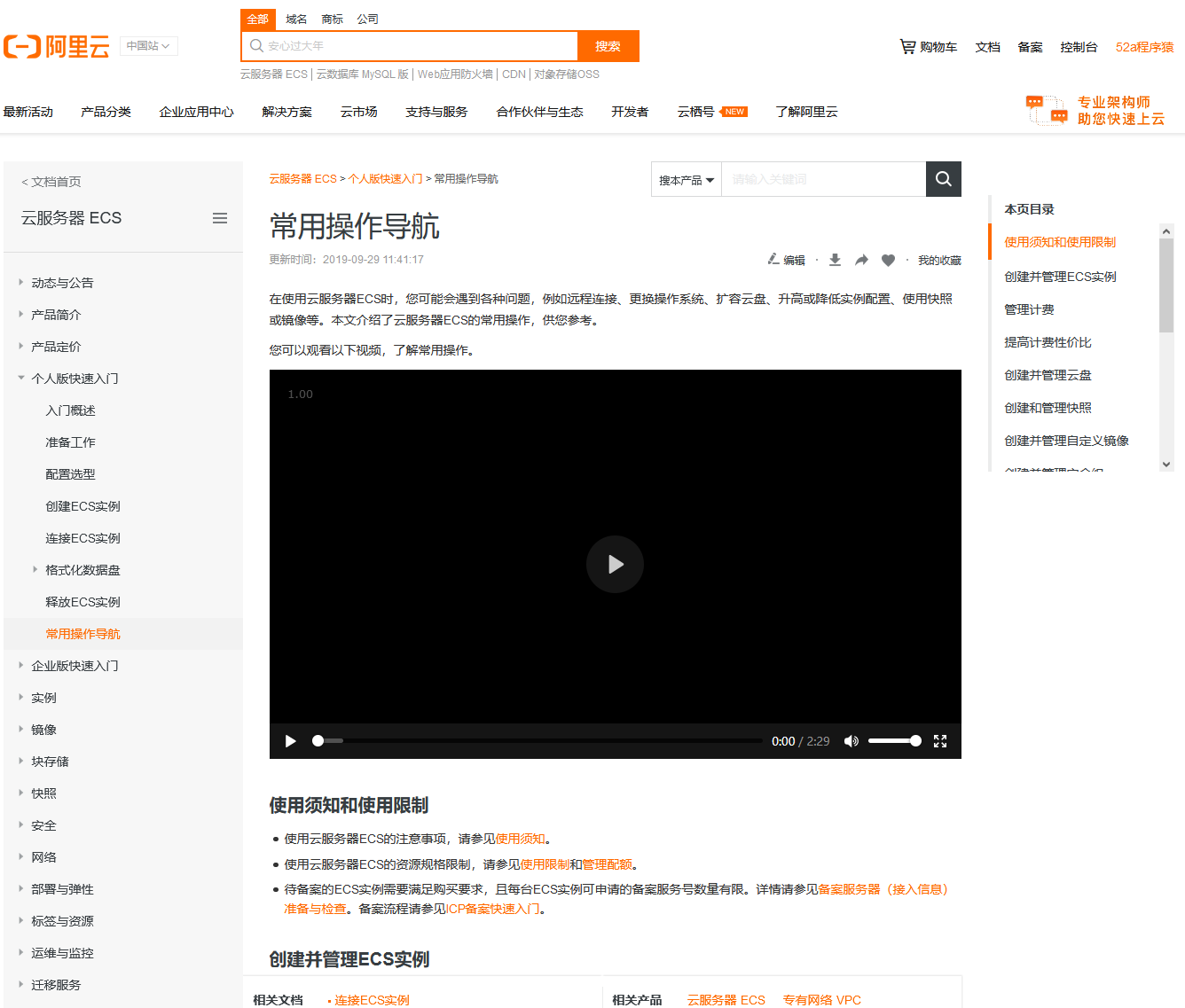
<https://help.aliyun.com/document_detail/25429.html?spm=5176.2020520101.0.0.1d7b4df5MsAhnp>

