

Virtual Private Cloud

Práticas recomendadas

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Práticas recomendadas

- Migração da rede clássica para o VPC

 - Soluções de migração

 - Exemplo: Migração de um CLB da rede pública

 - Exemplo: Configuração do acesso híbrido para um CLB da rede privada

- Configuração de um CVM de gateway público

- Criação de cluster principal/secundário de alta disponibilidade usando HAVIP + Keepalived

- Criação de um banco de dados de alta disponibilidade usando HAVIP + cluster de failover do Windows Server

- Comunicação principal/secundária de nuvem híbrida (DC e VPN)

- Comunicação principal/secundária de nuvem híbrida (CCN e VPN)

Práticas recomendadas

Migração da rede clássica para o VPC

Soluções de migração

Last updated : 2024-01-24 17:44:04

Este documento descreve como migrar uma instância da rede clássica para a VPC e configurar a solução de acesso híbrido durante a migração.

Migração de uma única instância

Você pode migrar com facilidade uma instância da rede clássica para uma VPC. Consulte os detalhes abaixo.

Tipo de instância	Descrição
CVM	A instância será reiniciada. O IP da rede clássica será convertido imediatamente em um IP da VPC.
TencentDB for MySQL	Tanto o IP da rede clássica quanto o IP da VPC ficam disponíveis por um período. O IP da rede clássica original permanece válido da seguinte forma: MySQL: período padrão: 24 horas (1 dia); período máximo: 168 horas (7 dias) MariaDB: válido por 24 horas (1 dia) TDSQL: válido por 24 horas (1 dia) Redis: opções disponíveis: liberar agora, liberar após 1 dia, liberar após 2 dias, liberar após 3 dias e liberar após 7 dias MongoDB: o endereço IP original se tornará inválido imediatamente para a versão 4.0 ou posterior. As outras versões apresentam as opções: liberar agora, liberar após 1 dia, liberar após 2 dias, liberar após 3 dias e liberar após 7 dias
TencentDB for MariaDB	
TDSQL for MySQL	
TencentDB for Redis	
TencentDB for MongoDB	

Nota :

Se você quiser manter os endereços IP do recurso inalterados após a alternância de rede, tente criar uma VPC que tenha IPs da rede clássica. Se isso for impossível, consulte a seguinte solução:

Crie um serviço Private DNS e resolva seu nome de domínio. Após migrar os recursos para uma VPC, use o [Private DNS](#) da Tencent Cloud.

Use um IP público.

Solução de acesso híbrido durante a migração

O acesso híbrido significa que os serviços que estão sendo migrados podem acessar a rede clássica e uma VPC. A Tencent Cloud fornece a seguinte solução de acesso híbrido:

A acessibilidade do IP da rede clássica e do IP da VPC do serviço TencentDB garante o acesso híbrido no nível da instância do TencentDB.

O acesso ao Cloud Object Storage (COS) por meio de nome de domínio fornece a capacidade de acesso híbrido.

Para implementar a interconexão durante a migração, use junto com:

Classiclink: permite que as CVMs baseadas na rede clássica se interconectem com os recursos da VPC, como as instâncias da CVM, do TencentDB e do CLB.

Conexão de terminal: permite que as instâncias em uma VPC se comuniquem com os recursos na rede clássica (exceto as CVMs).

Nota:

Se você deseja estabelecer uma conexão de terminal, [envie um tíquete](#). Essa funcionalidade apenas possibilita o acesso a CVMs baseadas na rede clássica. Recomendamos migrar os seus recursos para uma VPC.

Para saber mais sobre as soluções VPC e Classiclink, consulte [Comunicação com a rede clássica](#). Para mais informações sobre como configurar um Classiclink, consulte [Classiclink](#).

Exemplo: Migração de um CLB da rede pública

Last updated : 2024-01-24 17:44:05

Este documento descreve como migrar sem interrupções o seu serviço do CLB da rede pública da rede clássica para uma VPC.

Nota:

Este exemplo é apenas para referência. Na migração real, avalie cuidadosamente o impacto e elabore o plano de migração com antecedência.

Cenário

Configuração de recursos de negócios baseados na rede clássica:

O nome de domínio DNS é resolvido para o VIP do CLB da rede pública na rede clássica.

O CLB da rede pública está vinculado à duas CVMs (CVM 1 e CVM 2) como servidores de back-end.

As aplicações implantadas na CVM 1 e na CVM 2 podem acessar os serviços de back-end do TencentDB for Redis e do TencentDB for MySQL.

Processo de migração

1. Criar uma VPC
2. Migrar os serviços do TencentDB
3. Criar instâncias da CVM e implantar aplicações
4. Criar um CLB da rede pública e associá-lo às CVMs
5. Alterar o endereço IP do nome de domínio DNS
6. Liberar os recursos da rede clássica

Instruções para a migração

1. Crie uma VPC conforme instruído em [Criação de VPCs](#).
2. Migre as instâncias do [TencentDB for MySQL](#) e do [TencentDB for Redis](#) para a VPC.

Nota:

Durante a migração, as instâncias do TencentDB ainda permanecem conectadas. Tanto o IP original da rede clássica quanto os endereços IP da VPC permanecem válidos por um determinado período após a migração, mantendo assim a disponibilidade do serviço. Conclua a migração dos demais recursos dentro desse período.

3. Crie imagens para a CVM 1 e a CVM 2 baseadas na rede clássica conforme instruído em [Criação de imagens personalizadas](#) e [use as imagens](#) para criar duas instâncias da CVM na VPC. Depois, teste se as CVMs conseguem acessar as instâncias do TencentDB.

Nota:

Se a reinicialização das instâncias da CVM durante a migração for aceitável para os seus negócios, você poderá alternar diretamente para a VPC fora do horário de pico. Para obter instruções detalhadas, consulte [Alternância para a VPC](#).

4. Crie um CLB da rede pública na VPC, e associe-a às duas CVMs criadas na etapa anterior. Para mais informações, consulte [Introdução ao CLB](#). Execute uma verificação de integridade para evitar a interrupção do serviço devido a uma exceção.

5. Resolva o nome de domínio DNS para o VIP do CLB da rede pública na VPC.

6. Verifique se a VPC está funcionando corretamente. Se estiver, libere os recursos originais do CLB e da CVM da rede pública na rede clássica para concluir a migração.

Nota:

O IP original da rede clássica de uma instância do TencentDB será liberado automaticamente após a expiração.

Exemplo: Configuração do acesso híbrido para um CLB da rede privada

Last updated : 2024-01-24 17:44:05

Este documento fornece uma configuração de exemplo para o cenário em que a VPC e a rede clássica são necessárias durante a migração de negócios.

Cenário

Configuração de recursos de negócios baseados na rede clássica:

O cliente da CVM acessa um CLB da rede privada.

O CLB da rede privada está vinculado às duas CVMs (CVM 1 e CVM 2) como servidores reais.

As aplicações implantadas na CVM 1 e na CVM 2 podem acessar os serviços de back-end do TencentDB for MySQL.

Solicitações:

Migra os recursos da rede clássica para uma VPC

Os clientes baseados na VPC têm acesso prioritário ao serviço do CLB da rede privada na rede clássica.

O acesso à rede clássica permanece disponível por um mês após a migração.

Processo de migração

1. Criar uma VPC
2. Migrar os serviços do TencentDB
3. Configurar uma conexão de terminal
4. Criar um CLB da rede privada e configurar seu serviço de back-end
5. Configurar um Classiclink
6. Liberar os recursos da rede clássica

Etapas

1. Crie uma VPC conforme instruído em [Criação de VPCs](#).
2. Migre os serviços do TencentDB for MySQL para a VPC conforme instruído em [Alternância de rede](#).

Nota:

Durante a migração, as instâncias do TencentDB ainda permanecem conectadas. Tanto o IP original da rede clássica quanto os endereços IP da VPC permanecem válidos após a migração, mantendo assim a disponibilidade do serviço.

3. Configure um serviço de conexão de terminal para permitir que o cliente da CVM na VPC acesse o serviço do CLB da rede pública na rede clássica.
4. Crie uma instância do CLB da rede privada e seu servidor real na VPC, e configure os serviços relacionados.

5. Configure um Classiclink para permitir que a CVM baseado na rede clássica acesse a instância do CLB da rede privada na VPC. Teste se a VPC está fornecendo serviços normalmente.
6. Após o serviço da VPC estiver normal, e a CVM baseada na VPC começar a acessar o CLB da rede privada na VPC, exclua a conexão de terminal, mantenha o Classiclink e libere os recursos na rede clássica.

Configuração de um CVM de gateway público

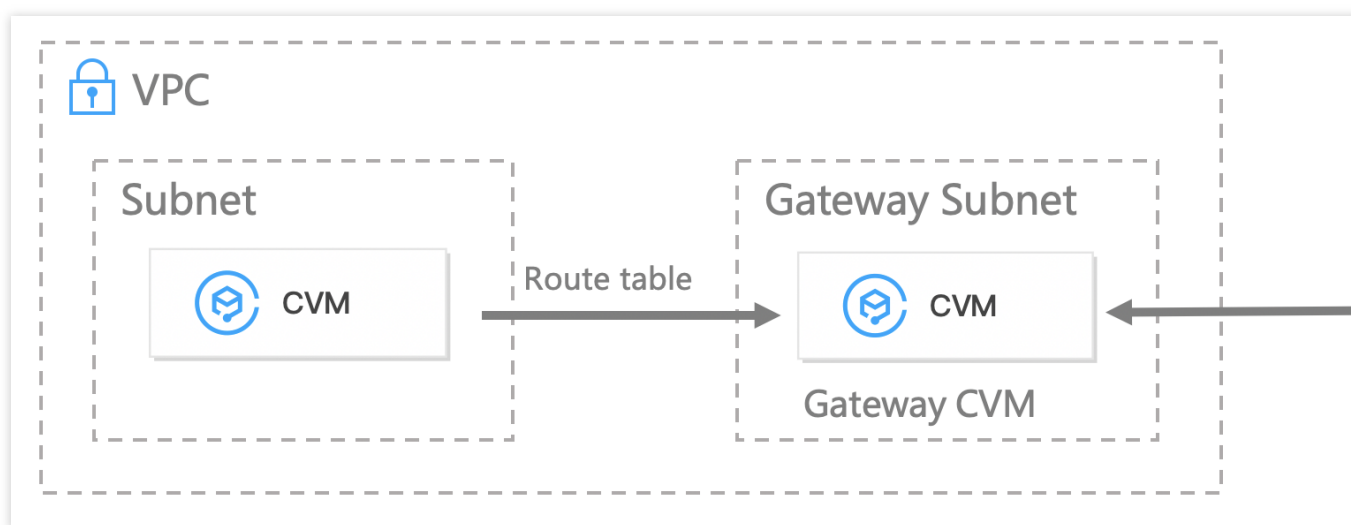
Last updated : 2024-01-24 17:44:05

Atenção:

A partir de 6 de dezembro de 2019, o Tencent Cloud não oferece mais suporte à configuração de um CVM como o gateway público na página de aquisição do CVM. Se for necessário configurar um gateway, siga as instruções abaixo.

Visão geral

Você pode acessar a internet usando um CVM de gateway público com um IP público ou EIP quando alguns de seus CVMs baseados no VPC não possuem IPs públicos. O CVM de gateway público converte o IP de origem do tráfego de saída. Quando outros CVMs acessarem a internet por meio do gateway público CVM, os IPs de origem serão convertidos em IPs públicos do CVM de gateway público. Consulte a figura abaixo.



Pré-requisitos

Você está logado no [console do CVM](#).

O CVM de gateway público e os CVMs que precisam acessar a internet pelo CVM de gateway público devem estar localizados em sub-redes diferentes porque o CVM de gateway público só consegue encaminhar solicitações de outras sub-redes.

O CVM de gateway público deve ser do Linux. Os CVMs do Windows não funcionarão.

Instruções

Etapa 1: vincule um EIP (opcional)

Nota:

Pule esta etapa se o CVM de gateway público já tiver um endereço IP público.

1. Faça login no [console do CVM](#) e selecione **EIP** na barra lateral esquerda.
2. Localize o EIP para vincular a instância, selecione **More (Mais) > Bind (Vincular)** na coluna **Operation (Operação)**.

Status	Elastic IP address	Billing Mode	Bind resources	Bound resource
Not bound, incurring idle fee	129.204.187.154	by traffic	-	-
Bound	193.112.218.92	by traffic	nat-5m0583kq test	NAT Gateway

3. Na janela pop-up, selecione um CVM a ser configurado e vincule-o ao EIP.

Bind resources

Please select the resource to be bound with the EIP eip-r143dxye.

CVM Instances NAT Gateway ENI

Instance ID/Name	Availability Zone	Private IP
------------------	-------------------	------------

Etapa 2: configure uma tabela de rotas para a sub-rede do gateway

Atenção:

A sub-rede do gateway e outras sub-redes não podem compartilhar a mesma tabela de rotas. É necessário criar uma tabela de rotas separada para a sub-rede do gateway.

1. [Crie uma tabela de rotas personalizada.](#)
2. Associe a tabela de rotas com a sub-rede onde o CVM de gateway público está localizado.

