

SDN网络服务

快速入门

产品版本: v6.3.1

发布日期: 2023-11-20

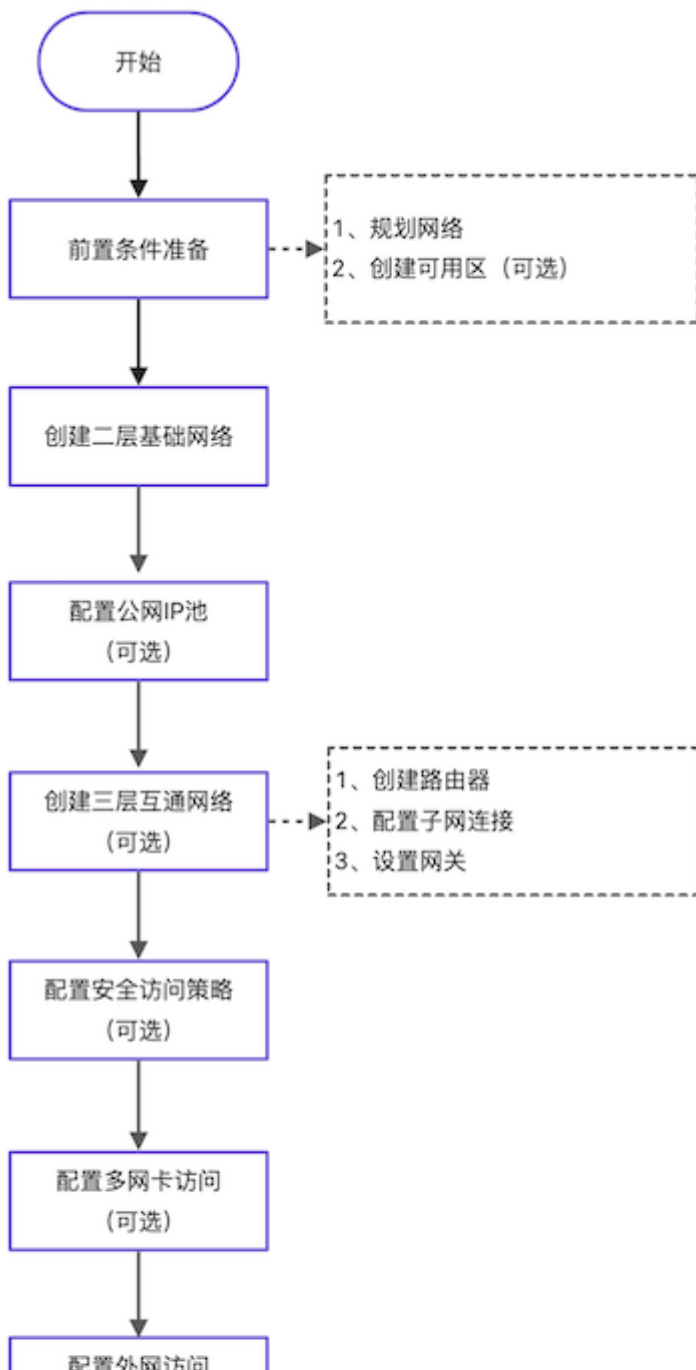
目录

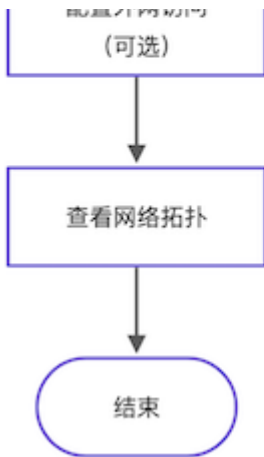
| | |
|------------------------|----|
| 1 快速入门..... | 1 |
| 1.1 操作指引..... | 1 |
| 1.2 前置条件准备..... | 4 |
| 1.3 创建二层基础网络..... | 5 |
| 1.4 配置公网IP池（可选）..... | 8 |
| 1.5 配置三层互通网络（可选）..... | 10 |
| 1.6 配置安全组访问策略（可选）..... | 12 |
| 1.7 配置网络ACL（可选）..... | 13 |
| 1.8 配置网关防火墙（可选）..... | 15 |
| 1.9 配置多网卡访问（可选）..... | 17 |
| 1.10 配置外网访问（可选）..... | 19 |
| 1.11 查看网络拓扑..... | 21 |

