vBRAS做PPPoE用户认证与NAT联动支持冗余备份配置举例

vBRAS 王鹤1 2018-03-15 发表

vBRAS A和vBRAS B组成IRF的组网环境下，希望实现IRF主备倒换时NAT业务不中断，以及接收、处理、发送都能在同一台成员设备上进行。具体要求如下：

· 主机作为PPPoE Client，运行PPPoE客户端拨号软件。

· 冗余组节点1和vBRAS A绑定，作为主节点；冗余组节点2和vBRAS B绑定，作为备节点。

· vBRAS A作为PPPoE Server，与RADIUS服务器配合对主机进行远程CHAP认证，并通过PPP地址池为主机分配IP地址。

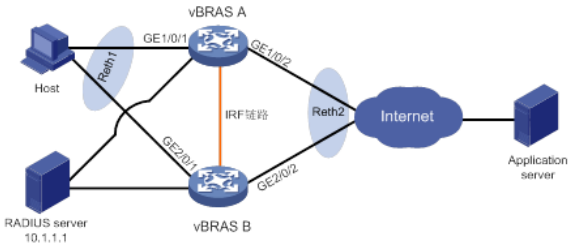
· vBRAS A与认证、授权、计费RADIUS服务器交互报文时的共享密钥均为expert，向RADIUS服务器发送的用户名要携带域名。

· vBRAS A上实现NAT与BRAS联动，在主机通过认证并分配私网地址的同时，为该主机分配公网地址和端口块。

· 将vBRAS A上的CGN单板作为备份组的主节点，vBRAS B上的CGN单板作为备份组的备节点，并将此备份组作为冗余组成员。开启NAT端口块备份功能和会话业务热备份功能，实现NAT端口块表项和会话表项的热备份。冗余组发生倒换，备节点切换成主节点接替原主节点工作时，备份组也发生倒换，让备份组的备节点处于激活状态，从而保证倒换前后，NAT业务处理的连续性。

· 冗余组节点的倒回延时为5分钟，当冗余组倒回时，节点有充分的时间进行准备，准备完毕后，再将业务从优先级低的节点倒换到优先级高的节点。从而尽可能的避免主备节点表项不同步的情况发生。

PPPoE用户认证与NAT联动支持冗余备份配置组网图



(1) 配置vBRAS A和vBRAS B组成IRF

搭建成的IRF中，vBRAS A的成员设备编号为1，vBRAS B的成员设备编号为2，并保证vBRAS A为主设备。IRF的具体配置请参见“虚拟化技术配置指导”中的“IRF”。

