

企业交换机

# 用户指南

文档版本 01  
发布日期 2024-12-09



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 安全声明

## 漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

---

# 目录

---

<b>1 企业交换机</b>	<b>1</b>
1.1 购买企业交换机	1
1.2 查看企业交换机	4
1.3 修改企业交换机	4
1.4 删除企业交换机	4
<b>2 二层连接</b>	<b>5</b>
2.1 创建二层连接	5
2.2 查看二层连接	7
2.3 修改二层连接	7
2.4 删除二层连接	7
<b>3 权限管理</b>	<b>9</b>
3.1 创建用户并授权使用 ESW	9
<b>4 使用 CES 服务监控 ESW 网络指标</b>	<b>11</b>
4.1 ESW 支持的监控指标	11
4.2 查看 ESW 的监控指标	12
4.3 创建告警规则	13
4.4 配置监控数据存储至 OBS	13

# 1 企业交换机

## 1.1 购买企业交换机

### 操作场景

本章节指导用户购买企业交换机，企业交换机可以基于VPN或者云专线网络，在云下IDC和云上VPC之间建立二层网络通信。

### 前提条件

- 使用企业交换机之前，需要规划云下和云上所需的资源，资源规划请参考[企业交换机工作原理](#)。
- 企业交换机建立二层通信网络时，依赖云下IDC和云上VPC之间的三层网络，请提前使用云专线或者VPN，建立本端隧道子网和远端隧道子网之间的三层网络通信，具体请参见[使用云专线或VPN连通三层网络](#)。

### 约束与限制

- 企业交换机建立二层网络通信时，需要和IDC侧建立VXLAN隧道，IDC侧交换机必须支持VXLAN功能。
- 企业交换机会占用本端隧道子网的三个IP地址，用来做企业交换机实例主备节点的负载均衡，请您规划隧道子网的时候预留足够的IP地址。

### 操作步骤

1. 进入[购买企业交换机页面](#)。
2. 根据界面提示，配置企业交换机的基本信息，配置参数请参见[表1-1](#)。

表 1-1 参数说明

参数	参数说明	取值样例
计费模式	<p>必选参数</p> <p>支持包年/包月、按需付费两种计费方式。</p> <ul style="list-style-type: none"><li>• 购买包年/包月企业交换机时，需要一次性支付选定周期内企业交换机实例的费用。</li><li>• 按需计费，属于后付费。按秒计费，按小时结算，不足一小时以实际使用时长为准。</li></ul> <p><b>说明</b></p> <p>ESW包年/包月计费模式当前仅在“拉美-圣地亚哥”和“非洲-约翰内斯堡”区域上线。</p>	按需计费
区域	<p>必选参数。</p> <p>不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。</p>	拉美-圣地亚哥
主可用区	<p>必选参数。</p> <p>企业交换机实例部署采用主备模式，此处选择主节点所在的可用区。</p> <p>主可用区是当前承载流量的可用区，推荐与需要通信的云服务器部署在同一个可用区，从而实现更优访问性能。</p>	可用区1
备可用区	<p>必选参数。</p> <p>企业交换机实例部署采用主备模式，此处选择备节点所在的可用区。</p> <p>备可用区用于容灾备份，建议与主可用区不同。</p>	可用区2
规格	<p>必选参数。</p> <p>当前支持的企业交换机规格如下：</p> <ul style="list-style-type: none"><li>• 小型<ul style="list-style-type: none"><li>- 最大带宽：3 Gbit/s</li><li>- 最大发包数：500000 pps</li><li>- 连接子网数：1</li></ul></li><li>• 中型<ul style="list-style-type: none"><li>- 最大带宽：5 Gbit/s</li><li>- 最大发包数：1000000 pps</li><li>- 连接子网数：3</li></ul></li><li>• 大型<ul style="list-style-type: none"><li>- 最大带宽：10 Gbit/s</li><li>- 最大发包数：2000000 pps</li><li>- 连接子网数：6</li></ul></li></ul> <p>企业交换机创建完成后，不支持修改规格。</p>	大型