1 快速入门

1.1 操作指引

SDN网络服务云产品的主线使用流程及具体说明如下：





| 操作流程 | | 描述 |
|--------------|-----------|--|
| 前置条件准备 | 规划网络 | 遵循隔离性、扩展性和连接性等因素，预先规划并设计网络。 |
| | 创建可用区（可选） | 配置网络的可用区和主机集合，以提高其容灾性和隔离性。请根据客户实际业务需求酌情创建。如已有可用可用区或使用默认default-az时，可直接跳过本步骤。 |
| 创建二层基础网络 | | 为云主机、容器、安全容器或裸金属等资源创建二层隔离的私有基础网络环境。 |
| 配置公网IP池（可选） | | 创建外部网络，为三层网络互通或外网访问需求配置所需的公网IP地址池。 请根据客户实际业务需求酌情创建。如无三层网络互通或外网访问需求或已有可用外部网络，可直接跳过本步骤。 |
| 配置三层互通网络（可选） | 创建路由器 | 为云主机、容器、安全容器或裸金属等资源创建用于三层网络互连的路由器。 |
| | 配置子网连接 | 建立路由器与二层网络之间的连接，为各子网提供三层路由功能。 |
| | 设置网关 | 设置路由器网关，使其能够对外提供服务。 |
| 配置安全访问策略（可选） | | 为云主机或容器、安全容器等资源配置安全组策略，以提供相同的访问策略给具有相同安全保护需求并相互信任的资源。请根据客户实际业务需求酌情配置。如已有可用安全组或使用默认default时，可跳过本步骤。 |

| 操作流程 | 描述 |
|-------------|---|
| 配置多网卡访问（可选） | 为云主机或裸金属等资源绑定多个虚拟网卡，扩展其原有网络接入端口，使资源能够同时连接到多个网络链路。 请根据客户实际业务需求酌情配置。当资源无多网卡访问需求时，可直接跳过本步骤。 |
| 配置外网访问（可选） | 为云主机或裸金属等资源配置公网IP，使其能直接通过该公网IP对外提供服务。 请根据客户实际业务需求酌情配置。当资源无外网访问需求时，可直接跳过本步骤。 |
| 查看网络拓扑 | 直观明了地查看当前云平台的网络拓扑结构，确认各设备与资源之间的结构关系。 |

1.2 前置条件准备

在使用SDN网络服务前，请先完成以下准备工作。

规划网络

本操作用于根据客户的具体业务需求，对网络进行预规划和设计。

请根据客户的具体业务需求，遵循隔离性、扩展性和连接性等因素，规划并设计网络的设备类型、数量和网段等信息。

创建可用区（可选）

本操作用于为网络创建可用区和主机集合，以提高其容灾性和隔离性，请根据客户实际业务需求酌情创建。如有可用的可用区或使用默认default-az时，可跳过本步骤。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[计算]-[可用区与主机集合]，进入“可用区与主机集合”页面。
2. 单击 **创建主机集合** ，弹出“创建主机集合”对话框。输入集合名称和可用区名称后，单击 **创建** ，完成主机集合和可用区的创建。
3. 在“可用区与主机集合”页面中，选择上述新建的主机集合后，单击 **管理主机** ，添加节点至该主机集合和可用区中，并单击 **保存** ，完成操作。