Bind Subnets ×

Select the subnet to be associated

	Subnet ID/name	Subnet CIDR	The route table associated
<input checked="" type="checkbox"/>	subnet-368scdxa test2	192.168.0.0/24	rtb-1nzo5m26 default
<input type="checkbox"/>	subnet-pudx8w46 1	192.168.2.0/24	rtb-1nzo5m26 default

Note: each subnet can only be bound with one route table. Once you click Confirm, the existing route table will be replaced with: 1 (rtb-barwmkte)

OK Cancel

Etapa 3: configure uma tabela de rotas para outras sub-redes

Essa tabela de rotas direciona todo o tráfego dos CVMs sem um IP público para o gateway público, para que eles também possam acessar as redes públicas.

Adicione as seguintes políticas de roteamento à tabela de rotas:

Destination (Destino): o IP público que você deseja acessar.

Next hop type (Tipo de próximo salto): CVM.

Next hop (Próximo salto): o IP privado da instância do CVM ao qual o EIP foi vinculado na Etapa 1.

Para obter mais informações, consulte [Gerenciamento de tabela de rotas](#).

Add routing

Destination	Next hop type	Next hop
<input type="text"/>	Cloud Virtual Machine ▼	<input type="text" value="Enter the private IP"/> Create a CVM

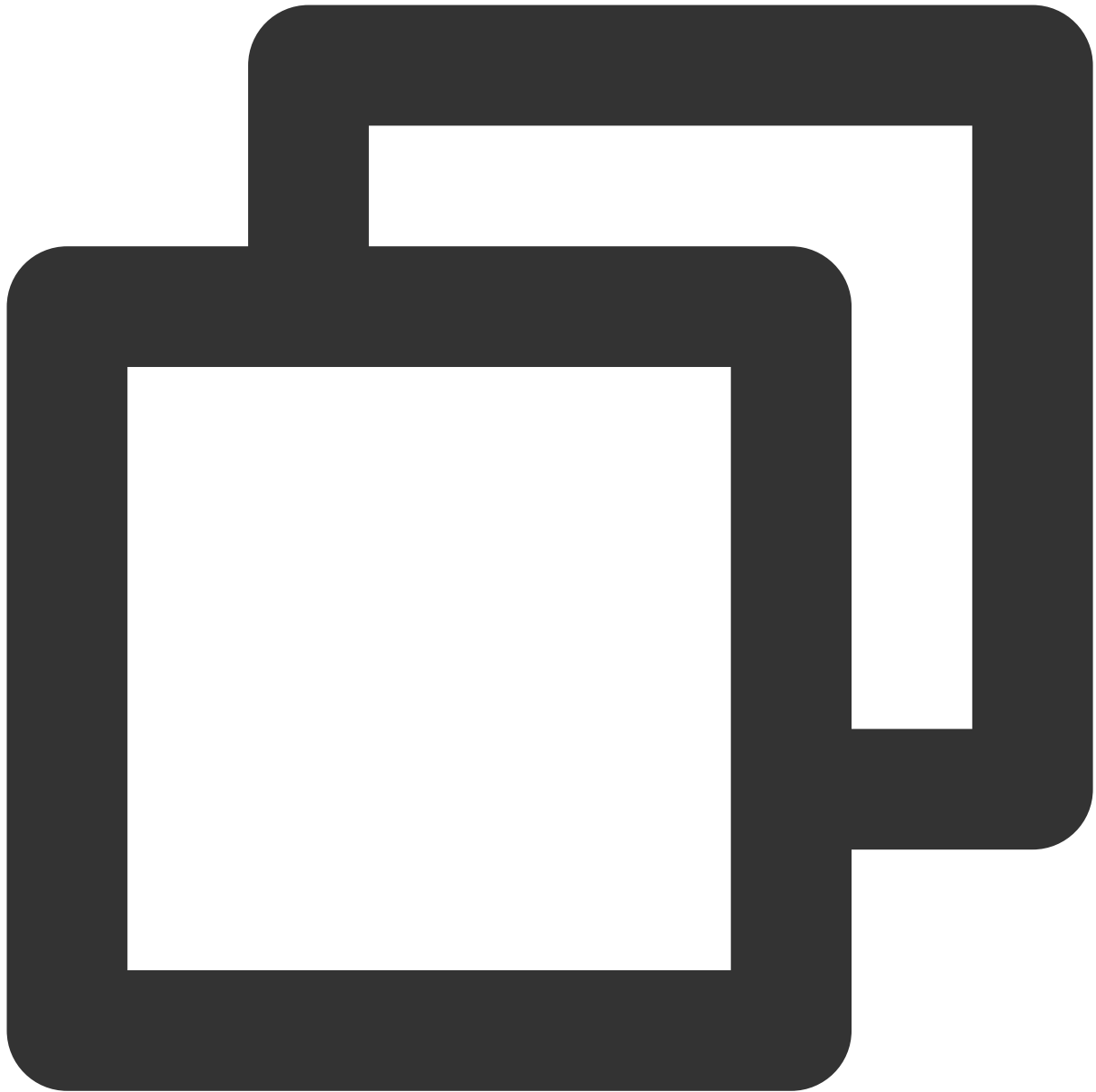
[+ New Line](#)

Adding a routing entry may affect your business. Please double check before continuing.

Etapa 4: configure o gateway público

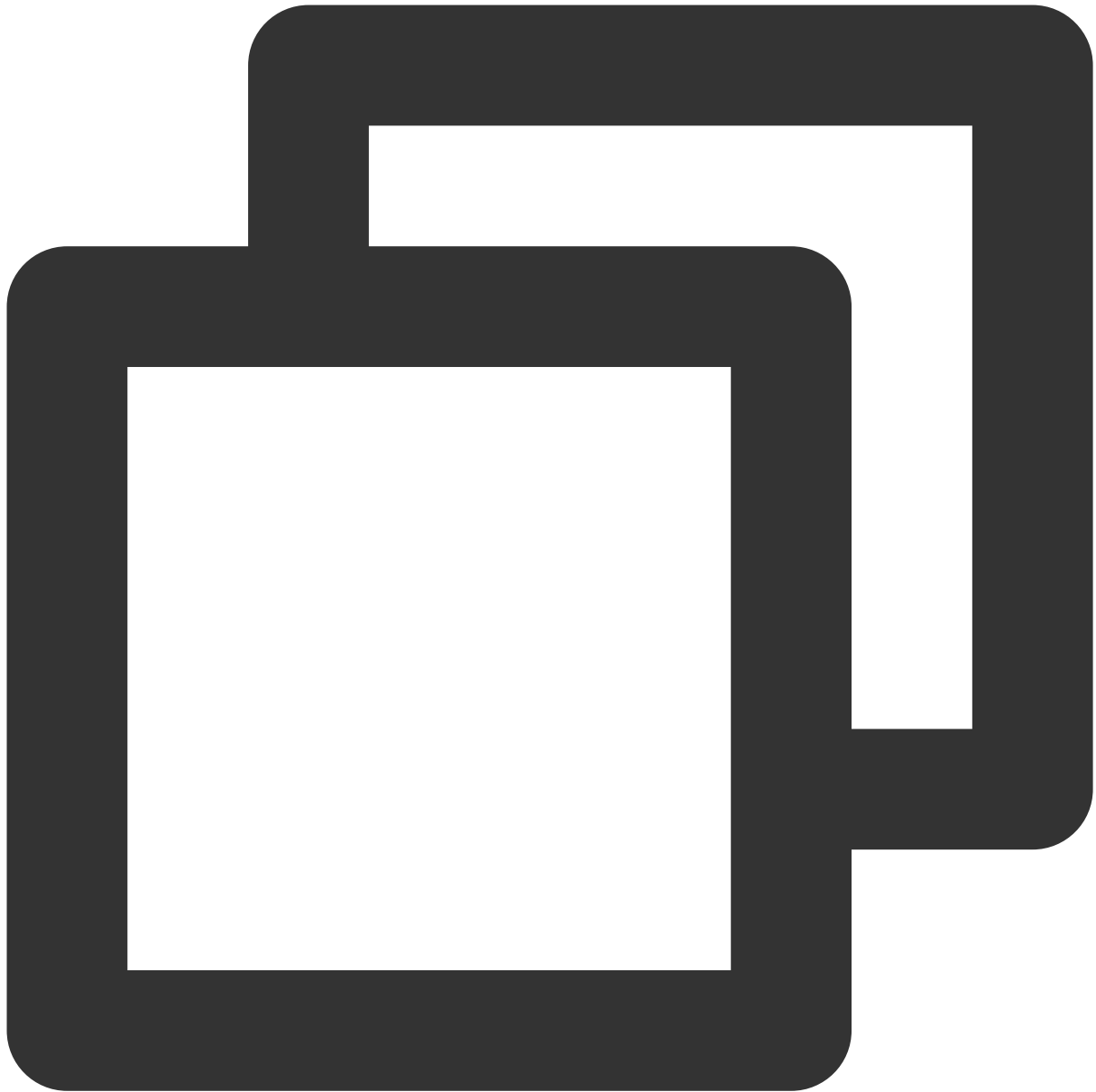
1. [Faça login no CVM de gateway público](#) e execute as etapas abaixo para habilitar o encaminhamento de rede e o proxy NAT.

1.1 Execute o seguinte comando para criar o script `vpcGateway.sh` em `usr/local/sbin`.



```
vim /usr/local/sbin/vpcGateway.sh
```

1.2 Pressione **i** para alternar ao modo de edição e adicione o seguinte código no script.

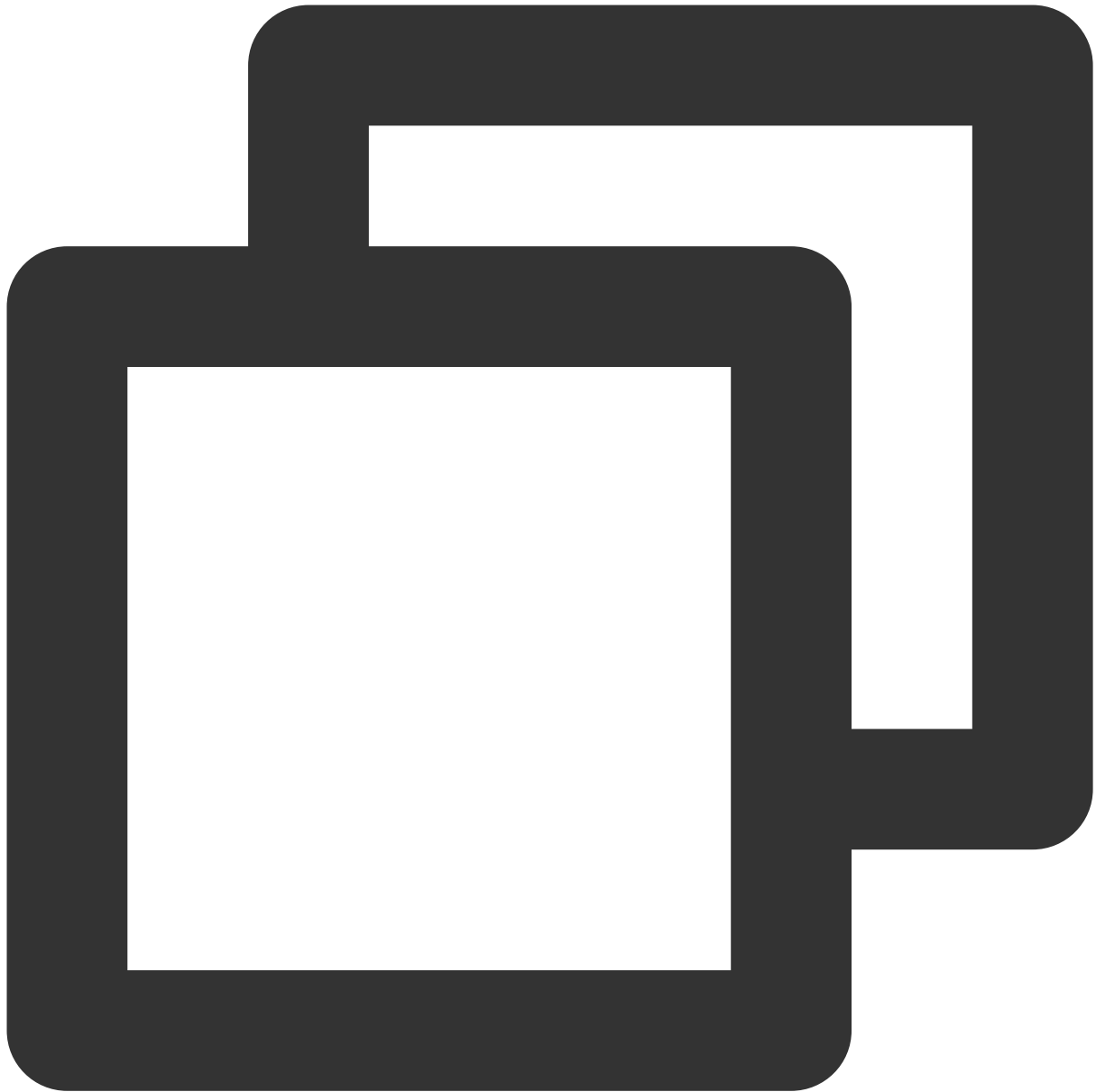


```
#!/bin/bash
echo "-----"
echo "`date`"
echo "(1)ip_forward config....."
file="/etc/sysctl.conf"
grep -i "^net\\.ipv4\\.ip_forward\\.*" $file &>/dev/null && sed -i \\
's/net\\.ipv4\\.ip_forward\\.*/net\\.ipv4\\.ip_forward = 1/' $file || \\
echo "net.ipv4.ip_forward = 1" >> $file
echo 1 >/proc/sys/net/ipv4/ip_forward
[ `cat /proc/sys/net/ipv4/ip_forward` -eq 1 ] && echo "-->ip_forward:Success" || \\
echo "-->ip_forward:Fail"
```

```
echo "(2)Iptables set....."
iptables -t nat -A POSTROUTING -j MASQUERADE && echo "-->nat:Success" || echo "-->n
iptables -t mangle -A POSTROUTING -p tcp -j TCPOPTSTRIP --strip-options timestamp &
echo "-->mangle:Success" || echo "-->mangle:Fail"
echo "(3)nf_contrack config....."
echo 262144 > /sys/module/nf_contrack/parameters/hashsize
[ `cat /sys/module/nf_contrack/parameters/hashsize` -eq 262144 ] && \
echo "-->hashsize:Success" || echo "-->hashsize:Fail"
echo 1048576 > /proc/sys/net/netfilter/nf_contrack_max
[ `cat /proc/sys/net/netfilter/nf_contrack_max` -eq 1048576 ] && \
echo "-->nf_contrack_max:Success" || echo "-->nf_contrack_max:Fail"
echo 10800 >/proc/sys/net/netfilter/nf_contrack_tcp_timeout_established \
[ `cat /proc/sys/net/netfilter/nf_contrack_tcp_timeout_established` -eq 10800 ] \
&& echo "-->nf_contrack_tcp_timeout_established:Success" || \
echo "-->nf_contrack_tcp_timeout_established:Fail"
```