(2) 配置RADIUS服务器

在RADIUS服务器上设置与vBRAS交互报文时的共享密钥为expert；添加PPP用户名及密码。

(3) 配置RADIUS方案

创建RADIUS方案rad。

<Sysname> system-view

[Sysname] radius scheme rad

配置主认证服务器和主计费服务器的IP地址为10.0.0.1，并配置主认证、计费服务器的UDP端口号分别为1812和1813。

[Sysname-radius-rad] primary authentication 10.0.0.1 1812

[Sysname-radius-rad] primary accounting 10.0.0.1 1813

配置与认证、计费服务器交互报文时的共享密钥为明文expert。

[Sysname-radius-rad] key authentication simple expert

[Sysname-radius-rad] key accounting simple expert

配置向RADIUS服务器发送的用户名要携带域名。

[Sysname-radius-rad] user-name-format with-domain

[Sysname-radius-rad] quit

创建名称为user的用户组。

[Sysname] user-group user

[Sysname-ugroup-user] quit

创建ISP域cgn。

[Sysname] domain name cgn

为PPP用户配置AAA认证方法为RADIUS认证/授权/计费。

[Sysname-isp-cgn] authentication ppp radius-scheme rad

[Sysname-isp-cgn] authorization ppp radius-scheme rad

[Sysname-isp-cgn] accounting ppp radius-scheme rad
配置用户地址类型为私网IPv4地址。该地址类型的用户认证成功后将触发NAT地址分配。
[Sysname-isp-cgn] user-address-type private-ipv4
设置ISP域cgn下的用户授权属性为**user-group。**
[Sysname-isp-cgn] authorization-attribute user-group user
[Sysname-isp-cgn] quit
(4) 配置以太网冗余接口
创建Reth1，成员接口为GigabitEthernet1/0/1和GigabitEthernet2/0/1，其中GigabitEthernet1/0/1的优先级为100，GigabitEthernet2/0/1的优先级为80。
[Sysname] interface reth 1
[Sysname-Reth1] member interface gigabitEthernet1/0/1 priority 100
[Sysname-Reth1] member interface gigabitEthernet2/0/1 priority 80
创建Reth2，IP地址为111.8.0.101/24，成员接口为GigabitEthernet1/0/2和GigabitEthernet2/0/2，其中GigabitEthernet1/0/2的优先级为100，GigabitEthernet2/02的优先级为80。
[Sysname] interface reth 2
[Sysname-Reth2] ip address 111.8.0.101 255.255.255.0
[Sysname-Reth2] member interface gigabitEthernet1/0/2 priority 100
[Sysname-Reth2] member interface gigabitEthernet2/0/2 priority 80
(5) 配置Track，监测GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet2/0/1和GigabitEthernet2/0/2的状态。
[Sysname] track 1 interface gigabitethernet 1/0/1 physical
[Sysname] track 2 interface gigabitethernet 1/0/2 physical
[Sysname] track 3 interface gigabitethernet 2/0/1 physical
[Sysname] track 4 interface gigabitethernet 2/0/2 physical
(6) 配置备份组
创建名称为vbras的备份组。
[Sysname] failover group vbras
将vBRAS A上的slot指定为备份组的主节点，vBRAS B上的slot指定为备份组的备节点。
[Sysname-failover-group-vbras] bind slot 1 primary
[Sysname-failover-group-vbras] bind slot 2 secondary
[Sysname-failover-group-vbras] quit
(7) 配置冗余组
创建Node 1，Node 1和vBRAS A绑定，为主节点。关联的Track项为1和2。
[Sysname] redundancy group aaa
[Sysname-redundancy-group-aaa] node 1
[Sysname-redundancy-group-aaa-node-1] bind slot 1
[Sysname-redundancy-group-aaa-node-1] priority 100
[Sysname-redundancy-group-aaa-node-1] track 1 interface gigaitEthernet 1/0/1
[Sysname-redundancy-group-aaa-node-1] track 2 interface gigaitEthernet 1/0/2
创建Node 2，Node 2和vBRAS B绑定，为备节点。关联的Track项为3和4。
[Sysname-redundancy-group-aaa] node 2
[Sysname-redundancy-group-aaa-node-1] bind slot 2
[Sysname-redundancy-group-aaa-node-1] priority 80
[Sysname-redundancy-group-aaa-node-1] track 3 interface gigaitEthernet 2/0/1
[Sysname-redundancy-group-aaa-node-1] track 4 interface gigaitEthernet 2/0/2
[Sysname-redundancy-group-aaa-node-1] quit
将Reth1、Reth2和备份组vbras添加到冗余组中。
[Sysname-redundancy-group-aaa] member interface reth 1
[Sysname-redundancy-group-aaa] member interface reth 2
[Sysname-redundancy-group-aaa] member failover group vbras
配置冗余组节点的倒回等待时间为5分钟。
[Sysname-redundancy-group-aaa] preempt-delay 5
[Sysname-redundancy-group-aaa] quit
(8) 配置PPPoE Server
配置虚拟模板接口1的参数，采用CHAP认证对端，并使用PPP地址池1为对端分配IP地址。
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp authentication-mode chap domain vbras
[Sysname-Virtual-Template1] remote address pool 1
[Sysname-Virtual-Template1] ip address 10.210.0.1 24
创建名为pool1地址池，IP地址范围为10.210.0.2到10.210.0.255。
[Sysname] ip pool pool1 10.210.0.2 10.210.0.255
在以太网冗余接口Reth1上启用PPPoE Server协议，并将该接口与虚拟模板接口1绑定。
[Sysname] interface reth 1
[Sysname-Reth1] pppoe-server bind virtual-template 1

[Sysname-Reth1] quit
(9)　配置NAT
配置ACL 3000，仅允许对内部网络中10.210.0.0/24网段的用户报文进行地址转换。
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 0 permit ip source 10.210.0.0 0.0.0.255 user-group user
[Sysname-acl-ipv4-adv-3000] quit
配置地址组1与备份组vbras绑定，包含一个外网地址111.8.0.200，外网地址的端口范围为1024～65535，端口块大小为10。
[Sysname] nat address-group 1
[Sysname-address-group-1] failover-group vbras
[Sysname-address-group-1] port-block block-size 10
[Sysname-address-group-1] port-range 1024 65535
[Sysname-address-group-1] address 111.8.0.200 111.8.0.200
在冗余口Reth2上配置出方向动态地址转换，允许使用地址组1中的地址对匹配ACL 3000的报文进行源地址转换，并在转换过程中使用端口信息。
[Sysname] interface reth 2
[Sysname-Reth2] nat outbound 3000 address-group 1
[Sysname-Reth2] quit
配置处理基于会话业务的备份组，即仅允许将匹配ACL 3000的报文引流到备份组vbras的主节点上进行业务处理。
[Sysname] session service-location acl 3000 failover-group vbras
(10) 开启热备功能
开启NAT动态端口块备份功能。
[Sysname] nat port-block synchronization enable
开启会话业务备份功能。
[Sysname] session synchronization enable

配置完成后，可以用如下步骤验证结果：
主机安装PPPoE客户端软件后，使用正确的用户名和密码即可接入到Internet。当用户登录成功后，可以在IRF设备上通过**display ppp access-user**命令查看PPP用户的详细信息（包括分配的私网IP地址、转换后的公网IP地址以及端口块），同时还可以通过以下显示命令看到为该用户生成的动态端口块表项。
[Sysname] display nat port-block dynamic
Slot 1:
Local VPN　Local IP　　Global IP　　Port block　Connections　Extend
---　　10.210.0.4　　111.8.0.200　　1024-1323　1　　---
Total mappings found: 1
正常情况下，由备份组vbras的主节点处理NAT业务。
[Sysname] display failover group
Stateful failover local group information:
ID　Name　　Primary　Secondary　　Active status
1　vbras　　1　　2　　Primary
备份组vbras的主节点故障时，由备节点处理NAT业务。
[Sysname] display failover group
Stateful failover local group information:
ID　Name　　Primary　Secondary　　Active status
1　vbras　　1　　2　　Secondary