1.3 创建二层基础网络

本操作用于在云平台中根据客户实际网络规划，为云主机、容器、安全容器或裸金属等资源创建二层隔离的私有基础网络环境。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
2. 单击 **创建网络** ，进入“创建网络”页面。
3. 配置参数后，单击 **创建网络** ，完成操作。其中，由于本操作创建的网络将用作云主机、容器、安全容器或裸金属等资源之间的网络通信，所以“网络类型”请选择“内部网络”。

| 参数 | | 说明 |
|------|------|---|
| 基础配置 | 资源池 | 该网络所属的资源池。 |
| | 名称 | 该网络的名称。 |
| | 可用区 | 该网络所属的可用区。 当需要部署高可用网络时，请为其选择多个可用区，以便保证任何时间都有可用区的网络可使用，网络服务不中断。 Warning: 为确保云主机、容器、安全容器或裸金属等资源能够正常获取IP地址，请在资源创建时确保其可用区与该网络可用区之间的网络互通。 |
| | 网络类型 | 该网络的网络类型。该参数值可选内部网络或外部网络。 * 内部网络：用于云主机、容器、安全容器和裸金属等资源之间的网络通信。 * 外部网络：用作公网IP池，为云主机和路由器提供外网访问服务。 |
| | 可见性 | 该网络的可见范围。该参数值可选项目共享或全局共享。 * 项目共享：该网络仅可在所选项目内使用。 * 全局共享：该网络所有项目均可共享使用。 |

| 参数 | 说明 | |
|-----------------------|--|--|
| 网络模式 | 该网络的模式。 * 当网络类型为“内部网络”时，该参数值可选VLAN或Geneve。但是，当该内部网络需要配置三层互通时，该参数值仅能选择Geneve。 * 当网络类型为“外部网络”时，该参数值可选VLAN或Flat(No VLAN)。 | |
| GENEVE VNI | 该Geneve模式网络的网络标识符（VNI, Virtual Network Identifier）。 仅当网络模式选择“Geneve”时，才需设置此参数。 | |
| 物理网络 | 该网络所属的物理网络。 仅当网络模式选择“VLAN”或“Flat(No VLAN)”时，才需设置此参数。 | |
| VLAN ID | 该VLAN模式网络的ID。 仅当网络模式选择“VLAN”时，才需设置此参数。 | |
| 标签（可选） | 该网络的标签。 | |
| 默认/新增IPv4子网 | IPv4子网名称 | 该网络中，IPv4子网的名称。 |
| | IPv4子网网段 | 该网络中，IPv4子网的网段。 该参数值可以手动输入，也可以单击输入框下方“推荐内网网段”的 <input type="button" value="选择"/> 自动指定。 |
| | 高级配置（可选） | 该网络中，IPv4子网的网关地址和地址池范围等配置。 * 网关地址：用于设置该网络内云主机、容器、安全容器或裸金属等资源的缺省网关。 当该网络是外部网络时，请确保子网网关可达，否则该子网将无法正常使用。 * 地址池范围：用于精细化管理子网的IP地址。即网络可用的IP地址范围由此地址池指定。 |
| 新增IPv6子网 (仅内部网络支持) | IPv6子网名称 | 该网络中，IPv6子网的名称。 |
| | | |

| 参数 | 说明 |
|----------|---|
| IPv6子网网段 | 该网络中，IPv6子网的网段。 目前仅提供Stateful-DHCP的地址分配方式，所以请以fd/FD/2/3为起始填写且前缀长度应该在64~125区间内。 |

