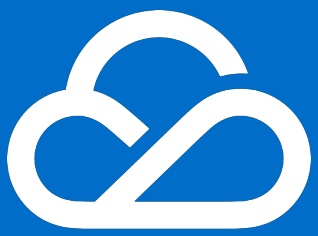
腾讯云容器服务

购买指导

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

购买指导

购买容器集群

购买集群配额限制

针对每个用户，腾讯云容器服务集群每个地域分配了固定配额。

1）每个用户每个地域可

购买的容器集群配额如下,如果您需要更多的集群数量，可通过配额申请工单提出配额申请。

北京	上海	广州
5	5	5

2）每个集群下最多拥有的节点数量为20个,若您的集群需要更多的主机，可通过配额申请工单提出配额申请。

3）腾讯云容器服务生产的云主机同时需满足云服务的购买限制，点击查看详情。

容器及节点网络设置

设置集群和节点网络

集群网络与容器网络是集群的基本属性。通过设置集群网络和容器网络可以规划集群的网络划分。

- 集群网络：将为集群内主机分配在节点网络地址范围内的 IP 地址，您可以选择私有网络中的子网用于集群的节点网络，更多私有网络介绍可看 私有网络和子网 。
- 容器网络：将为集群内容器分配在容器网络地址范围内的 IP 地址，您可以自定义三大私有网段作为容器网络，根据您选择的集群内服务数量的上限，自动分配适当大小的CIDR段用于kubernetes service，同时容器网络自动为集群内每台云主机分配一个24位的网段用于该主机分配Pod的IP地址。

集群网络与容器网络的关系

- 集群网络和容器网络网段不能冲突
- 同一VPC内，不同集群的容器网络网段不能冲突
- 容器网络和 VPC 路由冲突时，优先在容器网络内转发

集群网络与腾讯云其他资源通信

- 集群内容器与容器之间互通
- 集群内容器与节点直接互通
- 集群内容器与 云数据库CDB、云存储Redis、云缓存Memcached 等资源同一VPC下内网互通

容器节点硬盘设置

说明

容器服务创建集群和扩展集群时可设置容器节点的系统盘的类型和大小、数据盘的类型和大小，可选择不同类型的硬盘来满足您不同业务的要求。

建议

1.容器的目录存储在系统盘中，建议您创建50G的系统盘。

2.如果您对系统盘有要求，可以在集群初始化时，将docker的目录自行调整到数据盘上。

容器服务节点公网IP说明

如果对业务安全有要求不希望业务直接暴露到公网，同时又希望访问公网，您可以使用腾讯云 NAT网关 。下文将介绍如何使用 NAT 网关来访问公网。

公网 IP

在默认的情况下，创建集群会为集群的节点分配公网 IP 。分配的公网 IP 将提供以下作用：

- 通过公网 IP 登录到集群的节点机器。
- 通过公网 IP 访问外网服务

外网带宽

创建外网服务时，外网负载均衡使用的是节点的带宽和流量，若需提供外网服务，节点需要有外网带宽。如果业务不需要外网服务，可以选择不购买外网带宽。

NAT 网关

云主机不绑定弹性公网 IP ，所有访问 Internet 流量通过 NAT 网关转发。此种方案中，云主机访问 Internet 的流量会通过内网转发至 NAT 网关，因而不会受云主机购买时公网带宽的带宽上限限制，NAT 网关产生的网络流量费用也不会占用云主机的公网带宽出口。通过 NAT 网关访问 Internet，您需要完成以下两个步骤：

第一步：创建 NAT 网关

1. 登录 腾讯云控制台，选择顶部导航栏中的 云产品，选择 云计算与网络 下的 私有网络，进入 私有网络控制台，单击左侧导航栏中的【NAT 网关】。
2. 单击左上角【新建】按钮，在弹出框中依次输入或确定以下参数：
3. 网关名称。
4. 网关类型（网关类型创建后可更改）。
5. NAT 网关服务的私有网络。
6. 为 NAT 网关分配弹性 IP，您可以选择已有的弹性 IP，或者重新购买并分配弹性 IP。
7. 选择结束后点击【确认】按钮，即可完成 NAT 网关的创建。