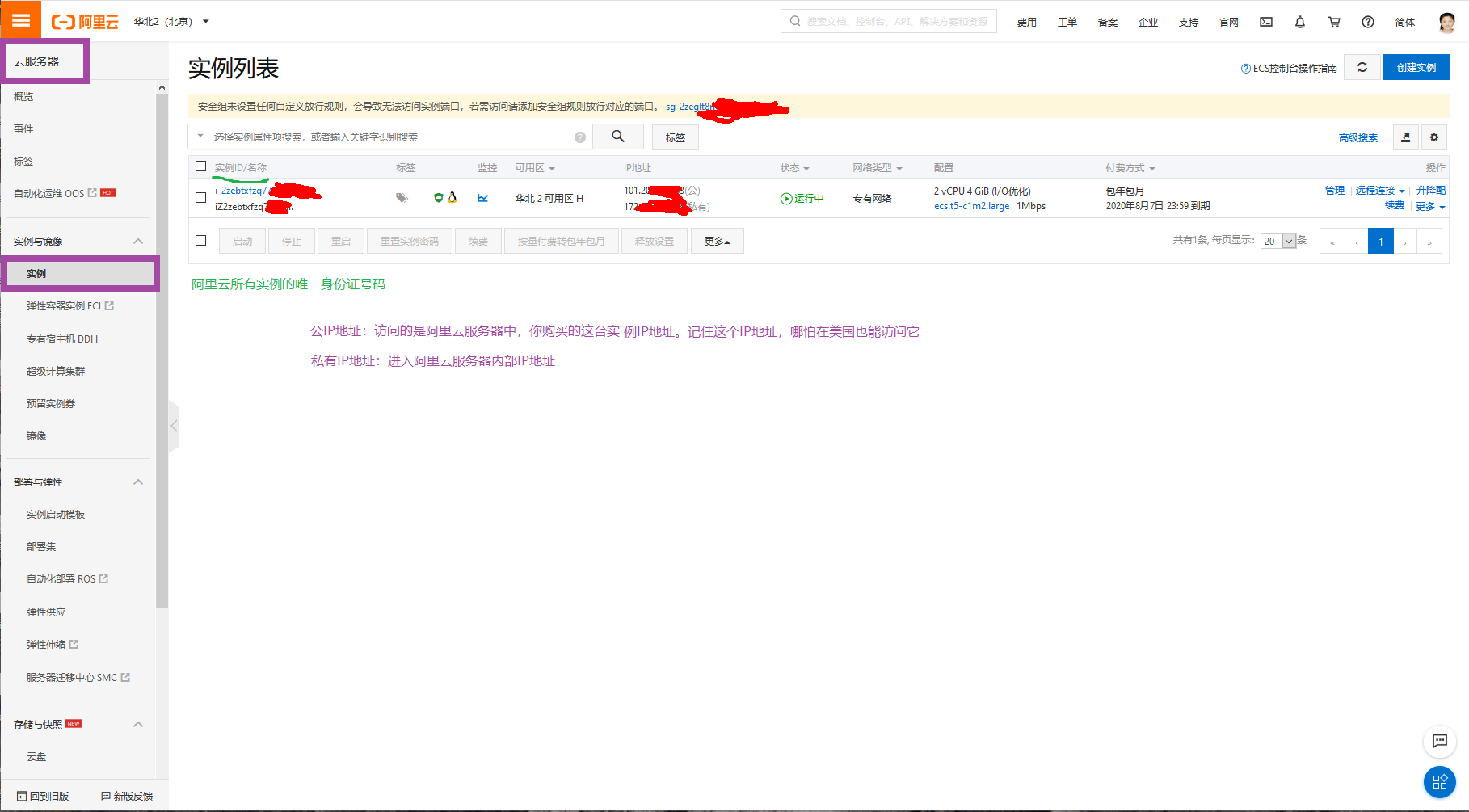
[www.aliyun.com](http://www.aliyun.com)



打开“控制台”，寻找“已开通的云产品”栏目的“云服务器ECS”