1.4 配置公网IP池（可选）

本操作用于在云平台中创建用于分配公网IP地址的外部网络。当需要为云主机、容器、安全容器或裸金属等资源配置三层互通网络或配置外网访问时，可以使用系统默认创建的外部网络（public_net）或已有的可用外部网络，也可以根据客户实际业务需求新建外部网络。如需新建外部网络，则必须执行本操作。否则，可直接跳过本步骤。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络]，进入“网络”页面。
2. 单击 **创建网络** ，进入“创建网络”页面。
3. 配置参数后，单击 **创建网络** ，完成操作。其中，由于本操作创建的网络将用作分配公网IP地址，所以“网络类型”请选择“外部网络”。

| 参数 | | 说明 |
|------|------|--|
| 基础配置 | 资源池 | 该网络所属的资源池。 |
| | 名称 | 该网络的名称。 |
| | 可用区 | 该网络所属的可用区。 当需要部署高可用网络时，请为其选择多个可用区，以便保证任何时间都有可用区的网络可使用，网络服务不中断。 |
| | 网络类型 | 该网络的网络类型。该参数值可选内部网络或外部网络。 * 内部网络：用于云主机、容器、安全容器和裸金属等资源之间的网络通信。 * 外部网络：用作公网IP池，为云主机和路由器提供外网访问服务。 |
| | 可见性 | 该网络的可见范围。该参数值可选项目共享或全局共享。 * 项目共享：该网络仅可在所选项目内使用。 * 全局共享：该网络所有项目均可共享使用。 |

| 参数 | 说明 | |
|-------------|--|--|
| 网络模式 | 该网络的模式。 * 当网络类型为“内部网络”时，该参数值可选VLAN或Geneve。但是，当该内部网络需要配置三层互通时，该参数值仅能选择Geneve。 * 当网络类型为“外部网络”时，该参数值可选VLAN或Flat(No VLAN)。 | |
| GENEVE VNI | 该Geneve模式网络的网络标识符（VNI，Virtual Network Identifier）。 仅当网络模式选择“Geneve”时，才需设置此参数。 | |
| 物理网络 | 该网络所属的物理网络。 仅当网络模式选择“VLAN”或“Flat(No VLAN)”时，才需设置此参数。 | |
| VLAN ID | 该VLAN模式网络的ID。 仅当网络模式选择“VLAN”时，才需设置此参数。 | |
| 标签（可选） | 该网络的标签。 | |
| 默认/新增IPv4子网 | IPv4子网名称 | 该网络中，IPv4子网的名称。 |
| | IPv4子网网段 | 该网络中，IPv4子网的网段。 该参数值可以手动输入，也可以单击输入框下方“推荐内网网段”的 <input type="button" value="选择"/> 自动指定。 |
| | 高级配置（可选） | 该网络中，IPv4子网的网关地址和地址池范围等配置。 * 网关地址：用于设置该外部网络的缺省网关，请确保子网网关可达，否则该子网将无法正常使用。 * 地址池范围：用于精细化管理子网的IP地址。即网络可用的IP地址范围由此地址池指定。 |

1.5 配置三层互通网络（可选）

本操作用于在云平台中根据客户实际网络规划，为云主机、容器、安全容器或裸金属等资源创建三层互通的网络环境，以便不同子网资源之间的互相联通，或内网资源与外部网络之间的互相访问。当资源无需跨子网访问和无需访问外部网络时，可直接跳过本步骤。

创建路由器

本操作用于在云平台中创建路由器，以作为不同子网之间或内网与外网之间的三层网络互连设备。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[路由器]，进入“路由器”页面。
2. 单击 **创建路由器** ，弹出“创建路由器”对话框。
3. 配置参数后，单击 **创建** ，完成操作。

| 参数 | 说明 |
|-----|---|
| 名称 | 该路由器的名称。 |
| 可用区 | 该路由器的可用区。 当部署高可用网络时，请为其选择与网络高可用相一致的多个可用区，以保证任何时间都有可用区的网络可使用，网络服务不中断。 |