8. 创建完 NAT 网关，您需要在私有网络控制台路由表页配置路由规则，以将子网流量指向 NAT 网关。

   注意：
   NAT 网关创建时将会冻结 1 小时的租用费用。

第二步：配置相关子网所关联的路由表

1. 登录 腾讯云控制台，选择顶部导航栏中的 云产品，选择 云计算与网络 下的 私有网络，进入 私有网络控制台，单击左侧导航栏中的【路由表】。
2. 在路由表列表中，单击需要访问 Internet 的子网所关联的路由表 ID
   进入路由表详情页，在路由策略中单击【编辑】。
3. 单击【新增一行】，填入目的端，下一跳类型选择【NAT 网关】，并选择已创建的 NAT 网关 ID。
4. 单击【确定】。
5. 完成以上配置后，关联此路由表的子网内的云主机访问 Intenet 的流量将指向 NAT 网关。

其他方案

方案1：使用弹性公网 IP

云主机只绑定弹性公网 IP ，不使用 NAT 网关。此种方案，云主机所有访问 Internet 流量通过弹性公网 IP 出，会受到云主机购买时公网带宽的带宽上限限制。访问公网产生的相关费用，根据云主机网络计费模式而定。
使用方法：见 弹性公网IP操作指南。

方案2：同时使用 NAT 网关和弹性公网 IP

如果你同时使用 NAT 网关和弹性公网 IP，此种方案中，所有云主机主动访问 Internet 的流量只通过内网转发至 NAT 网关，回包也经过 NAT 网关返回至云主机。此部分流量不会受云主机购买时公网带宽的带宽上限限制，NAT 网关产生的网络流量费用不会占用云主机的公网带宽出口。如果来自 Internet 的流量主动访问云主机的弹性公网 IP，则云主机回包统一通过弹性公网 IP 返回，这样产生的公网出流量收到云主机购买时公网带宽的带宽上限限制。访问公网产生的相关费用，根据云主机网络计费模式而定。

注意：

如果用户账号开通了带宽包共享带宽功能，则 NAT 网关产生的出流量按照带宽包整体结算（不再重复收取 0.8元/GB 的网络流量费），建议您限制 NAT 网关的出带宽，以避免因为 NAT 网关出带宽过高产生高额的带宽包费用。

容器服务安全组设置

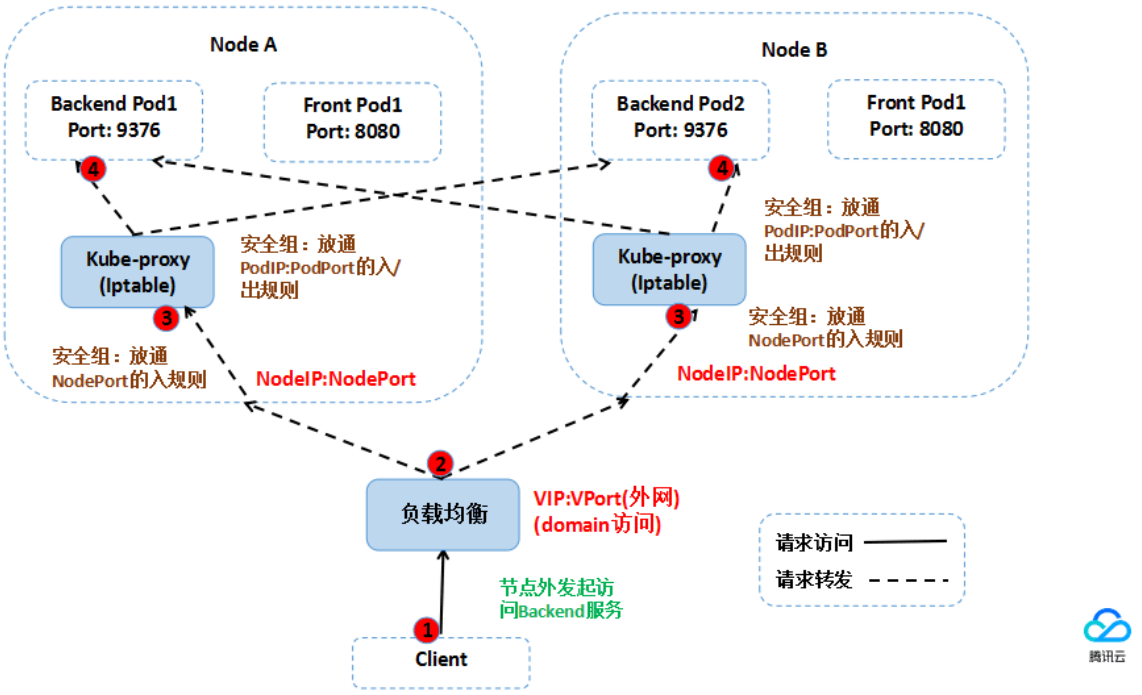
安全问题向来是一个大家非常关注的问题，腾讯云将安全性作为产品设计中的最高原则，严格要求产品做到安全隔离，容器服务同样非常看重这一点。腾讯云的基础网络可以提供充分的安全保障，容器服务选择了网络特性更丰富的 VPC腾讯云私有网络
来作为容器服务的底层网络，本文档主要介绍容器服务下使用安全组的最佳实践，帮助大家选择安全组策略。

