阿里云
专有网络VPC

访问控制

文档版本：20200514

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止：** 重置操作将丢失用户配置数据。
	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告：** 重启操作将导致业务中断，恢复业务时间约十分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	 **注意：** 权重设置为0，该服务器不会再接受新请求。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明：** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	单击**设置** > **网络** > **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令。	执行cd /d C:/window命令，进入Windows系统文件夹。
斜体	表示参数、变量。	bae log list --instanceid Instance_ID
[]或者[a|b]	表示可选项，至多选择一个。	ipconfig [-all|-t]
{}或者{a|b}	表示必选项，至多选择一个。	switch {active|stand}

目录

1 VPC访问控制概述

专有网络VPC不仅可以通过网络ACL实现访问控制，还可以依赖各个云产品的访问控制能力来实现安全访问，例如云服务器ECS通过设置安全组来进行访问控制，负载均衡SLB和云数据库RDS通过白名单来进行访问控制。

网络ACL

网络ACL是VPC中的网络访问控制功能。您可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中ECS实例的流量的访问控制。详细信息，请参见#unique_4。

ECS安全组

安全组是一种虚拟防火墙，具备状态检测和数据包过滤能力，用于在云端划分安全域。通过配置安全组规则，您可以控制安全组内一台或多台ECS实例的入流量和出流量。详细信息，请参见#unique_5。

RDS白名单

在VPC中使用云数据库RDS实例，需要将云服务器的IP地址加入到需要访问的RDS的白名单中，云服务器才能访问RDS实例，而其他IP地址将拒绝访问RDS实例。详细信息，请参见#unique_6。

SLB白名单

负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。您可以为负载均衡监听设置允许转发请求的IP地址，适用于只允许特定IP访问应用的场景。详细信息，请参见#unique_7。

2 ECS安全组配置案例

当您创建专有网络类型的ECS实例时，可以使用系统提供的默认安全组规则，也可以选择VPC中已有的其它安全组。安全组是一种虚拟防火墙用来控制ECS实例的出站和入站流量。

本文档介绍了常用的专有网络ECS实例的安全组设置。

案例一：内网互通

VPC类型的ECS实例互通分以下两种情况：

- 同一VPC内的相同安全组下的ECS实例，默认互通。
- 不同VPC内的ECS实例，无法互通。首先需要使用高速通道、VPN网关、云企业网等产品打通两个VPC之间的通信，然后确保两个VPC内的ECS实例的安全组规则允许互相访问，如下表所示。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
VPC 1中的ECS实例的安全组配置	入方向	允许	Windows: RDP 3389/3389	地址段访问	要访问的VPC2中的ECS实例的私网IP。 **说明：** 如果允许任意ECS实例登录，填写0.0.0.0/0。
	入方向	允许	Linux: SSH 22/22	地址段访问	
	入方向	允许	自定义TCP 自定义	地址段访问	
VPC 2中的ECS实例的安全组配置	入方向	允许	Windows: RDP 3389/3389	地址段访问	要访问的VPC1中的ECS实例的私网IP。 **说明：** 如果允许任意ECS实例登录，填写0.0.0.0/0。
	入方向	允许	Linux: SSH 22/22	地址段访问	
	入方向	允许	自定义TCP 自定义	地址段访问	

案例二：拒绝特定IP或特定端口的访问

您可以通过配置安全组拒绝特定IP或特定端口对专有网络ECS实例的访问，如下表所示。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
拒绝特定IP地址段对ECS实例所有端口的入站访问	入方向	拒绝	全部 -1	地址段访问	要拒绝访问的IP地址段，如10.0.0.1/32。
拒绝特定IP地址段对ECS实例TCP 22端口的入站访问	入方向	拒绝	SSH(22) 22/22	地址段访问	要拒绝访问的IP地址段，如10.0.0.1/32。

案例三：只允许特定IP远程登录ECS

如果您为VPC中的ECS实例配置了公网IP，如NAT网关、EIP等。您可以根据具体情况，添加如下安全组规则允许Windows远程登录或Linux SSH登录。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
允许Windows远程登录	入方向	允许	RDP 3389/3389	地址段访问	允许登录ECS实例的指定IP地址。 **说明：** 如果允许任意公网IP登录ECS，填写0.0.0.0/0。
允许Linux SSH登录	入方向	允许	SSH 22/22	地址段访问	允许登录ECS实例的指定IP地址。 **说明：** 如果允许任意公网IP登录ECS，填写0.0.0.0/0。

案例四：允许从公网访问ECS实例部署的HTTP/HTTPS服务

如果您在专有网络的ECS实例上部署了一个网站，通过EIP、NAT网关对外提供服务，您需要配置如下安全组规则允许用户从公网访问您的网站。

安全组规则	规则方向	授权策略	协议类型和端口范围	授权类型	授权对象
允许来自HTTP 80端口的入站访问	入方向	允许	HTTP 80/80	地址段访问	0.0.0.0/0
允许来自HTTPS 443端口的入站访问	入方向	允许	HTTPS 443/443	地址段访问	0.0.0.0/0
允许来自TCP 80端口的入站访问	入方向	允许	TCP 80/80	地址段访问	0.0.0.0