配置子网连接

本操作用于建立路由器与二层网络之间的连接，为各子网提供三层路由功能，以满足业务访问需要。

1. 在“路由器”页面中，单击上述路由器名称，进入其详情页面。
2. 在[路由器连接]页签中，单击 **连接子网** ，弹出“连接子网”对话框。
3. 配置参数后，单击 **连接** ，完成操作。

| 参数 | 说明 |
|----|----|
|----|----|

| 参数 | 说明 |
|-------------|---|
| 路由器名称(不可编辑) | 该路由器的名称。 |
| 子网 | 该路由器所连接的子网的名称。 请选择上述创建二层基础网络操作中新建网络的子网。 |
| 子网IP | 该路由器所连接的子网的IP地址。 当所连接的子网已设置网关时，此IP地址只能选择子网的网关地址。 |

设置网关

本操作用于为路由器设置网关，使其能够使用此IP地址对外提供服务。

- 在上述路由器的详情页面中，单击 **更多操作** - **设置网关**，弹出“设置路由器网关”对话框。
- 配置参数后，单击 **设置**，完成操作。

| 参数 | 说明 |
|--------|---|
| 外部网络 | 该路由器网关地址的所属外部网络。 |
| 分配外部IP | 该路由器网关地址的分配方式。该参数值可选自动分配或手动选择。 当选择“手动选择”时，请手动选择子网和外部IP地址信息。 |
| QoS | 该路由器网关的QoS（Quality of Service，服务质量）功能是否激活。 当选择激活QoS时，请设置该路由器网关的带宽限制。 |
| 开启SNAT | 该路由器网关是否开启SNAT（Source Network Address Translation，源地址转换）。 * 当开启SNAT时，云主机、容器、安全容器或裸金属等资源在进行三层通信时，源IP地址将修改为该路由器网关地址。 * 当未开启SNAT时，云主机、容器、安全容器或裸金属等资源在进行三层通信时，将通过路由转发的方式实现。 |

1.6 配置安全组访问策略（可选）

本操作用于在云平台中根据客户实际网络规划，为云主机、裸金属等资源创建安全组并定义各种访问规则，用于为具有相同安全保护需求并相互信任的资源提供相同的访问策略。如已有可用安全组或使用默认default时，可跳过本步骤。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[访问控制]，进入“安全组”页面。
2. 在“安全组”页面中，单击 **创建安全组** ，弹出“创建安全组”对话框。配置参数后，单击 **创建** ，完成安全组创建。

| 参数 | 说明 |
|--------|---------------|
| 名称 | 该安全组的名称。 |
| 是否有状态 | 安全组里的规则是否有状态。 |
| 描述（可选） | 该安全组的描述信息。 |

3. 在“安全组”详情页面中，添加“入方向规则”，“出方向规则”，完成操作。

说明：

当指定的安全组规则需要删除时，请直接单击该规则所在行的 **删除** ，然后，在弹出的“删除安全组规则”提示框中，单击 **删除** 即可。

| 参数 | 说明 |
|-------|---|
| 协议和端口 | 该安全组规则的作用范围。可以选择基本协议，也可以选择常见协议端口。 |
| 源地址 | 该安全组规则的作用对象。该参数值可选CIDR或安全组。 * 当选择“CIDR”时，请输入具体地址。该安全组规则将作用于该地址段。 * 当选择“安全组”时，该安全组规则将作用于所有选择当前安全组的资源，而且各资源之间可以通过指定的协议互相访问。当安全组发生更新时，规则将同步更新至所有选择此安全组的资源。 |

1.7 配置网络ACL（可选）

本操作通过创建网络ACL，将其与子网关联并配置相应的出/入方向的规则可以有效地控制出入子网的数据流。

1. 创建网络ACL。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[网络ACL]，进入“网络ACL列表”页面。
2. 单击 **创建网络ACL** ，弹出“创建网络ACL”对话框。
3. 配置参数后，单击 **创建** ，完成操作。

| 参数 | 说明 |
|----|-----------|
| 名称 | 网络ACL的名称。 |
| 描述 | 网络ACL的描述。 |

2. 关联子网。

1. 点击已经创建的网络ACL，进入该网络ACL的详情页面，单击 **关联子网** - **关联** ，弹出“关联子网”对话框。
2. 选择子网，单击 **关联** 。