参数	参数说明	取值样例
虚拟私有云	必选参数。 企业交换机所属VPC。 当“隧道连接方式”选择“云专线”或者“VPN”时，此处默认选择云专线虚拟网关或VPN网关所在的VPC。	vpc-01
隧道子网	必选参数。 企业交换机所属VPC的子网，为本端隧道子网，该子网需要与远端隧道子网建立三层网络通信。 隧道子网基于云专线或者VPN实现三层网络通信，包括本端隧道子网和远端隧道子网。企业交换机需要基于隧道子网之间的三层网络，为需要互通的云上和云下子网提供二层连接通道。	subnet-01
本端隧道IP	必选参数。 此处为本端隧道IP，即云上VPC侧的隧道IP，当前支持自动分配或手动分配IP地址。 企业交换机需要和云下IDC建立VXLAN隧道实现二层网络通信，VXLAN隧道两端各需要一个隧道IP，包括本端隧道IP和远端隧道IP，两个IP地址不能冲突。	自动分配
名称	必选参数。 输入企业交换机的名称。要求如下： <ul style="list-style-type: none"><li>长度范围为1~64位。</li><li>名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。</li></ul>	esw-01
描述	可选参数。 您可以根据需要在文本框中输入对该企业交换机的描述信息。	-
购买时长	包年包月场景需要选择，购买企业交换机的时长。	2个月

- 单击“下一步”。
- 在产品配置信息确认页面，再次核对企业交换机信息，确认无误后，单击“提交”，开始创建企业交换机。

企业交换机的创建过程一般需要3~6分钟，当企业交换机的状态为“运行中”时，表示创建成功。

## 后续操作

企业交换机创建成功后，您还需要创建二层连接、配置远端隧道网关，具体请参见[企业交换机快速入门](#)。

## 1.2 查看企业交换机

### 操作场景

本章节指导用户查看企业交换机的基本信息。

### 操作步骤



1. 进入[企业交换机页面](#)。
2. 选择对应的“企业交换机”名称页签，可以查看该企业交换机的基本信息。

## 1.3 修改企业交换机

### 操作场景

本章节指导用户修改企业交换机的名称和描述信息。

### 操作步骤

1. 进入[企业交换机页面](#)。  
选择对应的“企业交换机”名称页签。
2. 根据界面提示，单击企业交换机或者描述旁的，输入对应的信息。
3. 单击，完成信息修改。

## 1.4 删除企业交换机

### 操作场景

本章节指导用户删除企业交换机，企业交换机创建后，如果您不再需要使用，可以删除企业交换机，释放资源，节省费用。

### 约束与限制

企业交换机中存在二层连接时，需先删除二层连接，具体请参见[删除二层连接](#)。

### 操作步骤

1. 进入[企业交换机页面](#)。  
选择对应的“企业交换机”名称页签。
2. 在企业交换机详情页面右上角，单击“删除”。  
弹出删除确认对话框。
3. 确认无误后，单击“确定”，删除企业交换机。  
企业交换机的删除过程一般需要10~30秒。



# 2 二层连接

## 2.1 创建二层连接

### 操作场景

企业交换机购买完成后，您还需要创建二层连接，建立本端二层连接子网和远端VXLAN交换机之间的二层网络通信。本章节指导用户创建二层连接。

### 约束与限制

- 一个二层连接可以连通一对本端和远端二层连接子网，一个企业交换机最多支持建立6个二层连接，即同时连接6对二层连接子网。
- 基于同一个企业交换机建立二层连接时，这些二层连接可以共用隧道IP，但是隧道号不能相同，隧道号是隧道的标识。
- 通过二层连接连通本端二层连接子网和企业交换机时，需要占用本端二层连接子网中的两个IP地址，用作主接口IP与备接口IP。这两个IP地址不能被本端资源占用，也不能与远端二层连接子网内的其他IP地址冲突。

### 操作步骤

1. 进入[企业交换机页面](#)。  
选择对应的“企业交换机”名称页签。
2. 在企业交换机详情页面右下方，单击“创建连接”。  
进入二层连接创建页面。
3. 根据界面提示，配置二层连接的基本信息，配置参数请参见[表2-1](#)。

表 2-1 参数说明

参数	参数说明	取值样例
企业交换机	企业交换机的名称，不用设置。	l2cg-01

参数	参数说明	取值样例
虚拟私有云	企业交换机绑定的VPC名称，即本端隧道子网所属的VPC，不用设置。 选择的VPC	vpc-01
二层连接子网	必选参数。 二层连接子网是云上VPC与云下IDC准备建立二层互通的子网，包括本端二层连接子网和远端二层连接子网。此处选择本端二层连接子网，即云上VPC的子网。 <ul style="list-style-type: none"><li>本端和远端二层连接子网网段可以重叠，但是本端和远端子网内需要通信的服务器地址不能相同，否则无法正常通信。</li><li>已被企业交换机二层连接绑定的VPC子网，不能再被其他二层连接或者企业交换机使用。</li></ul>	subnet-01
接口IP	必选参数。 本端二层连接子网接入到企业交换机接口的IP，包括主接口IP和备接口IP，当前支持自动分配或手动分配IP地址。	自动分配
远端接入信息 > 隧道号	必选参数。 云下IDC连接企业交换机所需的VXLAN隧道号，即VXLAN网络标识号（VNI），类似VLAN ID，用于区分VXLAN段。对于同一个VXLAN隧道，云下IDC和云上隧道号一致。	10001
远端接入信息 > 隧道IP	必选参数。 云下IDC连接企业交换机所需的VXLAN隧道IP。	-
远端接入信息 > 隧道端口	云下IDC连接企业交换机所需的VXLAN隧道端口号。默认为4789，不用设置。	4789
名称	必选参数。 输入二层连接的名称。要求如下： <ul style="list-style-type: none"><li>长度范围为1~64位。</li><li>名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成</li></ul>	l2conn-01