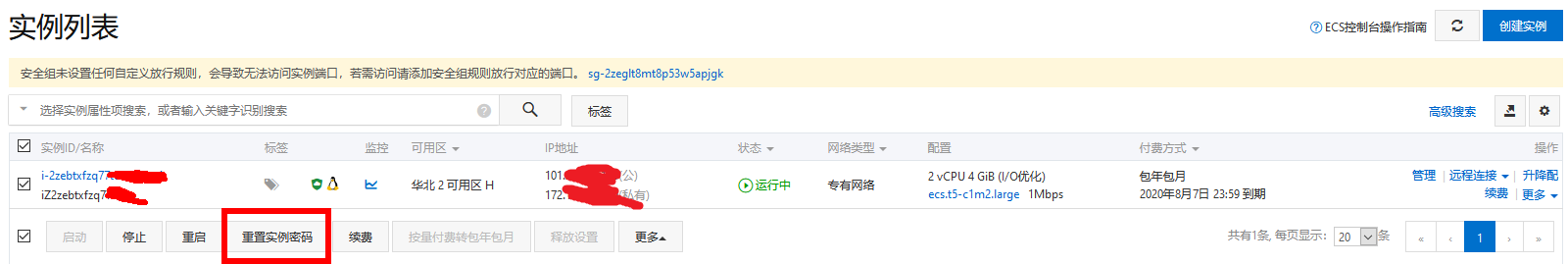


实例=装有linux操作系统的电脑

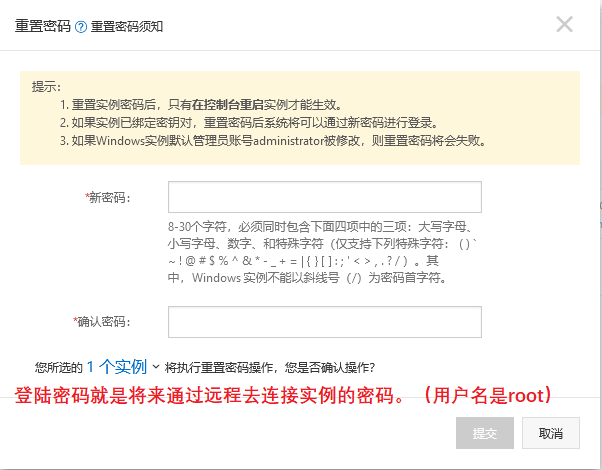


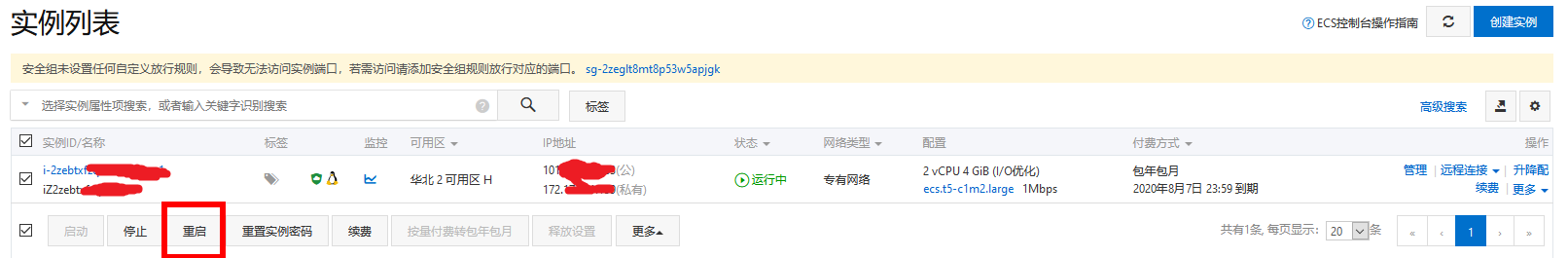
设置实例密码和启动实例

设置用户root密码，然后重新启动电脑



登陆密码就是将来通过远程去连接实例的密码。（用户名是root）





设置安全组

默认申请实例成功后会自动生成一个安全组

安全组的等级，端口设置，作用规则可以作用到实例上。

安全组作用到实例上，则显示“相关实例1”

<https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq>

**安全组应用案例**

更新时间：2019-12-06 16:58:06

本文介绍了几个常见的安全组应用案例，同时包括专有网络VPC和经典网络的安全组设置说明。

## 应用案例概述

ECS实例主要通过配置安全组规则，允许或禁止安全组内的ECS实例对公网或私网的访问。创建安全组和添加安全组规则的详细操作，请参见[创建安全组](https://help.aliyun.com/document_detail/25468.html#concept-ocl-bvz-xdb)和[添加安全组规则](https://help.aliyun.com/document_detail/25471.html#concept-sm5-2wz-xdb)。以下列举了常见的安全组规则配置案例供您参考：