1.3 Pressione **Esc** e digite **:wq** para salvar e fechar o arquivo.

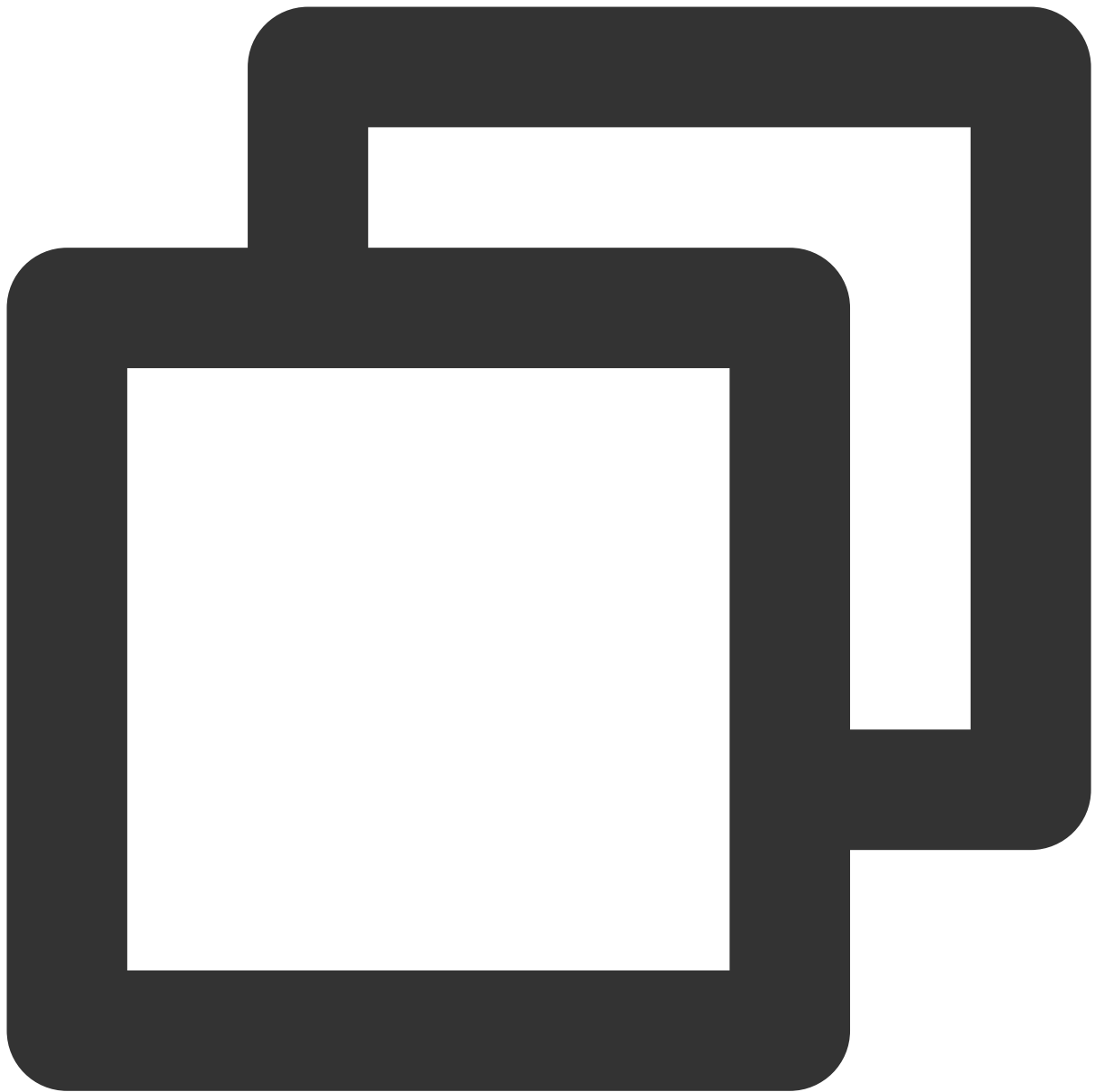
1.4 Execute o seguinte comando para definir a permissão do script.



```
chmod +x /usr/local/sbin/vpcGateway.sh
echo "/usr/local/sbin/vpcGateway.sh >/tmp/vpcGateway.log 2>&1" >> /etc/rc.local
```

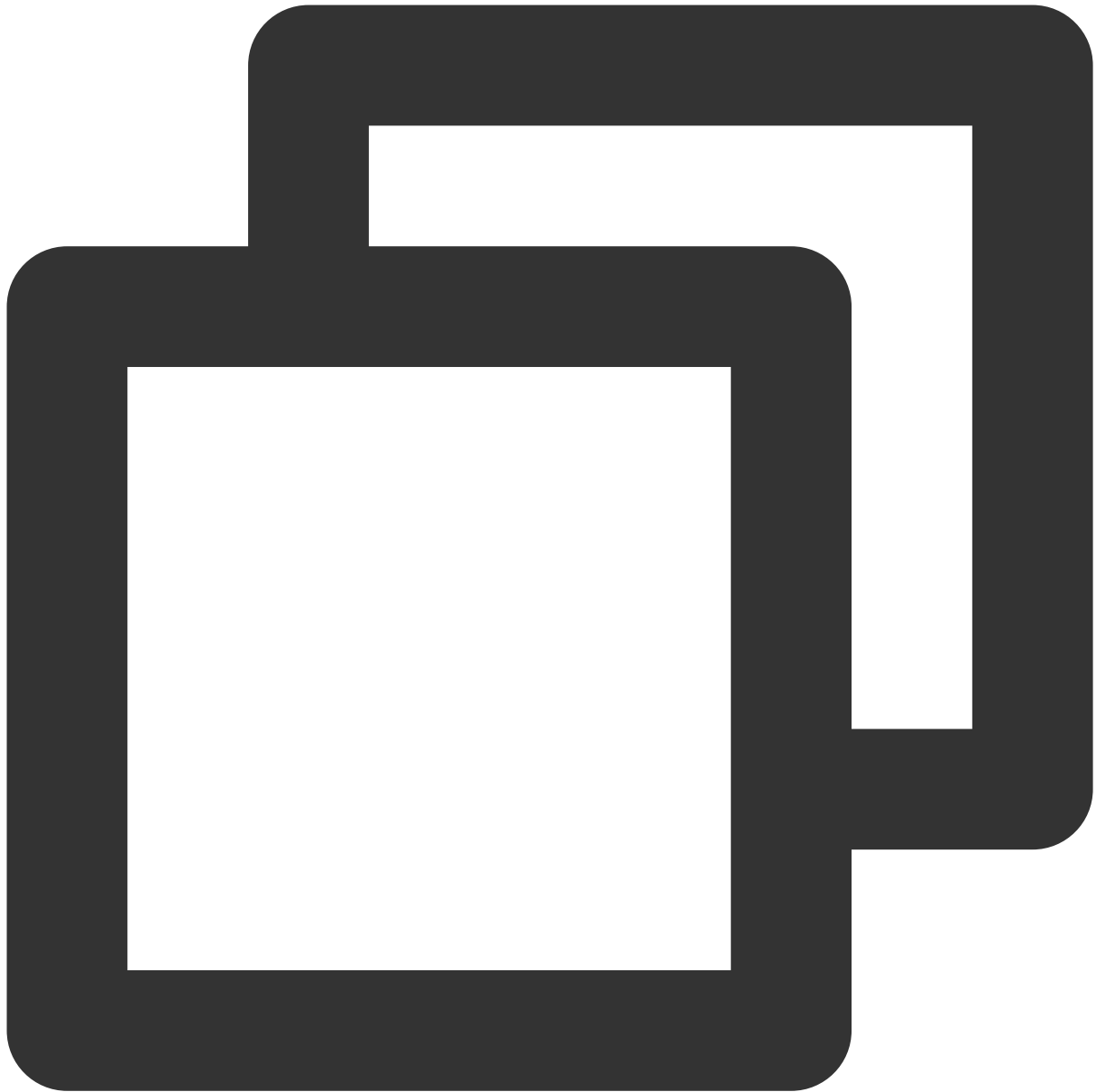
2. Defina o RPS do gateway público.

2.1 Execute o seguinte comando para criar o script `set_rps.sh` em `usr/local/sbin` .



```
vim /usr/local/sbin/set_rps.sh
```

2.2 Pressione **i** para alternar ao modo de edição e adicione o seguinte código no script.



```
# !/bin/bash
echo "-----"
date
mask=0
i=0
total_nic_queues=0
get_all_mask() {
  local cpu_nums=$1
  if [ $cpu_nums -gt 32 ]; then
    mask_tail=""
    mask_low32="ffffffff"
  fi
}
```

```
idx=$((cpu_nums / 32))
cpu_reset=$((cpu_nums - idx * 32))
if [ $cpu_reset -eq 0 ]; then
mask=$mask_low32
for ((i = 2; i <= idx; i++)); do
mask="$mask,$mask_low32"
done
else
for ((i = 1; i <= idx; i++)); do
mask_tail="$mask_tail,$mask_low32"
done
mask_head_num=$((2 ** cpu_reset - 1))
mask=$(printf "%x%s" $mask_head_num $mask_tail)
fi
else
mask_num=$((2 ** cpu_nums - 1))
mask=$(printf "%x" $mask_num)
fi
echo $mask
}
set_rps() {
if ! command -v ethtool &>/dev/null; then
source /etc/profile
fi
ethtool=$(which ethtool)
cpu_nums=$(cat /proc/cpuinfo | grep processor | wc -l)
if [ $cpu_nums -eq 0 ]; then
exit 0
fi
mask=$(get_all_mask $cpu_nums)
echo "cpu number:$cpu_nums mask:0x$mask"
ethSet=$(ls -d /sys/class/net/eth*)
for entry in $ethSet; do
eth=$(basename $entry)
nic_queues=$(ls -l /sys/class/net/$eth/queues/ | grep rx- | wc -l)
if (($nic_queues == 0)); then
continue
fi
cat /proc/interrupts | grep "LiquidIO.*rxtx" &>/dev/null
if [ $? -ne 0 ]; then # not smartnic
#multi queue don't set rps
max_combined=$(
$ethtool -l $eth 2>/dev/null | grep -i "combined" | head -n 1 | awk '{print $2}'
)
#if ethtool -l $eth goes wrong.
[[ ! "$max_combined" =~ ^[0-9]+$ ]] && max_combined=1
if [ ${max_combined} -ge ${cpu_nums} ]; then
```

```
echo "$eth has equally nic queue as cpu, don't set rps for it..."
continue
fi
else
echo "$eth is smartnic, set rps for it..."
fi
echo "eth:$eth queues:$nic_queues"
total_nic_queues=$((total_nic_queues + $nic_queues))
i=0
while (($i < $nic_queues)); do
echo $mask >/sys/class/net/$eth/queues/rx-$i/rps_cpus
echo 4096 >/sys/class/net/$eth/queues/rx-$i/rps_flow_cnt
i=$((i + 1))
done
done
flow_entries=$((total_nic_queues * 4096))
echo "total_nic_queues:$total_nic_queues flow_entries:$flow_entries"
echo $flow_entries >/proc/sys/net/core/rps_sock_flow_entries
}
set_rps
```

2.3 Pressione **Esc** e digite **:wq** para salvar e fechar o arquivo.

2.4 Execute o seguinte comando para definir a permissão do script.



```
chmod +x /usr/local/sbin/set_rps.sh
echo "/usr/local/sbin/set_rps.sh >/tmp/setRps.log 2>&1" >> /etc/rc.local
chmod +x /etc/rc.d/rc.local
```

3. Reinicie o CVM de gateway público para aplicar as configurações. Depois, teste se um CVM sem um IP público consegue acessar a internet pelo CVM de gateway público.

Criação de cluster principal/secundário de alta disponibilidade usando HAVIP + Keepalived

Last updated : 2024-01-24 17:44:05

Este documento descreve como usar o Keepalived com o [HAVIP](#) para criar um cluster principal/secundário de alta disponibilidade na VPC da Tencent Cloud.