说明：

- 关联子网后，网络ACL默认拒绝所有出入子网的流量，直至添加放通规则。
- 需要关联的子网必须是带子网网关且绑定了路由器的。

3. 配置网络ACL出入方向规则。

1. 在网络ACL的详情页面，单击 **入方向规则** - **添加规则** ，出现规则编辑框。
2. 配置：**类型**：ipv4 ， **策略**：允许 ， **协议**：全部 ， **源地址**：0.0.0.0/0 ， **源端口范围**：全部 ， **目的地址**：0.0.0.0/0 ， **目的端口范围**：全部 ，单击 **确认** ，完成操作。

3. 单击 **出方向规则** - **添加规则** ，出现规则编辑框。

4. 配置： **类型**： ipv4 ， **策略**： 允许 ， **协议**： 全部 ， **源地址**： 0.0.0.0/0 ， **源端口范围**： 全部 ， **目的地址**： 0.0.0.0/0 ， **目的端口范围**： 全部 ， 单击 **确认** ，完成操作。

| 参数 | 说明 |
|--------|-----------------------|
| 类型 | ipv4或者ipv6。 |
| 策略 | 允许或者拒绝流量。 |
| 协议 | ip协议，全部，tcp，udp或icmp。 |
| 源地址 | 报文的源ip地址。 |
| 源端口范围 | 报文的tcp/udp源端口范围。 |
| 目的地址 | 报文的目的ip地址。 |
| 目的端口范围 | 报文的tcp/udp目的端口范围。 |
| 描述 | 规则的描述。 |

1.8 配置网关防火墙（可选）

本操作通过创建网关防火墙，将其与外部网关关联，并配置相应的规则可以有效地控制内/外部网络的出入路由器的数据流。

1. 创建网关防火墙。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[访问控制]-[网关防火墙]，进入“网关防火墙列表”页面。
2. 单击 **创建网关防火墙** ，弹出“创建网关防火墙”对话框。
3. 配置参数后，单击 **创建** ，完成操作。

| 参数 | 说明 |
|----|-----------|
| 名称 | 网关防火墙的名称。 |
| 描述 | 网关防火墙的描述。 |

2. 关联路由器。

1. 点击已经创建的网关防火墙，进入该网关防火墙的详情页面，单击 **关联路由器** - **关联** ，弹出“关联路由器”对话框。
2. 选择路由器，点击 **关联** 。

说明：

- 关联路由器后，网关防火墙默认拒绝所有出入路由器网关的流量，直至添加放通规则。
- 需要关联的路由器已经设置网关。

3. 配置网关防火墙出方向规则。

1. 在网关防火墙的详情页面，单击 **出方向规则** - **添加规则** ，出现规则编辑框。
2. 配置：**类型**：ipv4 ， **策略**：允许 ， **协议**：全部 ， **源地址**：0.0.0.0/0 ， **源端口范围**：全部 ， **目的地址**：0.0.0.0/0 ， **目的端口范围**：全部 ，单击 **确认** ，完成操作。

| 参数 | 说明 |
|--------|--------------------------|
| 类型 | ipv4或者ipv6。 |
| 策略 | 允许或者拒绝流量。 |
| 协议 | ip协议, 全部, tcp, udp或icmp。 |
| 源地址 | 报文的源ip地址。 |
| 源端口范围 | 报文的tcp/udp源端口范围。 |
| 目的地址 | 报文的目的ip地址。 |
| 目的端口范围 | 报文的tcp/udp目的端口范围。 |
| 描述 | 规则的描述。 |

1.9 配置多网卡访问（可选）

本操作通过为云主机或裸金属等资源绑定多个虚拟网卡，扩展其原有网络接入端口，使资源能够同时连接到多个网络链路。请根据客户实际业务需求酌情配置。当资源无多网卡访问需求时，可直接跳过本步骤。