* [案例一：同一个地域、同一个账号下的实例实现内网互通](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#section-i35-nll-ngb)

场景举例：如果您需要同一个地域、同一个账号下的ECS实例之间拷贝资源，您可以通过安全组设置实现两台ECS实例内网互通后再拷贝资源。

* [案例二：同一个地域、不同账号下的实例实现内网互通](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#section-sfg-zll-ngb)

场景举例：如果您需要同一个地域、不同账号下的ECS实例之间拷贝资源，您可以通过安全组设置实现两台ECS实例内网互通后再拷贝资源。

* [案例三：只允许特定IP地址远程登录到实例](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#specifyIpAccess)

场景举例：如果您的ECS实例被黑客远程控制，您可以修改远程登录端口号，并设置只允许特定的IP地址远程登录到您的ECS实例。

* [案例四：只允许实例访问外部特定IP地址](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#specifyInstanceAccess)

场景举例：如果您的ECS实例被黑客远程控制，对外恶意扫描或发包，您可以通过安全组设置您的ECS实例只能访问外部特定IP或端口。

* [案例五：拒绝实例访问外部特定IP地址](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#section-qtl-vhz-ngb)

场景举例：如果您不希望您的ECS实例访问某个特定的外部IP地址，您可以通过安全组设置，拒绝实例访问外部特定IP地址。

* [案例六：允许公网远程连接实例](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#allowRemoteAccess)

场景举例：您可以通过公网远程连接到实例上，管理实例。

* [案例七：允许内网其他账号下某个安全组内的ECS实例远程连接实例](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#section-tkx-fyq-ngb)

场景举例：您可以通过内网其他账号下某个安全组内的ECS实例远程连接到实例上，管理实例。

* [案例八：允许公网通过HTTP、HTTPS等服务访问实例](https://help.aliyun.com/document_detail/25475.html?spm=5176.2020520101.121.1.34fe4df5qzzWxq#allowHttp)

场景举例：您在实例上架设了一个网站，希望您的用户能通过HTTP或HTTPS服务访问到您的网站。

**说明** 网络互访场景的常用端口，请参见[常用端口的典型应用](https://help.aliyun.com/document_detail/40724.html#concept-gbt-s21-ydb)。本文主要以IPv4为例说明安全组规则的配置案例，如果ECS实例分配了IPv6地址，您可以将文中涉及的IP地址授权对象修改为IPv6地址或地址段。本文主要以单一IP地址或者CIDR网段格式为例说明安全组规则的配置案例，如12.1.1.1或13.1.1.1/25，多组授权对象可以在添加安全组规则时用半角逗号（,）隔开。

## 案例一：同一个地域、同一个账号下的实例实现内网互通

同一地域、同一账号的两个实例：

* 如果在同一个安全组内，默认内网互通，不需要设置。
* 如果在不同的安全组内，默认内网不通。此时，在实例所在安全组中分别添加一条安全组规则，授权另一个安全组内的实例访问本安全组内的实例，实现内网互通。根据网络类型做不同的安全组规则设置：

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **优先级** | **授权类型** | **授权对象** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 专有网络 | 不需要设置 | 入方向 | 允许 | 设置适用的协议类型 | 设置端口范围 | 1 | 安全组访问（本账号授权） | 选择允许访问的实例所在的安全组 ID |
| 经典网络 | 内网 |

**说明**

对于VPC网络类型的ECS实例，如果它们在同一个VPC网络内，可以通过安全组规则实现内网互通。如果ECS实例不在同一个VPC内（无论是否属于同一个账号或在同一个地域里），您可以使用云企业网实现VPC互通。详情请参见 *《*云企业网文档*》* [步骤一 网络规划](https://help.aliyun.com/document_detail/128508.html#concept-1546434)。

## 案例二：同一个地域、不同账号下的实例实现内网互通

此案例仅适用于经典网络类型的ECS实例。

UserA在华东1有一台经典网络类型的ECS实例InstanceA（内网IP：A.A.A.A），InstanceA所属的安全组为GroupA。

UserB在华东1有一台经典网络的ECS实例InstanceB（内网IP：B.B.B.B），InstanceB所属的安全组为GroupB。

您需要在GroupA和GroupB中分别添加安全组规则，授权InstanceA和InstanceB内网互通。

* 在GroupA中添加安全组规则，授权InstanceB内网访问InstanceA，如下表所示。

| **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 内网 | 入方向 | 允许 | 选择适用的协议类型 | 设置端口范围 | 安全组访问（跨账号授权） | GroupB的ID，并在账号ID里填写UserB的ID | 1 |