#### 4. 单击“创建”，开始创建二层连接。

二层连接的创建过程一般需要20~60秒，当二层连接的状态为“未连接”或“已连接”，表示二层连接已创建成功。

## 2.2 查看二层连接

### 操作场景

本章节指导用户查看二层连接的基本信息和连接拓扑，包括本端和远端二层连接子网、本端和远端隧道IP地址以及连通性等信息。

### 操作步骤



1. 进入[企业交换机页面](#)。  
选择对应的“企业交换机”名称页签。
2. 在企业交换机详情页面下方，查看二层连接基本信息和二层连接拓扑。

## 2.3 修改二层连接

### 操作场景

本章节指导用户修改二层连接的名称。

### 操作步骤

1. 进入[企业交换机页面](#)。  
选择对应的“企业交换机”名称页签。
2. 在企业交换机详情页面下方，找到待修改名称的二层连接。
3. 根据界面提示，单击二层连接名称旁的，输入对应的信息。
4. 单击，完成信息修改。

## 2.4 删除二层连接

### 操作场景

本章节指导用户删除二层连接，二层连接创建后，如果您不再需要使用该二层连接，则可以删除该二层连接。

### 约束与限制

待删除的二层连接不能处于中间状态，例如“创建中”。

### 操作步骤

1. 进入[企业交换机页面](#)。  
选择对应的“企业交换机”名称页签。
2. 在企业交换机详情页面下方，找到待删除的二层连接。
3. 在页面右下方，单击“删除连接”。

弹出删除确认对话框。

4. 确认无误后，单击“确定”，删除二层连接。  
二层连接的删除过程一般需要10~30秒。

# 3 权限管理

## 3.1 创建用户并授权使用 ESW

如果您需要对您所拥有的ESW进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用ESW资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将ESW资源委托给更专业、高效的其他华为账号或者云服务，这些华为账号或者云服务可以根据权限进行代运维。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用ESW服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见[IAM产品介绍](#)。

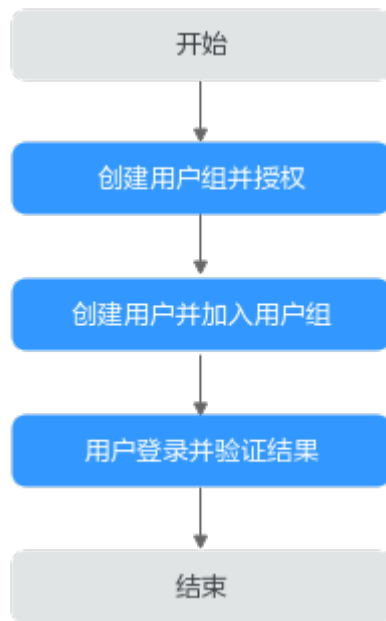
本章节为您介绍对用户授权的方法，操作流程如[图3-1](#)所示。

### 前提条件

给用户组授权之前，请您了解用户组可以添加的ESW权限，并结合实际需求进行选择，ESW服务没有独立的系统权限，和VPC共用一套系统权限，请参见：[系统权限](#)。如果您需要对除ESW之外的其它服务授权，IAM支持服务的所有权限请参见[系统权限](#)。

## 示例流程

图 3-1 给用户授予 ESW 权限流程



1. **创建用户组并授权**

在IAM控制台创建用户组，并授予VPC只读权限“VPC ReadOnlyAccess”。

2. **创建用户并加入用户组**

在IAM控制台创建用户，并将其加入1中创建的用户组。

3. **用户登录**并验证权限。

新创建的用户登录控制台，切换至授权区域，验证权限：

- 在“服务列表”中选择企业交换机，进入ESW主界面，单击右上角“购买”，尝试购买企业交换机，如果无法购买企业交换机（假设当前权限仅包含VPC ReadOnlyAccess），表示“VPC ReadOnlyAccess”已生效。
- 在“服务列表”中选择弹性云服务器（假设当前策略仅包含VPC ReadOnlyAccess），如果提示权限不足，表示“VPC ReadOnlyAccess”已生效。