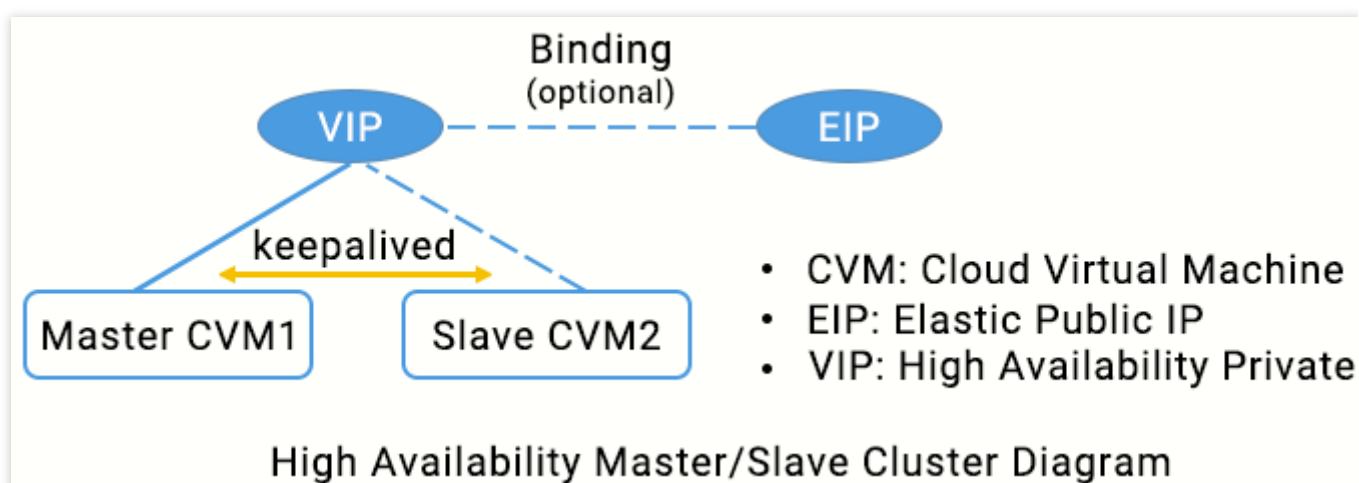
Nota:

Atualmente, o HAVIP está em período de testes beta. Alternar entre os servidores principal/secundário pode levar 10 segundos. Para testá-lo, envie uma solicitação para ser um usuário da versão beta.

Princípio básico

Normalmente, um cluster principal/secundário de alta disponibilidade consiste em dois servidores: um servidor principal ativo e um servidor secundário em espera. Os dois servidores compartilham o mesmo VIP (IP virtual), que é válido apenas para o servidor principal. Quando o servidor principal falhar, o servidor secundário assumirá o VIP para continuar fornecendo serviços. Este modo é amplamente usado na alternância de origem/réplica do MySQL e no acesso à web do Nginx.

O Keepalived é um software de alta disponibilidade baseado em VRRP que pode ser usado para criar um cluster principal/secundário de alta disponibilidade entre CVMs baseadas na VPC. Para usar o Keepalived, primeiro conclua sua configuração no arquivo `keepalived.conf`.



Em redes físicas tradicionais, o status principal/secundário pode ser negociado com o protocolo VRRP do Keepalived. O dispositivo principal envia mensagens ARP gratuitas periodicamente para limpar a tabela MAC ou a tabela ARP do terminal da troca de uplink, a fim de acionar a migração do VIP para o dispositivo principal. Em uma VPC da Tencent Cloud, um cluster principal/secundário de alta disponibilidade também pode ser implementado ao implantar o Keepalived em CVMs, com as seguintes diferenças:

O VIP deve ser um [HAVIP](#) solicitado da Tencent Cloud.

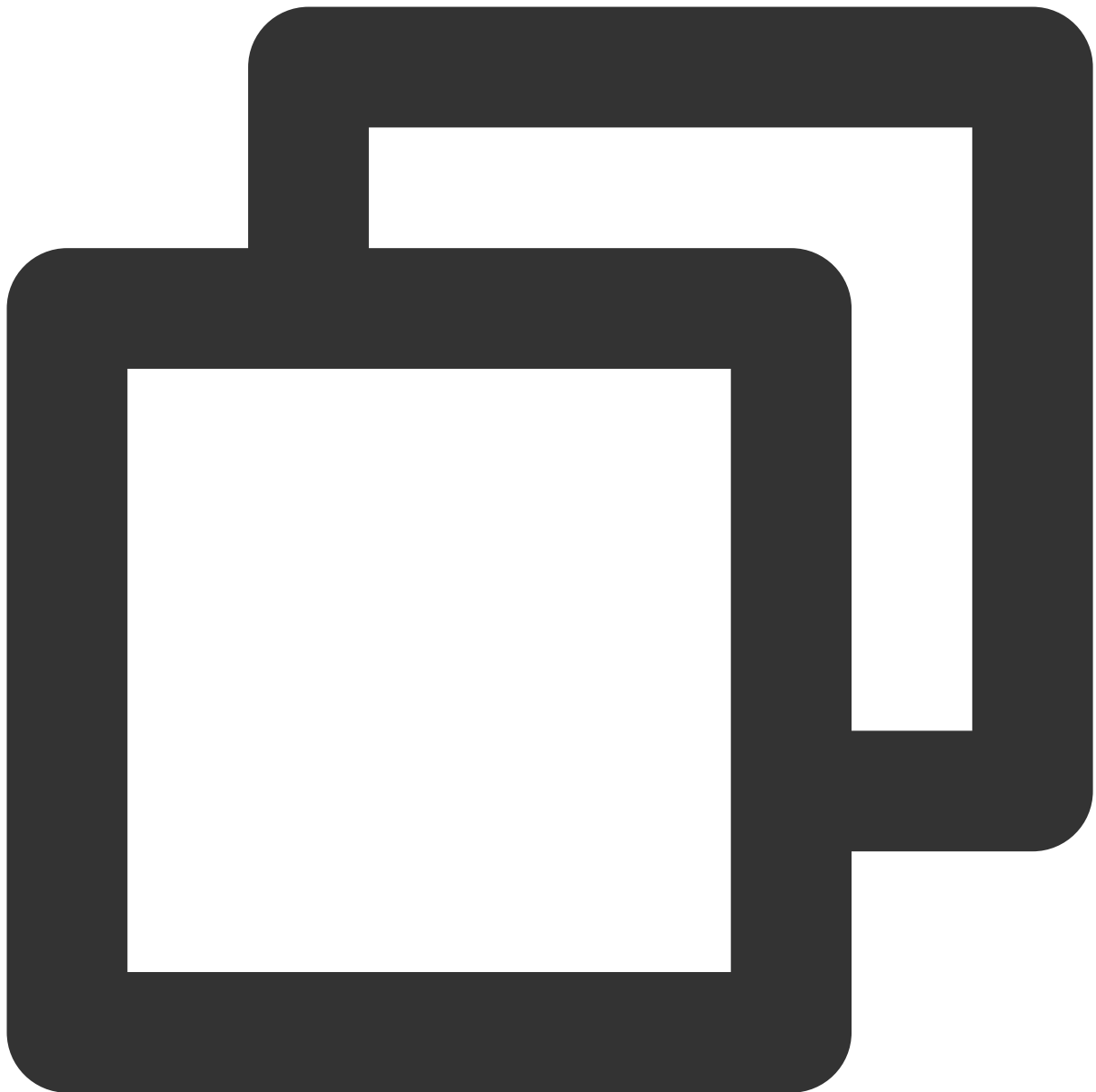
O HAVIP é sensível à sub-rede e só pode ser vinculado a um servidor na mesma sub-rede por meio de anúncio.

Observações

Recomendamos comunicações VRRP em modo unicast.

Recomendamos que você use o Keepalived **1.2.24 ou versões posteriores**.

Certifique-se de que os parâmetros `garp` foram configurados. Como o Keepalived depende de mensagens ARP para atualizar o endereço IP, essas configurações garantem que o dispositivo principal sempre envie mensagens ARP para a comunicação.



```
garp_master_delay 1
garp_master_refresh 5
```

Configure um ID de roteador VRRP exclusivo para cada cluster principal/secundário na VPC.

Não use o modo strict (estrito). Certifique-se de que as configurações “vrrp_strict” foram excluídas.

Controle a quantidade de HAVIPs vinculados a uma única ENI para não ser mais do que cinco. Se você precisar usar vários VIPs, adicione ou modifique `vrrp_garp_master_repeat 1` na seção “global_defs” do arquivo de configuração do Keepalived.

Especifique o parâmetro `adver_int` corretamente para equilibrar a instabilidade antirrede e a velocidade de recuperação de desastres. Se o parâmetro `advert_int` for definido muito pequeno, alternâncias frequentes e **ativo-ativo (partição de rede)** temporários podem ocorrer em caso de instabilidade da rede. Se o parâmetro `advert_int` for definido muito grande, levará muito tempo para que a alternância principal-secundário ocorra após a falha do servidor principal, o que causa uma longa interrupção do serviço. **Avalie completamente o impacto do status ativo-ativo (partição de rede) em seus negócios.**

Defina o parâmetro `interval` no item de execução específico do script `track_script` (como `checkhaproxy`) para um valor maior, evitando o status `FAULT` causado pelo tempo limite de execução do script.

Opcional: esteja ciente do aumento do uso do disco devido à impressão de logs. Isso pode ser resolvido usando o `logrotate` ou outras ferramentas.

Instruções

Atenção:

Este documento usa os ambientes abaixo como exemplo. Substitua por suas configurações reais.

CVM principal: HAVIP-01, 172.16.16.5

CVM secundário: HAVIP-02, 172.16.16.6

HAVIP: 172.16.16.12

EIP: 81.71.14.118

Imagem: CentOS 7.6 64 bits

Etapa 1: solicitar um VIP

1. Faça login no [Console da VPC](#).
2. Selecione **IP and ENI (IP e ENI)** > **HAVIP** na barra lateral esquerda para acessar a página de gerenciamento do HAVIP.
3. Selecione a região relevante na página de gerenciamento do HAVIP e clique em **Apply (Solicitar)**.
4. Na caixa de diálogo pop-up, digite o nome, selecione uma VPC e uma sub-rede para o HAVIP e clique em **OK**.


Nota:


O endereço IP do HAVIP pode ser atribuído automaticamente ou especificado manualmente. Se você optar por inserir um endereço IP, certifique-se de que o endereço IP privado inserido está dentro do intervalo de IP da sub-rede e não é um endereço IP reservado do sistema. Por exemplo, se o intervalo de IP da sub-rede for `10.0.0.0/24`, o endereço IP privado inserido deve estar dentro de `10.0.0.2 - 10.0.0.254`.

Application Highly Available Virtual IP ✕


Name

Region **Guangzhou**

Virtual Private Cloud **vpc-**  ▼

Subnet **subnet-**  ▼

Availability Zone **Guangzhou Zone 1**

Subnet CIDR 

Available IPs **252**

Assignable **1/10**

IP address **Automatic Assignment** ▼

OK

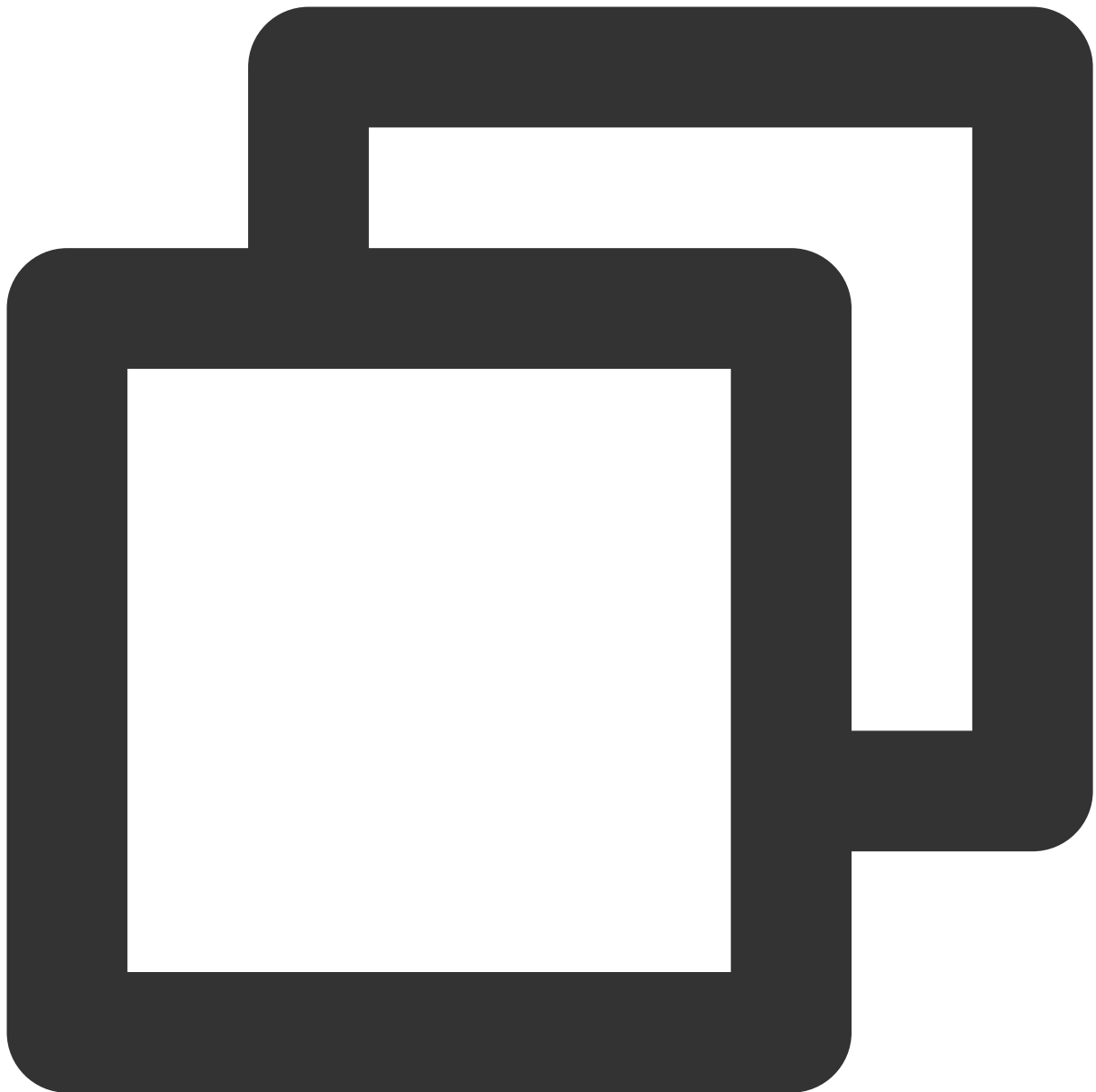
Depois disso, você pode exibir o HAVIP solicitado.