* 在GroupB中添加安全组规则，授权InstanceA内网访问InstanceB，如下表所示。

| **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 内网 | 入方向 | 允许 | 选择适用的协议类型 | 设置端口范围 | 安全组访问（跨账号授权） | GroupA的ID，并在账号ID里填写UserA的ID | 1 |

* **说明** 出于安全性考虑，经典网络的内网入方向规则，授权类型优先选择安全组访问；如果选择地址段访问，则仅支持单IP授权，授权对象的格式只能是a.b.c.d/32，其中IP地址应根据您的实际需求设置，子网掩码必须是/32。

## 案例三：只允许特定IP地址远程登录到实例

如果您只想让某些特定IP地址远程登录到实例，可以参考以下示例的步骤在实例所在安全组里添加规则：

* Linux实例

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | SSH (22) | 22/22 | 地址段访问 | 允许远程连接的IP地址，例如1.2.3.4/32或10.0.0.0/8。 | 1 |
| 经典网络 | 公网 |

* Windows实例

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | RDP (3389) | 3389/3389 | 地址段访问 | 允许远程连接的IP地址，例如1.2.3.4/32或10.0.0.0/8。 | 1 |
| 经典网络 | 公网 |

## 案例四：只允许实例访问外部特定IP地址

如果您只想让实例访问特定的IP地址，参考以下示例的步骤在实例所在安全组中添加安全组规则：

* 禁止实例以任何协议访问所有公网IP地址，优先级应低于允许访问的规则（如本例中设置优先级为2）。安全组规则如下表所示。

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 出方向 | 拒绝 | 全部 | -1/-1 | 地址段访问 | 0.0.0.0/0 | 2 |
| 经典网络 | 公网 |

* 允许实例访问特定公网IP地址，优先级应高于拒绝访问的安全组规则的优先级（如本例中设置为1）。

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 出方向 | 允许 | 选择适用的协议类型 | 设置端口范围 | 地址段访问 | 允许实例访问的特定公网IP地址，例如1.2.3.4/32或10.0.0.0/8。 | 1 |
| 经典网络 | 公网 |

添加了安全组规则后，再连接实例，执行ping、telnet等测试。如果实例只能访问授权对象中设置的IP地址，说明安全组规则已经生效。

## 案例五：拒绝实例访问外部特定IP地址

如果您不希望您的ECS实例访问某个特定的外部IP地址，您可以参考以下示例在实例所在安全组中添加安全组规则：

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 出方向 | 拒绝 | 全部 | -1/-1 | 地址段访问 | 拒绝实例访问的特定公网IP地址，例如1.2.3.4/32或10.0.0.0/8。 | 1 |
| 经典网络 | 公网 |

## 案例六：允许公网远程连接实例

如果要允许公网远程连接实例，添加如下安全组规则：

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | Windows：RDP (3389) | 3389/3389 | 地址段访问 | 如果允许任意公网IP地址连接实例，填写0.0.0.0/0。如果只允许特定IP地址远程连接实例，请参见案例三：只允许特定IP地址远程登录到实例。 | 1 |
| Linux：SSH (22) | 22/22 |
| 自定义TCP | 自定义，例如8080/8080 |
| 经典网络 | 公网 | 入方向 | 允许 | Windows：RDP (3389) | 3389/3389 | 地址段访问 | 如果允许任意公网IP地址连接实例，填写0.0.0.0/0。如果只允许特定公网IP地址连接实例，请参见案例三：只允许特定IP地址远程登录到实例。 | 1 |
| Linux：SSH (22) | 22/22 |
| 自定义TCP | 自定义，例如8080/8080 |

自定义远程连接端口的详细操作，请参见[修改服务器默认远程端口](https://help.aliyun.com/document_detail/51644.html#concept-51644-zh)。