# 4 使用 CES 服务监控 ESW 网络指标

## 4.1 ESW 支持的监控指标

### 功能说明

本节定义了企业交换机上报给云监控服务的监控指标信息，包括命名空间、监控指标列表和测量维度，您可以通过云监控提供的管理控制台来检索企业交换机产生的监控指标和告警信息。

### 命名空间

SYS.ESW

### 监控指标

通过云监控服务，您可以监控企业交换机实例的网络情况。

- [企业交换机实例支持的监控指标](#)

表 4-1 企业交换机实例支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
up_bandwidth	出网带宽	该指标用于统计企业交换机实例出云平台的网络速度。 单位：比特/秒	$\geq 0$	企业交换机实例	1分钟
down_bandwidth	入网带宽	该指标用于统计企业交换机实例入云平台的网络速度。 单位：比特/秒	$\geq 0$	企业交换机实例	1分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
up_stream	出网流量	该指标用于统计企业交换机实例出云平台的网络流量。 单位：字节	≥ 0	企业交换机实例	1分钟
down_stream	入网流量	该指标用于统计企业交换机实例入云平台的网络流量。 单位：字节	≥ 0	企业交换机实例	1分钟
up_pps	出网pps	该指标用于统计企业交换机实例出云平台，每秒接收的数据包数。 单位：包/秒	≥ 0	企业交换机实例	1分钟
down_pps	入网pps	该指标用于统计企业交换机实例入云平台，每秒发送的数据包数。 单位：包/秒	≥ 0	企业交换机实例	1分钟

## 维度

企业交换机实例支持的监控指标测量维度为：instance\_id。

Key	Value
instance_id	企业交换机实例

## 4.2 查看 ESW 的监控指标

### 操作场景

本章节指导用户查看企业交换机实例的监控指标。



### 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在页面左上角单击图标，选择区域，选择“管理与部署 > 云监控”。

进入云监控服务页面。



- 步骤3** 在管理控制台左上角单击 ，选择区域和项目。
- 步骤4** 在页面左上角单击  图标，打开服务列表，选择“管理与部署 > 云监控服务”。
- 步骤5** 单击页面左侧的“云服务监控”，选择“企业交换机”。
- 步骤6** 单击“操作”列的“查看监控指标”。
- 进入监控指标详情页面。
- 步骤7** 在监控指标详情页面，根据页面提示设置参数，查看企业交换机实例的监控指标。

#### 说明

在监控指标详情页面，参数的详细说明，请参见[查看云服务监控指标](#)。

----结束

## 4.3 创建告警规则



### 操作场景

本章节指导用户为企业交换机实例创建告警规则和通知。

告警功能为您提供监控数据的告警服务。您可以通过创建告警规则来定义告警系统如何检查监控数据，并在监控数据满足告警策略时发送报警通知。

对重要监控指标创建告警规则后，便可在第一时间得知指标数据发生异常，迅速处理故障。

### 操作步骤

1. 登录管理控制台。
  2. 在管理控制台左上角单击 ，选择区域和项目。
  3. 在页面左上角单击  图标，打开服务列表，选择“管理与监管 > 云监控服务”。
  4. 在左侧导航栏，选择“告警 > 告警规则”。
  5. 在“告警规则”界面，单击“创建告警规则”进行添加，或者选择已有的告警规则进行修改。
  6. 规则参数设置完成后，单击“确定”。
- 告警规则设置完成后，当符合规则的告警产生时，系统会自动进行通知。

#### 说明

更多关于监控规则的信息，请参见[《云监控用户指南》](#)。

## 4.4 配置监控数据存储至 OBS


### 操作场景


本章节指导用户为企业交换机实例配置OBS存储，用来存储历史监控数据。

云监控服务各监控指标的原始数据的保留周期为两天，超过保留周期后原始数据将不再保存。您开通对象存储服务（Object Storage Service，以下简称OBS）后，可将原始数据同步保存至OBS，以保存更长时间。

## 操作步骤

**步骤1** 登录管理控制台。

**步骤2** 在管理控制台左上角单击 ，选择区域和项目。

**步骤3** 在页面左上角单击  图标，打开服务列表，选择“管理与部署 > 云监控服务”。

**步骤4** 单击页面左侧的“云服务监控”，选择“企业交换机”。

**步骤5** 在企业交换机列表中，单击目标企业交换机所在行的操作下的“配置数据存储”。  
进入“配置数据存储”页面。

**步骤6** 在“配置数据存储”页面，根据页面提示设置参数，为企业路由器实例配置OBS存储。

----结束