ID/Name	Status	Address	Backend ENI	Server	EIP	Virtual Private Clo...	Subn
havip-1wmd7lx6 test	Not bound with CVM yet		-	-	-	vpc-	subne

Etapa 2: instalar o Keepalived (versão 1.2.24 ou posterior) nos CVMs principal e secundário

Este documento usa o CentOS 7.6 como exemplo para instalar o Keepalived.

1. Execute o comando abaixo para verificar se a versão do Keepalived atende aos requisitos.



```
yum list keepalived
```

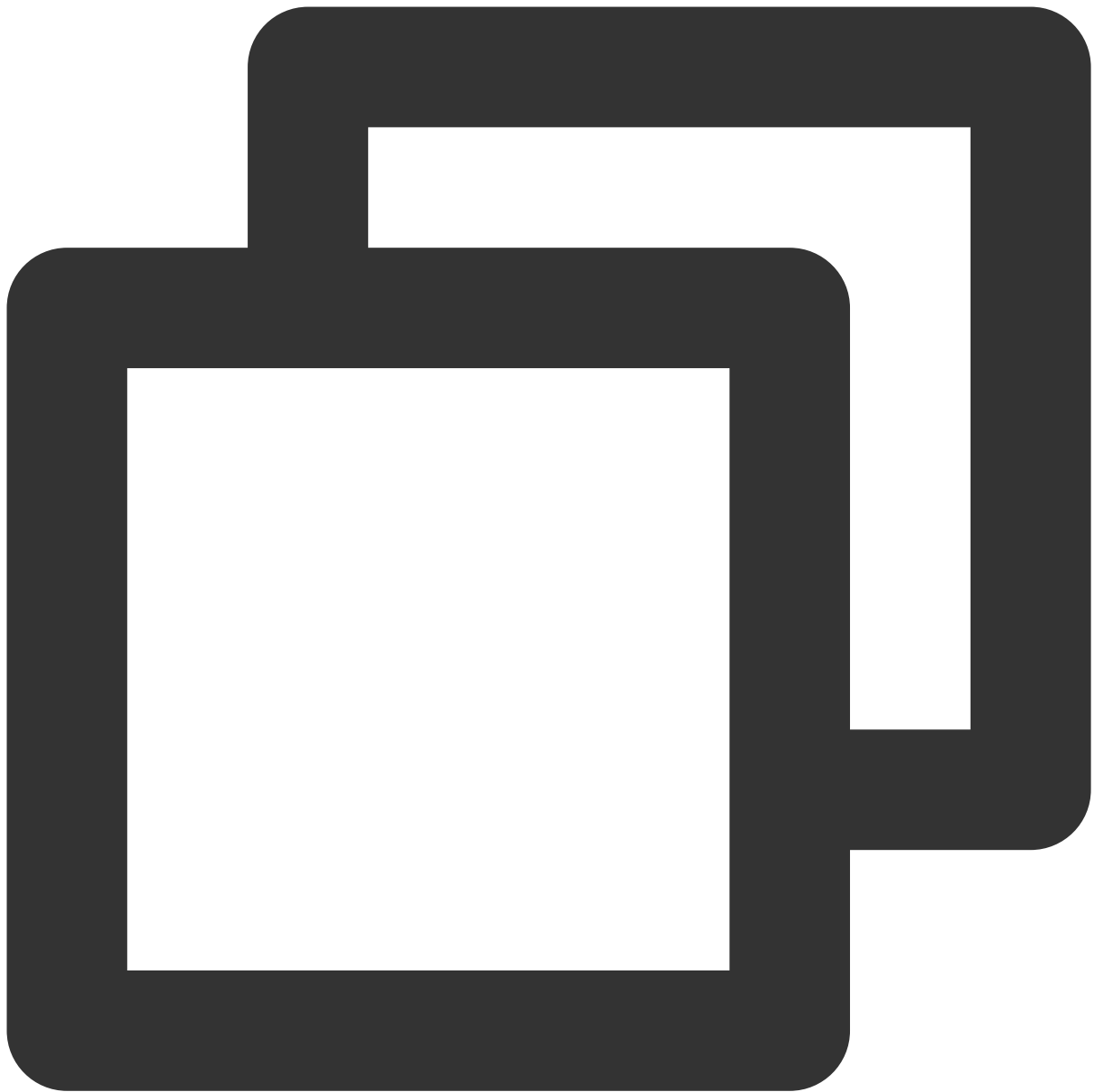
Se sim, prossiga para a [Etapa 2](#)

Caso contrário, prossiga para a [Etapa 3](#)

2. Ins

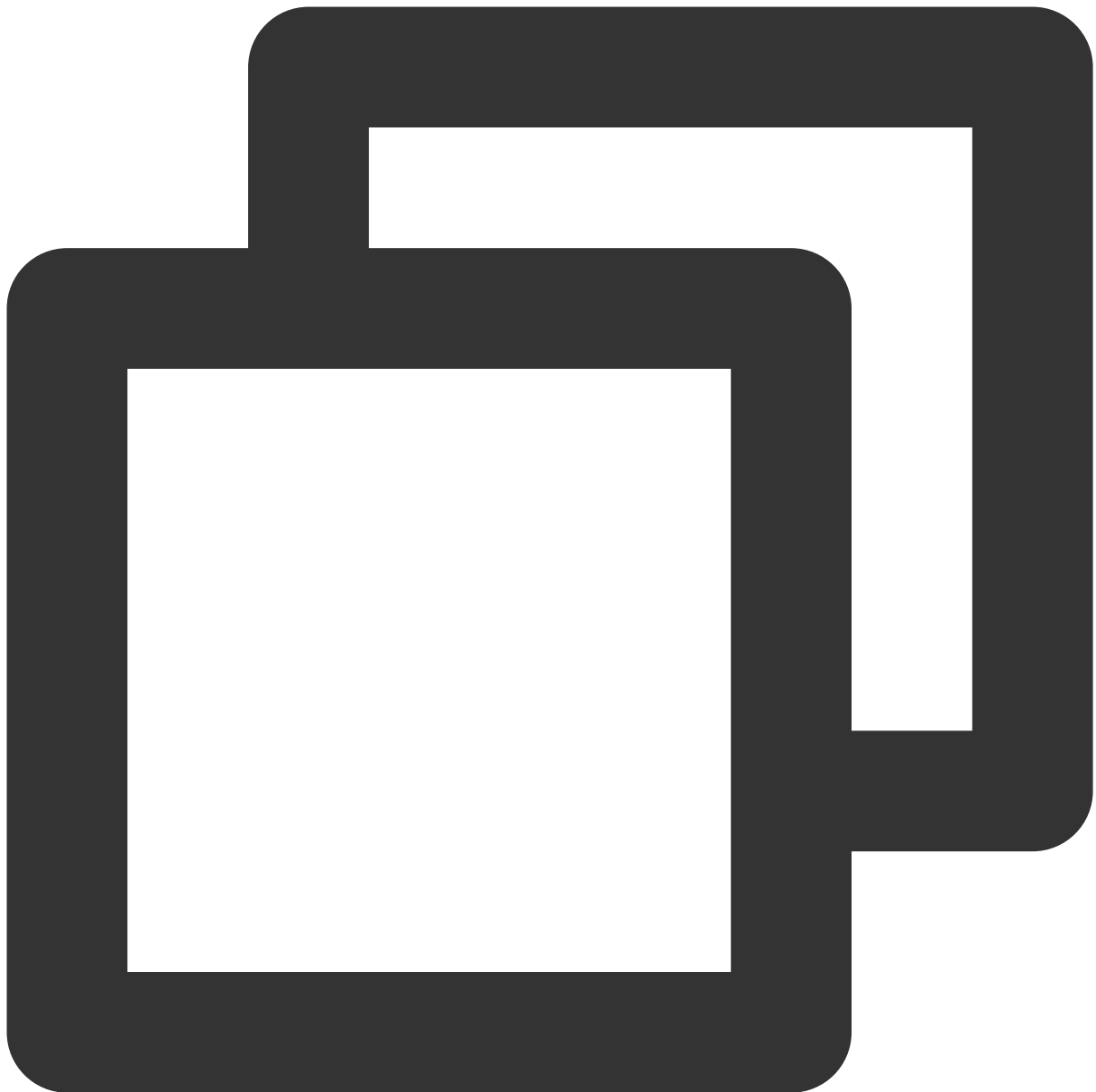
tales o pacote

de software usando o comando `yum`.



```
yum install -y keepalived
```

3. Instale o pacote de software usando o código-fonte.



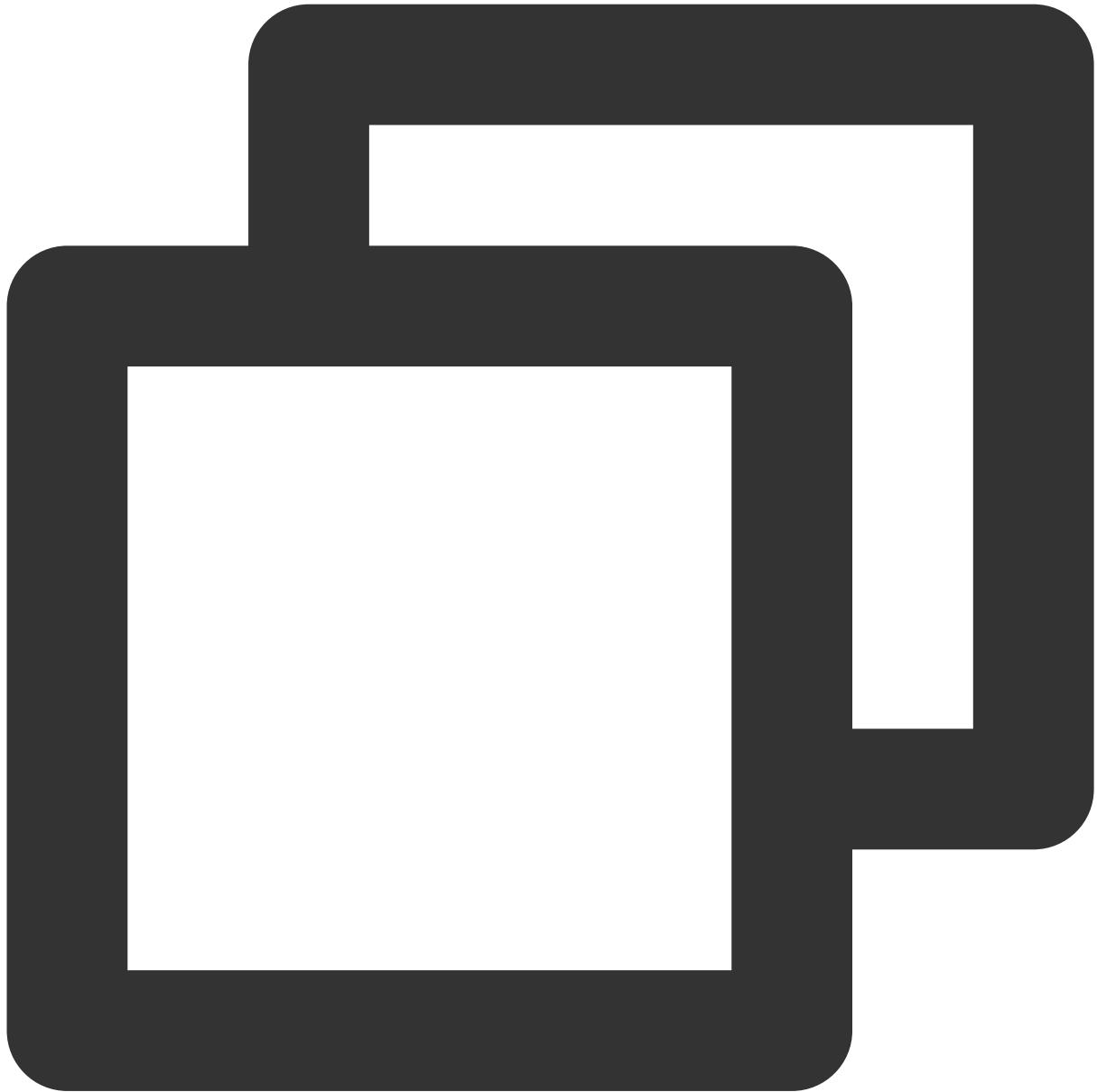
```
tar zxvf keepalived-1.2.24.tar.gz
cd keepalived-1.2.24
./configure --prefix=/
make; make install
chmod +x /etc/init.d/keepalived // Evite a ocorrência de env: /etc/init.d/keepali
```

Etapa 3: configurar o Keepalived e vincular o HAVIP às CVMs principal e secundária

1. Faça login no HAVIP-01 da CVM principal e execute `vim /etc/keepalived/keepalived.conf` para modificar suas configurações.