安全组

安全组是一种有状态的包过滤功能的虚拟防火墙，它用于设置单台或多台云服务器的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。更多安全组的介绍可以查看 安全组。

使用容器服务选择安全组的原则

1. 由于在容器集群中，服务实例采用分布式的方式进行部署，不同的服务实例混部在集群的节点上。建议同一个集群下的主机绑定同一个安全组，集群的安全组不添加其他云主机。
2. 安全组只对外开放最小权限。
3. 需放通以下容器服务使用规则：
    - 放通容器实例网络和集群节点网络
      当服务访问到达主机节点后，会通过 Kube-proxy 模块设置的 iptables 规则将请求进行转发到服务的任意一个实例。由于服务的实例有可能在另外的节点上，这时会出现跨节点访问。访问的目的 IP 为服务的实例的 IP ，访问的目的 IP 为节点 IP (或者节点上集群 cbr0 网桥的 IP)。这就需要在对端节点上放通容器实例网络和集群节点网络访问。
    - 同一 VPC 不同集群互访的情况，需要放通对应集群的容器网络和节点网络
    - 需要 SSH 登录节点的放通 22 端口
    - 放通节点 30000 ~ 32767 端口
      在访问路径中，需要通过负载均衡器将数据包转发到容器集群的 NodeIP：NodePort 上。其中 NodeIP 为集群中任意一节点的主机 IP ，而 NodePort 是在创建服务时容器集群为服务默认分配的，NodePort 的范围为 30000 ~ 32768 。
      下图以外网访问服务为例：



建议

建议通过容器服务提供的安全组模板来配置集群的安全组。安全组的具体配置规则如下：

入站规则：

协议	端口	网段	是否允许	说明
TCP	30000-32768	0.0.0.0/0	允许	放通所有 IP 对 30000-32768 端口 TCP 访问
UDP	30000-32768	0.0.0.0/0	允许	放通所有 IP 对 30000-32768 端口 UDP 访问
All	traffic ALL	10.0.0.0/8	允许	放通 10.0.0.0/8 内网网段的访问
All	traffic ALL	172.16.0.0/12	允许	放通 172.16.0.0/12 内网网段的访问
All	traffic ALL	192.168.0.0/16	允许	放通 192.168.0.0/16 内网网段的访问
TCP	22	0.0.0.0/0	允许	放通所有 IP 对 22

协议	端口	网段	是否允许	说明
				端口的访问
All	traffic ALL	0.0.0.0/0	拒绝	未匹配已有规则，则拒绝

出站规则：

协议	端口	网段	是否允许	说明
All	traffic ALL	0.0.0.0/0	允许	放通所有规则

容器节点配置该规则，能够满足不同的访问方式访问集群中服务。

集群中服务的访问方式，可以参考 服务访问方式设置 。

集群新增资源所属项目说明

集群新增资源所属项目说明

总述

如需要通过分项目进行财务核算等，请先阅读以下内容：

1. 集群无项目属性， 集群内云主机、负载均衡器等资源有项目属性。
2. 集群新增资源所属项目：仅将新增到该集群下的资源归属到该项目下。

建议

1. 建议集群内的所有资源在同一个项目
2. 如若需要集群内云主机分布在不同的项目，请自行前往云主机控制台迁移项目。
3. 若云主机项目不同，那么云主机所属的

   安全组实例

   不同， 请尽量让同一集群下的云主机的

   安全组规则

   相同.

计费说明

容器服务暂不收取服务本身费用，按用户实际使用的云资源收费。使用容器服务涉及以下产品，详情见对应产品计费模式。

- 按量计费云主机
- 按量计费硬盘
- 负载均衡计费说明

购买渠道

官方购买

登录到腾讯云容器服务购买页，可以购买容器服务产品。