG-6000(F)(config-if-eth0/0)#
SG-6000(F)(config-if-eth0/0)# _
```

备云界实例的状态由备设备变为主设备，即状态由 B 变为 M

```
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
The session is timeout, exit!
login:
login:
login: hillstone
password:
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
SG-6000(M)#
```

在这个切换的过程中，之前通过 SSH 弹性 IP 连接到环境中 web_server 的会话一直保持，并未发生中断

```
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  Hwaddr 00:16:3e:0d:3f:93
          inet addr:172.16.7.212  Bcast:172.16.7.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe0d:3f93/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:112 errors:0 dropped:0 overruns:0 frame:0
          TX packets:159 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13234 (13.2 KB) TX bytes:21336 (21.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
ubuntu@ubuntu:~$
```

因此通过实践可知，山石云·界可以很好地与阿里云 HA VIP 结合使用为用户提供 HA 解决方案。