Nota:

Neste exemplo, o HAVIP-01 e o HAVIP-02 são configurados com o mesmo peso. Ambos estão no status **BACKUP**, com prioridade 100. Isso reduzirá a quantidade de alternâncias causadas pela instabilidade da rede.

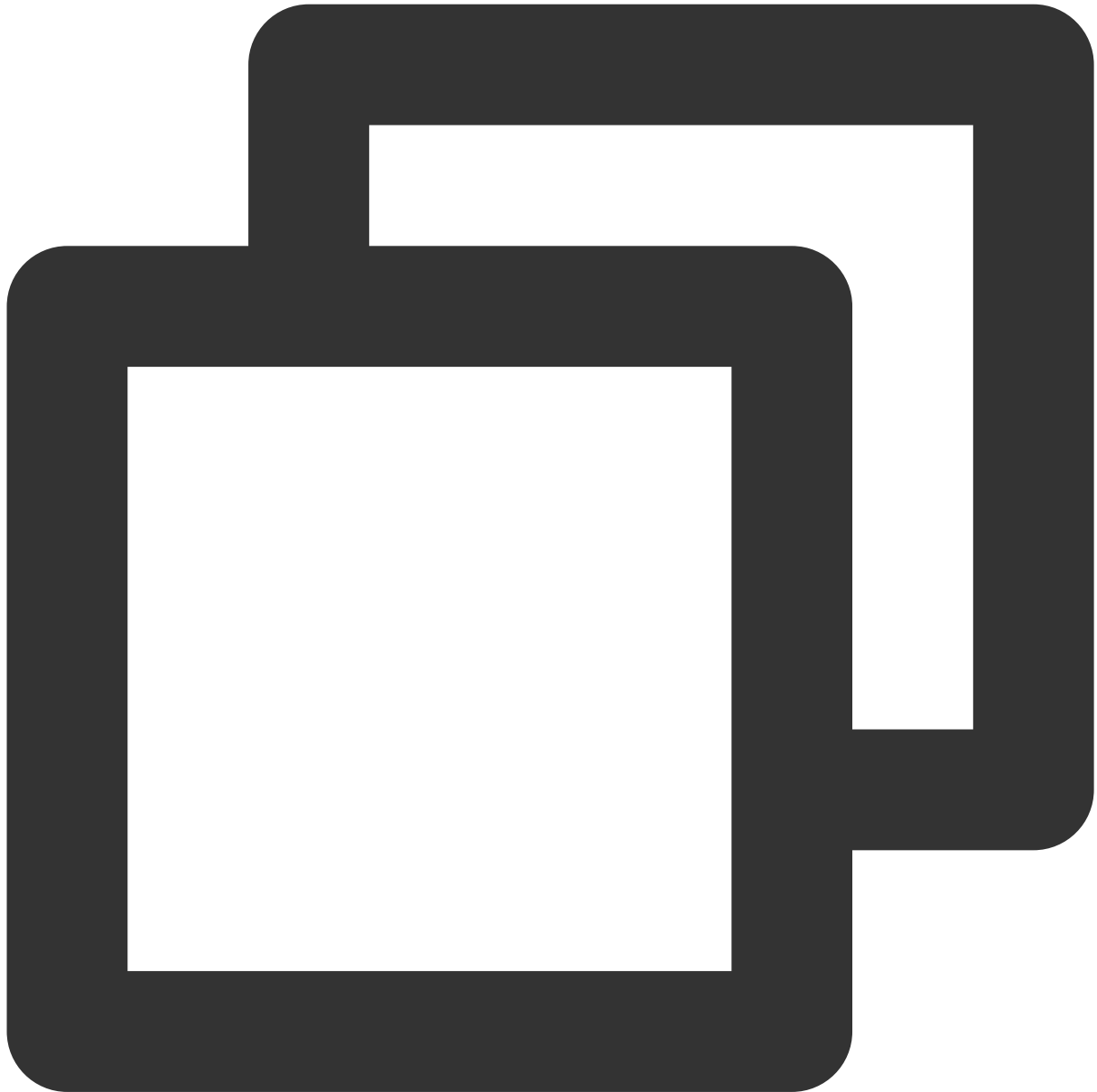


```
! Configuration File for keepalived
global_defs {
    notification_email {
        acassen@firewall.loc
        failover@firewall.loc
        sysadmin@firewall.loc
    }
}
```

```
notification_email_from Alexandre.Cassen@firewall.loc
smtp_server 192.168.200.1
smtp_connect_timeout 30
router_id LVS_DEVEL
vrrp_skip_check_adv_addr
vrrp_garp_interval 0
vrrp_gna_interval 0
}
vrrp_script checkhaproxy
{
    script "/etc/keepalived/do_sth.sh" # Verifique se o processo do serviço é
    interval 5
}
vrrp_instance VI_1 {
# Seleccione os parâmetros adequados para as CVMs principal e secundário.
state BACKUP # Defina o status inicial como `Backup`
    interface eth0 # O ENI (como `eth0`) usado para vincular um VIP
    virtual_router_id 51 # O valor `virtual_router_id` para o cluster
    nopreempt # Modo Non-preempt
    # preempt_delay 10 # Eficaz somente quando `state` é `MASTER`
    priority 100 # Configure o mesmo peso para os dois dispositivos
    advert_int 5
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 172.16.16.5 # Endereço IP privado do dispositivo local
    unicast_peer{
        172.16.16.6 # Endereço IP do dispositivo de par
    }
    virtual_ipaddress {
        172.16.16.12 # HAVIP
    }
    notify_master "/etc/keepalived/notify_action.sh MASTER"
    notify_backup "/etc/keepalived/notify_action.sh BACKUP"
    notify_fault "/etc/keepalived/notify_action.sh FAULT"
    notify_stop "/etc/keepalived/notify_action.sh STOP"
    garp_master_delay 1 # Quanto tempo levará para que o cache de ARP possa s
    garp_master_refresh 5 # Intervalo de tempo entre o qual o nó principal env

    track_interface {
        eth0 # ENI vinculado ao VIP, como `eth0`
    }
    track_script {
        checkhaproxy
    }
}
```

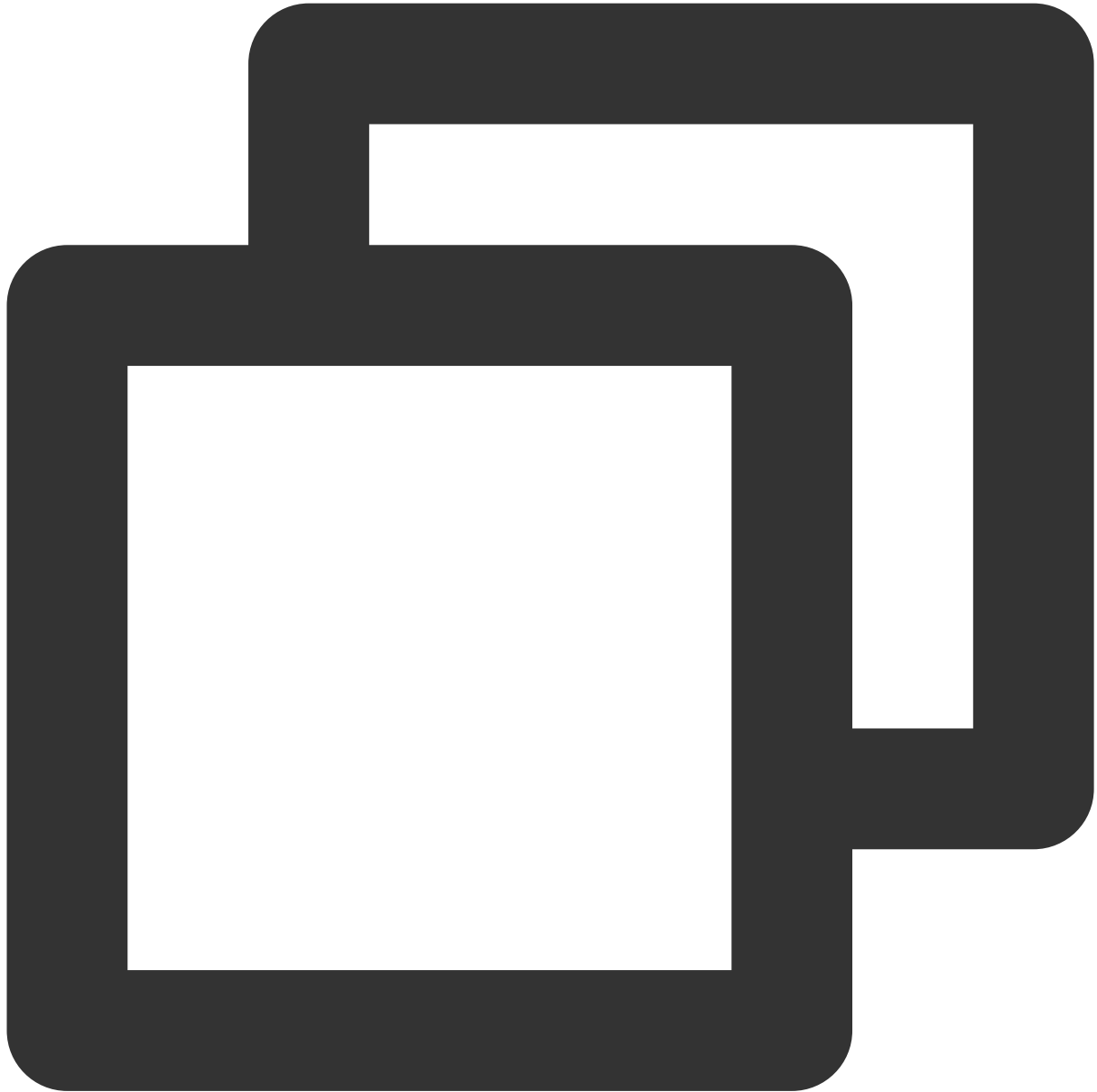

2. Pressione **Esc** para sair do modo de edição e digite **:wq!** para salvar e fechar o arquivo.
3. Faça login no HAVIP-02 da CVM secundário e execute `vim /etc/keepalived/keepalived.conf` para modificar suas configurações.



```
! Configuration File for keepalived
global_defs {
    notification_email {
        acassen@firewall.loc
        failover@firewall.loc
        sysadmin@firewall.loc
```

```
}
notification_email_from Alexandre.Cassen@firewall.loc
smtp_server 192.168.200.1
smtp_connect_timeout 30
router_id LVS_DEVEL
vrrp_skip_check_adv_addr
vrrp_garp_interval 0
vrrp_gna_interval 0
}
vrrp_script checkhaproxy
{
    script "/etc/keepalived/do_sth.sh"
    interval 5
}
vrrp_instance VI_1 {
# Seleccione os parâmetros adequados para as CVMs principal e secundário.
state BACKUP          #Defina o status inicial como `Backup`
    interface eth0      #O ENI (tais como `eth0`) usado para vincular um VIP
    virtual_router_id 51  #O valor `virtual_router_id` para o cluster
    nopreempt           #Modo Non-preempt
    # preempt_delay 10   #Eficaz apenas quando "state MASTER"
    priority 100        # Configure o mesmo peso para os dois dispositivos
    advert_int 5
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 172.16.16.6 #IP privado do dispositivo local
    unicast_peer{
        172.16.16.5           #Endereço IP do dispositivo de par
    }
    virtual_ipaddress {
        172.16.16.12          #HAVIP
    }
    notify_master "/etc/keepalived/notify_action.sh MASTER"
    notify_backup "/etc/keepalived/notify_action.sh BACKUP"
    notify_fault  "/etc/keepalived/notify_action.sh FAULT"
    notify_stop   "/etc/keepalived/notify_action.sh STOP"
    garp_master_delay 1    # Quanto tempo levará para que o cache de ARP possa ser
    garp_master_refresh 5  #Intervalo de tempo entre o qual o nó principal envia m
    track_interface {
        eth0                # ENI (omo `eth0`) que vincula um VIP
    }
    track_script {
        checkhaproxy
    }
}
}
```

4. Pressione **Esc** para sair do modo de edição e digite **:wq!** para salvar e fechar o arquivo.
5. Reinicie o Keepalived para que a configuração tenha efeito.



```
systemctl start keepalived
```

6. Verifique o status principal/secundário das duas CVMs, e confirme se ambos têm o HAVIP vinculado corretamente.

Nota:

Neste exemplo, o HAVIP-01 inicia o Keepalived primeiro e normalmente servirá como o nó principal.

Faça login no console do [HAVIP](#). Você verá que o HAVIP está vinculado ao HAVIP-01 da CVM principal, conforme mostrado abaixo.