1. 创建虚拟网卡。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[虚拟网卡]，进入“虚拟网卡”页面。
2. 单击 **创建虚拟网卡** ，弹出“创建虚拟网卡”对话框。
3. 配置参数后，单击 **创建** ，完成操作。

| 参数 | 说明 |
|-------|--|
| 网卡名称 | 该虚拟网卡的名称。 |
| 项目 | 该虚拟网卡的所属项目。 |
| 类型 | 该虚拟网卡的类型。该参数值可选IPv4、IPv6或网络双栈（即同时设置IPv4和IPv6网卡）。 请在选择类型后，设置对应的子网和IP地址。其中，IP地址不能与所选的二层基础网络的子网网关相同。 |
| MAC地址 | 该虚拟网卡的Mac地址。该参数值可选自动分配或手动输入。 当选择“手动选择”时，请手动选择Mac地址信息。 |
| 安全组 | 该虚拟网卡绑定的安全组。 |
| QoS | 该虚拟网卡的QoS（Quality of Service，服务质量）功能是否激活。 当选择激活QoS时，请设置该虚拟网卡的带宽限制。 |

2. 绑定虚拟网卡到资源。

1. 在“虚拟网卡”页面中，勾选上述虚拟网卡后，单击 **绑定到资源** ，弹出“绑定资源”对话框
2. 配置参数后，单击 **绑定** ，完成操作。

| 参数 | 说明 |
|------------|----------------|
| 网卡名称（不可编辑） | 该虚拟网卡的名称。 |
| 资源 | 该虚拟网卡将绑定的具体资源。 |

1.10 配置外网访问（可选）

本操作通过为云主机或裸金属等资源配置公网IP，使其能直接通过该公网IP对外提供服务。当资源无外网访问需求时，可直接跳过本步骤。

1. 为项目申请IP。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[公网IP]，进入“公网IP”页面。
2. 单击 **为项目申请IP** ，弹出“为项目申请IP”对话框。
3. 配置参数后，单击 **分配** ，完成操作。

| 参数 | 说明 |
|------|----------------|
| 项目 | 本次申请公网IP地址的项目。 |
| 资源池 | 该公网IP地址所属的资源池。 |
| 公网IP | 本次申请的公网IP地址。 |
| 带宽 | 该公网IP地址的带宽。 |

2. 绑定到虚拟网卡。

1. 在“公网IP”页面中，勾选上述公网IP后，单击 **更多** - **绑定到虚拟网卡** ，弹出“绑定到虚拟网卡”对话框。
2. 配置参数后，单击 **绑定** ，完成操作。

说明：

- 公网IP只能绑定给类型为“IPv4”或“网络双栈”的虚拟网卡。
- 当虚拟网卡所处子网未连接到路由器，或者连接的路由器未设置网关时，其将不会显示在此对话框的虚拟网卡下拉框中。

| 参数 | 说明 |
|-------------|--------------------------------------|
| 公网IP（不可编辑） | 该公网IP的地址。 |
| 部门（不可编辑） | 该公网IP的所属部门。 |
| 项目（不可编辑） | 该公网IP的所属项目。 |
| 虚拟网卡是否绑定到资源 | 该公网IP是否绑定到资源。该参数值可选是或否。在本操作中，请选择“是”。 |
| 虚拟网卡 | 该公网IP所绑定的虚拟网卡。 |

1.11 查看网络拓扑

本操作用于直观明了地查看当前云平台的网络拓扑结构，以确认各设备与资源之间的结构关系。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]-[网络拓扑]，进入“网络拓扑”页面。
2. 在“网络拓扑”页面中，查看当前云平台的网络拓扑结构图，确认各设备与资源之间的结构关系。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：

北京市海淀区西北旺东路10号院东区1号楼1层107-2号

南京易捷思达软件科技有限公司：

江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：

contact@easystack.cn (业务咨询)

partners@easystack.cn(合作伙伴咨询)

marketing@easystack.cn (市场合作)