## 案例七：允许内网其他账号下某个安全组内的ECS实例远程连接实例

如果您的账号与同地域其他账号内网互通，而且您想允许内网其他账号下某个安全组内的ECS实例远程连接实例，按以下示例添加安全组规则。

* 允许内网其他账号某个实例内网IP地址连接您的实例，您需要添加如下安全组规则。其中，VPC网络类型实例先保证2个账号的实例通过云企业网内网互通，再添加安全组规则。详情请参见 *《*云企业网文档*》* [步骤一 网络规划](https://help.aliyun.com/document_detail/128508.html#concept-1546434)。

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | Windows：RDP (3389) | 3389/3389 | 地址段访问 | 对方实例的私有IP地址 | 1 |
| Linux：SSH (22) | 22/22 |
| 自定义TCP | 自定义，例如8080/8080 |
| 经典网络 | 内网 | 入方向 | 允许 | Windows：RDP (3389) | 3389/3389 | 地址段访问 | 对方实例的内网IP地址，出于安全性考虑，仅支持单IP授权，例如：a.b.c.d/32。 | 1 |
| Linux：SSH (22) | 22/22 |
| 自定义TCP | 自定义，例如8080/8080 |

* 允许内网其他账号某个安全组里的所有ECS实例连接您的实例，您需要添加如下安全组规则。其中，VPC类型的实例，先保证2个账号的实例通过云企业网内网互通，再添加如下表所示的安全组规则。详情请参见 *《*云企业网文档*》* [步骤一 网络规划](https://help.aliyun.com/document_detail/128508.html#concept-1546434)。

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | Windows：RDP (3389) | 3389/3389 | 安全组访问（跨账号授权） | 对方ECS实例所属的安全组ID，并填写对方账号ID | 1 |
| Linux：SSH (22) | 22/22 |
| 自定义TCP | 自定义，例如8080/8080 |
| 经典网络 | 内网 | 入方向 | 允许 | Windows：RDP (3389) | 3389/3389 | 安全组访问（跨账号授权） | 对方ECS实例所属的安全组ID，并填写对方账号ID | 1 |
| Linux：SSH (22) | 22/22 |
| 自定义TCP | 自定义，例如8080/8080 |

## 案例八：允许公网通过HTTP、HTTPS等服务访问实例

如果您在实例上架设了一个网站，希望您的用户能通过HTTP或HTTPS服务访问到您的网站，您需要在实例所在安全组中添加以下安全组规则。

* 允许公网上所有IP地址访问您的网站。

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | HTTP (80) | 80/80 | 地址段访问 | 0.0.0.0/0 | 1 |
| HTTPS (443) | 443/443 |
| 自定义TCP | 自定义，例如8080/8080 |
| 经典网络 | 公网 | 入方向 | 允许 | HTTP (80) | 80/80 | 地址段访问 | 0.0.0.0/0 | 1 |
| HTTPS (443) | 443/443 |
| 自定义TCP | 自定义，如8080/8080 |

* 允许公网上部分IP地址访问您的网站。

| **网络类型** | **网卡类型** | **规则方向** | **授权策略** | **协议类型** | **端口范围** | **授权类型** | **授权对象** | **优先级** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| VPC | 不需要配置 | 入方向 | 允许 | HTTP (80) | 80/80 | 地址段访问 | 允许访问您网站的主机的公网IP地址，可以为一个或多个公网IP地址，例如1.2.3.4/32或10.0.0.0/8。 | 1 |
| HTTPS (443) | 443/443 |
| 自定义TCP | 自定义，例如8080/8080 |
| 经典网络 | 公网 | 入方向 | 允许 | HTTP (80) | 80/80 | 地址段访问 | 允许访问您网站的主机的公网IP地址，可以为一个或多个公网IP地址，例如1.2.3.4/32或10.0.0.0/8。 | 1 |
| HTTPS (443) | 443/443 |
| 自定义TCP | 自定义，例如8080/8080 |

用SSH将windows与阿里云服务器联接互传文件

打开Xshell的会话窗口，或者**SecureCRT的快速联接**

**输入公网地址，22号端口连接成功后会要求输入root用户名及实例密码，此时就登陆ubuntu18系统成功。**

HTTP (80)设置意义允许访问您网站的主机的公网IP地址，可以为一个或多个公网IP地址，例如1.2.3.4/32或10.0.0.0/8。

上传windows上的文件

阿里云ubuntu18 配置桌面环境