ID/Name	Status	Address	Backend ENI	Server	EIP	Virtual Private Clo...	Subne
ha- test			-	ins-23u5qn9l HAVIP-01	-		

Etapa 4: vincular um EIP ao HAVIP (opcional)

1. Faça login no console do [HAVIP](#), localize o HAVIP solicitado na [Etapa 1](#) e clique em **Bind (Vincular)**.

ID/Name	Status	Address	Backend ENI	Server	EIP	Virtual Private Clo...	Subne
havip- test			-	-	-	vpc	subne

2. Na caixa de diálogo pop-up, selecione o EIP a ser vinculado e clique em **OK**. Se nenhum EIP estiver disponível, primeiro acesse o console do [EIP](#) para solicitar.

Bind Elastic IP

If the HAVIP is not bound with an instance, the EIP bound to this HAVIP will be in idle state, billed by \$0.03/hr. An idle fee occurs. Please configure the highly availability application correctly to ensure the binding is successful.

Please select the EIP to be bound with "Private IP" 's EIP

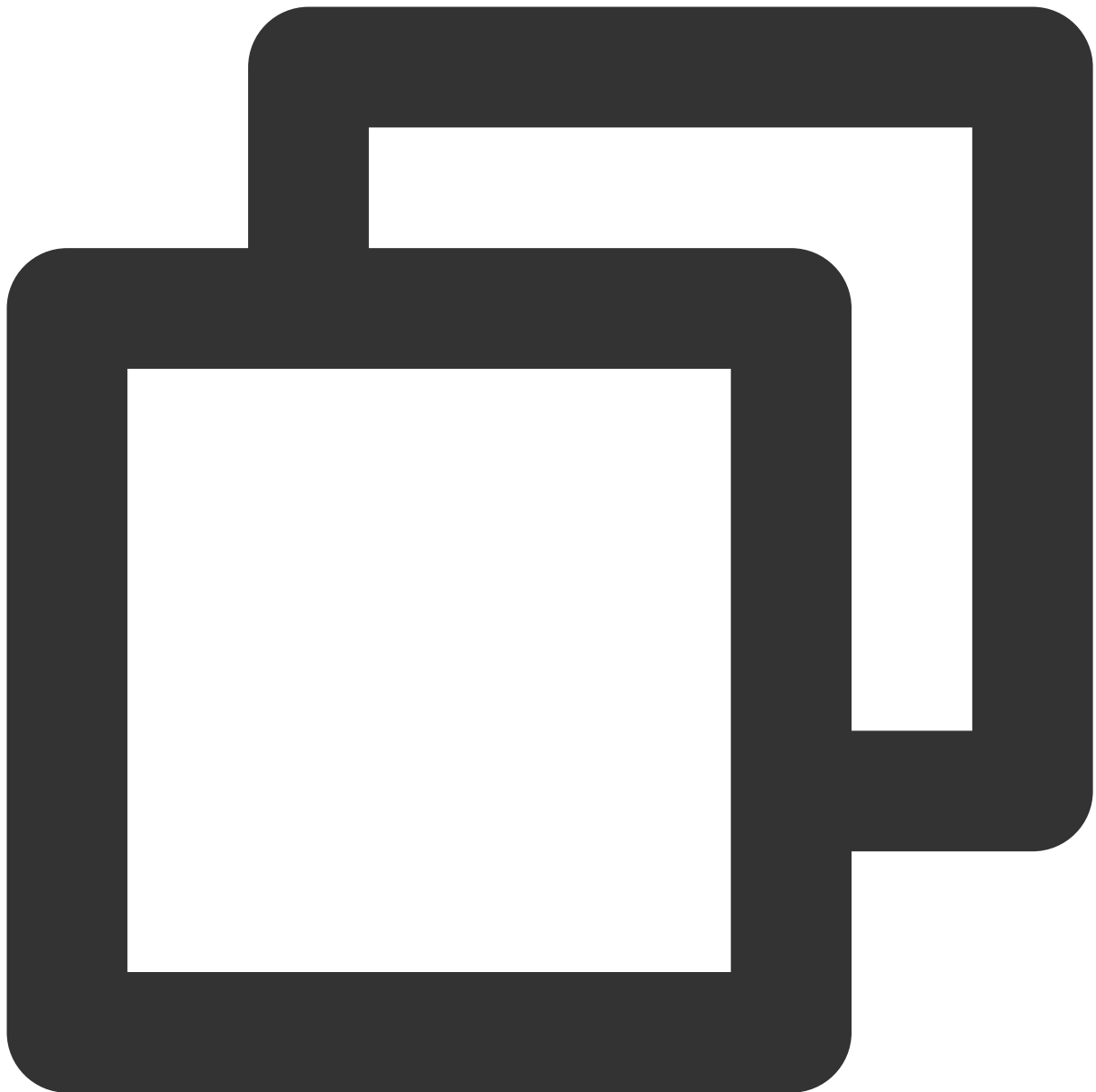
Please enter the keyword

IP address	Status
<input type="radio"/>	Bound

Etapa 5: usar o notify_action.sh para registro em log simples (opcional)

Os logs principais do Keepalived ainda são registrados em `/var/log/message`, e você pode adicionar o script `notify` para registro em log simples.

1. Faça login na CVM e execute o comando `vim /etc/keepalived/notify_action.sh` para adicionar o seguinte script `notify_action.sh`.



```
#!/bin/bash
#/etc/keepalived/notify_action.sh
log_file=/var/log/keepalived.log
log_write()
{
    echo "[`date '+%Y-%m-%d %T`] $1" >> $log_file
}
[ ! -d /var/keepalived/ ] && mkdir -p /var/keepalived/

case "$1" in
    "MASTER" )
```

```
    echo -n "$1" > /var/keepalived/state
    log_write " notify_master"
    echo -n "0" /var/keepalived/vip_check_failed_count
    ;;
"BACKUP" )
    echo -n "$1" > /var/keepalived/state
    log_write " notify_backup"
    ;;
"FAULT" )
    echo -n "$1" > /var/keepalived/state
    log_write " notify_fault"
    ;;
"STOP" )
    echo -n "$1" > /var/keepalived/state
    log_write " notify_stop"
    ;;
*)
    log_write "notify_action.sh: STATE ERROR!!!"
    ;;
esac
```

2. Execute o comando `chmod a+x /etc/keepalived/notify_action.sh` para modificar a permissão do script.

Etapa 6: verificar se o VIP e o IP público são alternados normalmente durante a alternância principal/secundária

Simule a falha da CVM reiniciando o processo do Keepalived ou reiniciando a CVM para verificar se o VIP pode ser migrado.

Se a alternância principal/secundária tiver êxito, a CVM secundário se tornará o servidor vinculado ao HAVIP no console.

Você também pode executar ping em um VIP de dentro da VPC para verificar o lapso de tempo desde a interrupção da rede até a recuperação. Cada alternância pode causar uma interrupção por cerca de 4 segundos. Se você executar ping no EIP vinculado ao HAVIP em uma rede pública, o resultado será o mesmo.

Execute o comando `ip addr show` para verificar se o HAVIP está vinculado à ENI principal.

Criação de um banco de dados de alta disponibilidade usando HAVIP + cluster de failover do Windows Server

Last updated : 2024-01-24 17:44:04

1. Criação de HAVIPs

Faça login no [console do VPC](#) e crie um HAVIP. Para obter instruções detalhadas, consulte [Criação de HAVIPs](#).

2. Vinculação e configuração

A configuração é igual à do modo tradicional. O servidor de back-end declara e negocia no dispositivo que será vinculado ao HAVIP criado. Basta especificar o endereço IP virtual no arquivo de configuração como HAVIP.

No gerenciador de cluster, adicione o HAVIP que acabou de ser criado.

3. Verificação

Depois que a configuração for concluída, alterne diretamente os nós para teste.

Em situações normais, você verá que a rede se recupera após uma breve interrupção (nenhuma interrupção será notada se a alternância for rápida o suficiente), e os serviços online não serão afetados.

Comunicação principal/secundária de nuvem híbrida (DC e VPN)

Last updated : 2024-01-24 17:44:05

Se os seus negócios estiverem implantados em um IDC local e em uma VPC da Tencent Cloud, você poderá conectá-los pelo Direct Connect ou pela VPN. Para melhorar a disponibilidade dos negócios, configure o DC e a VPN Connections como a ligação principal e secundária para comunicação redundante. Este documento orienta você sobre como configurar o DC e a VPN Connection como ligações principal/secundária para conectar seu IDC à nuvem.

Nota:

Atualmente, a funcionalidade de prioridade de rota está em teste beta. Para testá-la, [envie um tíquete](#).

O próximo tipo de salto determina a prioridade da rota na tabela de rotas da VPC. Por padrão, a prioridade de rota de alta para baixa é: CCN, gateway do Direct Connect, VPN Gateway e outros.

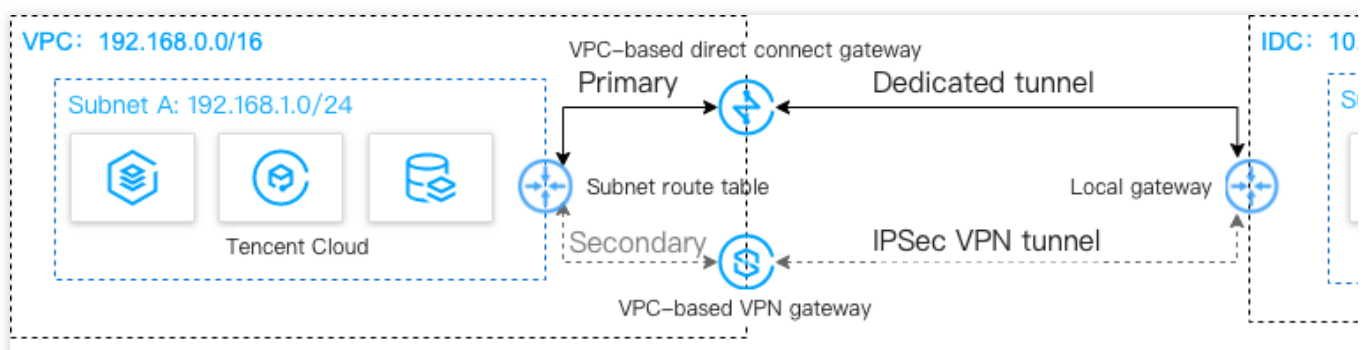
Atualmente, não é possível ajustar a prioridade da rota no console. Se precisar alterá-la, [envie um tíquete](#).

Cenários

Você implantou negócios em uma VPC da Tencent Cloud e em um IDC. Para interconectá-los, você precisa configurar os serviços de conexão de rede para comunicações de alta disponibilidade da seguinte forma:

Direct Connect (principal): conecta o IDC local a um gateway do Direct Connect baseado na VPC por meio de uma conexão. Quando a ligação da conexão estiver normal, todo o tráfego de dados entre o IDC e a VPC será encaminhado por meio da conexão.

VPN Connection (secundário): estabelece um túnel VPN IPsec para interconectar o IDC local e a VPC da Tencent Cloud. Quando a ligação de conexão falhar, o tráfego será encaminhado usando essa ligação para garantir a disponibilidade dos negócios.



Pré-requisitos

O seu dispositivo de gateway do IDC local deve permitir a funcionalidade VPN IPsec, e pode atuar como um gateway do cliente para criar um túnel VPN com a VPN Gateway.

O dispositivo de gateway do IDC foi configurado com um endereço IP estático.

Dados de exemplo e configuração:

Item de configuração		Valor de exemplo	
Rede	Informações da VPC	Bloco CIDR da sub-rede	192.168.1.0/24
		IP público da VPN Gateway	203.xx.xx.82
	Informações do IDC	Bloco CIDR da sub-rede	10.0.1.0/24
		IP público do gateway	202.xx.xx.5

Etapas

1. [Conectar o IDC à VPC pelo Direct Connect](#)
2. [Conectar o IDC à VPC pela VPN Connection](#)
3. [Configurar sondas de rede](#)
4. [Configurar uma política de alarme](#)
5. [Alternar entre as rotas principal e secundárias](#)

Instruções

Etapa 1: conectar o IDC à VPC pelo Direct Connect

1. Faça login no console do Direct Connect, abra os [Dedicated Tunnels \(Túneis dedicados\)](#) e clique em **Connections (Conexões)** na barra lateral esquerda para criar uma conexão.
2. Faça login no [Console da VPC](#) e clique em **Direct Connect Gateway (Gateway do Direct Connect)** na barra lateral esquerda. Clique em **+New (+Novo)** para criar um gateway padrão do Direct Connect para o qual a **Associate Network (Rede associada)** seja o **VPC**. Se o intervalo de IP do IDC entrar em conflito com o intervalo de IP da VPC, selecione o **NAT Type (Tipo de NAT)**.
3. Acesse a página **Dedicated Tunnels (Túneis dedicados)** e clique em **+New (+Novo)** para criar um túnel dedicado. Insira o nome do túnel, selecione o tipo de conexão e a instância de gateway do Direct Connect recém-criada. Configure os endereços IP na Tencent Cloud e no IDC, selecione a rota estática e insira o intervalo IP do CPE.

Após a conclusão da configuração, clique em **Download configuration guide (Baixar o guia de configurações)** e conclua as configurações do dispositivo IDC conforme as instruções do guia.

4. Na tabela de rotas associada à sub-rede da VPC para a comunicação, configure uma política de roteamento com o gateway do Direct Connect como o próximo salto e o intervalo de IP do IDC como o destino.

Nota:

Para obter as configurações detalhadas, consulte [Introdução](#).

Etapa 2: conectar o IDC à VPC por meio de uma VPN Connection

1. Faça login no [Console da VPN Gateway](#) e clique em **+New (+Novo)** para criar uma VPN Gateway para o qual a **Associate Network (Rede associada)** seja uma **Virtual Private Cloud**.

2. Clique em **Customer Gateway (Gateway do cliente)** na barra lateral esquerda, e clique em **+New (+Novo)** para configurar um gateway do cliente (um objeto lógico da VPN Gateway no IDC). Insira o endereço IP público da VPN Gateway no IDC, como `202.xx.xx.5`.

3. Clique em **VPN Tunnel (Túnel VPN)** na barra lateral esquerda, e clique em **+New (+Novo)** para concluir as configurações, como política SPD, IKE e IPsec.

4. Configure o mesmo túnel VPN que a Etapa 3 no dispositivo de gateway local do IDC, para garantir uma conexão normal.

5. Na tabela de rotas associada à sub-rede da VPC para a comunicação, configure uma política de roteamento com a VPN Gateway como o próximo salto e o intervalo de IP do IDC como o destino.

Nota:

Para obter instruções detalhadas, consulte [Conexão da VPC ao IDC \(Tabela de rotas\)](#).

Etapa 3: configurar sondas de rede

Nota:

Após as duas primeiras etapas, há duas rotas da VPC para o IDC. Ou seja, tanto o gateway do Direct Connect quanto a VPN Gateway agem como o próximo salto. Por padrão, a rota do gateway do Direct Connect tem uma prioridade mais alta, tornando-a o caminho principal, e a VPN Gateway, o caminho secundário.

Para acompanhar a qualidade da conexão principal/secundária, configure duas sondas de rede separadamente, a fim de monitorar as principais métricas, como latência e taxa de perda de pacotes, e verifique a disponibilidade das rotas principal/secundária.

1. Faça login no [Console da VPC](#).

2. Clique em **+New (+Novo)** para criar uma sonda de rede. Insira um nome e um IP de destino, selecione uma VPC e uma sub-rede, e defina **Source Next Hop (Próximo salto da fonte)** como o gateway do Direct Connect.

3. Repita a [Etapa 2](#) e defina **Source Next Hop (Próximo salto da fonte)** como a VPN Gateway. Após a conclusão da configuração, você pode verificar a latência e a taxa de perda de pacotes da rede sondada do gateway do Direct Connect e do VPN Connection.

Nota:

Para obter as configurações detalhadas, consulte [Sonda de rede](#).

Etapa 4: configurar uma política de alarme

Você pode configurar uma política de alarme para ligações. Quando uma ligação tem uma exceção, são enviadas notificações de alarme a você automaticamente por e-mail e mensagem SMS, alertando-o antecipadamente sobre os riscos.

1. Faça login no console do CM e acesse a página [Alarm Policy \(Política de alarme\)](#).
2. Clique em **Create (Criar)**. Insira o nome da política, selecione VPC/Network Probe (VPC/Sonda de rede) para o tipo de política, especifique as instâncias da sonda de rede como o objeto de alarme, e configure as condições de disparo, as notificações de alarme e outras informações. Depois, clique em **Complete (Concluir)**.

Etapa 5: alternar entre as rotas principal/secundária

Após receber os alarmes de exceção sobre o gateway do Direct Connect, você precisa desativar manualmente a rota principal e encaminhar o tráfego para a VPN Gateway da rota secundária.

1. Faça login no console da VPC e acesse a página [Route Tables \(Tabelas de rotas\)](#).
2. Localize a tabela de rotas associada à sub-rede da VPC para a comunicação, clique em **ID/Name (ID/Nome)** para acessar sua página de detalhes. Clique em



para desativar a rota principal com a CCN como o próximo salto. Em seguida, o tráfego da VPC destinado ao IDC será encaminhado para a VPN Gateway, em vez do gateway do Direct Connect.

Comunicação principal/secundária de nuvem híbrida (CCN e VPN)

Last updated : 2024-01-24 17:44:04

Se os seus negócios estiverem implantados em um IDC local e em uma VPC da Tencent Cloud, você poderá conectá-los pela Cloud Connect Network (CCN) ou pela VPN. Para melhorar a disponibilidade dos negócios, configure a CCN e a VPN Connections como a ligação principal e secundária para comunicação redundante. Este documento orienta você sobre como configurar a CCN e a VPN Connection como ligações principal/secundária para conectar seu IDC à nuvem.

Nota:

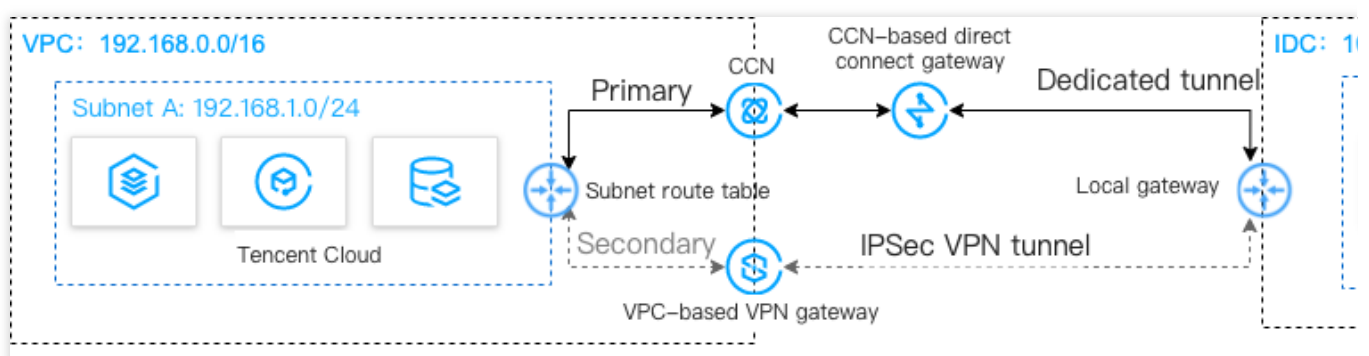
Atualmente, a funcionalidade de prioridade de rota está em teste beta. Para testá-la, [envie um tíquete](#).

Cenários

Suponha que você tenha implantado os seus negócios na VPC da Tencent Cloud e em um IDC. Para interconectá-los, você precisa configurar os serviços de conexão de rede para comunicações de alta disponibilidade da seguinte forma:

CCN (principal): conecta o IDC local a um gateway do Direct Connect baseado na CCN por meio de uma conexão física, e adiciona o gateway do Direct Connect e a VPC a uma CCN para habilitar a interconexão. Quando a ligação da conexão estiver normal, todo o tráfego de dados entre o IDC e a VPC será encaminhado pela CCN por meio da conexão física.

VPN Connection (secundário): estabelece um túnel VPN IPsec para interconectar o IDC local e a VPC da Tencent Cloud. Quando a ligação de conexão falhar, o tráfego será encaminhado usando essa ligação para garantir a disponibilidade dos negócios.



Pré-requisitos

O seu dispositivo de gateway do IDC local deve permitir a funcionalidade VPN IPsec e pode atuar como um gateway do cliente para criar um túnel VPN com a VPN Gateway.

O dispositivo de gateway do IDC foi configurado com um endereço IP estático.

Dados de exemplo e configuração:

Item de configuração			Valor de exemplo
Rede	Informações da VPC	Bloco CIDR da sub-rede	192.168.1.0/24
		IP público da VPN Gateway	203.xx.xx.82
	Informações do IDC	Bloco CIDR da sub-rede	10.0.1.0/24
		IP público do gateway	202.xx.xx.5

Etapas

1. [Configurar uma instância do Direct Connect](#)
2. [Configurar uma VPN Connection](#)
3. [Configurar sondas de rede](#)
4. [Configurar uma política de alarme](#)
5. [Alternar entre as rotas principal e secundárias](#)

Instruções

Etapa 1: conectar o IDC à VPC por meio da CCN

1. Faça login no [Console do Direct Connect](#) e clique em **Connections (Conexões)** na barra lateral esquerda para criar uma conexão.
2. Faça login no [Console da VPC](#) e clique em **Direct Connect Gateway (Gateway do Direct Connect)** na barra lateral esquerda. Clique em **+New (+Novo)** para criar um gateway do Direct Connect para o qual a **Associate Network (Rede associada)** seja a **CCN**.
3. Clique no **ID/Name (ID/Nome)** do gateway do Direct Connect recém-criado para acessar sua página de detalhes. Selecione a guia **IDC IP Range (Intervalo de IP do IDC)** para inserir o intervalo de IP do IDC, como `10.0.1.0/24`.
4. Acesse a página do [CCN](#) e clique em **+New (+Novo)** para criar uma instância do CCN.
5. Acesse a página [Dedicated Tunnels \(Túneis dedicados\)](#) e clique em **+New (+Novo)** para criar um túnel dedicado para conectar o gateway do Direct Connect baseado no CCN. Insira o nome do túnel, selecione **CCN** para **Access Network (Rede de acesso)** e, em seguida, selecione a instância de gateway do Direct Connect baseada no CCN

criada anteriormente. Configure os endereços IP na Tencent Cloud e no IDC, e selecione a rota BGP. Após a conclusão da configuração, clique em **Download configuration guide (Baixar o guia de configurações)** e conclua as configurações do dispositivo IDC conforme as instruções do guia.

6. Associe a VPC e o gateway do Direct Connect baseado no CCN à instância da CCN para interconectar a VPC e o IDC.

Nota:

Para obter instruções detalhadas, consulte [Migração do IDC para a nuvem por meio da CCN](#).

Etapa 2: conectar o IDC à VPC por meio de uma VPN Connection

1. Faça login no [Console da VPN Gateway](#) e clique em **+New (+Novo)** para criar uma VPN Gateway para o qual a **Associate Network (Rede associada)** seja uma **Virtual Private Cloud**.
2. Clique em **Customer Gateway (Gateway do cliente)** na barra lateral esquerda e clique em **+New (+Novo)** para configurar um gateway do cliente (um objeto lógico da VPN Gateway no IDC). Insira o endereço IP público da VPN Gateway no IDC, como `202.xx.xx.5`.
3. Clique em **VPN Tunnel (Túnel VPN)** na barra lateral esquerda e clique em **+New (+Novo)** para concluir as configurações, como política SPD, IKE e IPsec.
4. Configure o mesmo túnel VPN que a [Etapa 3](#) no dispositivo de gateway local do IDC para garantir uma conexão normal.
5. Na tabela de rotas associada à sub-rede da VPC para comunicação, configure uma política de roteamento com a VPN Gateway como o próximo salto e o intervalo de IP do IDC como o destino.

Nota:

Para obter as configurações detalhadas de VPN Gateways em diferentes versões,

Para uma VPN Gateway v1.0 e v2.0, consulte [Conexão da VPC ao IDC \(Política SPD\)](#).

Para uma VPN Gateway v3.0, consulte [Conexão da VPC ao IDC \(Tabela de rotas\)](#).

Etapa 3: configurar sondas de rede

Nota:

Após as duas primeiras etapas, há duas rotas da VPC para o IDC. Ou seja, tanto a CCN quanto a VPN Gateway agem como o próximo salto. A rota da CCN tem uma prioridade mais alta, tornando-a o caminho principal e a VPN Gateway, o caminho secundário.

Para acompanhar a qualidade da conexão principal/secundária, configure duas sondas de rede separadamente para monitorar as principais métricas, como latência e taxa de perda de pacotes, e verifique a disponibilidade de rotas principal/secundária.

1. Acesse a página [Network Probe \(Sonda de rede\)](#) no console da VPC.
2. Clique em **+New (+Novo)** para criar uma sonda de rede. Insira um nome e um IP de destino, selecione uma VPC e uma sub-rede, e defina **Source Next Hop (Próximo salto da fonte)** como a CCN.
3. Repita a [Etapa 2](#) e defina **Source Next Hop (Próximo salto da fonte)** como a VPN Gateway. Após a conclusão da configuração, você pode verificar a latência da rede sondada e a taxa de perda de pacotes da CCN e da VPN

Connection.

Nota:

Para obter as configurações detalhadas, consulte [Sonda de rede](#).

Etapa 4: configurar uma política de alarme

Você pode configurar uma política de alarme para ligações. Quando uma ligação tem uma exceção, são enviadas notificações de alarme a você automaticamente por e-mail e mensagem SMS, alertando-o antecipadamente sobre os riscos.

1. Faça login no console da CM e acesse a página [Alarm Policy \(Política de alarme\)](#).
2. Clique em **Create (Criar)**. Insira o nome da política, selecione VPC/Network Probe (VPC/Sonda de rede) para o tipo de política, especifique as instâncias da sonda de rede como o objeto de alarme e configure as condições de disparo, as notificações de alarme e outras informações. Depois, clique em **Complete (Concluir)**.

Etapa 5: alternar entre as rotas principal/secundária

Após receber um alarme de exceção de rede da CCN, você precisa desativar manualmente a rota principal e encaminhar o tráfego para a VPN Gateway da rota secundária.

1. Faça login no console da VPC e acesse a página [Route Tables \(Tabelas de rotas\)](#).
2. Localize a tabela de rotas associada à sub-rede da VPC para comunicação, clique em **ID/Name (ID/Nome)** para acessar sua página de detalhes. Clique em



para desativar a rota principal com a CCN como o próximo salto. Em seguida, o tráfego da VPC destinado ao IDC será encaminhado para a VPN Gateway, em vez da CCN.